

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт  
Факультет приборостроения,  
информационных технологий и  
электроники

Кафедра  
«Информационная безопасность  
систем и технологий»

Специальность 100503 –

Специализация -

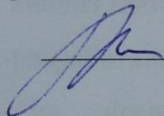
Информационная безопасность  
автоматизированных систем  
Защищенные автоматизированные  
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

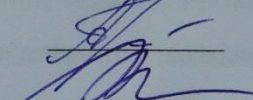
на тему

УСТРОЙСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ ПРИ РАБОТЕ С  
ВНЕШНИМИ НОСИТЕЛЯМИ («КРИПТО-КАРТРИДЕР»)

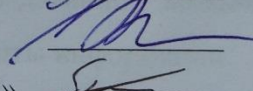
Студент

 Тыкушин Анатолий Владимирович

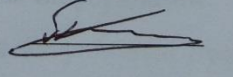
Руководитель

 Грунющкин А.В.

Нормоконтролёр

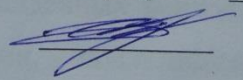
 Иванов А.П.

Рецензент ведущий инженер АО «ПНИЭИ»

 Печилейский С.В.

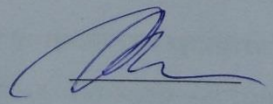
Работа допущена к защите (протокол заседания кафедры от 20.06.2016 № 14)

Заведующий кафедрой

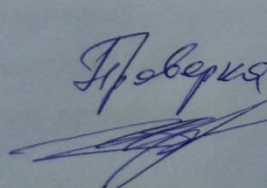
 С.Л. Зефи́ров

Работа защищена с отметкой отлично (протокол заседания ГЭК  
от 24.06.16 № 13)

Секретарь ГЭК

 А.П. Иванов

Пенза 2016

 Проверка ВКР – Лобачев  
С.Л. Зефи́ров

## РЕФЕРАТ

Отчёт 89 с., 25 рис., 21 табл., 13 источников.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ШИФРСИСТЕМА, КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, ШИФРОВАНИЕ ИНФОРМАЦИИ, ВНЕШНИЕ НОСИТЕЛИ ИНФОРМАЦИИ.

Цель работы: проанализировать проблему обеспечения конфиденциальности отдаваемой на внешние носители информации, предложить способы по организации защиты путем создания новых программно-аппаратных комплексов/компонентов автоматизированной системы с возможностью интеграции с существующими системы защиты информации.

Предметом исследования является конфиденциальность информации.

Объектом исследование является автоматизированная система, в которой информация подлежит извлечению путем передачи на внешние носители информации.

Метод проведения работы: анализ проблемы, обзор существующих решений, моделирование прототипа, синтез разработанной модели, проведение исследований соответствия требованиям задания, исследование возможности интеграции устройства с существующими системами защиты информации.

В результате работы были рассмотрены актуальные проблемы, связанные с защитой данных, выведенных из автоматизированной системы, осуществлен поиск решений данной проблемы. На основании найденных решений были выбраны и обоснованы способы защиты информации, подлежащей извлечению из автоматизированной системы на внешние носители информации, сформулированы требования к разрабатываемому устройству. На основе сформулированных требований был разработан прототип (макет) устройства криптографической защиты данных при работе с внешними носителями (крипто-картридер), включающий схемы электрические структурную и принципиальную, алгоритмы работы программный модулей, а также осуществлена реализация программного обеспечения криптографического модуля. На разработанном макете произведен расчет производительности (пропускной способности), сделаны соответствующие выводы о

степени достижения поставленных задач. После этого был осуществлен анализ степени совместимости крипто-картридера в качестве компонента с существующими системами защиты информации, автоматизированными системами в защищенном исполнении по предъявленным критериям.

Степень внедрения разработанного устройства – интегрирование в качестве компонента в существующие средства защиты информации, автоматизированные системы организаций.

## СОДЕРЖАНИЕ

|                                                                                                                                                            |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Введение.....                                                                                                                                              | 10 |
| 1 Анализ и обзор актуальных проблем, связанных с защитой информации, хранящейся на внешних накопителях .....                                               | 13 |
| 2 Выбор и обоснование способов обеспечения защиты данных, хранящихся на внешних носителях .....                                                            | 21 |
| 2.1 Выбор варианта реализации устройства.....                                                                                                              | 21 |
| 2.2 Выбор механизмов обеспечения конфиденциальности.....                                                                                                   | 22 |
| 2.3 Требования к механизму обеспечения конфиденциальности .....                                                                                            | 24 |
| 2.3.1 Требования к стойкости .....                                                                                                                         | 24 |
| 2.3.2 Требования к производительности .....                                                                                                                | 24 |
| 2.3.3 Смена ключей шифрования .....                                                                                                                        | 26 |
| 2.3.4 Требования к криптографическому алгоритму .....                                                                                                      | 26 |
| 2.4 Определение модели обрабатываемой информации.....                                                                                                      | 27 |
| 2.4.1 Определение защищаемой информации .....                                                                                                              | 27 |
| 2.4.2 Идентификация источников служебной информации.....                                                                                                   | 27 |
| 2.5 Обзор и анализ достоинств и недостатков существующих криптографических алгоритмов. Выбор на основе полученных данных криптографического алгоритма..... | 29 |
| 2.5.1 Обзор известных симметричных криптоалгоритмов.....                                                                                                   | 29 |
| 2.5.2 Тест производительности криптоалгоритмов.....                                                                                                        | 32 |
| 2.6 Выбор на основе полученных данных криптоалгоритма .....                                                                                                | 38 |
| 3 Анализ существующих аппаратных средств и выбор элементной базы, наиболее точно удовлетворяющей техническим требованиям .....                             | 40 |
| 3.1 Анализ требований технического задания .....                                                                                                           | 40 |
| 3.2 Выбор аппаратной платформы, удовлетворяющий требованиям технического задания.....                                                                      | 41 |
| 3.2.1 Выбор аппаратного обеспечения вычислительного модуля .....                                                                                           | 41 |
| 3.2.2 Выбор аппаратного обеспечения модуля защиты данных от недоверенной среды.....                                                                        | 44 |

|                                                                                                                                                                            |    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 3.3 Описание интерфейсов обмена данными .....                                                                                                                              | 45 |
| 3.3.1 Последовательный серийный интерфейс .....                                                                                                                            | 45 |
| 3.3.2 Универсальная последовательная шина.....                                                                                                                             | 48 |
| 3.3.3 Описание технологии Ethernet .....                                                                                                                                   | 53 |
| 4 Разработка аппаратного обеспечения устройства криптографической защиты<br>данных при работе с внешними носителями по единой системе конструкторской<br>документации..... | 57 |
| 4.1 Разработка схемы электрической структурной .....                                                                                                                       | 57 |
| 4.2 Разработка схемы электрической принципиальной.....                                                                                                                     | 58 |
| 5 Разработка спецификации программного обеспечения .....                                                                                                                   | 60 |
| 5.1 Общие положения разрабатываемой спецификации .....                                                                                                                     | 60 |
| 5.2 Функциональное описание системы .....                                                                                                                                  | 61 |
| 5.2.1 Общая функциональная схема модулей крипто-картридера .....                                                                                                           | 61 |
| 5.2.2 Описание модуля маскиратора.....                                                                                                                                     | 62 |
| 5.2.3 Описание модуля вычисления ключа шифрования .....                                                                                                                    | 63 |
| 5.2.4 Описание модуля интерфейса обмена данными с периферией .....                                                                                                         | 65 |
| 5.2.6 Модель взаимодействия программного обеспечения модулей .....                                                                                                         | 69 |
| 6 Тестирование программного обеспечения модулей крипто-картридера.<br>Анализ соответствия требованиям технического задания.....                                            | 72 |
| 6.1 Тестирование разработанного программного обеспечения .....                                                                                                             | 72 |
| 6.1.1 Общее тестирование программного обеспечения<br>криптографического модуля.....                                                                                        | 72 |
| 6.1.2 Тестирование корректности работы шифратора .....                                                                                                                     | 73 |
| 6.1.3 Исследование производительности работы криптопроцессора при<br>базовом и ускоренном алгоритмах шифрования .....                                                      | 73 |
| 6.2 Анализ соответствия разработанного устройства требованиям<br>технического задания.....                                                                                 | 75 |
| 7 Анализ возможной интеграции устройства криптографической защиты<br>данных с существующими системами защиты информации .....                                              | 77 |
| Заключение .....                                                                                                                                                           | 79 |

|                                                                                                                                           |    |
|-------------------------------------------------------------------------------------------------------------------------------------------|----|
| Список использованных источников .....                                                                                                    | 81 |
| Приложение А. Схема электрическая структурная (Э1) устройства<br>криптографической защиты данных при работе с внешними носителями.....    | 83 |
| Приложение Б. Схема электрическая принципиальная (Э3) устройства<br>криптографической защиты данных при работе с внешними носителями..... | 85 |

## НОРМАТИВНЫЕ ССЫЛКИ

В настоящем отчете использованы ссылки на следующие стандарты:

ГОСТ 2.702-2011 «Единая система конструкторской документации. Правила выполнения электрических схем»

ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры»

ГОСТ 19781-90 «Единая система программной документации. Термины и определения»

ГОСТ 28147-89 «Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

ГОСТ Р 51897-2011 «Менеджмент риска»

## ОПРЕДЕЛЕНИЯ

В настоящем отчете применяют следующие термины с соответствующими определениями.

Программное обеспечение - совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ (ГОСТ Р 51897).

Драйвер - программа, предназначенная для управления работой периферийных устройств, обычно в мини- и микроэлектронных вычислительных машин (ГОСТ 19781-90).

Шифрование – процесс преобразования открытых данных в зашифрованные при помощи шифра (ГОСТ 19781-90).

Компиляция - трансляция программы с языка высокого уровня в форму, близкую к программе на машинном языке (ГОСТ 19781-90).

Компилятор - программа или техническое средство, выполняющие компиляцию (ГОСТ 19781-90).

Программный модуль - программа или функционально завершенный фрагмент программы, предназначенный для хранения, трансляции, объединения с другими программными модулями и загрузки в оперативную память. (ГОСТ 19781-90).

Криптографическая стойкость (стойкость шифра) - способность криптографического алгоритма противостоять криптоанализу.

Риск – следствие влияние неопределенности на достижение поставленных целей (ГОСТ Р 51897).

## ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем отчёте применяются следующие сокращения с соответствующими расшифровками:

- АС – автоматизированная система;
- НСД – несанкционированный доступ;
- ПЭМИН – побочные электромагнитные излучения и наводки;
- ЛВС – локальная вычислительная сеть;
- УБИ – угрозы безопасности информации;
- СВТ – средство вычислительной техники;
- АРМ – автоматизированное рабочее место;
- ПЗУ – постоянное запоминающее устройство;
- ПО – программное обеспечение;
- ЦП – центральный процессор;
- ОС – операционная система.

## ВВЕДЕНИЕ

В настоящее время уже практически завершилась интеграция человеческого общества и компьютерных технологий. Из года в год создаются все более передовые и перспективные образцы информационных технологий, разработки(концепты).

С каждым годом создаются новые автоматизированные системы (АС), обладающие более богатыми функциональными возможностями, улучшенными характеристиками и направленные на решение более широкого круга задач. Человечество все больше доверяет свою жизнь информационным технологиям: хранит личные, персональные, служебные данные в облаках, денежные средства в электронном виде в банках, не всегда задумываясь об их сохранности. В связи с этим эволюционировали и системы и средства, обеспечивающие безопасность информации. Наблюдается тенденция повышения спроса на более дешевые и производительные компоненты, обеспечивающие конфиденциальность, целостность, доступность информации.

В масштабах организаций угрозы утечки, несанкционированного доступа (НСД) к информации несут в себе высокие риски потери капитала как осязаемого, так и неосязаемого, а также нарушения бизнес-процессов. Объектом защиты в данном случае являются информация, информационные активы организации. Статистика экономического ущерба от НСД и утечек информации показывает, что большинство информационных систем предприятий уязвимо. По данным Forreest Research, IDC в США ежегодные потери от компьютерной преступности оцениваются в 100 миллиардов долларов, в Западной Европе - 30 миллиардов долларов. Средний и максимальный ущерб от одного компьютерного преступления составляет, соответственно, 450 тысяч долларов и 1 миллиард долларов. Ежегодные потери некоторых фирм США достигают 5 миллиарда долларов. Для России аналогичная оценка дает порядка 1-2 миллиарда долларов в год. Более 80% компаний несут убытки из-за ненадежного обеспечения безопасности данных. Приведенная статистика не отражает многих аспектов проблемы НСД, но подтверждает ее существование и актуальность.

Для предотвращения утечек информации стали использоваться все более эффективные методы защиты от побочных электромагнитных излучений и наводок (ПЭМИН), более эффективные криптографические алгоритмы, методики разработки защищенного программного обеспечения.

Объектом исследования дипломного проекта является информация в автоматизированных системах в защищенном исполнении, подлежащие записи на внешние носители информации, как бумажные, так и электронные

Целью данной работы является определение концептуальной модели разрабатываемого устройства криптографической защиты данных при работе с внешними носителями, выбор аппаратных средств и разработка программного обеспечения отдельных модулей, удовлетворяющих требованиям по защите информации 4 уровня.

В первом разделе приведен анализ и обзор актуальных проблем, связанных с защитой информации, хранящейся на внешних накопителях, включая сам процесс передачи информации на внешние носители.

Второй раздел посвящен выбору и обоснованию способов обеспечения защиты данных, хранящихся на внешних носителях. Кроме того, в данном разделе сформированы требования к разрабатываемой концептуальной модели устройства.

В третьем разделе осуществлен поиск элементной базы, удовлетворяющий требованиям, сформированным во втором разделе, а также приведены описания интерфейсов обмена данными USB, SPI, Ethernet.

В четвертом разделе на основе требований, подобранной элементной базы, требований иных документов и стандартов по защите информации разработаны схема электрическая структурная и схема электрическая принципиальная с прилагаемым к ней перечнем элементов

В пятом разделе приведен процесс разработки алгоритмов работы и взаимодействия программных модулей. Так, выделены пять основных программных модулей устройства: модуль обмена данными с периферией, модуль обмена данными по интерфейсу Ethernet, криптографический модуль, модуль маскиратора, модуль вычисления ключа шифрования.

Шестой раздел содержит результаты исследований производительности и пропускной способности крипто-картридера, анализ соответствия полученных результатов исследования предъявляемым требованиям в техническом задании.

В седьмом разделе сформирована комплексная оценка разработанного прототипа устройства, произведен анализ возможной интеграции устройства с существующими системами защиты информации.

Результатом выполнения работы является разработанный прототип устройства криптографической защиты при работе с внешними носителями с прилагающимися схемами электрической структурной и электрической принципиальной, алгоритмами работы и взаимодействия программных модулей.

1 Анализ и обзор актуальных проблем, связанных с защитой информации, хранящейся на внешних накопителях

В процессе развития любая организация сталкивается с необходимостью внедрения локальной вычислительной сети (далее – ЛВС) с дальнейшим разворачиванием систем электронного документооборота. Однако, в связи с различной степенью конфиденциальности электронных документов (открытые, коммерческая тайна, персональные данные, сведения, составляющие государственную тайну и иные сведения, подлежащие защите в соответствии с законодательством РФ) возникает проблема обеспечения конфиденциальности, целостности, доступности таких документов с помощью организационно-технических мер.

По мере накопления определенного количества электронных документов, файлов, появляется потребность в дублировании (обеспечении избыточности) информации. Избыточность информации достигается несколькими способами: архивирование, зеркалирование. Архивирование информации позволяет достичь две важных цели:

- снижение нагрузки на дисковую систему (ускорение поиска файлов, оптимизация запросов);
- сохранение сжатых/несжатых копий файлов на случай выхода из строя ЛВС организации, носителей информации.

Зеркалирование информации достигается путем использования RAID-массивов (анг. redundant array of independent disks – избыточный массив независимых дисков). RAID – технология виртуализации данных, которая объединяет несколько дисков в логический элемент для избыточности и повышения производительности [1].

Не редкость для организации и случаи, когда необходимо передать данные корреспонденту, с которым нет связи по ЛВС или глобальным вычислительным сетям (далее – ГВС). В таких ситуациях, электронный документ извлекается из системы на внешние носители информации. Внешними носителями информации могут быть либо бумажный носитель, либо электронный носитель (USB-Flash накопитель, CD-диск, HDD-жесткий диск).

После записи информации на внешние носители, дальнейшие действия с информацией считаются неподконтрольными, так как производятся вне «юрисдикции» ЛВС организации. Кроме того, отчуждение информации на внешние носители может производиться и несанкционированным путем, например, по каналам утечки конфиденциальной информации. В связи с этим появляется ряд проблем:

- 1) обеспечение конфиденциальности, целостности данных при записи их на внешний носитель;
- 2) избежание потерь производительности процедур записи/чтения данных при работе с внешними носителями;
- 3) обеспечение конфиденциальности, целостности, доступности данных хранящихся на внешнем носителе.

Актуальность проблемы обеспечения производительности процедур записи/чтения объясняется тем, что в настоящее время увеличивается объем информации, которая подлежит защите в соответствии с нормативными документами РФ, международными актами, а также стандартами и локальными документами организаций. При увеличении объемов информации без роста производительности систем неизбежно растет и время обработки, замедляя при этом производственные процессы. Необходимо применение новейших технологий для повышения производительности автоматизированных систем, в которых циркулирует информация. При этом все больше наблюдается тенденция в производительных и эффективных системах защиты информации.

Обоснование актуальности первой и третьей проблемы целесообразным будет осуществить путем приведения списка актуальных угроз безопасности информации для данных процессов. В таблице 1 приведено соответствие проблем безопасности информации к основным (наиболее вероятным и опасным) угрозам безопасности информации (далее – УБИ), найденный в ходе анализа единого банка данных УБИ ФСТЭК.

Таблица 1 - Соответствие проблем информационной безопасности к угрозам информационной безопасности

| Проблема                                                                                    | УБИ с описанием                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Обеспечение конфиденциальности, целостности данных при записи их на внешний носитель</p> | <p>УБИ.088: Угроза несанкционированного копирования защищаемой информации</p> <p><u>Описание угрозы:</u> Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне. Реализация данной угрозы возможна в случае отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде.</p> <p><u>Последствия реализации угрозы:</u></p> <p>нарушение конфиденциальности</p> |

Продолжение таблицы 1

| Проблема                                                                                    | УБИ с описанием                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Обеспечение конфиденциальности, целостности данных при записи их на внешний носитель</p> | <p>УБИ.093: Угроза несанкционированного управления буфером</p> <p><u>Описание угрозы:</u> Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к данным, содержащимся в буфере обмена, в интересах ознакомления с хранящейся там информацией или осуществления деструктивного программного воздействия на систему (например, переполнение буфера для выполнения произвольного вредоносного кода). Данная угроза обусловлена слабостями в механизме разграничения доступа к буферу обмена, а также слабостями в механизмах проверки вводимых данных. Реализация данной угрозы возможна в случае осуществления нарушителем успешного несанкционированного доступа к сегменту оперативной памяти дискредитируемого объекта, в котором расположен буфер обмена</p> <p><u>Последствия реализации угрозы</u></p> <p>Нарушение конфиденциальности, целостности, доступности</p> |

Продолжение таблицы 1

| Проблема                                                                                    | УБИ с описанием                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Обеспечение конфиденциальности, целостности данных при записи их на внешний носитель</p> | <p>УБИ.111: Угроза передачи данных по скрытым каналам</p> <p><u>Описание угрозы:</u> Угроза заключается в возможности осуществления нарушителем неправомерного вывода защищаемой информации из системы 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) и т.п.</p> <p>Данная угроза обусловлена недостаточностью мер защиты информации от утечки, а также контроля потоков данных.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя прав в дискредитируемой системе: установки специализированного программного обеспечения, реализующего функции внедрения в пакеты данных, формируемых для передачи в системе, собственной информации; доступа к каналам передачи данных</p> <p><u>Последствия реализации угрозы</u></p> <p>Нарушение конфиденциальности</p> |

Продолжение таблицы 1

| Проблема                                                                                    | УБИ с описанием                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Обеспечение конфиденциальности, целостности данных при записи их на внешний носитель</p> | <p>УБИ. 143 Угроза программного выведения из строя средств хранения, обработки и/или ввода/вывода/передачи информации</p> <p><u>Описание угрозы:</u> Угроза заключается в возможности прерывания нарушителем технологии обработки информации в дискредитируемой системе путём осуществления деструктивного программного (локально или удалённо) воздействия на средства хранения (внешних, съёмных и внутренних накопителей), обработки (процессора, контроллера устройств и т.п.) и (или) ввода/вывода/передачи информации (клавиатуры и др.), в результате которого объект защиты перейдёт в состояние «отказ в обслуживании». При этом вывод его из этого состояния может быть невозможен путём простой перезагрузки системы, а потребует проведения ремонтно-восстановительных работ. Данная угроза обусловлена наличием уязвимостей микропрограммного обеспечения средств хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при наличии у нарушителя прав на отправку команды или специально сформированных входных данных на средства хранения, обработки и (или) ввода/вывода/передачи информации</p> <p><u>Последствия реализации угрозы:</u></p> <p>Нарушение доступности</p> |

Продолжение таблицы 1

| Проблема                                                                                       | УБИ с описанием                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Обеспечение конфиденциальности, целостности, доступности данных хранящихся на внешнем носителе | <p>УБИ.156: Угроза утраты носителей информации.</p> <p><u>Описание угрозы:</u> Угроза заключается в возможности раскрытия информации, хранящейся на утерянном носителе (в случае отсутствия шифрования данных), или её потери. Данная угроза обусловлена слабостями мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников.</p> <p><u>Последствия реализации угрозы:</u></p> <p>Нарушение конфиденциальности, доступности</p>                                                                                                                                                                                                 |
|                                                                                                | <p>УБИ.158: Угроза форматирования носителей информации</p> <p><u>Описание угрозы:</u> Угроза заключается в возможности утраты хранящейся на формируемом носителе информации, зачастую без возможности её восстановления, из-за преднамеренного или случайного выполнения процедуры форматирования носителя информации. Данная угроза обусловлена слабостью мер ограничения доступа к системной функции форматирования носителей информации. На реализацию данной угрозы влияют такие факторы как: Время после форматирования; тип носителя информации; тип файловой системы; интенсивность взаимодействия с носителем после форматирования.</p> <p><u>Последствия реализации угрозы:</u></p> <p>Нарушение целостности, доступности</p> |

Как следует из таблицы 1, существует целый ряд УБИ, для нейтрализации или минимизации которых необходимо применить специальные организационно-технические решения.

