

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

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Специальность 10.05.03 -

Специализация -

Кафедра
«Информационная безопасность
систем и технологий»

Информационная безопасность
автоматизированных систем

Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

МЕХАНИЗМЫ ЗАЩИТЫ ПРОГРАММНО-АППАРАТНОГО
КРИПТОКОШЕЛЬКА

Студент

Руководитель

Нормоконтролёр

Рецензент начальник отдела АО «ПНИЭИ»

Работа допущена к защите (протокол заседания кафедры от 15.06.20 № 13)

Заведующий кафедрой

Ковалерова Валентина Сергеевна

Романов И.О.

Иванов А.П.

Оськин Р.С.

С.Л. Зефирова

Работа защищена с отметкой отлично (протокол заседания ГЭК
от 25.06.20 № 4)

Секретарь ГЭК

А.П. Иванов

Пенза 2020

Оглавление

Введение.....	4
1 Область применения и условия функционирования программно-аппаратного криптокошелька.....	6
1.1 Область применения программно-аппаратного криптокошелька.....	6
1.2 Обзор существующих программно-аппаратных криптокошельков....	9
1.2.1 Основные методы «холодного» хранения.....	9
1.2.2 Зашифрованный бумажный кошелек.....	11
1.2.3 Подпись транзакций офлайн.....	12
1.2.4 Фрагментирование закрытых ключей.....	13
1.2.5 Мультиподпись.....	14
1.2.6 Аппаратные кошельки.....	14
1.2.7 Онлайн кошелек.....	15
1.3 Условия функционирования программно-аппаратного криптокошелька.....	16
2 Состав СКЗИ и назначение основных компонентов.....	20
3 Разработка модели нарушителя и модели угроз безопасности информации, обрабатываемой с использованием программно-аппаратного криптокошелька. .	23
3.1 Модель обеспечения информационной безопасности.....	23
3.1.1 Типы угроз безопасности информации и их источники.....	23
3.1.2 Условия размещения и особенности функционирования ИС. .	25
3.1.3 Объекты защиты и их описание	26
3.2 Модель нарушителя.....	27
3.2.1 Режим и степень участия персонала в обработке конфиденциальной информации.....	27
3.2.2 Классификация нарушителей и источников атак	28
3.3 Угрозы безопасности информации.....	30
4 Выбор организационных, физических и технических мер защиты	

информации, обрабатываемой с использованием программно-аппаратного криптокошелька.....	34
5 Анализ и оценка соответствия механизмов защиты Рекомендации по стандартизации с учетом класса КСЗ.....	38
5.1 Принципы применения криптографических механизмов в СКЗИ....	38
5.2 Механизм шифрования.....	38
5.3 Механизм предпускового контроля.....	39
5.4 Механизм защиты от НСД.....	41
5.5 Механизм аутентификации.....	41
5.6 Механизм контроля правильности работы механизма шифрования программно-аппаратного криптокошелька.....	42
6 Разработка и описание алгоритмов работы механизмов защиты информации, обрабатываемой с использованием программно-аппаратного криптокошелька.....	44
6.1 Алгоритм механизма криптографического преобразования информации.....	44
6.2 Алгоритм механизма предпускового контроля.....	46
6.3 Алгоритм механизма защиты от НСД.....	48
6.4 Алгоритм механизма аутентификации.....	49
6.5 Алгоритм механизма контроля правильности работы криптографических механизмов программно-аппаратного криптокошелька.....	50
7 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	53
7.1 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации	53
7.2 Методы и средства физической культуры, снижающие их воздействие.....	54
Заключение.....	58
Список используемых источников.....	60

Введение

Обеспечению конфиденциальности информации уделялось существенное внимание на протяжении всего времени. Существуют различные способы защиты информации, к примеру такие как, охрана носителей защищаемой информации физическими лицами и шифрование (криптографическое преобразование), которое является наиболее надежным и широко применяется в настоящее время.

Под криптографической защитой информации понимается преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий. В качестве исходных данных для криптографического преобразования используются алгоритм преобразования и ключ - изменяемый параметр в виде последовательности символов, определяющего криптографическое преобразование. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма криптографического преобразования.

