**Федеральное государственное автономное образовательное учреждение высшего образования    
«Московский физико-технический институт (национальный исследовательский университет)»    
Физтех-школа радиотехники и компьютерных технологий    
Кафедра защиты информации**

|  |
| --- |
| УТВЕРЖДАЮ  Зав. кафедрой защиты информации д.т.н.  Конявский В. А.  «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_ г.  М.П. |

**ПРОГРАММА ДЛЯ РАБОТЫ С КРИПТОВАЛЮТНЫМИ КЛЮЧАМИ**

**Техническое задание**

**ЛИСТ УТВЕРЖДЕНИЯ**

**Листов 21**

|  |  |  |
| --- | --- | --- |
| СОГЛАСОВАНО  Научный консультант |  | Исполнитель, студ. гр. С01-419 |
| Елькин В.М. |  | Шарапов Р. А. |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_ г. |  | «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_ г. |
|  |  |  |
| Начальник Отдела инновационных разработок |  |  |
| Батраков А.Ю. |  |  |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_ г. |  |  |
|  |  |  |
| Заместитель генерального директора ЗАО "ОКБ САПР" |  |  |
| Счастный Ю.Д. |  |  |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_ г. |  |  |
|  |  |  |
| Руководитель группы разработки firmware СЗИ ЗАО "ОКБ САПР" |  |  |
| Алтухов А. А. |  |  |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_ г. |  |  |

УТВЕРЖДЕН

**ПРОГРАММА ДЛЯ РАБОТЫ С КРИПТОВАЛЮТНЫМИ КЛЮЧАМИ**

**Техническое задание**

**Листов 21**

2020

# СОДЕРЖАНИЕ

[СОДЕРЖАНИЕ](#_Toc13996)

[1 ВВЕДЕНИЕ](#_Toc19978)

[1.1 Наименование программы](#_Toc32465)

[1.2 Область применения программы](#_Toc12744)

[2 ОСНОВАНИЕ ДЛЯ РАЗРАБОТКИ](#_Toc2865)

[3 НАЗНАЧЕНИЕ РАЗРАБОТКИ](#_Toc8569)

[3.1 Функциональное назначение программы](#_Toc19150)

[3.2 Эксплуатационное назначение программы](#_Toc20281)

[4 ТРЕБОВАНИЯ К ПРОГРАММЕ](#_Toc12776)

[4.1 Требования к функциональным характеристикам](#_Toc9850)

[4.1.1 Требования к составу выполняемых функций](#_Toc28054)

[4.1.2 Требования к организации входных данных](#_Toc31159)

[4.1.3 Требования к организации выходных данных](#_Toc290)

[4.1.4 Требования к временным характеристикам](#_Toc14060)

[4.2 Требования к надежности](#_Toc803)

[4.2.1 Требования к обеспечению надежного (устойчивого) функционирования программы](#_Toc8362)

[4.2.2 Время восстановления после отказа](#_Toc8380)

[4.2.3 Отказы из-за некорректных действий оператора](#_Toc14598)

[4.3 Условия эксплуатации](#_Toc32603)

[4.3.1 Климатические условия эксплуатации](#_Toc13485)

[4.3.2 Требования к видам обслуживания](#_Toc6643)

[4.3.3 Требования к численности и квалификации персонала](#_Toc16353)

[4.4 Требования к составу и параметрам технических средств](#_Toc23688)

[4.5 Требования к информационной и программной совместимости](#_Toc27700)

[4.5.1 Требования к исходным кодам и языкам программирования](#_Toc6522)

[4.5.2 Требования к программным средствам, используемым программой](#_Toc5430)

[4.5.3 Требования к защите информации и программ](#_Toc3591)

[4.6 Специальные требования](#_Toc15218)

[5 ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ](#_Toc6090)

[6 ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ](#_Toc4202)

[7 СТАДИИ И ЭТАПЫ РАЗРАБОТКИ](#_Toc2884)

[8 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ](#_Toc890)

[ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ](#_Toc23482)

[ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ](#_Toc24263)

# ВВЕДЕНИЕ

## Наименование программы

«Программа для работы с криптовалютными ключами»

## Область применения программы

Программа предназначена для генерации криптовалютных ключей и подписи хэш-сумм криптовалютных транзакций.