Как было отмечено ранее, основное внимание следует уделить обеспечению конфиденциальности и целостности информации, отчуждаемой на внешние носители, при этом избежать потерь производительности передачи информации без потерь качества обеспечения безопасности информации.

В тексте пояснительной записки внимание будет уделено лишь решению технической части вопроса обеспечения безопасности информации, передаваемой на внешние носители, так как организационные меры не рассматриваются в рамках дипломного проектирования.

## 2 Выбор и обоснование способов обеспечения защиты данных, хранящихся на внешних носителях

### 2.1 Выбор варианта реализации устройства

Как известно, в качестве внешних носителей могут быть использованы следующие форм-факторы: USB-Flash, карты памяти SD/SDHC/MMC/Micro SD, жесткие диски (твердотельные накопители типа HDD и SSD), оптические диски. Запись/чтение информации на накопители такого типа осуществляется через специализированные порты или приводы с помощью стандартных средств и утилит операционных систем, установленных на средствах вычислительной техники (далее – СВТ), которыми оборудованы автоматизированные рабочие места (далее – АРМ).

Перечень способов реализации а также достоинства и недостатки механизмов защиты приведены в таблице 2.

Таблица 2 - Достоинства и недостатки реализаций механизмов защиты

| Способ реализации     | Преимущества                                                                                                                                                                | Недостатки                                                                  |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Программный           | гибкость исполнения;<br>возможность легкой замены алгоритма шифрования; высокая скорость работы;                                                                            | расход ресурсов системы;<br>подверженность компрометации;                   |
| Аппаратный            | наивысшая скорость работы;<br>неподверженность компрометациям системы;                                                                                                      | стоимость реализации;<br>повышенная сложность смены алгоритма шифрования    |
| Программно-аппаратный | гибкость исполнения;<br>возможность легкой замены алгоритма шифрования; высокая скорость работы, приемлемая стоимость реализации; не подверженность компрометациям системы; | скорость шифрования несколько ниже, чем у аппаратной реализации шифрования; |

Программно-аппаратное решение может быть двух типов:

- с прозрачной логикой (не влияет на работу основной системы, не требует специального управляющего ПО);
- с управляемой логикой (поставляется с пакетом ПО, предустанавливаемого на АРМ).

По таблице 2 наиболее подходящий по таким критериям, как трудоемкость разработки, себестоимость устройства, степени защищенности вариант – разработка программно-аппаратного устройства с прозрачной логикой работы.

## 2.2 Выбор механизмов обеспечения конфиденциальности

В качестве механизма обеспечения конфиденциальности выбран метод шифрования данных криптографически-стойким алгоритмом. Шифратор, в случае выбранного п. 2.1 варианта исполнения реализуется непосредственно на устройстве (выносной тип шифратора).

Достоинства метода реализации выносного типа шифратора:

- повышенное доверие к процессу шифрования;
- возможность реализации шифрования на различных уровнях (уровень файловой системы / уровень секторов данных);
- позволяет не создавать стороннее ПО.

При всех своих преимуществах выбранная архитектура накладывает ограничения на потребителя:

- повышенное энергопотребление устройства за счет наличия дополнительных компонентов-потребителей;
- меньшая производительность по сравнению с аппаратным шифрованием.

Перечисленные ограничения можно обойти применением современной высокопроизводительной элементной базой с низкими характеристиками потребления.

Как было отмечено ранее, шифрование данных может осуществляться:

- на уровне блоков данных (надстройка над протоколом/интерфейсом обмена данными);

– на уровне файловой системы (настройка над файловой системой).

Далее приведено обоснование выбора способа шифрования на уровне блоков данных несмотря на очевидные достоинства каждого из способов.

Первый случай наиболее предпочтителен по причине того, что в таком варианте гораздо проще настраивать фильтр данных для шифрования их криптопроцессором. Во втором случае реализация требует внушительных ресурсозатрат как от разработчиков, так и от используемой аппаратной платформы.

В настоящее время существуют различные классы запоминающих устройств, использующие интерфейсы обмена данными для работы с внешними носителями. Самыми часто встречающимися на данный момент являются: USB, SPI, SATA. Для каждого из интерфейсов существует наиболее приемлемая реализация алгоритмов шифрования. Реализация может быть как программной, так и аппаратной. Аппаратная реализация наиболее производительна в случаях применения ASIC (анг. application-specific integrated circuit – интегральная схема специального назначения) – интегральной схемы, предназначенной для решения конкретной задачи. Пример приведен в таблице 3.

Таблица 3 – Способ реализации шифрования в зависимости от используемого интерфейса обмена данными

| Интерфейс                      | Способ реализации криптоалгоритма | Аппаратная база                              |
|--------------------------------|-----------------------------------|----------------------------------------------|
| COM                            | Программный                       | Микроконтроллер с 16-битным RISC-процессором |
| USB 2.0 и ниже                 | Программный                       | Микропроцессор Intel, ARM                    |
| SPI                            | Программный                       | Микропроцессор Intel, ARM                    |
| USB3.0 и выше<br>SATA I/II/III | Аппаратный                        | ПЛИС (ASIC)                                  |

Выбор способа шифрования зависит:

– от вида защищаемой информации (документальная, телефонная, телевизионная, компьютерная и т.д.);

- от объема и требуемой скорости передачи шифрованной информации;
- от ценности защищаемой информации;
- от возможностей владельцев защищаемой информации, а также от возможностей нарушителя.

## 2.3 Требования к механизму обеспечения конфиденциальности

К криптографическим методам защиты информации применяется множество требований, поэтому ниже приведены только основные требования:

- 1) стойкость;
- 2) производительность алгоритма;
- 3) регламент смены главного ключа шифрования.

### 2.3.1 Требования к стойкости

Шифр при статистической надежности ключа должен быть вычислительно стойким - потенциальная возможность вскрыть шифр существует, но при выбранных параметрах и ключах шифрования на практике атакующий на современном этапе развития технологий не может обладать достаточными вычислительными ресурсами для вскрытия шифра за приемлемое время.

### 2.3.2 Требования к производительности

Для определения требования к производительности необходимо учесть следующие аспекты:

- 1) объем данных для шифрования/расшифрования;
- 2) возможность реализации механизмов ускорения выполнения вычислительных операций при шифровании/расшифровании на выбранной платформе;
- 3) пропускная способность канала обмена данными.

2.3.2.1 Размер защищаемых файлов определяется из того, в какой отрасли возможно применение разрабатываемого устройства.

Далее приведены возможные области применения крипто-картридера:

- системы электронного документооборота в организациях;
- системы резервного копирования данных.

Исходя из вышеприведенного перечня можно сделать вывод, что основной процесс работы будет осуществляться с офисными документами. На рисунке 1 показана зависимость количества файлов (ось ординат) в организации от их размера в килобайтах. (ось абсцисс). Данные получены компанией Microsoft после сбора информации на серверах Microsoft SharePoint.

Как видно по рисунку 1, исследования показывают, что средний размер офисного файла составляет 321 кб. Так, 1000000 файлов займет порядка 306 Гб места, а 10000000 млн файлов – около 2,98 Тб. Из них 40% документов приходится на формат pdf [2].

По полученным данным можно сделать вывод, что для задач системы электронного документооборота нет необходимости добиваться предельных скоростей шифрования. Однако, для системы резервного копирования необходимо максимальное быстродействие. Но разрабатываемая система предполагается для разворачивания в системах электронного документооборота предприятий.

2.3.2.2 В качестве интерфейса обмена данными выбраны USB спецификации 2.0 и SPI. В таблице 4 приведены предельные значения скоростей обмена данными для выбранных интерфейсов.

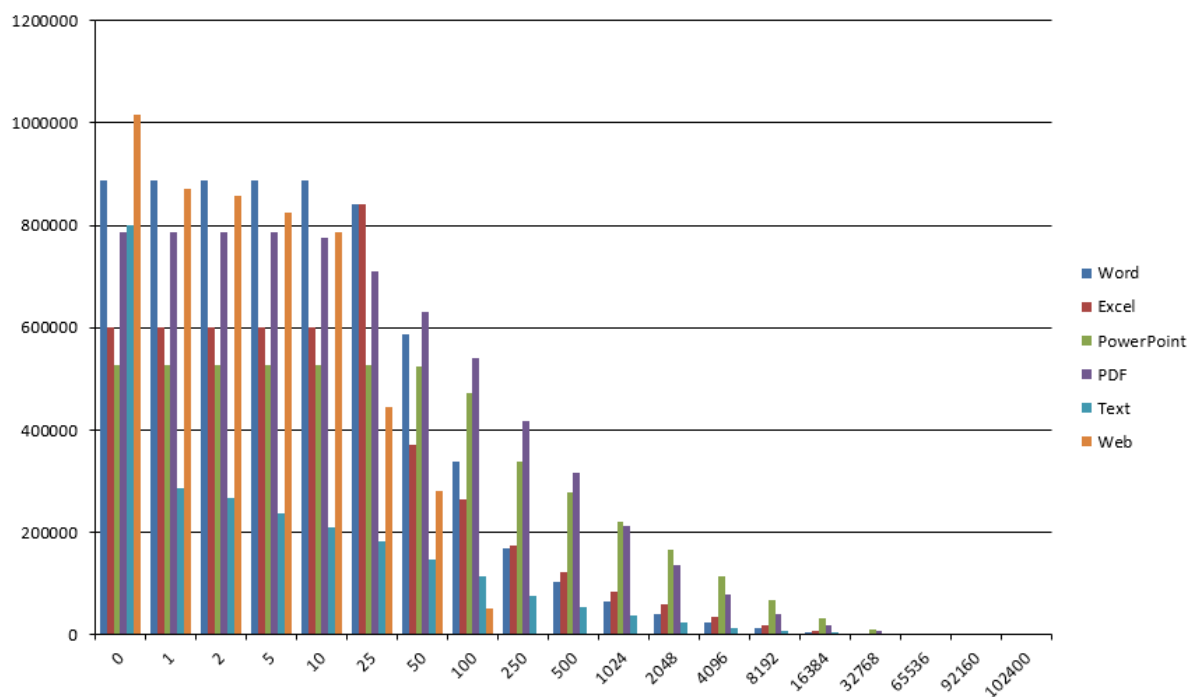


Рисунок 1 – Статистика соотношения количества данных в зависимости от их объема

2.3.2.3 Исходя из пп.2.3.2.1-2.3.3.2 необходимой и достаточной скоростью шифрования будет 10 Мбит/с (1,25 Мбайт/с). Минимальная скорость шифрования должна составлять порядка 4 Мбит/с (0,5 Мбайт/с) в силу того, что карты SD ниже 4 класса сейчас обладают низкой популярностью.

Таблица 4 – Максимальные скорости обмена данными по интерфейсам

| Тип интерфейса<br>(спецификация) |            | Максимальная скорость обмена данными с учетом спецификации используемой аппаратной платформы |
|----------------------------------|------------|----------------------------------------------------------------------------------------------|
| USB 2.0                          | high-speed | 12 мбит/с                                                                                    |
|                                  | full-speed | 480 мбит/с                                                                                   |
| SD                               | Класс 2    | 2 мбит/с                                                                                     |
|                                  | Класс 4    | 4 мбит/с                                                                                     |
|                                  | Класс 6    | 6 мбит/с                                                                                     |
|                                  | Класс 10   | 10 мбит/с                                                                                    |

### 2.3.3 Смена ключей шифрования

Смена ключей шифрования производится для достижения следующих целей:

- ограничения объёма информации, зашифрованной на данном ключе, которая может быть использована для криптоанализа;
- ограничения размера ущерба при компрометации ключей;
- ограничения объёма машинного времени, которое может быть использовано для криптоанализа [3].

Требования к регламенту смены ключей шифрования:

- частота смены ключа не должна быть слишком высокой (не более 2 раз в год) для удобства разворачивания устройства на средних и крупных предприятиях;
- частота смены ключа не должна быть слишком низкой (не реже 1 раза в 2 года) для исключения негативных последствий.

### 2.3.4 Требования к криптографическому алгоритму

В таблице 5 перечислены требования к криптографическому алгоритму, сформированные в п. 2.3.1-2.3.3.

Таблица 5 – Требования к криптографическому алгоритму

| Наименование требования      | Величина                    |
|------------------------------|-----------------------------|
| стойкость                    | средняя                     |
| производительность           | 0,25 Мбайт/с – 1,25 Мбайт/с |
| время смены ключа шифрования | 1 раз в год                 |

## 2.4 Определение модели обрабатываемой информации

### 2.4.1 Определение защищаемой информации

Объектом защиты является информация, содержащаяся в системах электронного документооборота, подлежащая записи на внешние носители информации – офисные файлы (документы, формы заявления, отчеты, приказы). Для обеспечения конфиденциальности информации необходимо реализовать модуль шифратора, реализующий криптографический алгоритм.

Далее необходимо определить категории информации, циркулирующей в устройстве. Можно выделить 2 категории информации:

- служебная информация (не несет в себе семантической нагрузки, служит для обеспечения работоспособности протоколов обмена данными или корректной работы микросхем памяти);

- полезная нагрузка (payload) – информация, несущая в себе семантический смысл, содержимое файлов.

### 2.4.2 Идентификация источников служебной информации

На рисунке 2 приведены уровни абстракции данных.

По рисунку 2 видно, что физическое взаимодействие с носителями информации осуществляется на уровне контроля ввода/вывода в операционных системах (ОС). На рисунке 3 рассмотрим, что происходит на данной стадии.

На рисунке 3 показано, что пакет исходящих данных сначала проходит стадию присвоения вызова системы ввода/вывода (make I/O call, format, необходимые маркеры), разделения на блоки данных (защита (protection), блокировка (blocking), именование (naming), сериализацию, аллокацию (allocation) – присвоения соответствующих аппаратных адресов), а затем уже инкапсулируется в протокол передачи данных (setup device registers) и по достижению очереди отправляется по

каналу передачи данных в устройство. На аппаратном уровне осуществляется непосредственная передача данных.

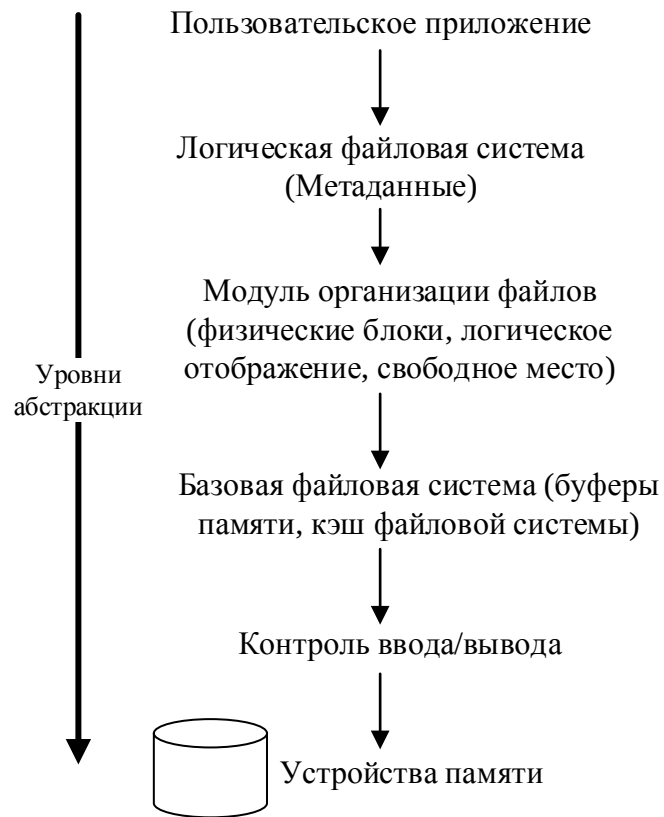
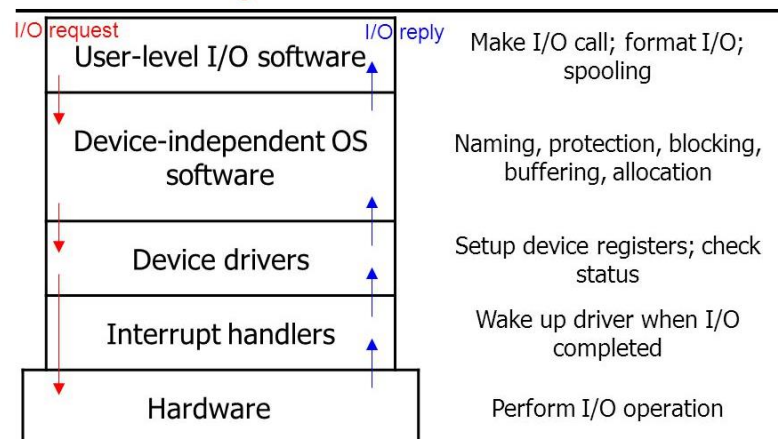


Рисунок 2 – Уровни абстракции данных

## Summary: I/O Software



53

Рисунок 3 – Процесс ввода/вывода в ОС

При приеме данных с носителя последовательность выполняется в обратном порядке.

Рассмотрев процесс передачи данных, начиная с уровня пользовательского приложения, можно идентифицировать источники служебной информации:

- дескриптор устройства хранения данных (информация для идентификации производителя микросхемы и дальнейшего использования драйвером);
- дескриптор устройства обмена данными (usb-дескрипторы);
- информация о секторах (и других физических блоках хранения данных) с которыми будут производиться операции чтения/записи;
- команды файловой системы (чтение, запись, удаление, копирование и иные команды по спецификации).

2.5 Обзор и анализ достоинств и недостатков существующих криптографических алгоритмов. Выбор на основе полученных данных криптографического алгоритма

#### 2.5.1 Обзор известных симметричных криптоалгоритмов

AES (Rijndael). В настоящее время является федеральным стандартом шифрования США. Утвержден министерством торговли в качестве стандарта 4 декабря 2001 года. Решение вступило в силу с момента опубликования в федеральном реестре (06.12.01). В качестве стандарта принят вариант шифра только с размером блока 128 бит. Общая информация об алгоритме приведена в таблице 6.

Таблица 6 – Общая информация об алгоритме AES

|                        |                                                           |
|------------------------|-----------------------------------------------------------|
| Время/место разработки | 1997 год, Бельгия                                         |
| Авторы                 | Йоан Дамен (Joan Daemen), Винсент Раймен (Vincent Rijmen) |
| Архитектура            | "Квадрат"                                                 |
| Размер ключа, бит      | 128, 192, 256                                             |
| Патент                 | Не запатентован                                           |

ГОСТ 28147-89. Стандарт Российской Федерации на шифрование и имитозащиту данных. Является улучшенным аналогом DES. Первоначально имел гриф «особой важности» или «совершенно секретно», затем гриф последовательно снижался, и к моменту официального проведения алгоритма через Госстандарт СССР

в 1989 году был снят. Алгоритм остался с грифом для служебного пользования (ДСП). В 1989 году стал официальным стандартом СССР, а позже, после распада СССР, федеральным стандартом Российской Федерации. Общая информация об алгоритме приведена в таблице 7.

Таблица 7 – Общая информация об алгоритме ГОСТ 28147-89

|                        |                                                                                                                                          |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Время/место разработки | Предположительно вторая половина 1970-1980. Разработан в бывшем 8 Главном Управлении КГБ СССР или в одном из секретных НИИ в его системе |
| Авторы                 | Не известны                                                                                                                              |
| Архитектура            | Классическая сбалансированная сеть Файстеля.                                                                                             |
| Размер ключа, бит      | 256                                                                                                                                      |
| Патент                 | Не запатентован                                                                                                                          |

Blowfish. Сложная схема выработки ключевых элементов существенно затрудняет атаку на алгоритм методом перебора, однако делает его непригодным для использования в системах, где ключ часто меняется, и на каждом ключе шифруется небольшие по объему данные. Алгоритм лучше всего подходит для систем, в которых на одном и том же ключе шифруются большие массивы данных. Общая информация об алгоритме приведена в таблице 8.