В асимметричных криптосистемах применяется сочетание пары ключей - «открытый-закрытый». Утрата и раскрытие закрытого ключа третьим лицам приводит к нарушению конфиденциальности защищаемой информации. Этим объясняются важность ключевой информации и необходимость обеспечения ее защищенности.

Для безопасной обработки информации с использованием программно-аппаратного криптокошелька требуется разработка механизмов защиты для данного устройства, которые должны соответствовать ряду требований по криптографической защите информации. Именно поэтому выбранная тема выпускной квалификационной работы является актуальной.

Целью выпускной квалификационной работы является проектирование механизмов защиты для программно-аппаратного криптокошелька таким образом, чтобы он обладал теми инженерно-криптографическими и другими свойствами, которые необходимы для обеспечения конфиденциальности информации, обрабатываемой и хранящейся в программно-аппаратном криптокошельке, которыми не обладают существующие криптокошельки, что свидетельствует о новизне выпускной квалификационной работы.

Задачами, поставленными на дипломное проектирование, являются:

- описание области применения и условия функционирования программно-аппаратного криптокошелька;
- разработка модели нарушителя и модели угроз безопасности информации, обрабатываемой с использованием программно-аппаратного криптокошелька;
- выбор организационных, физических и технических мер защиты информации, обрабатываемой с использованием программно-аппаратного криптокошелька;
- анализ и оценка соответствия механизмов защиты Рекомендации по стандартизации [1] с учетом класса КСЗ;
- разработка и описание алгоритмов работы механизмов защиты информации, обрабатываемой с использованием программно-аппаратного криптокошелька.

1 Область применения и условия функционирования программно-аппаратного криптокошелька

1.1 Область применения программно-аппаратного криптокошелька

Областью применения криптокошелька является хранение криптовалюты. Криптовалюты основаны на технологии блокчейн. Эта технология используется крупными банками и отдельными государственными учреждениями для упрощения обработки информации и транзакций. Криптовалюты представлены транзакциями, которые записаны в блокчейне и могут быть просмотрены любым пользователем. Транзакции, основанные на этой технологии, не зависят от правительственных учреждений и официальной валютной системы.

Криптокошелек - это программа, которая содержит открытые и закрытые криптографические ключи, то есть структура для хранения виртуальных денег на основе цепочки блоков, которые на самом деле представляют собой две цифры - уникальный идентификатор кошелька (адрес биткойна (открытый ключ), к которому привязаны все деньги) и закрытый ключ. Ключи позволяют работать с блокчейном от своего имени и выполнять транзакции с криптовалютой.

Открытый ключ служит адресом для транзакций. Его могут видеть все пользователи, совершающие на него транзакции или отслеживающие их в блокчейне.

Закрытый ключ знает только владелец кошелька и именно на этом ключе основывается безопасность виртуальных средств.

Для того, чтобы создать адрес кошелька система сначала генерирует закрытый ключ, а на его основе при помощи хэширования создает открытый ключ, который подходит исключительно под сгенерированный закрытый. Зная закрытый ключ, можно определить открытый, но подбор закрытого ключа на основе открытого невозможен.

Закрытый ключ — сложная криптограмма, идентифицирующая владельца и позволяющая получить доступ к криптовалюте, служащая своеобразной подписью при исходящих транзакциях. Закрытый ключ представляет собой 256-ти битное число, которое может быть записано в двоичной и шестнадцатеричной системе.

В двоичной системе комбинация из 256-символов нуля и единицы формирует закрытый ключ. Но оперирование такими длинными ключами не слишком практично, поэтому закрытый ключ записывают в виде 32-х байтного числа, где на каждый байт понадобится два числа из шестнадцатеричной системы, то есть 64 символа в диапазоне от 0 до 9 и от A до F.

На основе закрытого ключа формируется валидная цифровая подпись, которая служит доказательством того, что транзакция подтверждена владельцем открытого ключа. Как только отправленная в сеть транзакция доводится до назначения, начинается сопоставление цифровой подписи и открытого ключа. При этом никто из участников проверки не может узнать закрытый ключ отправителя транзакции. После того как проверка необходимого количества блоков подтвердит соответствие валидной подписи и открытого ключа — транзакция признается действительной и завершается, что обеспечивает надежность транзакций внутри системы.