Программа предназначена для последующего интегрирования в микропрограммное обеспечение (firmware), обеспечивающее доверенную загрузку ОС. Данное микропрограммное обеспечение предназначено для микроконтроллера at91sam3u4e, встроенного в микрокомпьютер m-TrusT.

# ОСНОВАНИЕ ДЛЯ РАЗРАБОТКИ

**Основанием** для разработки является задание на дипломный проект, подписанное консультантами и руководителем дипломного проекта и утвержденное заведующим кафедрой защиты информации МФТИ.

**Заказчиком** работ является кафедра защиты информации, которая относится к физтех-школе радиотехники и компьютерных технологий московского физико-технического института.

**Исполнителем** работ является студент кафедры защиты информации группы С01-419 ФРКТ МФТИ Шарапов Роман Андреевич.

# НАЗНАЧЕНИЕ РАЗРАБОТКИ

## Функциональное назначение программы

Функциональным назначением программы является генерация криптовалютных ключей по протоколам BIP 32, BIP 43, BIP 44; подпись криптовалютных транзакций; представление информации о используемых ключевых парах.

## Эксплуатационное назначение программы

Программа должна эксплуатироваться на микроконтроллере at91sam3u, интегрированном в микрокомпьютер m-TrusT. Конечными пользователями программы могут являться лица, которым необходимо совершать криптовалютные операции. Эти пользователи должны быть предварительно зарегистрированы в базе данных, хранящейся в постоянной памяти микроконтроллера.

# ТРЕБОВАНИЯ К ПРОГРАММЕ

## Требования к функциональным характеристикам

### Требования к составу выполняемых функций

Программа должна обеспечивать возможность выполнения перечисленных ниже функций:

1. Генерация неизвлекаемого мастер ключа с помощью ФДСЧ и его дальнейшая обработка с помощью хэш-функции HMAC-SHA512 по протоколу BIP 32.
2. Генерация дочерних иерархически детерминированных ключевых пар согласно протоколам BIP32, BIP 43 и BIP44.
3. Хэширование по алгоритмам SHA-256 и Ethash.
4. Подпись хэш сумм криптовалютных транзакций по алгоритму ECDSA.
5. Получение списка дочерних ключей проверки подписи.
6. Удаление неизвлекаемого мастер ключа из постоянной энергонезависимой памяти.
7. Удаление неизвлекаемого дочернего ключа из постоянной энергонезависимой памяти.
8. Идентификация / аутентификация пользователей с последующей передачей результатов процедуры идентификации/аутентификации в ОС.
9. Просмотр / редактирование списка разрешенных пользователей.
10. Генерация записей журнала событий аудита.
11. Просмотр журнала событий аудита.
12. Удаление журнала событий аудита.
13. Запрет выполнения операций, в случае переполнения журнала событий аудита.

### Требования к организации входных данных

Входными данными разрабатываемой программы должны являться:

1. идентификатор пользователя в системе Linux и его пароль, для обеспечения разграничение доступа пользователей к их ключевым парам, а также к записям журнала событий аудита;
2. хэш-суммы, сформированные по алгоритмам SHA-256 и Ethash, необходимые для вызова функций вычисления электронной подписи криптовалютных транзакций;
3. данные для вызова функций генерации ключей подписи;
4. данные для вызова функций удаления ключей подписи из энергонезависимой памяти;
5. данные для вызова функции чтения списка ключей проверки подписи.

Состав входных данных должен уточняться в соответствии с результатами технического проектирования.

### Требования к организации выходных данных

Выходными данными разрабатываемой программы должны являться:

1. мастер ключ в виде массива случайных байт с ФДСЧ;
2. дочерние ключи проверки подписи;
3. электронная подпись криптовалютной транзакции;
4. данные об успешной/неуспешной попытке аутентификации;
5. список разрешенных пользователей программы;
6. данные об успешном/неуспешном завершении операций;
7. сведения, содержащиеся в журнале событий аудита.

Состав выходных данных должен уточняться в соответствии с результатами технического проектирования.