Таблица 8 – Общая информация об алгоритме Blowfish

|                        |                                 |
|------------------------|---------------------------------|
| Время/место разработки | 1993 год                        |
| Авторы                 | Брюс Шнайер (Bruce Schneier)    |
| Архитектура            | Сбалансированная сеть Файстеля. |
| Размер ключа, бит      | 32 - 448                        |
| Патент                 | Не запатентован                 |

DES. Федеральный стандарт шифрования США в 1977-2001 годах. В качестве федерального стандарта США принят в 1977 году. В декабре 2001 года утратил свой статус в связи с введением в действие нового стандарта. Общая информация об алгоритме приведена в таблице 9.

Таблица 9 – Общая информация об алгоритме DES

|                        |                                                                                                         |
|------------------------|---------------------------------------------------------------------------------------------------------|
| Время/место разработки | Создан в 1972-1975 годы в исследовательской лаборатории корпорации IBM                                  |
| Авторы                 | Группа под руководством Тачмена                                                                         |
| Архитектура            | Классическая сбалансированная сеть Фейстеля с начальной и конечной битовыми перестановками общего вида. |
| Размер ключа, бит      | 56                                                                                                      |
| Патент                 | Не запатентован                                                                                         |

CAST. В некотором смысле считается аналогом DES. Общая информация об алгоритме приведена в таблице 10.

Таблица 10 – Общая информация об алгоритме CAST

|                   |                                               |
|-------------------|-----------------------------------------------|
| Авторы            | К. Адамс (C. Adams) и С. Таварес (S. Tavares) |
| Размер ключа, бит | 128, 256                                      |
| Патент            | Не запатентован                               |

Кузнечик (ГОСТ 34.12-2015). Стандарт утвержден приказом от 19 июня 2015 года № 749-ст. Стандарт вступил в действие с 1 января 2016 года. Стандарт вступил в действие с 1 января 2016 года. Шифр разработан Центром защиты информации и специальной связи ФСБ России с участием ОАО «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»). Внесен Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации». В отличие от ГОСТ 28147-89 новый шифр представляет собой не сеть Фейстеля, а SP-сеть: преобразование, состоящее из нескольких одинаковых раундов, при этом каждый раунд состоит из нелинейного и линейного преобразований, а также операции наложения ключа. В отличие от сети Фейстеля, при использовании SP-сети преобразуется весь входной блок, а не его половина. Ожидается, что новый блочный шифр «Кузнечик» будет устойчив ко всем видам атак на блочные шифры.

Общая информация об алгоритме приведена в таблице 11.

Таблица 11 – Общая информация об алгоритме

|                        |                           |
|------------------------|---------------------------|
| Время/место разработки | ФСБ России, АО «ИнфоТеКС» |
| Авторы                 | Не известны               |
| Архитектура            | SP-сеть                   |
| Размер ключа, бит      | 256                       |
| Размер блока, бит      | 128                       |

## 2.5.2 Тест производительности криптоалгоритмов

2.5.2.1 В пунктах 2.5.2.2 – 2.5.2.4 будут приведены результаты теста производительности только 3 алгоритмов: «Кузнечик», ГОСТ 28147-89, AES. Остальные криптоалгоритмы имеют либо критические уязвимости (подвержены криптоанализу), либо требуют слишком больших ресурсозатрат при проектировании и реализации. В качестве аппаратных платформ будут рассмотрены платформы на базе процессоров Intel x86, ARM, Эльбрус, МЦСТ. Шифрование будет производиться как в одноблочном, так и мультиблочном режиме. Мультиблочный режим – режим, в котором запускаются параллельные потоки шифрования блоков данных.

2.5.2.2 Производительность алгоритма ГОСТ 28147-89. Реализация алгоритма ГОСТ 28147–89 с помощью инструкций AVX (процессор Intel-архитектуры Sandy Bridge/Ivy Bridge) позволяет обрабатывать данные со скоростью 8,5 тактов/байт для одного ядра процессора (такая же скорость для алгоритма AES-256 без использования инструкций AES-NI). Для архитектуры Intel Haswell с поддержкой AVX2 производительность возрастает до 6,7 тактов/байт. Если целевая шифрующая система использует только центральный процессор (далее – ЦП), то ее производительность будет линейно расти от суммарного количества ядер ЦП (рисунок 4) в системе и их частоты. На платформе Intel Xeon 2 x E5-2697 v3 при обработке 16 потоков шифрования ГОСТ 28147–89 на одном ядре ЦП (AVX, рисунок 4) максимальная скорость составила 9425 Мбайт/с (10,5 Мбайт/с на 1 поток). При использовании инструкций AVX2 (32 потока шифрования) на тестовой платформе скорость составила 13133 Мбайт/с (7,3 Мбайт/с на 1 поток) или более 100 Гбит/с. Низкую скорость шифрования одного потока необходимо пояснить. Например, необходимо зашифровать 128 секторов на жестком диске (размер сектора 512 байт). Так как

сектора можно шифровать параллельно, то скорость шифрования на 1 ядре ЦП в этом случае составит  $10,5 \text{ Мбайт/с} \times 16 \text{ потоков} = 168 \text{ Мбайт/с}$  и  $7,3 \text{ Мбайт/с} \times 32 \text{ потока} = 233,3 \text{ Мбайт/с}$  для AVX и AVX2 соответственно. Стоит отметить, что технология Intel Hyper-threading позволяет увеличить суммарную скорость платформы на 30% при 50% снижении скорости на один поток. Для сравнения, на рисунке 5 приведены результаты тестов производительности ГОСТ 28147 на процессорах линейки Intel Xeon E5-2680 и AMD FX-4100.

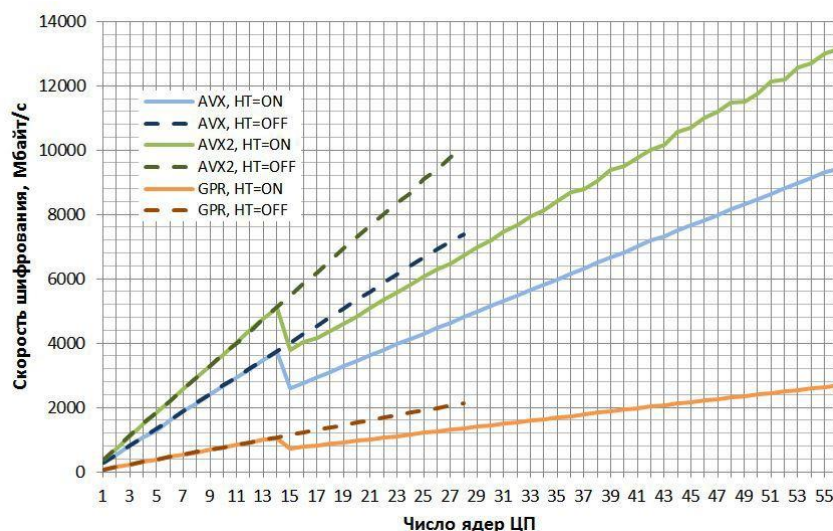


Рисунок 4 – Шифрование ГОСТ 28147-89 в режиме простой замены на ЦП при параллельной обработке буфера 8 Мбайт с помощью различных технологий на платформе 2 x Intel Xeon E5 v3 @ 2.6 ГГц

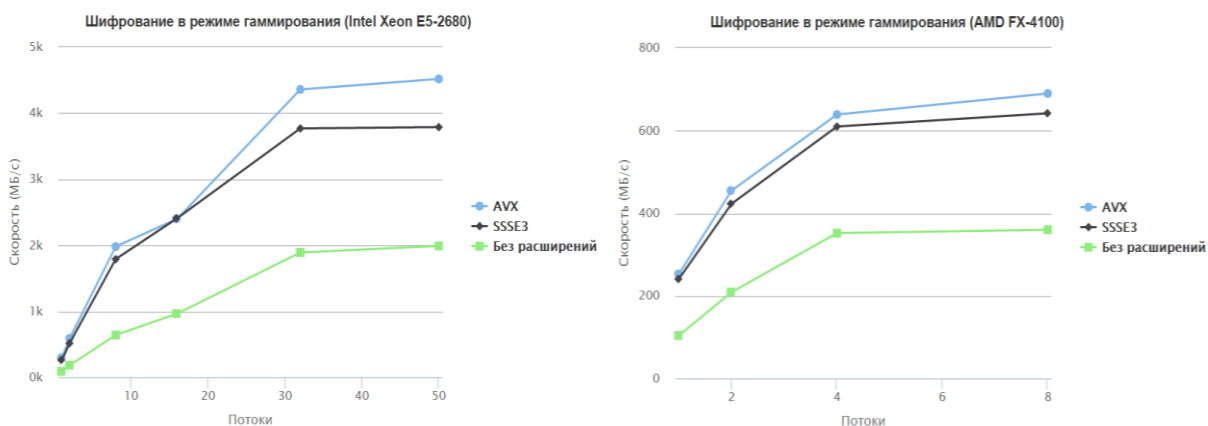


Рисунок 5 – Шифрование ГОСТ 28147-89 на процессорах Intel, AMD

Можно отметить, что для ускорения шифрования данных в настоящее время проводятся исследования на так называемых «гетерогенных<sup>1</sup>» системах. Существует ряд технических сложностей реализации такого вида шифрования, однако, результаты расчетов говорят о значительном увеличении пропускной способности шифратора. Удалось получить скорость шифрования на GPU (анг. graphic processor unit – графический процессор) Nvidia GeForce GTX 750 (архитектура Maxwell) 2588 Мбайт/с (161,8 Кбайт/с на 1 поток) или 21,2 Гбит/с. Для GPU AMD HD 7790 (архитектура GCN 1.1) скорость шифрования ~1700 Мбайт/с. Графический ускоритель от Intel хоть и не показал выдающихся результатов (295 Мбайт/с), но по распространенности ему нет равных. Его скорости будет достаточно для шифрования одного жесткого диска. Стоит отметить, что тестировались не самые производительные GPU, у Nvidia и AMD есть более производительные решения на аналогичных архитектурах: GeForce GTX 980 и FirePro W9100. Мы предполагаем, что скорость в этом случае увеличится пропорционально числу ALU этих GPU. В 4 раза для GTX 980 и 3 раза для FirePro W9100. При этом производительность шифрования на одном GPU не может превысить скорость передачи данных по шине PCI Express v3 в одном направлении (12 Гбайт/с) [4]. В заключении можно сделать вывод о том, что ГОСТ приближается к AES и может стать ему хорошей альтернативой.

2.5.2.3 Алгоритм AES. Данный криптоалгоритм, если можно так сказать, имеет «фору» перед остальными алгоритмами шифрования: почти во всей зарубежной элементной базе имеется его аппаратная реализация. У аппаратной реализации имеются свои неоспоримые преимущества:

- неподверженность влиянию стороннего ПО;
- оптимизированность реализации процедуры шифрования;
- отсутствие необходимости ресурсозатрат для реализации шифрования.

---

<sup>1</sup> Гетерогенные системы – системы, использующие для выполнения задач вычислительную мощность CPU (ЦПУ) и GPU (ГП – графический процессор)

Результаты исследований производительности AES на процессорах Intel Core i5-661 Clarkdale @ 3,33ГГц и Intel Core i7-870 @ 2,93 ГГц в лаборатории THG (Tom's Hardware Guide) приведены на рисунке 6.

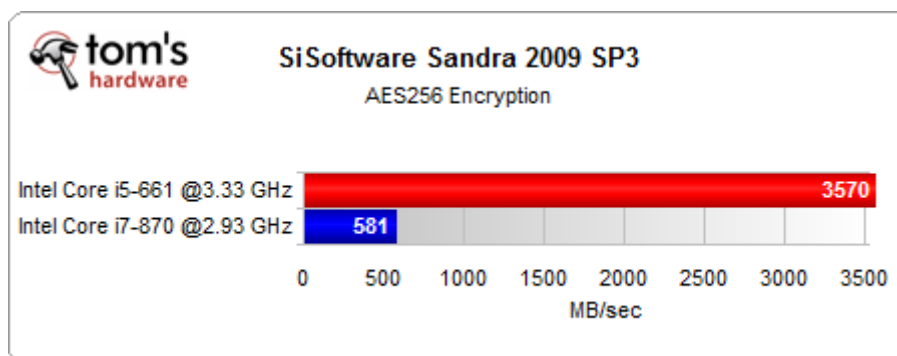


Рисунок 6 – Результаты теста производительности AES на процессорах Intel

По рисунку 6 видно, что результат теста шифрования совершенно иной: он говорит о том, что процессор Core i5 Clarkdale с ускорением AES до 3х быстрее четырёхъядерного Core i7-870. Именно поэтому результаты теста шифрования выглядят так хорошо: чистое шифрование AES-256 выполняется более чем в шесть раз быстрее на двухъядерном процессоре с аппаратным ускорением. Для сравнения, приведен тест вычисления алгоритма хэш-функции SHA-256 (рисунок 7).

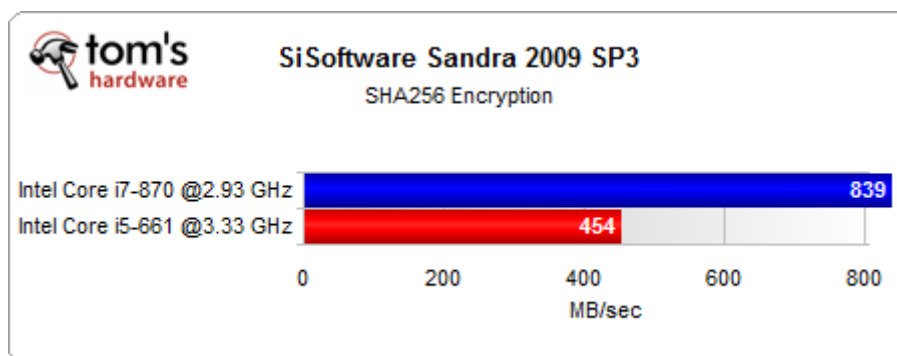


Рисунок 7 – Тест шифрования SHA-256

Тест шифрования SHA-256 доказывает, что данная функция ускоряет только алгоритм AES.

На рисунке 8 показан сравнительный тест криптоалгоритмов AES, 3-DES, DES, Blowfish.

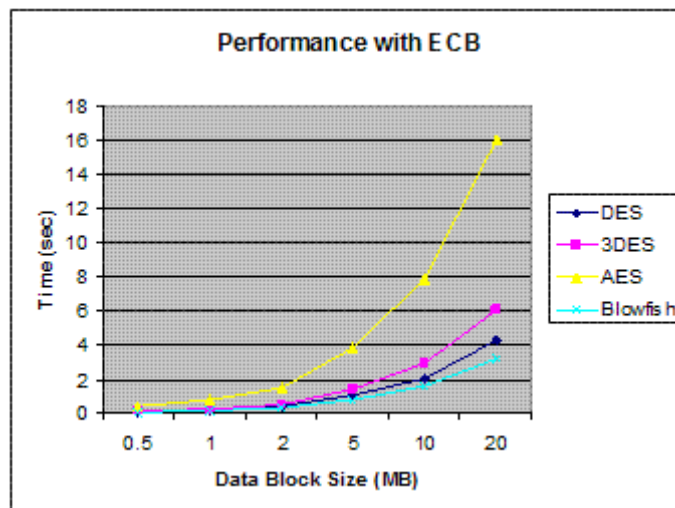


Рисунок 8 – Сравнительный тест производительности криптоалгоритмов

По рисунку 8 видно, по какой причине в тексте отчета не приведен анализ алгоритмов DES, 3-DES, Blowfish. Более того, в алгоритмах DES, 3-DES обнаружены критические уязвимости.

Наконец, приведем результаты теста производительности программной реализации AES на линейке процессоров «Эльбрус», Intel Core i7 (рисунок 9).

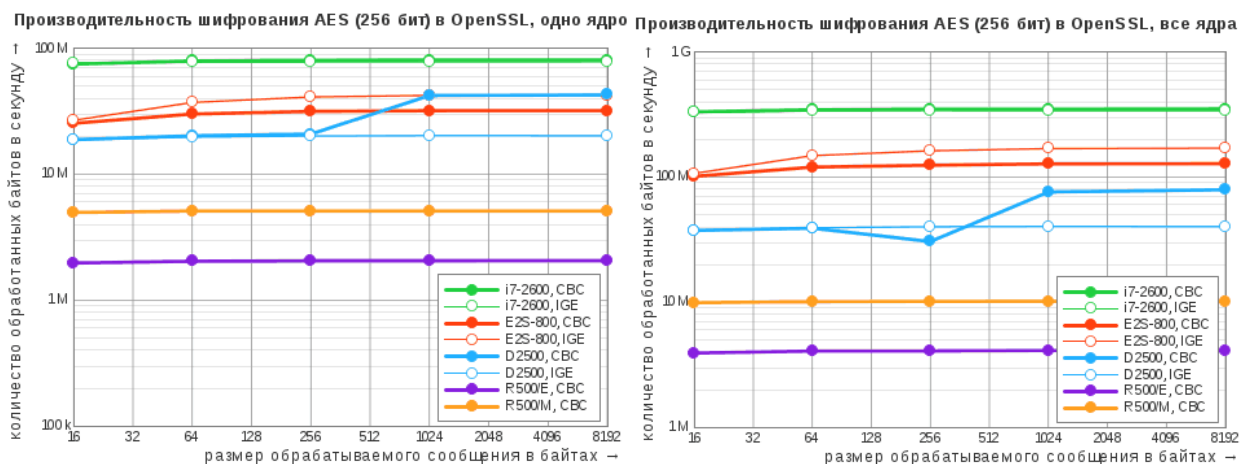


Рисунок 9 - Сравнение производительности алгоритма AES в OpenSSL на аппаратных платформах «Эльбрус», Intel Core i7-2600

По рисункам 5,6,9 видно, что AES выигрывает по производительности на порядок на различных аппаратных платформах. Однако, в пользу ГОСТ 28147-89 можно сказать следующее:

– алгоритм прекрасно поддается различным способом ускорения;

– алгоритм гораздо проще, а также менее затратно реализовать аппаратно (рисунок 10), что позволяет эффективно использовать ГОСТ 28147-89 в смарт-картах, сенсорах, RFID-метках [5].



Рисунок 10 – Данные, представленные компанией Крипто-Про о размере интегральных схем, реализующие различные алгоритмы симметричного шифрования

2.5.2.4 Алгоритм ГОСТ 34.12-2015 – «Кузнечик». В силу того, что данный алгоритм был опубликован недавно (2013г.), в сети не опубликовано результатов тестов производительности «Кузнечик». Однако, на экспертных сайтах опубликованы статьи с теоретическими обоснованиями преимуществ данного криптоалгоритма.

Структура ГОСТ 34.12-2015 называется AES-like (похожей на AES), однако, в отличие от последнего у «Кузнечика» есть ряд преимуществ:

- линейное преобразование может быть реализовано в с помощью регистра сдвига;

- ключевая развертка реализована с помощью сети Фейстеля, в которой в качестве функции используется раундовое преобразование исходного алгоритма [6].

В одной из рассмотренных статей приведен ряд преимуществ алгоритма «Кузнечик» по сравнению с AES. Использование MDS-матриц (анг. maximum distance separable – матрица максимальных разниц) необходимо для обеспечения "быстрого" перемешивания входного вектора. С криптографической точки зрения было бы

хорошо использовать большую MDS-матрицу для всего блока входных данных, однако хранить в памяти матрицу большого размера невыгодно с точки зрения эксплуатационных характеристик. В "Кузнечике" при синтезе MDS-преобразования использовался подход, предложенный отечественным ученым-алгебраистом Александром Нечаевым и заключающийся в генерации матрицы с помощью линейного регистра сдвига. Такой подход позволяет в некоторых случаях существенно экономить объем требуемой для реализации алгоритма памяти и получить матрицу для всего 128-битного блока, обрабатываемого алгоритмом, в отличие от алгоритма AES, для которого такие матрицы действуют только на 32-битных подблоках. Подход, используемый в "Кузнечике", предпочтительнее, поскольку позволил в 1,5 раза сократить число итераций по сравнению с AES и обеспечить большую защиту от атак по побочным каналам. Например, за счет блочности линейного преобразования AES при его реализации на платформе CUDA возможно практическое восстановление ключа с использованием Timing-атаки<sup>2</sup>. Для алгоритма "Кузнечик" такая атака не применима [7].

В данной статье приводятся теоретические обоснования повышенной стойкости Кузнечика криптоанализу, а также обладания более производительными и оптимизированными механизмами вычислений на стадии шифрования, что дает возможность сделать вывод о том, что ГОСТ 34.12-2015 обладает лучшими характеристиками по сравнению с AES.

## 2.6 Выбор на основе полученных данных криптоалгоритма

Основываясь на приведенные данные в п.2.5.2.2 – 2.5.2.4 можно сделать следующие выводы:

– ГОСТ 28147-89 не утратил актуальности, в настоящий момент проводятся исследования по его ускорению, однако он проигрывает по производительности AES, Кузнечику;

---

<sup>2</sup> Timing-атака (атака по времени) - это атака по сторонним каналам, в которой атакующий пытается скомпрометировать криптосистему с помощью анализа времени, затрачиваемого на исполнение криптографических алгоритмов

– AES имеет аппаратные реализации во множестве зарубежных платформах (процессора, микроконтроллеры), однако в силу того, что алгоритм не отечественный, могут возникнуть проблемы с сертификацией созданной на его базе средств криптографической защиты информации, а также вопросы по обеспечению доверия к данному алгоритму;

– ГОСТ 34.12-2015 создавался как более производительный и защищенный аналог AES. По принципу «больше большего» он опережает ГОСТ 28147-89. В подтверждение его криптостойкости, за 3 года не было найдено способов проведения эффективной криптоатаки на данный алгоритм. Максимально успешная атака на данный криптоалгоритм заключается в сокращении возможного диапазона ключей от  $2^{256}$  до  $2^{171}$ .