Отличия закрытого ключа от открытого приведены в таблице 1.

Таблица 1 — Отличия закрытого и открытого ключей

№ п/п	Параметр сравнения	Открытый ключ	Закрытый ключ
1	Основная функция	Открытый ключ используется в качестве адреса для кошелька.	Служит для обеспечения доступа к хранилищу криптовалют владельца. На его основе составляется валидная цифровая подпись, обеспечивающая безопасность транзакций.
2	Вид	Открытый ключ состоит из максимум 34-х символов цифр и букв латинского	Закрытый ключ состоит из 64 символов, состоящих из цифр от 0 до 9 и букв

Продолжение таблицы 1

№ п/п	Параметр сравнения	Открытый ключ	Закрытый ключ
		алфавита, за исключением букв "0", "O", "I", "i" (для защиты от ошибочных действий и мошенничества)	латинского алфавита от А до F.
3	Метод хранения	Открытые ключи хранятся в открытом доступе и могут быть предоставлены третьим лицам в качестве адреса для транзакции.	Цифровое значение закрытого ключа знает только владелец. Закрытые ключи следует хранить в полной конфиденциальности, исключая доступ третьим лицам.
4	Метод получения	Открытый и закрытый ключи формируются одновременно и связаны между собой определенным математическим соотношением (в зависимости от выбранного типа уравнения кривой).	
5	Безопасность	Открытый ключ можно узнать из реестра блокчейн цепи или при помощи закрытого ключа.	Закрытый ключ невозможно узнать при помощи математического вычисления из открытого ключа или цифровой подписи. Ключ сохраняется только пользователем и никогда не транспортируется при операциях.

Закрытый ключ подтверждает владение криптовалютой, хранящейся на соответствующем ему открытом ключе, и является конфиденциальной информацией, которая никогда не передается третьим лицам и не фиксируется системой. На основе закрытого ключа обеспечивается безопасность транзакций внутри системы. В случае потери закрытого ключа восстановить доступ к имеющимся на открытом ключе средствам будет невозможно.

Необходимо обеспечивать надежное хранение закрытого ключа, так как любой пользователь на его основе может произвести транзакции с кошелька в корыстных целях.

Система блокчейн обеспечивает полную безопасность проведения транзакций, которые невозможно подделать или отменить.

Главной проблемой функционирования программно-аппаратного криптокошелька является хранение криптовалюты. Основная цель злоумышленников — получение доступа к закрытым ключам, большинство которых хранится в Интернете или на носителях, подключенных к Интернету.

Выделяют следующие распространенные причины, из-за которых можно потерять доступ к средствам:

- хранение криптовалюты в онлайн-кошельке или на бирже. В этом случае закрытый ключ хранится на серверах биржи или сервиса. При удачной атаке злоумышленники могут получить доступ к серверам и ко всем закрытым ключам пользователей;

- слабые методы безопасности. Если при входе в онлайн-кошелёк не используется двухфакторная аутентификация, счёт уязвим;

- локальное хранение ключей (когда они находятся на персональном компьютере, а не на стороннем сервере) также имеет свои недостатки. Подключенный к Интернету компьютер может с тем же успехом стать жертвой злоумышленников, что и биржевой сервер. К тому же ключ можно безвозвратно потерять, если выйдет из строя винчестер;

- при «холодном» хранении (на устройствах без постоянного подключения к Интернету) безопасность также не обеспечивается на 100 %. Потеря устройства или серьёзная поломка могут стать причиной утраты закрытого ключа.

1.2 Обзор существующих программно-аппаратных криптокошельков

1.2.1 Основные методы «холодного» хранения

Если сравнивать два основных способа хранения криптовалюты — «холодный» (без постоянного подключения к Интернет) и «горячий» (с

постоянным подключением к Интернет), то по удобству выигрывает «горячий», особенно если нужно часто покупать или продавать криптовалюту, но «холодное» хранение обеспечивает высокую степень безопасности и является незаменимым при необходимости хранить большие суммы.

Существуют пять основных методов «холодного» хранения, которые позволяют снизить риск кражи средств до минимума:

- традиционные и зашифрованные бумажные кошельки;
- метод подписи транзакций офлайн;
- фрагментированные закрытые ключи;
- мультиподпись;
- аппаратные кошельки.