### Требования к временным характеристикам

Программа должна обеспечивать:

1. Процедуры идентификации/аутентификации должны осуществляться не более чем за 5 секунд.
2. Генерация неизвлекаемого мастер ключа с помощью ФДСЧ и его дальнейшая обработка по протоколу BIP 32 должна осуществляться не более чем за 10 секунд.
3. Генерация дочерних иерархически детерминированных ключевых пар согласно протоколам BIP32, BIP 43 и BIP44 должна осуществляться не более чем за 5 секунд.
4. Хэширование по алгоритму SHA-256 должно осуществляться не более чем за 5 секунд.
5. Хэширование по алгоритму Ethash должно осуществляться не более чем за 5 секунд.
6. Подпись криптовалютных транзакций по алгоритму ECDSA должна осуществляться не более чем за 5 секунд.
7. Получение списка дочерних ключей проверки подписи должно осуществляться не более чем за 5 секунды.

## Требования к надежности

### Требования к обеспечению надежного (устойчивого) функционирования программы

Надежное (устойчивое) функционирование программы должно быть обеспечено выполнением совокупности организационно-технических мероприятий, перечень которых приведен ниже:

1. организацией бесперебойного питания технических средств;
2. выполнением рекомендаций  Министерства труда и социального развития РФ, изложенных в Постановлении от 23 июля 1998 г. «Об утверждении межотраслевых типовых норм времени на работы по сервисному обслуживанию ПЭВМ и оргтехники и сопровождению программных средств»;
3. выполнением требований ГОСТ 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов;
4. необходимым уровнем квалификации сотрудников профильных подразделений.

### Время восстановления после отказа

Время восстановления после отказа, вызванного сбоем электропитания технических средств (иными внешними факторами), не фатальным сбоем (не крахом) операционной системы, не должно превышать времени, необходимого на перезагрузку операционной системы и запуск программы, при условии соблюдения условий эксплуатации технических и программных средств.

Время восстановления после отказа, вызванного неисправностью технических средств, фатальным сбоем (крахом) операционной системы, не должно превышать времени, требуемого на устранение неисправностей технических средств и переустановки программных средств.

### Отказы из-за некорректных действий оператора

Отказы программы возможны вследствие некорректных действий оператора (пользователя) при взаимодействии с операционной системой. Во избежание возникновения отказов программы по указанной выше причине следует обеспечить работу конечного пользователя без предоставления ему административных привилегий.

## Условия эксплуатации

### Климатические условия эксплуатации

Климатические условия эксплуатации, при которых должны обеспечиваться заданные характеристики разрабатываемой программы, должны удовлетворять требованиям, предъявляемым к техническим средствам, описанным в п. 4.4, в части условий их эксплуатации.

### Требования к видам обслуживания

Для обеспечения устойчивого функционирования программы технические средства, используемые программой, должны обслуживаться администратором. Требования к квалификации администратора описаны в п.4.3.3

### Требования к численности и квалификации персонала

Разрабатываемая программа должна обслуживаться пользователем (1 чел.) и администратором (1 чел.). Требования к квалификации пользователя не предъявляются.

Администратор должен иметь техническое образование. В перечень задач, выполняемых администратором, должны входить:

1. задача поддержания работоспособности технических средств, обозначенных в п.4.4;
2. задачи установки (инсталляции) и поддержания работоспособности системных программных средств - операционной системы;
3. задача установки (инсталляции) программы.

## Требования к составу и параметрам технических средств

Разрабатываемая программа должна функционировать на микроконтроллере at91sam3u4e, встроенным в микрокомпьютер m-TrusT. Характеристики микроконтроллера:

1. Микропроцессор ARM Cortex-M3 с тактовой частотой 96 МГц;
2. 2 x 128 Кбайт двухплоскостной встроенной Flash памяти;
3. 52 Кбайт встроенной SRAM;
4. 16 Кбайт ПЗУ со встроенными программами загрузчика (UART, USB) и программами IAP;
5. Контроллер статической памяти (SMC): поддержка SRAM, NOR, NAND. Флэш-контроллер NAND с буфером оперативной памяти 4 Кбайт и ECC;
6. Поддержка USB 2.0 с пропускной способностью 480 Мбит/с;
7. Поддержка SPI;