Используя данные приведенные выше, в качестве алгоритма шифрования выбирается ГОСТ 34.12-2015.

3 Анализ существующих аппаратных средств и выбор элементной базы, наиболее точно удовлетворяющей техническим требованиям

### 3.1 Анализ требований технического задания

В техническом задании приведен следующий перечень аппаратных требований к разрабатываемому устройству:

- тип процессора ARM® 32-bit Cortex®-M4 CPU с FPU;
- объем встроенной памяти от 128 кбайт статической ОЗУ;
- тактовая частота работы процессора до 168 МГц;
- объем встроенной энергонезависимой памяти от 256 кбайт;
- поддерживаемые карты памяти: SD, Micro SD, SDHC, MMC, USB-Flash;
- ввод пользовательского ключа шифрования: отдельный разъем форм-фактора SD;
- ввод пользовательского ключа шифрования: 10/100 Мбит/с Ethernet с поддержкой IEEE-802.3-2002;
- поддерживаемый интерфейс обмена данными с управляющим устройством: USB 2.0.

На основании данного перечня можно привести количественные характеристики к подбираемому аппаратному обеспечению. Количественные характеристики сведены в таблицу 12.

Таблица 12 – Требования к аппаратному обеспечению

| Требование              | Количественная характеристика    |
|-------------------------|----------------------------------|
| Тип процессора          | ARM® 32-bit Cortex®-M4 CPU с FPU |
| Энергопотребление       | менее 500 мА                     |
| Объем встроенной памяти | от 256 кбайт до 1024 кбайт       |
| Интерфейсов SPI*        | более 3                          |
| Интерфейсов USB         | 2                                |
| Интерфейсов Ethernet    | 1                                |

## 3.2 Выбор аппаратной платформы, удовлетворяющий требованиям технического задания

### 3.2.1 Выбор аппаратного обеспечения вычислительного модуля

В качестве вычислительного модуля выбрана платформа на основе микроконтроллера со встроенным процессором. Для реализации криптографического алгоритма ГОСТ 34.12-2015 необходима как минимум 32-разрядная архитектура микропроцессора. На основании требований технического задания (п. 3.1) в результате поиска подходящей микросхемы выбор встал между тремя производителями: NXP, Texas Instruments, ST Microelectronics. Каждая из компаний имеет лицензию ARM на интеллектуальную собственность архитектуры Cortex-M0, M0+, M3, M4 и производство микроконтроллеров на базе данных процессоров.

На рисунках 11-13 приведены наиболее удовлетворяющие линейки микросхем перечисленных компаний.

| LPC1800 specifications at a glance |                                          | LPC4300 specifications at a glance |                                                                                                                 |
|------------------------------------|------------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Core                               | 180 MHz Cortex-M3                        | Core                               | 204 MHz Cortex-M4F and 204 MHz Cortex-M0                                                                        |
| Flash                              | 0 kB - 1 MB                              | Flash                              | 0 kB - 1 MB                                                                                                     |
| RAM (kB)                           | 104 - 200                                | RAM (kB)                           | 104 - 282                                                                                                       |
| EEPROM (kB)                        | 0 - 16                                   | EEPROM (kB)                        | 0 - 16                                                                                                          |
| I <sup>2</sup> C                   | 2                                        | I <sup>2</sup> C                   | 2*                                                                                                              |
| SPI/SSP                            | 3                                        | SPI/SSP                            | 1 - 3*                                                                                                          |
| UART                               | 4                                        | I <sup>2</sup> S                   | 2*                                                                                                              |
| GPIO                               | Up to 146                                | UART                               | 4*                                                                                                              |
| USB 2.0                            | 0 - 2 HS                                 | GPIO                               | Up to 164                                                                                                       |
| CAN 2.0B                           | 2                                        | USB 2.0                            | 0 - 2 HS                                                                                                        |
| 10/100 Ethernet                    | 0 - 1                                    | CAN 2.0B                           | 2                                                                                                               |
| Analog                             | 2x 8 ch/10-bit/400 ksp/s ADC, 10-bit DAC | 10/100 Ethernet                    | 0 - 1                                                                                                           |
| Supply voltage (V)                 | 2.2 - 3.6                                | SD/MMC                             | 1                                                                                                               |
| Active current                     | 400 µA/MHz                               | Analog                             | 2x up to 8 ch/10-bit 400 ksp/s ADC or 1x 6 ch/12-bit 80 Msp/s ADC plus 2x 8 ch/10-bit 400 ksp/s ADC, 10-bit DAC |
| Temp range (°C)                    | Up to +85 (Flashless) or +105 (Flash)    | Supply voltage (V)                 | 2.4 - 3.6                                                                                                       |
| Packages                           | LQFP100/144/208, LBGA256, TFBGA100/180   | Active current                     | 400 µA/MHz                                                                                                      |
|                                    |                                          | Temp range (°C)                    | Up to +85 (Flashless) or +105 (Flash)                                                                           |
|                                    |                                          | Packages                           | LBGA256, LQFP144/208, TFBGA100/180                                                                              |

\* Serial GPIO can be used to create additional serial channels, such as I<sup>2</sup>C, SPI, I<sup>2</sup>S, etc.

Рисунок 11 – Линейки микроконтроллеров LPC на базе ARM® 32-bit Cortex®-M3, -M4, NXP

ARM® Cortex®-M7 – 216 MHz

| ACCELERATION                           |  |  |     | F <sub>CPU</sub><br>(MHz) | L1<br>cache<br>(I/D) | FPU              | Flash<br>(bytes) | RAM<br>(KB)                                 | JPEG<br>codec | CAN | DF<br>SDM | TFT LCD<br>controller | MPI/D-DSI |
|----------------------------------------|--|-----------------------------------------------------------------------------------|-----|---------------------------|----------------------|------------------|------------------|---------------------------------------------|---------------|-----|-----------|-----------------------|-----------|
| • ART Accelerator™                     |  | Product                                                                           |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • L1 cache: data and instruction cache |  | STM32F7x9*                                                                        |     | 216                       | 16K+16K              | Double Precision | 1M to 2M (RWW)   | 512K (incl.64K DTCM) + 16K ITCM + 4K backup | •             | 3   | •         | •                     | •         |
| • Chrom-ART Accelerator™               |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • Floating Point Unit                  |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| CONNECTIVITY                           |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • 2 x USB2.0 OTG FS/HS                 |  | STM32F7x7*                                                                        |     | 216                       | 16K+16K              | Double Precision | 1M to 2M (RWW)   | 512K (incl.64K DTCM) + 16K ITCM + 4K backup | •             | 3   | •         | •                     |           |
| • SDIO (x2 on F76x & F779*)            |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • USART, UART, SPI, I2C                |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • CAN2.0                               |  | STM32F7x6*                                                                        |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • HDMI-CEC                             |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • Ethernet IEEE 1588                   |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • FMC                                  |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • MDIO slave (on F76x and F77x)        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • Camera I/F                           |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • Dual mode Quad-SPI                   |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| AUDIO                                  |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • I2S + audio PLL                      |  | STM32F7x5                                                                         | 765 | 216                       | 16K+16K              | Double Precision | 1M to 2M (RWW)   | 512K (incl.64K DTCM) + 16K ITCM + 4K backup |               | 3   | •         |                       |           |
| • 2 x SAI                              |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • 2 x 12-bit DAC                       |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • SPDIF-RX                             |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| OTHERS                                 |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • 16 and 32-bit timers                 |  | STM32F7x5                                                                         |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • 3 x 12-bit ADC (2.4Mps)              |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • Low voltage 1.7 to 3.6V              |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
| • 85 °C and 105 °C range               |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |
|                                        |  |                                                                                   |     |                           |                      |                  |                  |                                             |               |     |           |                       |           |

### MSP432P4xx

#### Key Features

**Performance**

- Up to 48 MHz CPU speed
- 32-bit ARM® Cortex®-M4F
- Full ARM instruction set
- Floating Point Unit (FPU)
- DSP extensions
- 3.4 Coremark/MHz
- Independent flash banks
- DriverLib in ROM

**Security**

- 256-bit AES encryption
- JTAG access lock
- 4 IP Protection regions

**EnergyTrace™ Technology**

- Real-time power measurement and debugging
- Generate application energy profiles including current and CPU state

**ADC**

- 24-ch 14-bit (13.2 ENOB) differential ADC
- Up to 1 MSPS
- 375 uA at full speed

**Voltage**

- 1.62 to 3.7 V operation

**Ultra-low power**

- 95 uA/MHz active mode
- 850 nA LPM3 (With RTC)
- Wake-up from standby mode in <10 uS
- 167.4 ULPBench score

**Memory**

- Up to 256 KB Flash
- Up to 64 KB RAM
- Selectable RAM retention

#### Block Diagram

[Enlarge](#)

#### Applications

- Consumer & portable electronics
- Building / Factory automation & control
- Smart grid & energy
- Medical / Healthcare / Fitness
- Wearables

| Part Number                                                                                      | CPU            | Frequency (MHz) | Non-volatile Memory (KB) | RAM (KB) | GPIO | I2C | SPI | DMA | ADC         | Comparators (Inputs) | Timers - 16-bit | Timers - 32-bit | UART | Multiplier | AES    | BSL            | Min VCC | Max VCC | Active Power (uA/MHz) | Standby Power (LPM3-uA) | Wakeup Time (us) | Special I/O                               | Additional Features                                                          |
|--------------------------------------------------------------------------------------------------|----------------|-----------------|--------------------------|----------|------|-----|-----|-----|-------------|----------------------|-----------------|-----------------|------|------------|--------|----------------|---------|---------|-----------------------|-------------------------|------------------|-------------------------------------------|------------------------------------------------------------------------------|
| MSP432P401M - Low-Power + High Performance 32-Bit ARM Cortex M4F With 128KB Flash and 32KB RAM   | ARM Cortex-M4F | 48              | 128                      | 32       | 84   | 4   | 8   | 8   | ADC14 -24ch | 2                    | 4               | 2               | 4    | 32x32      | AES256 | UART, I2C, SPI | 1.62    | 3.7     | 85                    | 0.85                    | 8                | 20mA High Drive I/O, Capacitive Touch I/O | IP Protection, Real-Time Clock, Watchdog, Temp Sensor, Brown Out Reset, IrDA |
| MSP432P401R - Low-Power and High Performance 32-Bit ARM Cortex M4F With 256KB Flash and 64KB RAM | ARM Cortex-M4F | 48              | 256                      | 64       | 84   | 4   | 8   | 8   | ADC14 -24ch | 2                    | 4               | 2               | 4    | 32x32      | AES256 | UART, I2C, SPI | 1.62    | 3.7     | 85                    | 0.85                    | 8                | 20mA High Drive I/O, Capacitive Touch I/O | IP Protection, Real-Time Clock, Watchdog, Temp Sensor, Brown Out Reset, IrDA |

Рисунок 13 – Линейки микроконтроллеров MSP432P4xx на базе ARM® 32-bit Cortex®-M4F, Texas Instruments

На рисунке 13 показана лишь одна линейка микроконтроллеров фирмы Texas Instruments MSP432P4xx, так как это единственная серия микросхем, которая одновременно удовлетворяет требованиям пониженного энергопотребления и высокой производительности.

По рисункам 11-13 можно сделать следующие выводы:

– микроконтроллеры линейки STM32F7xx компании ST Microelectronics – наиболее производительные, мощные системы, которые имеют избыточные ресурсы для разрабатываемого вычислительного модуля устройства, а также самые дорогостоящие;

– микроконтроллеры линейки LPC4300 компании NXP имеют привлекательные характеристики производительности, однако при этом имеют слишком высокое энергопотребление;

– микроконтроллеры линейки LPC1800 и STM32F4xx имеют схожие характеристики, однако STM32 при незначительно большей производительности (показатель DMIPS<sup>3</sup>) имеет одинаковые значения энергопотребления (~400 мкА/МГц);

– микроконтроллеры линейки MSP432P4xx от Texas Instruments обладают самым привлекательным соотношением производительность/ энергопотребление (всего 90 мкА/МГц), однако обладают недостаточными ресурсами для использования в качестве вычислительного модуля, т.к. максимальная тактовая частота работы процессора равна 48 МГц. При этом, в микросхемах отсутствуют модули Ethernet, USB2.0, что не удовлетворяет требованиям технического задания. Микроконтроллеры данной линейки будут задействованы в разрабатываемом устройстве для других целей.

По полученным данным анализа конкуренция в выборе микросхемы вычислительного модуля сложилась между микросхемами двух фирм: NXP серия LPC1800 и ST Microelectronics STM32F4xx. Однако, с незначительным преимуществом по выдвинутым критериям, выбор падает на микросхемы серии STM32F4xx.

В результате анализа основной микросхемой вычислительного модуля выбирается микроконтроллер STM32F407VGT6.

### 3.2.2 Выбор аппаратного обеспечения модуля защиты данных от недоверенной среды

Для обеспечения конфиденциальности информации со стороны внешних носителей информации (так как они находятся в недоверенной среде) необходимо

---

<sup>3</sup>DMIPS (анг. Dhrystone million instructions per second) - синтетический тест производительности компьютеров, нацеленный на тестирование целочисленной производительности процессоров общего назначения [8].

применение защитных мер. Одной из наиболее часто применяемых мер является реализация маскиратора для нейтрализации угрозы внедрения вредоносного кода.

При этом, маскиратор не должен нарушать целостность системы, а также являться «узким» местом, снижая пропускную способность каналов передачи информации. Дополнительное требование к маскиратору – микросхема должна быть другого производителя, нежели микросхема основного вычислителя. Так снижаются риски активации закладок на всех микросхемах.

В п.3.2.1 рассматривались микроконтроллеры фирмы Texas Instruments линейки MSP432P4xx в качестве устройств с высокой эффективностью работы и низким энергопотреблением. На рисунке 3 показаны микроконтроллеры MSP432P401M и MSP432P401P данной линейки. Различие у них лишь в объеме оперативной памяти и энергонезависимой (Flash) памяти. Огромное преимущество данного микроконтроллера заключается в наличии большого числа SPI интерфейсов (8 штук).

Таким образом, возможно пропускать через различные SPI интерфейсы параллельно несколько потоков данных, что дает возможность одновременно поддерживать несколько носителей информации одновременно. Проблема данного микроконтроллера заключается в том, что в нем отсутствуют USB-интерфейсы, что не удовлетворяет требованиям, приведенным в таблице 12.

В п.3.2.1 также рассматривались микроконтроллеры фирмы NXP линейки LPC1800. На сайте производителя был осуществлен поиск с фильтром по предъявленным в таблице 12 требованиям, в результате подобран оптимальный вариант – LPC1833JET100. Данная микросхема удовлетворяет всем требованиям, а также позволяет наращивать вычислительную мощность разрабатываемого устройства.

### 3.3 Описание интерфейсов обмена данными

#### 3.3.1 Последовательный серийный интерфейс

SPI (анг. Serial Peripheral Interface – последовательный серийный интерфейс) — интерфейс, который служит для обеспечения информационного обмена между периферией и микроконтроллера. Например, в качестве периферии может быть: дисплей, различные датчики, FLASH память, SD карта. В SPI всегда есть один

ведущий и один/несколько ведомых. Передачу данных всегда инициализирует ведущий.

В SPI используются четыре линии связи:

- MOSI или SI — выход ведущего, вход ведомого (анг. *MasterOutSlaveIn*).

Служит для передачи данных от ведущего устройства ведомому.

- MISO или SO — вход ведущего, выход ведомого (анг. *MasterInSlaveOut*).

Служит для передачи данных от ведомого устройства ведущему.

- SCLK или SCK — последовательный тактовый сигнал (анг. *SerialClock*).

Служит для передачи тактового сигнала для ведомых устройств.

- CS или SS — выбор микросхемы, выбор ведомого (анг. *Chip Select, Slave Select*).

SPI может быть реализован в микроконтроллере аппаратно, тогда задача по управлению интерфейсом решается для каждого микроконтроллера отдельно, т.к. реализации могут быть разными. Для передачи данных к ведомому устройству, нужно в сдвигающий регистр MASTER (на рисунке 14 обозначен как – «8 BIT SHIFT REGISTER») записать байт передаваемой информации. При этом автоматически на SCK начнет генерироваться синхросигнал. Это и есть аппаратная реализация.

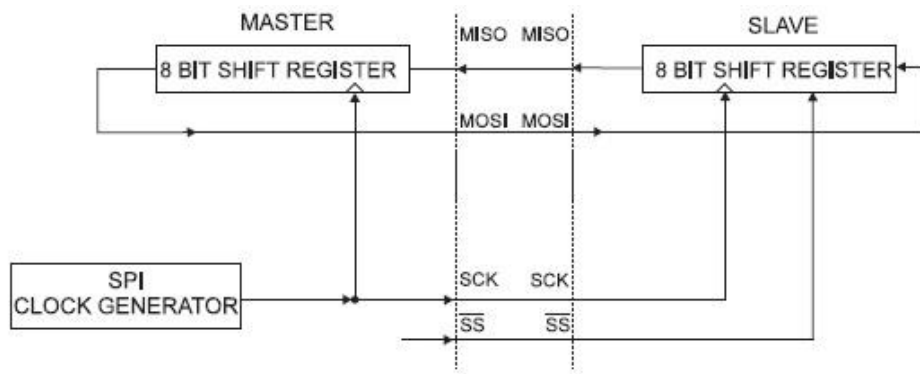


Рисунок 14 – Схема потоков данных интерфейса SPI

Если аппаратной поддержки SPI в микроконтроллере нет, то интерфейс SPI можно всегда реализовать программно, т.е. создать программу, управляющую портами ввода-вывода контролера согласно протоколу обмена SPI.

При этом, в связи с тем, что единого стандарта SPI нет, существуют различия в реализациях интерфейса SPI.

Ведомые микросхемы могут по-разному «интерпретировать» принятый сигнал по SPI, отличие может заключаться в следующих моментах:

- в размере передающих данных или размере пакета, обычно - 8 бит;
- в порядке следования бит, сначала старший бит или сначала младший бит;
- по какому уровню синхросигнала передаются данные (по уровню логической единицы (HIGH) или логическому нулю (LOW));
- типа синхронизации (по переднему фронту («0»→«1») или заднему фронту («1»→«0»)), или фаза синхронизации.

Комбинация «уровня синхронизирующего сигнала» и «фазы синхронизации» определяется в спецификациях как режимы работы SPI (таблица 13).

Таблица 13 – Режимы работы системы тактирования SPI

| Режим | Уровень сигнала (CPOL) | Фаза (CPHA) |
|-------|------------------------|-------------|
| 0     | 0                      | 0           |
| 1     | 0                      | 1           |
| 2     | 1                      | 0           |
| 3     | 1                      | 1           |

В столбце «Уровень сигнала» значение «1» означает, что бит данных, принимаются ведомым устройством, когда по линии синхронизации передается «0», другими словами – ведомое устройство ожидает и не принимает данные, когда на SCK установлена логическая «1».

В столбце «Фаза» значение «1», означает, что сигнал синхронизации определяется по спадающему фронту синхроимпульса, а логический «0» по нарастающему фронту синхроимпульса. На рисунке 5 показаны режимы тактирования SPI, приведенные в таблице 13 [9].

Figure 18-3. SPI Transfer Format with CPHA = 0

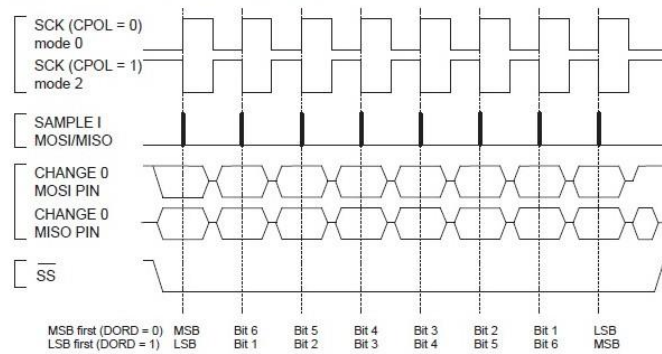


Figure 18-4. SPI Transfer Format with CPHA = 1

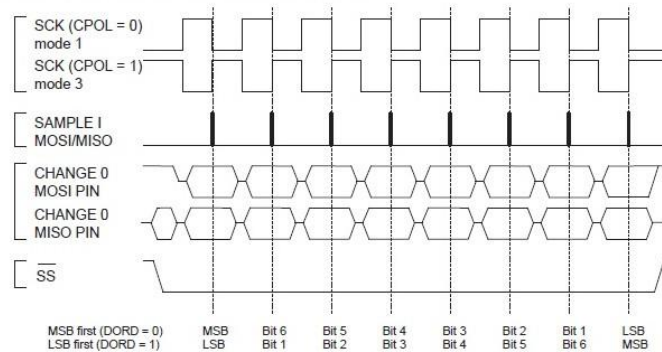


Рисунок 15 – Диаграмма режимов тактирования интерфейса SPI

### 3.3.2 Универсальная последовательная шина

USB (Universal Serial Bus) - универсальная последовательная шина последовательный интерфейс передачи данных для среднескоростных и низкоскоростных периферийных устройств в вычислительной технике.

Характеристики интерфейса обмена данными:

- «горячее подключение»;
- Автоматическая конфигурация;
- Совместное использование прерываний;
- Совместное использование и выделение полосы пропускания
- Питание USB.

"Горячее" подключение. Возможно подключение и отключение в любое время без выключения компьютера или иных действий.

Автоматическая конфигурация. Чипсет хост-контроллера USB, имеющийся на материнской плате или карте расширения, управляет программным обеспечением драйверов, и выделяет часть полосы пропускания каждому устройству,

подключенному к шине. Когда устройство добавляется или удаляется, хост-контроллер автоматически загружает или выгружает его драйвер.

Совместное использование прерываний. Хост-контроллер USB занимает одно прерывание, которое используется совместно, всеми подключенными к шине устройствами. Такое использование ресурсов позволяет устанавливать в один компьютер несколько хост-контроллеров. К каждому контроллеру можно подключить до 127 устройств, но рекомендуется равномерно распределять устройства между несколькими контроллерами.

Совместное использование и выделение полосы пропускания. Пропускная способность шины USB 1.1 составляет 12 Мбит/с, а USB 2.0 - 480Мбит/с. Полоса пропускания делится между всеми подключенными устройствами. Несколько устройств могут одновременно передавать данные по шине. Хорошие периферийные устройства и драйверы USB работают с полосой пропускания динамически, по возможности освобождая её для других устройств. Для изохронных задач, таких как аудио- и видеопотоков, где время является критическим фактором, USB предусматривает выделение конкретной полосы пропускания, причём эта полоса становится абсолютно недоступной для других устройств.

Встроенный разъём питания USB обеспечивает устройствам не только связь устройствам, но и электропитание. Однако мощность питания ограничена на уровне 500 мА (по спецификации 2.0).

Версии USB:

- USB 1.0;
- USB 1.1;
- USB 2.0;
- USB 3.0;
- USB 3.1.

Оригинальная версия стандарта – USB 1.0. Данная версия стандарта поддерживает скорости передачи данных 1,5 и 12 Мбит/с. USB 1.0-совместимые устройства, работают с портами USB 1.1 и USB 2.0 без всяких проблем. Устройства

USB 1.1 или USB 2.0 могут выдавать ошибки при подключении к интерфейсу USB 1.0.

Стандарт USB 1.1 поддерживает те же скорости передачи данных (1,5 и 12 Мбит/с), однако в нем устранены неоднозначности и неточности, имеющиеся в спецификации USB 1.0.

Стандарт USB 2.0 поддерживает скорости передачи 1.5, 12 и 480 Мбит/с и обладает полной совместимостью с устройствами USB 1.0 и USB 1.1. USB 2.0 определяет один хост-контроллера, который называется усовершенствованным (Enhanced Host Controller Interface - EHCI).

Спецификация USB 3.0 повышает максимальную скорость передачи информации до 5 Гбит/с — что на порядок больше 480 Мбит/с, которые может обеспечить USB 2.0. Таким образом, скорость передачи возрастает с 60 Мбайт/с (30 Мбайт/с эффективных) до 600 Мбайт/с и позволяет передать 1 ТБ не за 8—10 часов, а за 40—60 минут. Версия 3.0 отличается не только более высокой скоростью передачи информации, но и увеличенной силой тока с 500 мА до 900 мА. Таким образом, от одного хаба можно подпитывать большее количество устройств либо избавить сами устройства от отдельных блоков питания. На некоторых материнских платах и ноутбуках одно или несколько гнезд USB 3.0 могут быть помечены значком молнии. Это значит, что от данного порта можно подпитывать и заряжать устройства, потребляющие ток более 1 А, а также зарядка будет идти при выключенном компьютере.

Спецификация USB 3.1. 31 июля 2013 года USB 3.0 Promoter Group объявила о принятии спецификации следующего интерфейса, USB 3.1, скорость передачи которого может достигать 10 Гбит/с. Далее перечислены главные особенности нового интерфейса:

- скорость передачи данных до 10 Гбит/с;
- возможность запитывания от порта устройств с потребляемой мощностью вплоть до 100Вт;
- размеры коннектора сравнимые с micro-USB;
- симметричность разъёма;

- возможность запитывания устройства с напряжением до 20 вольт;
- однообразные коннекторы;
- конструкция разъёма способна выдерживать до 10 000 подключений;
- совместимость с USB 3.0 интерфейсом, с USB 2.0 (с помощью переходника).

Скорости работы интерфейса USB:

- низкая скорость (Low Speed);
- полная скорость (Full Speed);
- высокая скорость (High Speed).

Низкая скорость (Low Speed). Низкоскоростные USB-устройства передают данные со скоростью 1.5 Мбит/с и могут подключаться к интерфейсам USB 1.1 и USB 2.0. Низкая скорость передачи ориентирована на такие устройства, как мыши и клавиатуры. Дина низкоскоростного защищённого (captive) кабеля не должна превышать 3м. Реальная пропускная способность из-за накладных расходов оказывается равной 1,2 Мбит/с или около 150 Кбайт/с.

Полная скорость (Full Speed) Полноскоростные USB-устройства передают данные со скоростью 12 Мбит/с и могут подключаться к интерфейсам USB 1.1 и USB 2.0. Это максимально возможная скорость передачи для USB 1.0 и USB 1.1. Режим полной скорости ориентирован на устройства со средними требованиями к полосе пропускания, такие как принтеры и сканеры. Для подключения используется сменный (detachable) кабель, длина которого не может превышать 5м. Реальная пропускная способность полноскоростного USB редко превышает 900 Кбайт/с.

Высокая скорость (High Speed) Высокоскоростные USB-устройства передают данные со скоростью 480 Мбит/с и могут подключаться только к интерфейсам USB 2.0. Для подключения высокоскоростных устройств используются такие же кабели, что и для полноскоростных, с тем же ограничением на длину 5м. Реально наблюдаемая максимальная пропускная способность высокоскоростного USB обычно достигает 35-40 Мбайт/с. Этого вполне достаточно для всех накопителей, за исключением наиболее быстрых.

Для передачи пользовательских данных и управляющей информации между хост-контроллером и USB-устройствами используются односторонние и

двусторонние каналы (pipes). Устройство может использовать несколько каналов для различных целей, причём данные по разным каналам передаются независимо. Например: USB-принтер может принимать по одному каналу информацию, а по другому - отправлять на компьютер сведения о своём состоянии. USB определяет следующие виды потоков данных.

Режимы передачи данных USB:

- изохронная передача;
- передача по прерыванию;
- управляющая передача;
- групповая передача.

Изохронная передача (Isochronous Data Transfer) используется для периодического продолжительного взаимодействия между хост-контроллером и устройством, чаще всего в тех задачах, где время является критическим параметром, например, для передачи аудио- и видео потоков. Изохронная передача подразумевает резервирование требуемой частоты полосы пропускания для изохронного устройства. Полоса становится недоступной для других устройств, даже если в данный момент не используется. Если вся полоса пропускания будет зарезервирована для изохронной передачи, другие устройства на этой шине работать не смогут.

Передача по прерыванию (Interrupt Data Transfer) используется для передач малых объёмов с ограниченным временем ожидания, когда требуется своевременная надёжная доставка данных. Примером являются USB-мыши и модемы, передающие компьютеру информацию о своём состоянии. Передача по прерыванию имеет меньший приоритет при выделении полосы пропускания, чем изохронная.

Управляющая передача (Control Transfers) используется для настройки устройства при подключении к шине, управления другими каналами передачи, а также для передачи иных управляющих команд, сведений о состоянии и конфигурации. Обычно подразумевает небольшой объём данных и отсутствие критичности по времени. Имеет меньший приоритет при выделении полосы пропускания, чем передача по прерыванию.

Групповая передача (Bulk Data Transfer) используется для пересылки больших объёмов данных крупными пакетами без жёстких ограничений по времени, например, для отправки печатаемых страниц на USB-принтер. Групповая передача имеет самый низкий приоритет при распределении пропускной способности [10].

На рисунке 16 показаны контакты разъёма USB различных типов.

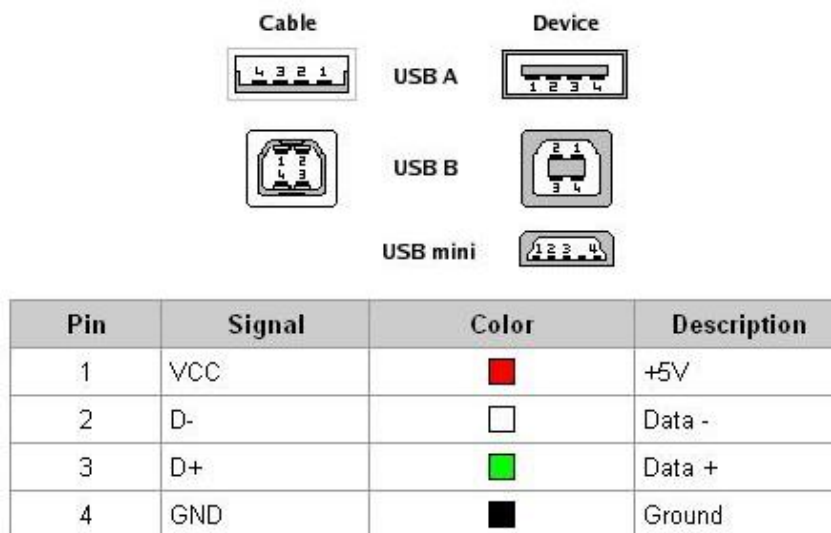


Рисунок 16 – Перечень контактов разъёма USB различных типов

### 3.3.3 Описание технологии Ethernet

Сеть Ethernet разработана в 1976 году Меткальфом и Боггсом (фирма Ксерокс). Ethernet совместно со своей скоростной версией Fast Ethernet, GigaEthernet (1 Гбит/с) и 10GE (10 Гигабит/с) занимает в настоящее время абсолютно лидирующую позицию. В настоящее время на основе этого стандарта строятся уже не только локальные, но и общегородские сети, а также межгородские каналы. В качестве сред передачи используются следующие: тонкий и толстый коаксиальный кабель, радио среда, витая пара категорий 3, 5, 5е, одномодовое и многомодовое оптоволокно. Скорости, которые поддерживает данное семейство технологий – 10, 100, 1000 и 10000 Мбит/с. 10 мегабитная технология Ethernet не представляет для нас особого интереса, более интересными являются стандарты со скоростями передачи 100 и 1000 Мбит/с.

100 МГц сеть Ethernet дешевле создать на базе скрученных пар. Существует несколько версий 100-мегагерцного Ethernet (100base-T4, 100base-TX, 100base-FX). Сегменты T4 (100base-T4) используют четыре скрученные пары телефонного качества (экранированные и неэкранированные скрученные пары проводов категории

3, 4 или 5) длиной до 100м. Провода должны быть скручены по всей длине, скрутка может быть прервана не больше чем в 12мм от разъема (данное требование справедливо и для сегментов типа TX).

Сегменты TX (100base-TX, стандарт ANSI TP-PMD) состоят из двух скрученных пар проводов информационного качества (волновое сопротивление 100-150 Ом, экранированные и неэкранированные скрученные пары проводов категории 5, длина до 100м).

FX-сегменты (100base-FX) представляют собой оптоволоконные кабели, отвечающие требованиям стандарта ANSI. Мультимодовое волокно 62,5/125 мкм работает в инфракрасном диапазоне 1350 нм. Максимальная длина сегмента составляет 412 метров, ограничение определяется соображениями допустимых задержек. Предельное ослабление сигнала в волокне не должно превышать 11 дБ, стандартный кабель имеет 1-5 дБ/км. Оптические разъемы должны отвечать тем же требованиям, что и разъемы, используемые в FDDI-сетях. Для оптоволоконной версии дуплексной связи предельная длина сегмента может достигать 2 км (для полудуплексного варианта предельная длина сегмента может достигать 412 м). Следует иметь в виду, что для локальных сетей целесообразнее применение мультимодового оптоволокна (дешевле и больше коэффициент захвата света, но больше удельное поглощение).

Для того, чтобы выявить, к какой модификации относится тот или иной сегмент, разработан специальный протокол распознавания, позволяющий строить сети, которые содержат оборудование и кабельные сегменты, отвечающие разным требованиям.

В настоящее время разрабатываются новые еще более скоростные варианты Ethernet IEEE 802.3z. Гигабитный Ethernet утвержден в качестве стандарта в 1998 году 1000base-FX. Эти сети ориентированы на применение 4-х скрученных пар категории 5 или выше (до 100м, разъем RJ-45) и оптоволоконных кабелей. Вместо манчестерского кода применяется кодировка 8B/10B. Эта нотация означает, что каждый байт кодируется при передаче десятью битами. При этом не должно быть более 4 идентичных бит подряд и ни в одном коде не должно быть более 6 нулей или

6 единиц. Так достигаются хорошие условия синхронизации и высокая стабильность постоянной составляющей. В рассматриваемом варианте по каждой паре передаются сигналы с частотой 125 МГц, и за каждый так транспортируется два бита.

Хотя Ethernet на 1 Гбит/с и не использовал все свои возможности, реализован уже 10 Гбитный Ethernet (IEEE 802.3ae, 10GBase-LW или 10GBase-ER). Этот стандарт утвержден в июне 2002 года и в случае использования для построения региональных каналов соответствует спецификациям OC-192c/SDH VC-4-46c (WAN). Опробован канал длиной 200 км с 10 сегментами. Существует серийное сетевое оборудование обеспечивающее надежную передачу на скорости 10 Гбит/с при длине одномодового кабеля 10 км ( $\lambda = 1310$  нм). При работе с оптическими волокнами могут применяться лазеры с вертикальными резонаторами и поверхностным излучением VCSEL (англ. Vertical Cavity Surface Emitting Laser). В случае мультимодовых вариантов используются волокна с градиентом коэффициента преломления. Такие каналы могут использоваться и в LAN для соединения переключателей сетевых кластеров. Соединение организуется по схеме точка-точка. Эта технология удобна для использования в фермах электронно-вычислительных машин (далее – ЭВМ). Стандартизованы порты: 10Gbase-LR (до 10 км по одномодовому волокну - для высокопроизводительных магистральных и корпоративных каналов), 10Gbase-ER (до 40 км по одномодовому волокну), 10Gbase-SR (до 28 м по мультимодовому волокну - для соединений переключателей друг с другом), а также 10Gbase-LX4 (до 300 м по мультимодовому волокну стандарта FDDI - для сетей в пределах одного здания). Обсуждается возможность построения 100 Гбит/с Ethernet. В 10Gbase для локальных сетей применяется кодирование 64B/66B (вместо 8B/10B, используемого в обычном гигабитном Ethernet), так как старая схема дает 25% увеличение паразитного трафика. Следует обратить внимание, что такое решение делает непригодными существующие оптоволоконные технологии SDH/SONET. К концу 2002 года технология 10 Гбит-Ethernet вторглась в область региональных (MAN) и даже межрегиональных (WAN) сетей, тесня SDH, Fibre Channel, OC-192, PCI Express и InfiniBand [11].



4 Разработка аппаратного обеспечения устройства криптографической защиты данных при работе с внешними носителями по единой системе конструкторской документации

#### 4.1 Разработка схемы электрической структурной

Схемы электрические структурные определяют основные части изделия, их назначения и служат для общего ознакомления с изделием. На структурной схеме раскрывается не принцип работы отдельных функциональных частей, а только взаимодействие между ними. Поэтому составные части изделия изображаются в виде прямоугольников различной формы, однако допускается также применять условные графические обозначения элементов. На линиях взаимосвязи стрелками указывают направление хода процессов, протекающих в изделии. На структурной схеме в виде таблицы обычно указываются наименования функциональных частей изделия. Кроме того, допускается на структурной схеме помещать поясняющие надписи, диаграммы, таблицы, а также указывать электрические параметры (токи, уровни напряжений) и формы сигналов в определенных точках схемы [12].

Разработка схемы электрической структурной начинается после анализа требований к аппаратному обеспечению технического задания. Требования к аппаратному обеспечению крипто-картридера приведены в таблице 12. В результате анализа требований был произведен выбор аппаратной платформы. Так, принято решение использовать следующее аппаратное обеспечение:

- основной вычислитель – микросхема, реализующую фильтрацию трафика, шифрование полезной нагрузки STM32F407VGT6;
- маскиратор – микросхема, реализующая операцию маскирования с целью защиты микросхемы основного вычислителя от угроз, которые могут возникнуть из внешней среды LPC1833JET100;
- модуль сопряжения с интерфейсом Ethernet – микросхема одночиповый трансивер физического уровня Ethernet, предназначенный для совместимости микросхемы основного вычислителя с Ethernet;
- вторичный источник питания – микросхема LT1129-3.3, предназначенная для преобразования первичного напряжения от USB (+5 В) до напряжения питания

микросхем основного вычислителя и маскиратора, модуля сопряжения с интерфейсом Ethernet, а также соединителями для разъемов SD/SDHC/MMC/MicroSD (+3,3 В);

- соединитель для разъемов SD/SDHC/MMC/MicroSD (слоты для карт памяти);
- кнопка НСД – предназначена для контроля наличия носителя ключевой информации в сеансе обмена данными с внешними носителями информации;
- светодиод «Статус» - 3х цветный светодиод (зеленый/красный/желтый) предназначенный для индикации состояния устройства в реальном времени.

В таблице 14 приведены интерфейсы, по которым взаимодействуют перечисленные аппаратные компоненты.

Таблица 14 – Интерфейсы взаимодействия компонентов устройства

| Компонент            | Компонент                                    | Интерфейс |
|----------------------|----------------------------------------------|-----------|
| Основной вычислитель | Маскиратор                                   | USB       |
| Основной вычислитель | Модуль сопряжения с интерфейсом Ethernet     | RMII      |
| Основной вычислитель | Светодиод «Статус»                           | GPIO      |
| Основной вычислитель | Кнопка НСД                                   | GPIO      |
| Маскиратор           | Соединители для разъемов SD/SDHC/MMC/MicroSD | SPI       |
| Маскиратор           | Гнездо для USB                               | USB       |

Разработанная схема электрическая структурная (Э1) приведена в приложении А.

#### 4.2 Разработка схемы электрической принципиальной

Схемы электрические принципиальные определяют полный состав изделия и дает детальное представление о принципе работы изделия. Данная схема строится на основе схемы электрической структурной. На основе схемы электрической принципиальной разрабатывают целый ряд других конструкторских документов – схемы соединений, чертежи печатных плат, перечни элементов и т.д. На схеме электрической принципиальной изображают все электрические элементы и

устройства, необходимые для осуществления и контроля в изделии соответствующих электрических процессов. Элементы изображают в виде условных графических обозначений (далее - УГО) в соответствии с ГОСТ 2.702-2011 «Единая система конструкторской документации (далее - ЕСКД). Правила выполнения электрических схем». Каждый элемент схемы электрической принципиальной должен иметь позиционное буквенно-цифровое обозначение. Порядковые номера элементам присваивают, начиная с единицы в пределах группы элементов, имеющих одинаковые буквенные обозначения (R1, R2, DD1, DD2 и так далее). Порядковые номера присваивают в соответствии с последовательностью расположения элементов или устройств на схеме сверху вниз, в направлении слева направо. Позиционное обозначение проставляют рядом с графическим обозначением элемента с его правой стороны или над ним. При изображении на схеме элемента разнесенным способом его позиционное обозначение проставляют около каждой части (например, DD1.1, DD1.2 и т.д.). Обязательным документом, выпускаемым совместно со схемой электрической принципиальной, является перечень элементов (ПЭЗ).

При выполнении схемы электрической принципиальной на поле схемы допускается помещать поясняющие текстовые данные, отдельных цепей (например, о питании микросхем). При выполнении схемы электрической принципиальной на нескольких листах соблюдается сквозная нумерация и выполняется общий перечень элементов [12].

Разработанная схема электрическая принципиальная (ЭЗ) в соответствии с ЕСКД с прилагающимся к ней перечнем элементов (ПЭЗ) приведены в приложении Б.

## 5 Разработка спецификации программного обеспечения

### 5.1 Общие положения разрабатываемой спецификации

Под общими положениями разрабатываемой спецификации следует понимать перечень следующих деталей:

- функциональные возможности – задачи ПО;
- внешние интерфейсы – пути взаимодействия ПО с человеком, аппаратными ресурсами системы, и иными аппаратными ресурсами и сторонним ПО;
- производительность – требования к скорости работы, доступности, времени реакции на команды пользователя;
- атрибуты – требования к портативности, корректности, ремонтпригодности, безопасности;
- конструктивных ограничений, наложенных на реализацию; требования существующих стандартов, нормативных документов; язык программирования, политика целостности, ограничения на использование ресурсов, иные требования.

В таблице 14 приведен перечень требований к ПО из технического задания на разработку устройства в соответствии с приведенной формой спецификации.