Характеристики микрокомпьютера m-TrusT:

1. Габаритные размеры: 90 мм на 105 мм;
2. Процессор: Quad-core ARM Cortex-A17 с тактовой частотой 1.8 ГГц;
3. ОЗУ: 2 ГБ DDR3;
4. ПЗУ: 16 ГБ NAND-flash;
5. Наличие разъемов microUSB и microHDMI;
6. Соединитель типа Розетка 87758-2016 MOLEX;
7. Разъем USB Type A;
8. Разъем Ethernet;
9. Физический датчик случайных чисел: двухплечевая схема Дебют с использованием диодов 2Г103А9;
10. Ethernet скоммутирован через LAN-трансформатор PSF-16221;
11. Разъем питания от источника постоянного напряжения 5 вольт;

## Требования к информационной и программной совместимости

### Требования к исходным кодам и языкам программирования

Для разработки программы должны использоваться языки программирования С, С++.

Для разработки программы должны использоваться следующие среды разработки:

1. Atmel Studio 7;
2. Keil µVision V4.03;

### Требования к программным средствам, используемым программой

Разрабатываемая программа должна быть интегрирована в уже существующее ПО микроконтроллера at91sam3u4e, осуществляющее доверенную загрузку.

Разрабатываемая программа должна принимать команды от приложений, функционирующих под управлением ОС Linux Ubuntu 16.04.

В ОС должен быть установлен демон, выполняющий функции идентификации/аутентификации пользователей, а также осуществляющий перехват вызовов криптографических функций и перенаправляющий их на РКБ

Перечень ПО, установленного в ОС должен уточняться в соответствии с результатами технического проектирования.

### Требования к защите информации и программ

Размещение и запуск программы должны происходить в flash-памяти микроконтроллера. Для защиты содержимого flash-памяти от несанкционированного копирования и дизассемблирования в ней необходимо установить бит секретности.

Криптографические ключи должны записываться в технологически защищенную внутреннюю память микропроцессора.

Доступ к программе имеют только пользователи, предварительно зарегистрированные в базе данных, хранящейся в постоянной памяти микроконтроллера. Перечень разрешенных пользователей может редактировать только администратор.

## Специальные требования

Требования к маркировке и упаковке не предъявляются.

Требования к транспортировке и хранению не предъявляются.

# ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ

**Требования к программной документации**

Состав документации:

1. техническое задание (ТЗ);
2. спецификация;
3. текст программы;
4. описание программы;
5. программа и методика испытаний (ПМИ);
6. пояснительная записка;
7. ведомость эксплуатационных документов;
8. формуляр;
9. описание применения;
10. руководство программиста;
11. руководство оператора.

Виды, комплектность и обозначения документов должны соответствовать требованиям ГОСТ 19.101-77 ЕСПД. Оформление текстовых документов должно осуществляться в соответствии с требованиями ГОСТ 2.105-95 (с Изменением №1 от июня 2006 г.), ГОСТ 2.106-96 (с Изменением №1 от июня 2006 г.).

# ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ

Ориентировочная экономическая эффективность не рассчитывается.

Предполагаемое число использования пр ограммы в год – 365 сеансов работы на одном рабочем месте.

# СТАДИИ И ЭТАПЫ РАЗРАБОТКИ

Состав и содержание работ приведены в Таблице.

Таблица.