Таблица 15 – Общие положения спецификации

| Категория требований       | Требования                                                                                                                      | Содержание требования                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Функциональные возможности | Устройство предназначено для применения в организациях в целях обеспечения конфиденциальности данных с грифом «конфиденциально» |                                                                                               |
| Внешние интерфейсы         | Интерфейсы обмена данными                                                                                                       | USB 2.0 (host, device), SDIO, SPI<br>Поддержка карт памяти SD, SDHC, Micro SD, MMC, USB-flash |
|                            | Интерфейс взаимодействия с пользователем                                                                                        | Индикация состояния: LED светодиод (2 цвета)                                                  |

Продолжение таблицы 15

| Категория требований        | Требования                      | Содержание требования                                                  |
|-----------------------------|---------------------------------|------------------------------------------------------------------------|
| Производительность          | Шифрование/расшифрование данных | не менее 0,4 Мбайт/с                                                   |
| Атрибуты                    | портативность                   | Совместимость с системой команд ARM Cortex-M                           |
|                             | Алгоритм шифрования данных      | ГОСТ 34.12-2015 «Кузнечик»                                             |
|                             | Безопасность                    | Организация защиты от недовверенной среды путем реализации маскиратора |
| Требования к написанию кода | Язык программирования           | C/C++                                                                  |
|                             | Компилятор                      | arm-none-eabi-gcc 4.6.2                                                |

## 5.2 Функциональное описание системы

### 5.2.1 Общая функциональная схема модулей крипто-картридера

В функциональное описание системы входит перечень всех функциональных блоков с описанием, приоритетом, алгоритмами работы, связями с другими модулями, движениями процессов, а также функциональными требованиями на основании спецификации.

На рисунке 17 приведена схема модели потоков данных Гейн-Сарсона. На данной схеме изображены все функциональные блоки разрабатываемого устройства, таким образом она является также и общей функциональной схемой устройства.

Перечень всех функциональных блоков устройства (по рисунку 17):

- интерфейс обмена данными с периферией;
- модуль обмена данными по интерфейсу Ethernet;
- модуль вычисления ключа шифрования;

- криптопроцессор;
- маскиратор.

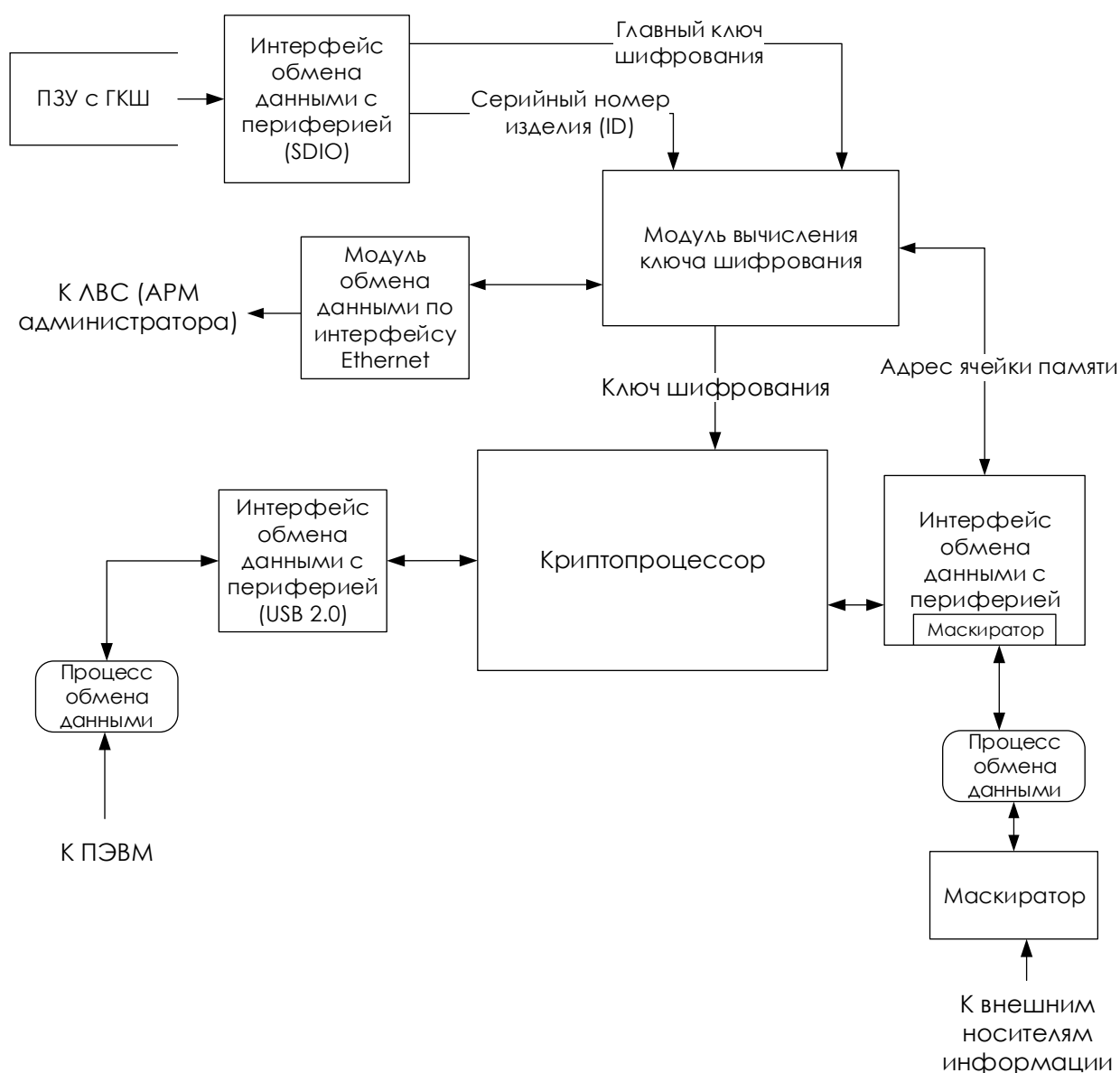


Рисунок 17 – Схема модели потоков данных Гейн-Сарсона

Примечание: обозначение на схеме ПЗУ с ГКШ – постоянное запоминающее устройство с главным ключом шифрования.

### 5.2.2 Описание модуля маскиратора

Данный модуль предназначен для обеспечения защиты от недоверенной среды путем наложения маски на данные на передающей стороне и снятия маски на принимающей стороне. За недоверенную среду в данном устройстве будем считать

внешнюю среду – среду внешних носителей. Проблемы обеспечения доверенной среды подробно рассмотрены

Маска генерируется в вычислительном модуле путем запуска аппаратного датчика случайных чисел (реализованного в микросхеме вычислительного модуля). Передача маски осуществляется перед сеансами связи. Маска представляет собой 256 бит случайно-сгенерированной последовательности. Частота смены маски – каждый раз при запуске устройства. Наложение маски осуществляется сложением по модулю 2. Снятие маски осуществляется аналогичным способом. Маска уникальная и вырабатывается для каждого интерфейса отдельно. Алгоритм работы маскиратора показан на рисунке 18.

### 5.2.3 Описание модуля вычисления ключа шифрования

Для функционирования алгоритма симметричного шифрования необходимо выполнить ряд организационно-технических мероприятий:

- выработка сеансовых ключей шифрования;
- хранение ключей шифрования для процедур расшифрования;
- обеспечение конфиденциальности ключей шифрования.

Учитывая все предъявленные требования к ключевой системе, разработана схема модуля вычисления ключа шифрования. Данная схема приведена на рисунке 19.

Ключ шифрования формируется на основе главного ключа шифрования и алгоритма формирования ключа шифрования сектора. При таком алгоритме формирования ключ шифрования сектора не хранится на внешнем носителе информации и не занимает дополнительное место.

Главный ключ шифрования хранится на отдельном носителе типа SD и хранится у пользователя. Перед началом работы необходимо установить SD в специальный разъем.

Алгоритм формирования ключа шифрования сектора использует следующие данные:

- серийный номер изделия ПЗУ;
- адрес ячейки памяти в ПЗУ, к которому планируется обращение.

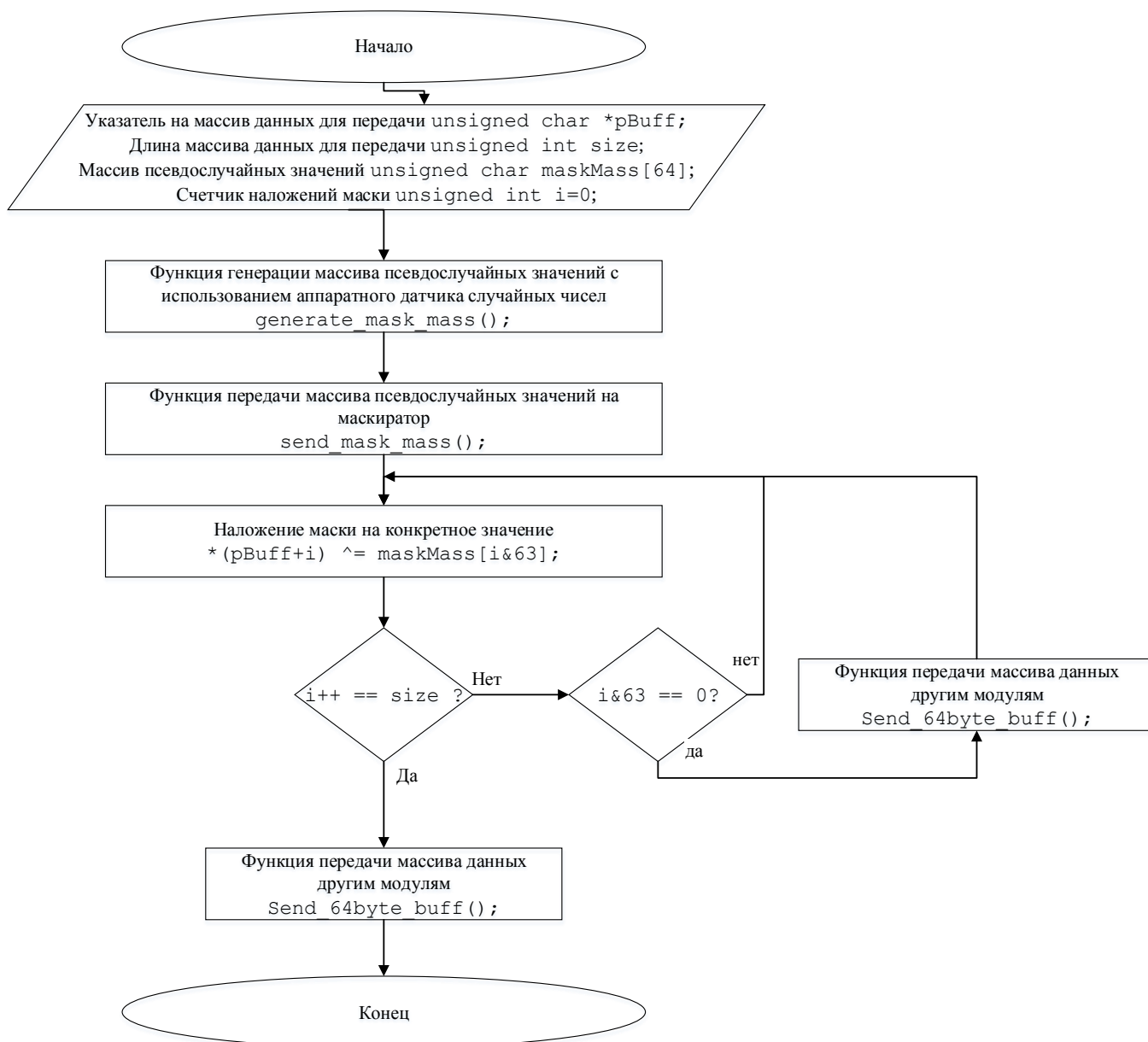


Рисунок 18 – Алгоритм работы модуля маскирования

На выработанном ключе шифруется сектор, а ключ после использования стирается.

Срок смены главного ключа шифрования – 1 раз в год.

Как было сказано ранее, шифрование в крипто-картридере реализовано на уровне секторов. Такое решение было принято по трем причинам.

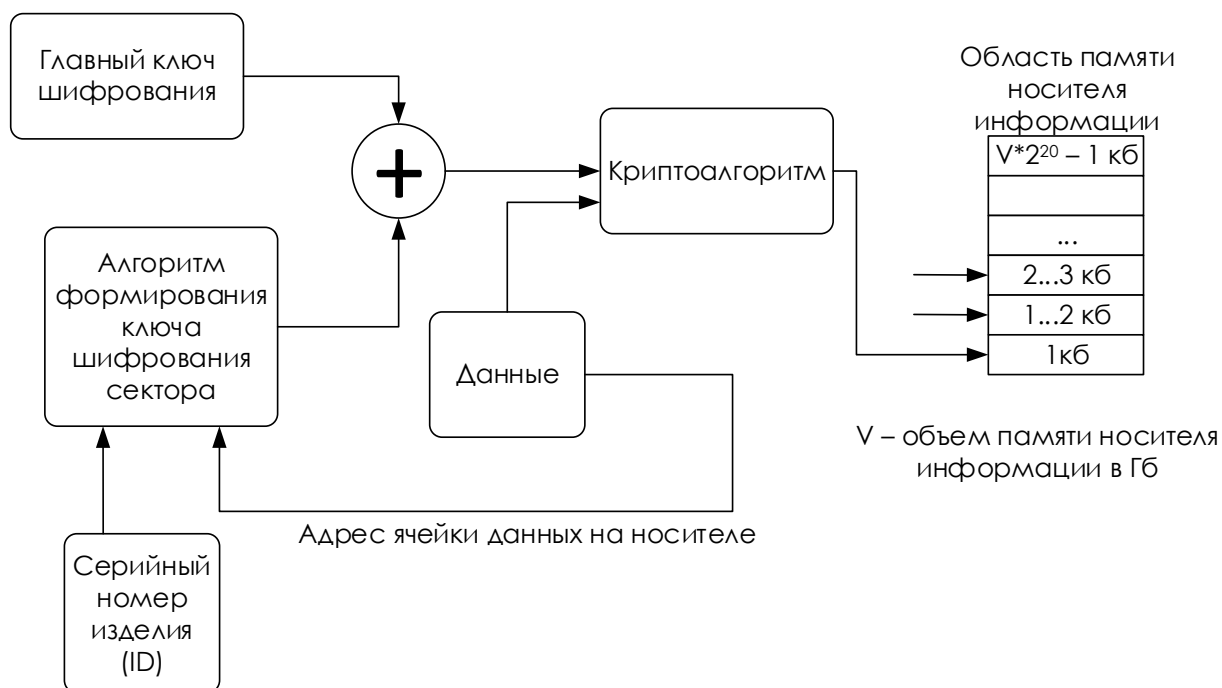


Рисунок 19 – Ключевая система крипто-картридера

Во-первых, в случае, если в устройстве реализовывать шифрование на уровне файлов, то необходимо осуществлять поддержку файловых систем. Как известно, файловых систем существует множество и все они не унифицированы. Можно рассмотреть только самые популярные: семейство fat(12/16/32), exfat, ntfs, ext(2,3,4).

Во-вторых, шифрование на уровне файлов дает некоторую гибкость в использовании: так один внешний носитель могут использовать несколько сотрудников. Дополнительная нагрузка на фильтр служебной информации может привести как к потере производительности, так и появление потенциальных уязвимостей в ПО. Однако, на уровне организаций данная проблема не является актуальной.

В-третьих, шифрование на уровне секторов позволит обеспечить большую защищенность данных, т.к. фильтр служебной информации в таком случае будет не так усложнен.

#### 5.2.4 Описание модуля интерфейса обмена данными с периферией

Данный интерфейс должен поддерживать обмен данными по следующим интерфейсам: USB2.0, SPI, SDIO, Ethernet; GPIO.

Требования к пропускным способностям интерфейсов:

- USB2.0 – high-speed режим (12 Мбит/с);

- SPI – не ниже 0,5 Мбайт/с (4Мбит/с);

- к интерфейсам SDIO, Ethernet требования не предъявляются, т.к. через них проходит незначительное количество информации (ключевая информация).

Приоритеты обработки интерфейсов в порядке убывания:

- GPIO;

- USB 2.0;

- SDIO;

- SPI;

- Ethernet.

Интерфейс GPIO обладает самым высоким приоритетом обработки прерываний. Данное решение произведено потому, что по данному интерфейсу осуществляется контроль НСД к носителю ключевой информации, соответственно, устройство должно незамедлительно реагировать на любые события, связанные с данной кнопкой.

Интерфейсы обмена данными с периферией имеют одну из самых значимых ролей при обеспечении работы устройства и находятся в постоянном взаимодействии с остальными модулями устройства (рисунок 17).

#### 5.2.5 Описание модуля криптопроцессора

Криптопроцессор – один из наиболее значимых модулей устройства. Данный модуль обеспечивает шифрование данных алгоритмом ГОСТ 34.12-2015 «Кузнечик» (таблица 15). В число задач модуля также входит фильтрация трафика: выделение полезной нагрузки (данных), преобразование их алгоритмом шифрования, пропускание команд и иных служебных данных. Схема потоков данных криптопроцессора приведена на рисунке 20.

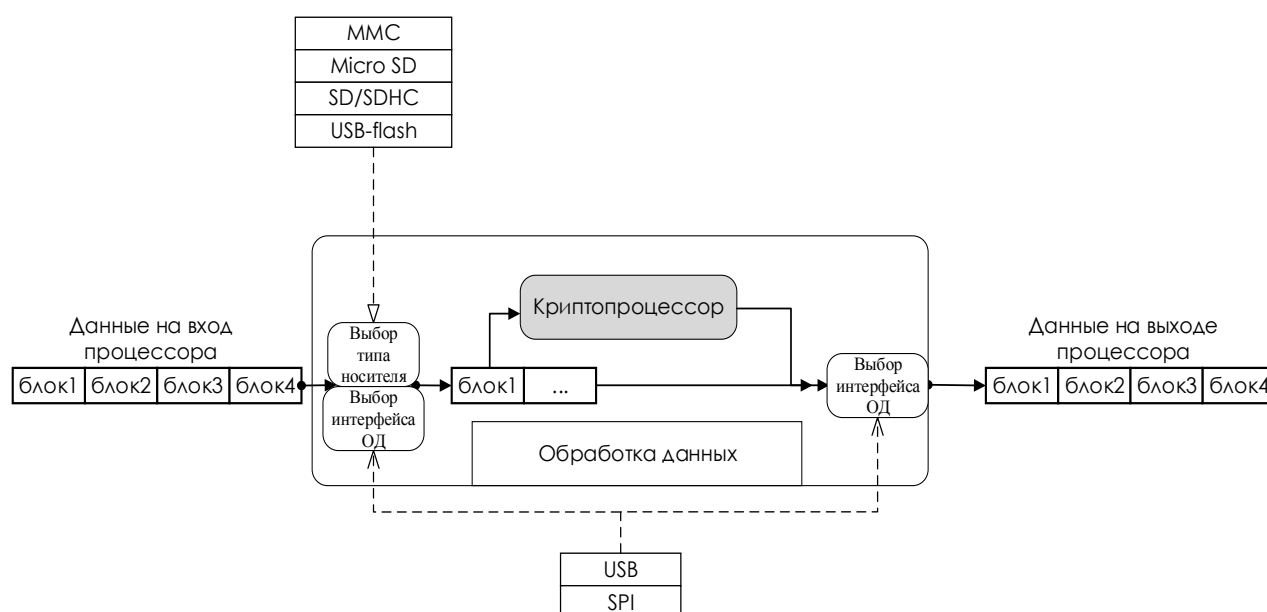


Рисунок 20 – Схема потоков данных криптопроцессора

На рисунке 20 показано, что фильтр трафика криптопроцессора не имеет привязки к типу файловой системы, а также интерфейсу обмена данными. Он поддерживает только служебные команды, которые могут передаваться на поддерживаемые носители данных.

Исходя из описания принципе работы криптопроцессора, можно предъявить требования к реализации данного модуля:

- производительность алгоритма шифрования: не менее 4 Мбит/с;
- алгоритм шифрования: ГОСТ 34.12-2015 «Кузнечик»;
- шифрование: на уровне секторов данных носителей информации.

По причине того, что производительности базового алгоритма шифрования может быть недостаточно для достижения требований технического задания. Для этого осуществлен поиск возможных способов ускорения работы алгоритма криптографического преобразования. На рисунке 21 показаны операции шифрования/расшифрования блока данных.

Идея ускорения шифрования основана на построении таблиц предвычислений. С такими таблицами не будет необходимости использовать преобразования  $S/S^{-1}$  и

$L/L^{-1}$  (рисунок 21) для каждого байта. Данное решение позволит значительно уменьшить количество операций для обработки блока входных данных.