| Стадии разработки | Этапы работ | Содержание работ |
| --- | --- | --- |
| 1. Техническое задание | Предпроектное обследование | Постановка задачи на разработку.  Обследование рынка криптовалютных активов.   Выбор и обоснование выбора критериев, на основе которых будет составлен перечень условий для безопасной работы с криптовалютными ключами.  Определение требований к техническим средствам программы.  Определение требований к функциональности программы.  Постановка целей и задач, подлежащих решению в процессе разработки. |
| Разработка и утверждение технического задания | Определение всех требований к программе.  Разработка технико-экономического обоснования разработки программы.  Определение стадий, этапов и сроков разработки программы и документации на нее.  Выбор языков программирования.  Согласование и утверждение технического задания. |
| 2.Эскизно -технический проект | Разработка эскизно -технического проекта | Разработка функциональности программы, определение структуры и формы представления входных и выходных данных функций.  Анализ алгоритмов и протоколов для работы с криптовалютами. Рассчеты требуемой вычислительной мощности.  Рассчеты количества требуемой памяти для хранения программы и данных.  Составление перечня ограничений, связанных с ограниченным количеством памяти и вычислительными мощностями выбранных технических средств.  Выбор способа размещения данных на аппаратном уровне.  Разработка общего описания алгоритма решения задачи.  Разработка структуры программы.  Разработка системы API, для пользовательских приложений. |
| Утверждение эскизно -технического проекта | Разработка пояснительной записки.  Согласование и утверждение эскизно -технического проекта |
| 4. Рабочий проект | Разработка программы | Программирование и отладка программы.  Изготовление программы-оригинала |
| Разработка программной документации | Разработка программных документов в соответствии с требованиями [ГОСТ 19.101](http://technicaldocs.ru/%D0%B3%D0%BE%D1%81%D1%8219/%D0%BD%D0%BF%D0%B0/%D0%B3%D0%BE%D1%81%D1%8219.101-77" \o "гост19:нпа:гост19.101-77)-77 |
| Испытания программы | Разработка, согласование и утверждение порядка и методики испытаний.  Корректировка программы и программной документации по результатам испытаний |
| 5. Прием проекта заказчиком | Подготовка и передача программы | Подготовка и передача программы и программной документации заказчику.  Оформление и утверждение акта о передаче программы. |

# ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

Настоящее ТЗ может быть уточнено или изменено в процессе работы. Уточнения и изменения ТЗ производятся по согласованию сторон. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего ТЗ.

Согласование и утверждение изменений производится в том же порядке и теми же должностными лицами, что и согласование и утверждение ТЗ.

Контроль и приемка работ осуществляются на основании ТЗ и соответствующих программ и методик испытаний. Приемочные испытания проводятся на площадях и технических средствах Заказчика и Исполнителя. Испытательный стенд создается Исполнителем.

На испытания Исполнитель предоставляет:

1. Согласованное ТЗ;
2. Согласованную ПМИ;
3. Комплект документации согласно ТЗ.

# ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

|  |  |
| --- | --- |
| API | Application Programming Interface |
| BIP | Bitcoin Improvement Proposal |
| НСД | Несанкционированный доступ |
| ОС | Операционная система |
| ПК | Персональный компьютер |
| ПО | Программное обеспечение |
| ФДСЧ | Физический датчик случайных чисел |
| ЭП | Электронная подпись |

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Блокчейн** — это распределенная база данных, в которой данные хранятся в виде последовательного набора блоков, при этом каждый блок включает в себя значение хэш-функции от предыдущего блока. Эта база данных хранится одновременно на множестве узлов сети.

**Демон** — компьютерная программа в системах класса UNIX, запускаемая самой системой и работающая в фоновом режиме без прямого взаимодействия с пользователем.

**Доверенная загрузка** — это загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и идентификации/аутентификации пользователя.

**Мастер ключи** — ключи из ключевой пары из криптографической системы с открытым ключом, из которой по протоколу BIP 32 генерируются дочерние иерархически детерминированные ключевые пары.

**Криптовалюта** — разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах и ведутся в блокчейн сетях.

**Криптографическая система с открытым ключом** — система асимметричного шифрования или электронной подписи (ЭП), при которой ключ проверки подписи (открытый ключ) передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется ключ подписи (закрытый ключ).

**Криптовалютные ключи** — ключи из ключевой пары из криптографической системы с открытым ключом, которая генерируется по семейству протоколов BIP.

**Пользователь** — субъект доступа к объектам (ресурсам) СВТ.

**Системный вызов** — механизм исполнения процедур системной задачи по запросу прикладной задачи. Для прикладной задачи системный вызов представляется обычной функцией языка Си.

**Управление криптовалютными активами** — деятельность клиента по манипуляции криптовалютами и токенами, направленная на сохранение и приумножение активов, а также совершение сделок и транзакций.

**Криптовалютная транзакция** — информация о действии или последовательности действий, направленных на создание, выпуск, обращение криптовалютных активов.