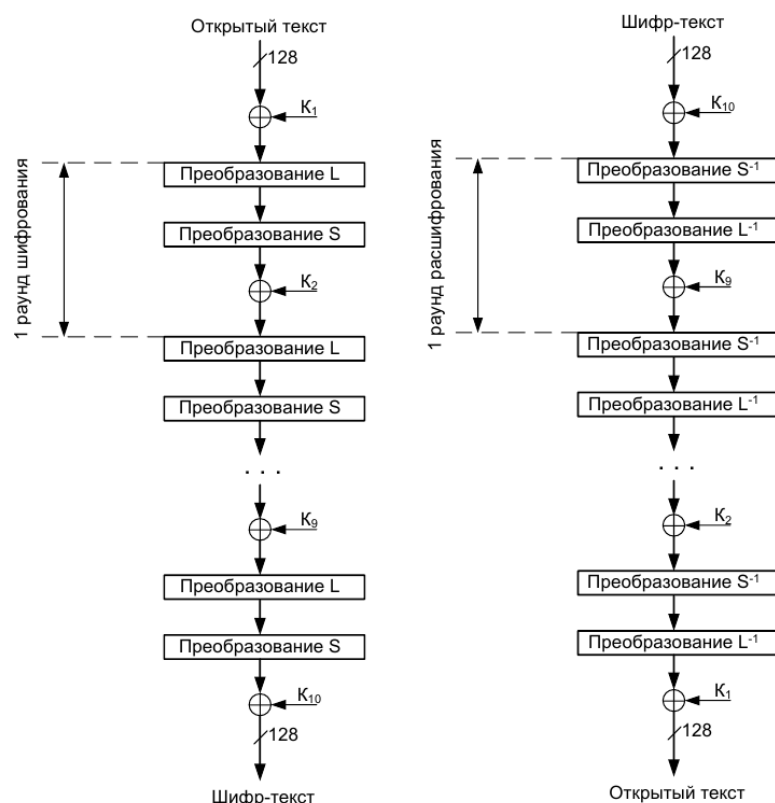


Рисунок 21 – Шифрование/расшифрование одного блока данных

Для реализации скоростного шифрования потребуется одна таблица предвычислений, отражающая совместную работу функций L и S. В реализации имеется таблица предвычислений для значения регистра сдвига с линейной обратной связью (таблица для умножения размерностью  $256 \times 256$  значений в поле Галуа), позволяющая быстро вычислять значения.

После построения таблицы схема шифрования выглядит следующим образом: входной блок данных складывается по модулю два с первым ключом, каждый байт полученного значения будет выступать индексом для таблицы №1. Таким образом, получится 16 значений, которые необходимо сложить по модулю два между собой и со следующим ключом; повторив операцию 9 раз, на выходе получится шифртекст [13]. В разделе «Тестирование программного обеспечения модулей криптокартридера. Анализ соответствия разработанного устройства требованиям технического задания» будет рассмотрен вопрос соответствия скорости шифрования требованиям технического задания.

### 5.2.6 Модель взаимодействия программного обеспечения модулей

В связи с тем, что структурно устройство состоит из модулей (объектов), а принцип работы заключается в том, что устройство постоянно может находиться в одном из возможных состояний, опишем модель работы программного обеспечения с помощью UML-диаграмм (unified modeling language – унифицированный язык моделирования), диаграммой конечного автомата.

На рисунке 22 приведена диаграмма состояний устройства, а также правила перехода между состояниями. В таблице 16 приведен перечень состояний криптокартридера, а также краткое описание каждого состояния

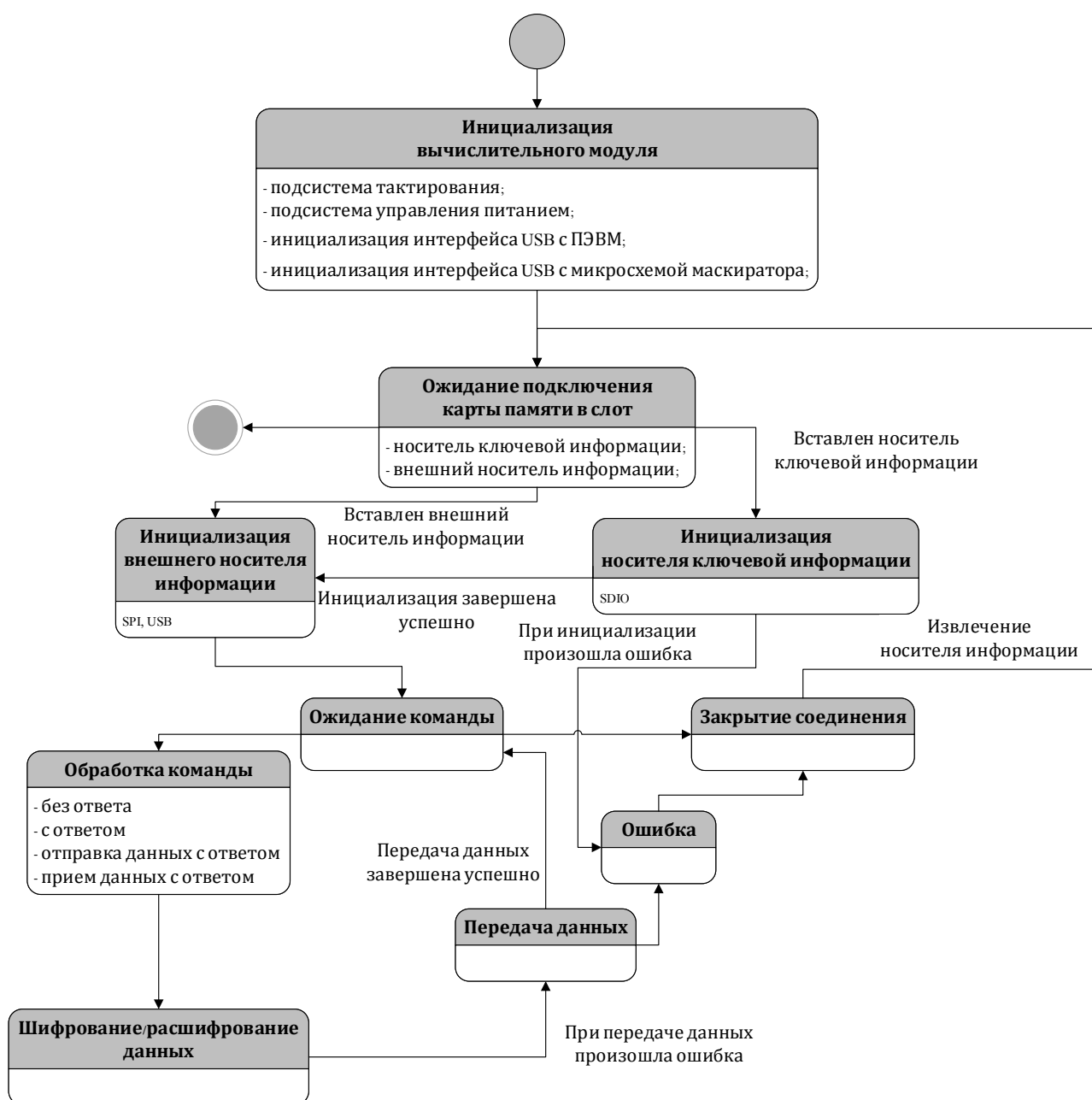


Рисунок 22 – Диаграмма состояний криптокартридера

Таблица 16 – Перечень состояний конечного автомата с описанием

| Состояние                                     | Описание                                                                                                                                    |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Инициализация<br>вычислительного модуля       | инициализация:<br>- подсистем тактирования, управления питанием;<br>- интерфейса USB с ПЭВМ;<br>- интерфейса USB с микросхемой маскиратора; |
| Ожидание подключения карты<br>памяти в слот   | Ожидание подключения:<br>- носителя ключевой информации;<br>- внешнего носителя информации;                                                 |
| Инициализация внешнего<br>носителя информации | По поддерживаемым интерфейсам: SPI, USB                                                                                                     |
| Инициализация носителя<br>ключевой информации | По поддерживаемому интерфейсу: SDIO<br>Возможные ошибки: нарушена целостность ключа                                                         |
| Ожидание команды                              | Ожидание команды от ПЭВМ                                                                                                                    |
| Закрытие соединения                           | Безопасное отключение программным способом модулей обмена данными, управляющих напряжений от носителя информации                            |
| Обработка команды                             | Тип команды: без ответа; с ответом; отправка данных с ответом; прием данных с ответом.                                                      |
| Передача данных                               | Обмен данными с носителем информации                                                                                                        |
| Шифрование/расшифрование<br>данных            | Выделение полезной нагрузки, шифрование                                                                                                     |
| Ошибка                                        | Статус завершения одной из операций                                                                                                         |

На рисунке 23 приведена диаграмма конечного автомата для процесса передачи данных с целью уточнения рисунка 22.

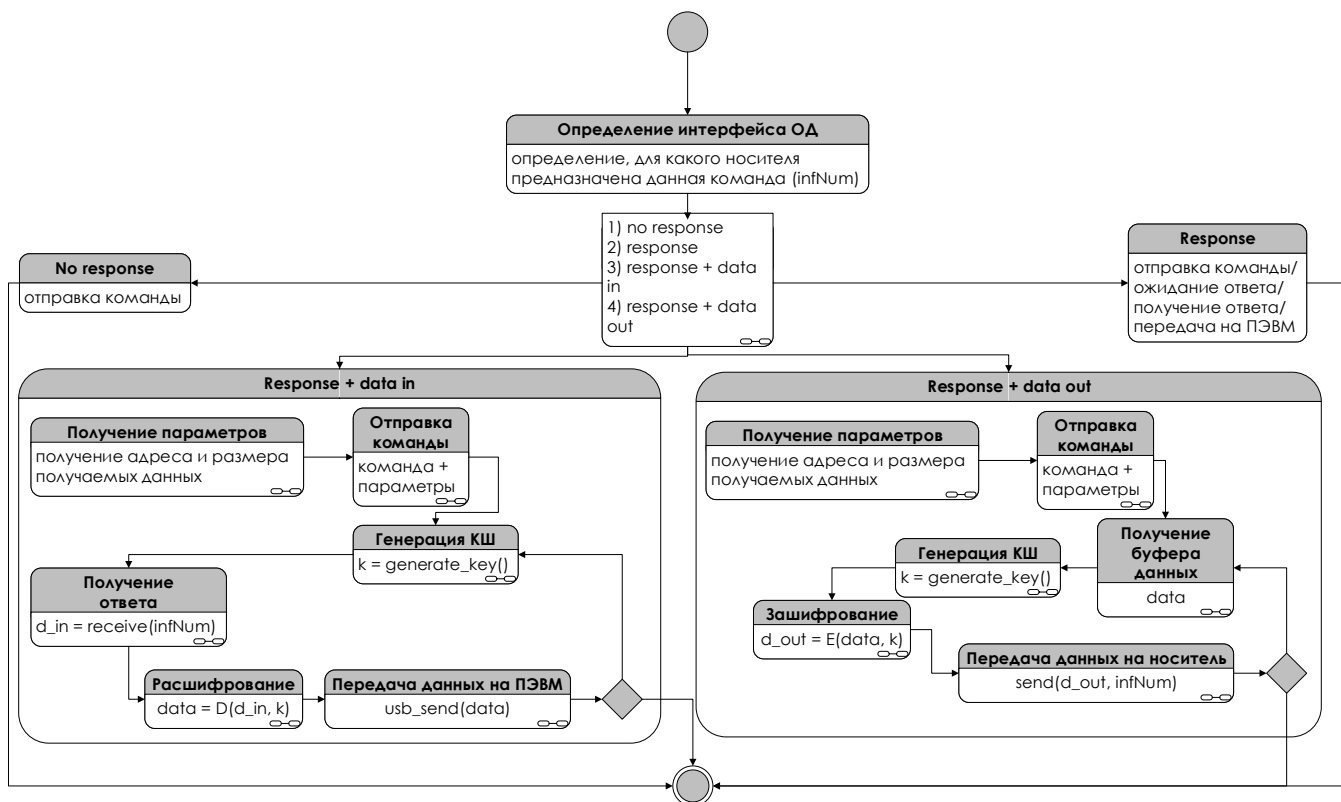


Рисунок 23 – Модель процесса передачи данных

На рисунке 23 показано различие между разными типами команд (типы команд приведены в таблице 16). Оно заключается в режиме работы шифратора (шифрование/расшифрование), а также логику работы обработчиков буферов данных (data, d\_in, d\_out).

## 6 Тестирование программного обеспечения модулей крипто-картридера.

### Анализ соответствия требованиям технического задания

#### 6.1 Тестирование разработанного программного обеспечения

##### 6.1.1 Общее тестирование программного обеспечения криптографического модуля

Общее тестирование проводится с целью проверки соответствия требованиям технического задания, а также спецификации программного обеспечения. В таблице 17 показаны ресурсы и исходные данные для проведения тестирования ПО.

Таблица 17 – Ресурсы и методы проведения исследования ПО

| Ресурс                                                                                  | Цель исследования                                                                                               | Метод исследования                                                                                                                             |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Встроенный симулятор процессоров ARM-Cortex M3/M4 в IAR Embedded Workbench for ARM 7.50 | Исследование корректности работы шифратора                                                                      | Симуляция операции шифрования на заранее известных открытом тексте, ключе, шифртексте                                                          |
|                                                                                         | Исследование производительности работы криптопроцессора при базовом алгоритме ГОСТ 34.12-2015 «Кузнечик»        | Симуляция операции шифрования на случайно-генерируемых открытом тексте и ключах шифрования (1 раз в 1Мб) с замером времени выполнения операции |
|                                                                                         | Исследование производительности работы криптопроцессора в режиме ускорения алгоритма ГОСТ 34.12-2015 «Кузнечик» |                                                                                                                                                |

Для замера времени выполнения операции использовался специальный регистр тактов процессора CYCLECOUNTER. Таким образом, зная значение регистра до и

после операции шифрования, а также тактовую частоту процессора (число тактов за 1 секунду), можно подсчитать время, затраченное на операцию шифрования.

#### 6.1.2 Тестирование корректности работы шифратора

Для проведения теста корректности работы шифратора были взяты эталонные (контрольные) значения из стандарта ГОСТ 34.12-2015. Результаты теста сведены в таблицу 18.

Таблица 18 – Тестирование корректности работы шифратора

| Параметр       | Значение                                                                |
|----------------|-------------------------------------------------------------------------|
| Шифрование     |                                                                         |
| Открытый текст | a = 1122334455667700ffeeddccbbaa9988                                    |
| Ключ           | K =<br>ffeeddccbbaa99887766554433221100f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff |
| Шифртекст      | b = 7f679d90bebc24305a468d42b9d4edcd.                                   |
| Расшифрование  |                                                                         |
| Шифртекст      | b = 7f679d90bebc24305a468d42b9d4edcd.                                   |
| Ключ           | K =<br>ffeeddccbbaa99887766554433221100f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff |
| Открытый текст | a = 1122334455667700ffeeddccbbaa9988                                    |

Результаты тестирования, приведенные в таблице 18 полностью соответствуют контрольным значениям, приведенным в приложении А к ГОСТ 34.12-2015.

#### 6.1.3 Исследование производительности работы криптопроцессора при базовом и ускоренном алгоритмах шифрования

Метод исследования времени выполнения операций был приведен в п.6.1.1. Различия между базовым и ускоренным алгоритмом шифрования приведены в п.5.2.5. Параметры исследования, а также данные, полученные в его результате приведены в таблице 19.

Таблица 19 – Параметры и результаты исследования

| Параметр                                                                                                               | Значение                  | Примечание                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Размеры блоков данных/ключа, бит                                                                                       | 128/256                   |                                                                                                                                                                                        |
| Объем шифруемых данных                                                                                                 | 1,5 Мбайт                 | Каждый блок данных генерировался из случайных чисел                                                                                                                                    |
| Время выполнения шифрования базовым алгоритмом в тактах процессора / секундах                                          | 940848659 / 5,6 с         |                                                                                                                                                                                        |
| Скорость шифрования базовым алгоритмом                                                                                 | 274 кбайт/с (~2,2 Мбит/с) |                                                                                                                                                                                        |
| Время выполнения шифрования ускоренным алгоритмом в тактах процессора / секундах                                       | 724446000 / 4,31 с        | Производительность ускоренного алгоритма выше на 32,4%                                                                                                                                 |
| Скорость шифрования ускоренным алгоритмом                                                                              | 363 кбайт/с (~3 Мбит/с)   |                                                                                                                                                                                        |
| Время выполнения шифрования ускоренным алгоритмом в тактах процессора / секундах с включенной оптимизацией по скорости | 53364327 / 3,17 с         | Производительность ускоренного алгоритма с включенной оптимизацией по скорости выше на 33,3% по сравнению с ускоренным алгоритмом без оптимизации и на 76,4% выше чем базовый алгоритм |
| Скорость шифрования ускоренным алгоритмом с включенной оптимизацией по скорости                                        | 484 кбайт/с (~3,8 Мбит/с) |                                                                                                                                                                                        |

Учитывая некоторую синтетичность исследования, обеспеченную за счет лабораторных условий, можно сделать следующие выводы:

– скорость шифрования в реальной работе останется прежней, однако будет снижаться общая пропускная способность устройства за счет

вспомогательных/смежных подсистем, а также в зависимости от реализации процессора производителем;

– учитывая небольшую производительность платформы (тактовая частота микроконтроллера STM32F407VGT6 - 168 МГц, производительность 210 DMIPS), а также скорость шифрования порядка 3,8 Мбит/с можно считать приемлемой;

– достоверно установлено, что производительность ускоренного алгоритма шифрования на 32,4% выше, чем базового, а с включением оптимизации по скорости кода на 76,4%.

6.2 Анализ соответствия разработанного устройства требованиям технического задания

В таблице 15 приводились требования спецификации программного обеспечения. В таблице 20 показаны результаты анализа соответствия требованиям спецификации.

Таблица 20 – Анализ соответствия требованиям спецификации программного обеспечения

| Категория требований       | Требования                                                                                                                      | Содержание требования                                                                         | Анализ соответствия                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Функциональные возможности | Устройство предназначено для применения в организациях в целях обеспечения конфиденциальности данных с грифом «конфиденциально» |                                                                                               | соответствует                                                             |
| Внешние интерфейсы         | Интерфейсы обмена данными                                                                                                       | USB 2.0 (host, device), SDIO, SPI<br>Поддержка карт памяти SD, SDHC, Micro SD, MMC, USB-flash | Программное обеспечение модуля не реализуется в рамках дипломного проекта |

Продолжение таблицы 20

| Категория требований        | Требования                               | Содержание требования                                                  | Анализ соответствия                                                       |
|-----------------------------|------------------------------------------|------------------------------------------------------------------------|---------------------------------------------------------------------------|
|                             | Интерфейс взаимодействия с пользователем | Индикация состояния: LED светодиод (2 цвета)                           | Программное обеспечение модуля не реализуется в рамках дипломного проекта |
| Производительность          | Шифрование/расшифрование данных          | не менее 0,4 Мбайт/с                                                   | Соответствует (484 кбайт/с)                                               |
| Атрибуты                    | портативность                            | Совместимость с системой команд ARM Cortex-M                           | соответствует                                                             |
|                             | Алгоритм шифрования данных               | ГОСТ 34.12-2015 «Кузнечик»                                             | соответствует                                                             |
|                             | Безопасность                             | Организация защиты от недовверенной среды путем реализации маскиратора | Программное обеспечение модуля не реализуется в рамках дипломного проекта |
| Требования к написанию кода | Язык программирования                    | C/C++                                                                  | Соответствует                                                             |
|                             | Компилятор                               | arm-none-eabi-gcc 4.6.2                                                | соответствует                                                             |

## 7 Анализ возможной интеграции устройства криптографической защиты данных с существующими системами защиты информации

Совместимость — один из наиболее ключевых принципов в разработке современных программно-аппаратных решений. В настоящее время существует два подхода к разработке технических решений: создание собственной экосистемы или гибкая и адаптивная архитектура для легкой совместимости с существующими решениями.

В пользу первого способа можно выделить только то, что разработчики в таком случае обладают полной свободой действий, могут реализовать любые технические решения. Недостатком такого способа является трудность поддержки и развития продукта, а также проблемы на пути завоевания «ниши» на рынке, так как не каждый потребитель разглядит видимые преимущества перехода на экосистему. Исключением может служить только компания Apple.

Во втором случае недостатки первого становятся сильными сторонами второго, и наоборот, преимущества первого обращаются в трудности и препятствия, ограничения, накладные расходы при разработке.

При проектировании устройства криптографической защиты данных при работе с внешними носителями информации был выбран второй подход. Для наиболее удобного использования разрабатываемое устройство должно быть совместимо с самыми популярными, передовыми интерфейсами обмена данных, а также легко вписываться в архитектуру современных автоматизированных систем.

С точки зрения аппаратного обеспечения, устройство удовлетворяет всем требованиям совместимости (поддержка интерфейса USB 2.0 для соединения с ПЭВМ). С точки зрения программного обеспечения, как утверждалось ранее, устройство не требует предустановки специальных драйверов или управляющего прикладного программного обеспечения. Поэтому для применения устройства не требуется никаких дополнительных технических решений. Из организационных мер нуждаются в разработке следующие документы:

- правила учета/выдачи/смены ключей шифрования;
- политика использования сторонних внешних носителей информации.

Данные документы носят исключительно индивидуальный характер для каждой организации и не могут быть унифицированы, так как зависят от инфраструктуры.

Таким образом, крипто-картридер можно охарактеризовать как достаточно гибкое в применении устройство, совместимое с любыми автоматизированными системами, системами защиты информации, имеющими поддержку интерфейса USB 2.0 и ниже, при этом не требующее дополнительного прикладного программного обеспечения.

## ЗАКЛЮЧЕНИЕ

В ходе выполнения дипломного проекта были идентифицированы основные проблемы обеспечения безопасности информации, отчуждаемой из автоматизированных систем на внешние носители. Таких проблем выделено три:

- обеспечение конфиденциальности, целостности данных при записи их на внешний носитель;
- избежание потерь производительности процедур записи/чтения данных при работе с внешними носителями;
- обеспечение конфиденциальности, целостности, доступности данных хранящихся на внешнем носителе.

В результате анализа проблем произведены идентификация доверенных и недоверенных зон, выбор метода защиты информации. Сформированы перечень основных компонентов устройства, разработаны и обоснованы технические требования к компонентам.

После этого проведен поиск современной элементной базы, удовлетворяющей представленным требованиям, описаны основные интерфейсы обмена данными, обладающие наибольшей распространенностью в электротехнике. На основе подобранной элементной базы в соответствие с единой системой конструкторской документации разработаны схема электрическая структурная и схема электрическая принципиальная, приведенные в приложениях А и Б.

Следующим этапом работы являлся процесс разработки алгоритмов работы и взаимодействия программных модулей:

- модуль обмена данными с периферией,
- модуль обмена данными по интерфейсу Ethernet,
- криптографический модуль,
- модуль маскиратора,
- модуль вычисления ключа шифрования.

Схема потоков данных устройства, включающая возможные взаимодействия программных модулей приведена на рисунке 17. Разработанные алгоритмы работы модулей приведены на рисунках 18,19,20,22,23.

После разработки программных алгоритмов осуществлена программная реализация криптографического модуля с последующим тестированием. Результаты тестирования показали, что устройство удовлетворяет техническим требованиям. Результаты тестирования приведены в таблице 19.

На заключительном этапе сформирована комплексная оценка разработанного прототипа устройства. Оценка возможности интеграции устройства с существующими системами защиты информации показала, что крипто-картридер можно интегрировать в автоматизированные системы любого масштаба.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 RAID [Электронный ресурс] : Википедия, свободная энциклопедия. – 2016. – Режим доступа: <https://ru.wikipedia.org/wiki/RAID>, свободный. – Загл. с экрана.

2 What is the average size of an office document [Электронный ресурс] : Microsoft TechNet, ред. Dan Gøran Lunde. – 2012. – Режим доступа: <https://blogs.technet.microsoft.com/dangl/2012/10/18/what-is-the-average-size-of-an-office-document/>, свободный. – Загл. с экрана.

3 Управление ключами [Электронный ресурс] : Википедия, свободная энциклопедия. – 2013. – Режим доступа: [https://ru.wikipedia.org/wiki/Управление ключами](https://ru.wikipedia.org/wiki/Управление_ключами), свободный. – Загл. с экрана.

4 Шифрование ГОСТ 28147-89 на x86- и GPU-процессорах [Электронный ресурс] : Хабрахабр, IT сообщество, Криптография, Высокая производительность, GPGPU, Блог компании Код Безопасности. – 2015. – Режим доступа: <https://habrahabr.ru/company/securitycode/blog/255863/>, свободный. – Загл. с экрана.

5 ГОСТ 28147-89: «Не спеши его хоронить». Часть 2. Эффективные реализации алгоритма [Электронный ресурс] : КРИПТО-ПРО, блог. – 2015. – Режим доступа: <https://www.cryptopro.ru/blog/2015/01/14/gost-28147-89-ne-speshi-ego-khoronit-chast-2-effektivnye-realizatsii-algoritma>, свободный. – Загл. с экрана.

6 В ГОСТе сидел «Кузнечик» [Электронный ресурс] : Хабрахабр, IT-сообщество, Криптография, Информационная безопасность, Алгоритмы. – 2015. – Режим доступа: <https://habrahabr.ru/post/266359/>, свободный. – Загл. с экрана.

7 ГОСТ Р 34.12–2015: чего ожидать от нового стандарта? [Электронный ресурс] : научный журнал «Information Security/Информационная безопасность». – Электрон. журн. – №4, 2015. – Режим доступа к журн.: <http://www.itsec.ru/articles2/crypto/gost-r-chego-ozhidat-ot-novogo-standarta/>, свободный. – Загл. с экрана.

8 Dhrystone [Электронный ресурс] : Википедия, свободная энциклопедия. – 2016. – Режим доступа: <https://ru.wikipedia.org/wiki/Dhrystone>, свободный. – Загл. с экрана.

9 Интерфейс SPI [Электронный ресурс] : Записки инженера, заметки по IT технологиям. – 2013. – Режим доступа: <http://s-engineer.ru/interfejs-spi/>, свободный. – Загл. с экрана.

10 Кратко о USB [Электронный ресурс] : Аксессуары Sony Ericsson. – 2013. – Режим доступа: <http://aks-es.narod.ru/Stat/KraUSB.html>, свободный. – Загл. с экрана.

11 Описание технологии Ethernet [Электронный ресурс] : Телком. – 2013. – Режим доступа: <http://tel-kom.ru/index.php/38-ethernet>, свободный. – Загл. с экрана.

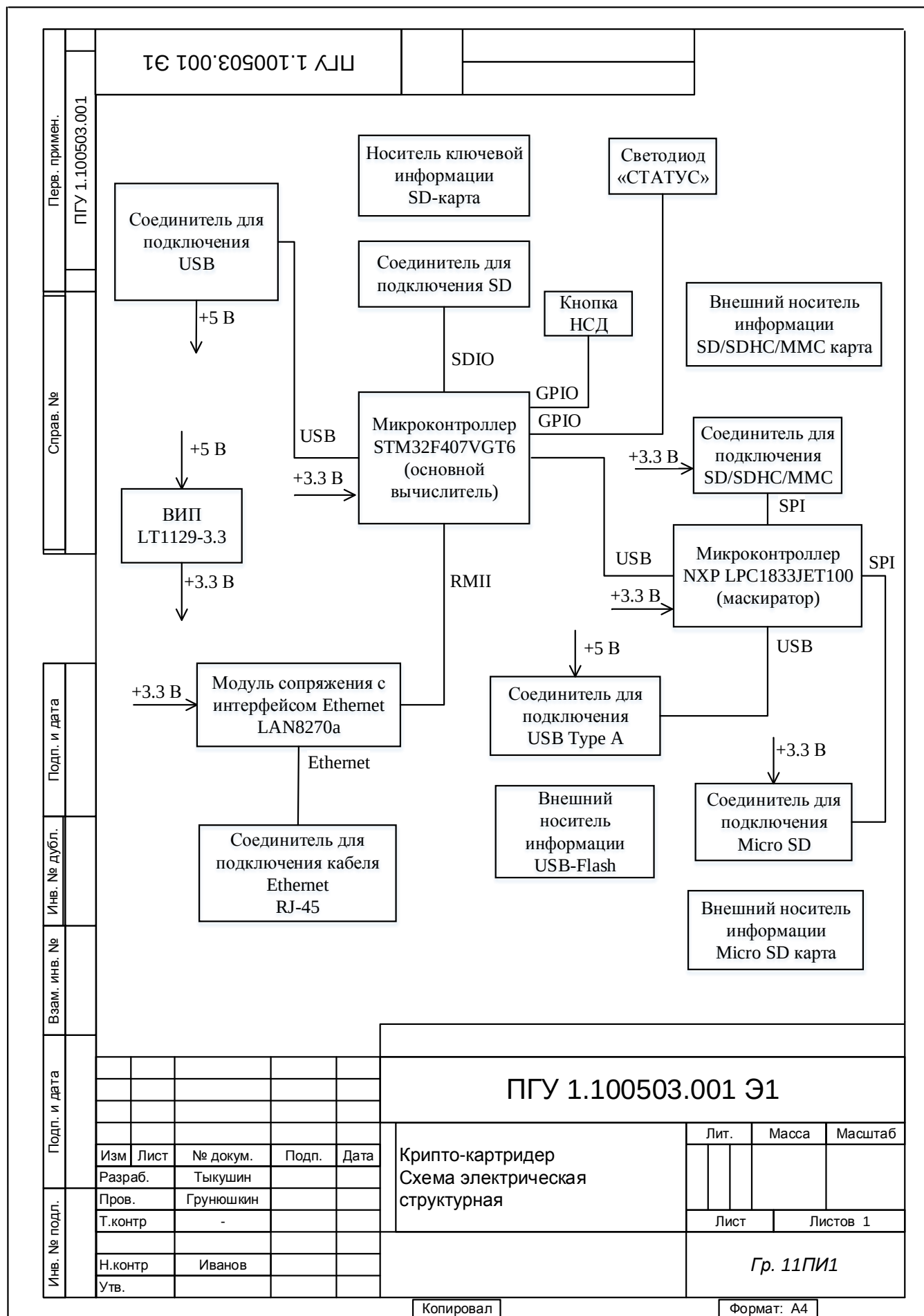
12 Стешенко, В.Б. P-CAD. Технология проектирования печатных плат. – БХВ-Петербург, 2003. – 720 с.

13 Разработка и реализация высокоскоростного шифрования данных с использованием алгоритма «Кузнечик» [Электронный ресурс] : Научная электронная библиотека «Киберленика». – Электрон. журн. – №4(8), 2015. – Режим доступа к журн.: <http://cyberleninka.ru/article/n/razrabotka-i-realizatsiya-vysokoskorostnogo-shifrovaniya-dannyh-s-ispolzovaniem-algoritma-kuznechik>, свободный. – Загл. с экрана.

## ПРИЛОЖЕНИЕ А

(обязательное)

Схема электрическая структурная (Э1) устройства криптографической защиты  
данных при работе с внешними носителями



## ПРИЛОЖЕНИЕ Б

(обязательное)

Схема электрическая принципиальная (ЭЗ) устройства криптографической защиты  
данных при работе с внешними носителями

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УДК 004.056.5

Политехнический институт  
Факультет приборостроения,  
информационных технологий и  
электроники

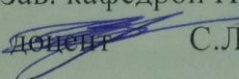
Выпускающая кафедра:

Информационная безопасность систем  
и технологий

Учебная группа 11ПИ1

УТВЕРЖДАЮ

Зав. кафедрой ИБСТ

к.т.н., доцент  С.Л. Зефирова

27 04 2016 г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ  
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ  
РАБОТУ**

студента группы 11ПИ1 Тыкушина Анатолия Владимировича

**Специальность 100503 –** Информационная безопасность  
автоматизированных систем

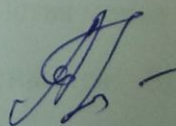
**Тема дипломного проекта:** «Устройство криптографической защиты  
данных при работе с внешними носителями («Крипто-картридер»))»

**Руководитель ВКР**  
начальник НИС-22

НИП «Аргус» филиал АО ПНИЭИ

**Нормоконтролер**

к.т.н., доцент



Грунющкин А.В.



Иванов А.П.

## **1 Цели и задачи ВКР**

Цели работы – определение концептуальной модели разрабатываемого устройства криптографической защиты данных при работе с внешними носителями, выбор аппаратных средств и разработка программного обеспечения отдельных модулей, удовлетворяющих требованиям по защите информации 4 уровня.

Устройство предназначено для применения в организациях в целях обеспечения конфиденциальности данных с грифом конфиденциально.

## **2 Тактико-технические требования к выполнению ВКР**

- аппаратное обеспечение должно соответствовать следующим требованиям:
- тип процессора ARM® 32-bit Cortex®-M4 CPU с FPU;
- тактовая частота работы процессора до 168 МГц;
- объем встроенной памяти от 128 кбайт статической ОЗУ;
- объем встроенной энергонезависимой памяти от 256 кбайт;
- напряжение питания плюс 5 В плюс/минус 10%;
- энергопотребление устройства менее 500 мА;
- поддерживаемые карты памяти: SD, Micro SD, SDHC, MMC, USB-Flash;
- ввод пользовательского ключа шифрования: отдельный разъем форм-фактора SD;
- ввод пользовательского ключа шифрования: 10/100 Мбит/с Ethernet с поддержкой IEEE-802.3-2002;
- поддерживаемый интерфейс обмена данными с управляющим устройством: USB 2.0;
- индикация состояния устройства (светодиодная/LCD индикация).
- программное обеспечение должно соответствовать следующим требованиям:

- программное обеспечение должно обеспечивать шифрование данных, записываемых на внешний носитель, и расшифрование данных, считываемых с внешнего носителя с обеспечением пропускной способности не менее 0,5 Мбит/с;

- свойство конфиденциальности хранимых данных должно обеспечиваться шифрованием информации согласно алгоритму блочного шифрования ГОСТ 34.15 – 2015;

- ввод главного ключ шифра с грифом конфиденциально, хранящегося на специальном съемном носителе, осуществлять по индивидуальному интерфейсу обмена данными;

- программное обеспечение должно поддерживать интерфейсы USB 2.0, SPI, SDIO для обмена данными с внешними носителями и управляющим устройством;

- используемый для разработки программного обеспечения компилятор arm-none-eabi-gcc 4.6.2;

- язык программирования – C++.

В ВКР должны быть рассмотрены следующие вопросы:

- анализ и обзор актуальных проблем, связанных с защитой данных, хранящихся на накопителях;

- анализ существующих аппаратных средств и выбор элементной базы, наиболее точно удовлетворяющих техническим требованиям;

- выбор и обоснование способов обеспечения защиты данных, хранящихся на внешних носителях;

- технические характеристики процессора с ядром ARM® 32-bit Cortex®-M4 CPU с FPU, применяемых в устройстве;

- описание интерфейсов обмена данными (USB 2.0, SPI, SDIO, Ethernet);

- описание структурной схемы устройства;

- разработка схема электрической принципиальной;

- разработка алгоритмов работы программных модулей;
- разработка программного обеспечения криптографического модуля;
- результаты экспериментальных исследований;
- анализ исследований и обобщение результатов проектирования;
- анализ возможной интеграции данного устройства с существующими системами защиты информации.

### **3 Требования к разрабатываемой документации**

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

- инфографика сравнения производительности устройств-аналогов, разработанного устройства, требования к разрабатываемому устройству защиты конфиденциальной информации - 1л., ф. А1 (плакат);
- схема электрическая структурная устройства защиты конфиденциальной информации - 1л., ф. А1;
- схема электрическая принципиальная крипто-картридера - 1л., ф. А1;
- криптографический модуль крипто-картридера – 1л., ф. А1 (плакат);
- схема информационных потоков крипто-картридера 1л., ф. А1 (плакат);
- алгоритм работы модуля фильтрации служебных данных 1л., ф. А1(плакат).

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.

### **4 Сроки выполнения ВКР**

Тема утверждена приказом ректора ПГУ № \_\_\_\_ от \_\_\_\_ 2016 г.

Дата выдачи задания «30» марта 2016 г.

Время дипломного проектирования с 18.04.2016 г. по 10.07.2016 г.

Задание к исполнению принял «30» марта 2016 г.

Исполнитель ВКР \_\_\_\_\_ Тыкушин А.В.

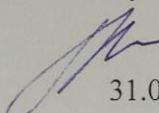
Ректору Пензенского  
государственного университета  
А. Д. Гулякову  
студента 5 курса ФПИТЭ  
очной формы обучения  
Тыкушина Анатолия Владимировича

заявление.

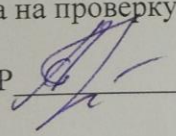
Я, Тыкушин Анатолий Владимирович, студент 5 курса очной формы обучения специальности 10.05.03 – «Информационная безопасность автоматизированных систем», прошу провести проверку с использованием системы «Антиплагиат» дипломного проекта на тему «Устройство криптографической защиты данных при работе с внешними носителями («Крипто-картридер»)), выполненной мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлен с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета.

 /А.В. Тыкушин/  
31.05.2016

ВКР представлена на проверку 31.05.2016.

Руководитель ВКР  /А.В. Грунющкин/

## Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Устройство криптографической защиты данных при работе с внешними носителями («Крипто-картридер»)) студента 5 курса А.В. Тыкушина специальности 10.05.03 – «Информационная безопасность автоматизированных систем».

Руководитель ВКР начальник сектора НИС-22 НИП «Аргус» филиал АО «ПНИЭИ» Груньюшкин Андрей Владиславович.

### Отчет о проверке № 1

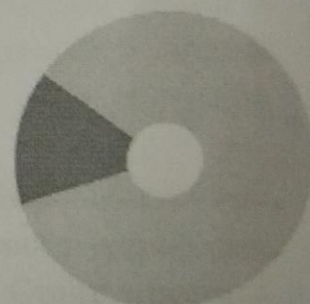
ФИО: Иванов Алексей Петрович  
дата загрузки: 03.06.2016 06:37:05  
пользователь: [ap\\_ivanov@mail.ru](mailto:ap_ivanov@mail.ru) / ID: 1267386  
отчет предоставлен сервисом «Антиплагиат»  
на сайте <http://www.antiplagiat.ru>

### Информация о документе

№ документа: 40  
Имя исходного файла: ВКР\_Тыкушин\_АВ\_11ПИ1.pdf  
Размер текста: 2481 кб  
Тип документа: Не указано  
Символов в тексте: 109301  
Слов в тексте: 12562  
Число предложений: 516

### Информация об отчете

Дата: Отчет от 03.06.2016 06:37:05 - Последний готовый отчет  
Комментарии: не указано  
Оценка оригинальности: 85.35%  
Заимствования: 14.65%  
Цитирование: 0%



Оригинальность: 85.35%  
Заимствования: 14.65%  
Цитирование: 0%

08.06.2016 г.

Секретарь ГЭК

А.В. Груньюшкин

А.П.Иванов

## ОТЗЫВ

на дипломный проект студента

Пензенского государственного университета

Тыкушина Анатолия Владимировича

Тема дипломного проекта "Устройство криптографической защиты данных при работе с внешними носителями («Крипто-картридер»)"

Целью дипломного проекта являлось определение концептуальной модели разрабатываемого устройства криптографической защиты данных при работе с внешними носителями, включающее выбор аппаратных средств и разработка программного обеспечения отдельных модулей, удовлетворяющих требованиям по защите информации 4 уровня («конфиденциально»).

В проекте приведены подробный обзор и анализ актуальных проблем, связанных с защитой данных, хранящихся на внешних накопителях, выбор и обоснование способов обеспечения защиты. В проекте содержится анализ существующих аппаратных средств, обзор способов построения концептуальной модели разрабатываемого устройства.

В ходе выполнения дипломного проектирования студентом было предложено множество оригинальных решений по реализации вновь создаваемого устройства, улучшающие его характеристики по сравнению с аналогами. Стоит отметить детальность проработки концептуальной модели устройства.

А.В. Тыкушин в короткие сроки освоил современные системы проектирования IAR Embedded Workbench, Mentor Graphics Xpedition, позволяющие разрабатывать программное и аппаратное обеспечение устройств.

Работы по всем пунктам технического задания выполнены полностью. Пояснительная записка и плакаты содержат необходимые сведения о проделанной работе. Степень грамотности изложения материала соответствует современным требованиям и стандартам.

Тема проработана на высоком уровне, ходе выполнения работы был создан достаточный задел для продолжения работ по данной тематике. Считаю, что дипломный проект выполнен в полном соответствии с заданием и заслуживает оценки «отлично», а дипломник А.В. Тыкушин достоин присвоения квалификации специалиста по информационной безопасности по специальности 10.05.03 – «Информационная безопасность автоматизированных систем»

Руководитель дипломного проекта

Начальник НИС-22 НИП «Аргус» филиал АО «НИИЭИ»

А.В. Грунюшкин

*количество баллов 16*



## РЕЦЕНЗИЯ

на выпускную квалификационную работу  
студента Пензенского государственного университета

Тыкушина Анатолия Владимировича

Тема дипломного проекта: «Устройство криптографической защиты информации  
при работе с внешними носителями («Крипто-картридер»))»

На рецензию были представлены: пояснительная записка на 89 листах и графическая часть на 6 листах.

В данной работе рассмотрена возможность создания концептуальной модели устройства, позволяющего обеспечить защиту конфиденциальности и целостности информации при ее отчуждении на внешние носители.

Обзор современных подходов к решению поставленной задачи выполнен довольно обстоятельно. Проведена попытка классификации рассмотренных решений, что показывает грамотный системный подход к выполнению задачи. На основании обзора сделаны правильные выводы о предпочтительных аппаратных платформах и методах построения ПО.

В пояснительной записке отражены проблемы по защите информации, возникшие из-за использования иностранной элементной базы, приведены возможные методы их решения.

К недостаткам, пожалуй, можно отнести, что реализованы не все-методы защиты (дублирование шифратора, защита от переадресации), однако их применение не требуется для защиты конфиденциальной информации.

При выполнении практической части были применены интересные технические решения. Например, было реализовано ускорение алгоритма шифрования ГОСТ 34.12-2015 на основе таблиц предвычислений.

За основу была взята платформа на базе архитектуры ARM, что существенно может снизить затраты разработки. Кроме того, может идти речь о переносимости программного обеспечения в связи с большой распространенностью данной архитектуры.

Данная работа может быть положена в основу создания серьезного программно-аппаратного продукта, предназначенного для криптографической защиты информации, отчуждаемой на внешние носители.

Все представленные на рецензию документы выполнены в соответствии с соблюдением требований ГОСТ 7.32-2001.

Дипломный проект соответствует всем предъявленным требованиям и заслуживает оценку «отлично».

Рецензент:

ведущий инженер АО «ПНИЭИ»



С.В. Печилейский