Среди всех известных методов «холодного» хранения криптовалюты бумажные кошельки — наиболее простой. Для создания такого кошелька нужно сгенерировать открытый и закрытый ключи (рекомендуется в офлайн-режиме) и распечатать их на обычном бумажном листе.

Таким образом можно хранить криптовалюту без доступа в Интернет. На открытый ключ бумажного кошелька можно переводить собственные средства с биржи или других «горячих» кошельков.

В таком случае бумажный кошелек выполняет роль сейфа, в который складываются накопления.

Также можно получать криптовалюту от других лиц. Для чего нужно передать открытый ключ тому, от кого должен поступить перевод.

Чтобы перевести средства, нужно осуществить импорт закрытого ключа в «горячий» кошелек, используемый для проведения операций в сети.

Если необходимо потратить только часть сбережений, а остальное - хранить «холодным» методом, то следует создать бумажный кошелек (с новыми ключами) и перевести на него остаток средств.

При хранении криптовалюты в бумажном кошельке присутствуют возможные риски и налагаются определенные ограничения, а именно:

- бумага — ненадежный физический носитель, так как легко повредить. Поэтому распечатанные ключи лучше хранить в надежном месте, где такой риск будет исключен. Например, в небольшом сейфе;
- обязательное удаление ключей с электронных носителей после печати/использования;
- запрет на производство электронных копий бумажного кошелька: скан-, фотокопии;
- сделать дубликат бумажного кошелька.

1.2.2 Зашифрованный бумажный кошелек

Данный метод позволяет ещё больше повысить уровень защиты закрытых ключей при хранении их на бумажных носителях.

В этом случае также распечатываются открытый и закрытый ключи на бумажном носителе. Но закрытый ключ распечатывается в зашифрованном виде.

Шифрование закрытого ключа значительно повышает защищённость бумажного кошелька от действий злоумышленников. Даже если бумажный носитель с ключами попадёт в руки к злоумышленникам, они не смогут воспользоваться закрытым ключом, так как его ещё нужно расшифровать, что сделать простым перебором вариантов маловероятно (вероятность успешного подбора на 1 попытку равна $1/2^{256}$ и составляет порядка $8,6 \times 10^{-78}$).

Для зашифрования бумажного кошелька нужно сгенерировать закрытый ключ на основании случайных значений.

После генерации приватного ключа необходимо ввести ключевую фразу для его шифрования (в качестве метода шифрования обычно используется ВР38).

Придумывая ключевую фразу или пароль для зашифровки ключа, не нужно экономить на количестве символов и мощности алфавита. Чем длиннее

пароль и разнообразнее символы — тем надёжнее шифрование. Не зная ключевой фразы, такой кошелек невозможно взломать.

Если потерять или забыть фразу для расшифровки, невозможно получить доступ к кошельку. Поэтому фразу лучше записать и хранить в надёжном месте, но отдельно от самого кошелька.

При этом заметным недостатком бумажного кошелька является то, что на время криптографических преобразований необходимо переводить закрытый ключ с бумажной формы в электронную, тем самым подвергая его опасности из-за возможных атак потенциального противника. Защита от такой угрозы реализуется к примеру с помощью офлайн подписи транзакций — метода «холодного» хранения, который рассмотрен в пункте 1.2.3.

1.2.3 Подпись транзакций офлайн

Данный метод предназначен для пользователей, оперирующих крупными объёмами криптовалюты и вынужденных регулярно проводить транзакции.

Данный метод несколько сложнее обычных способов хранения, но с его помощью возможно переводить криптовалюту другим пользователям, при этом закрытый ключ не будет скомпрометирован.

Для реализации офлайн-подписи транзакций понадобятся два компьютера. Первый компьютер всегда будет подключен к Интернету, но закрытые ключи на нём не хранятся.

Второй компьютер должен быть отключенным от Интернета. На нём хранятся закрытые ключи, а также устанавливается программа-кошелек с функцией цифровой подписи транзакций.

На первом компьютере нужно создать транзакцию, указав адрес получателя и объём средств, но транзакция не подписана. Далее необходимо неподписанную транзакцию скопировать на офлайн-компьютер.

На втором компьютере необходимо подписать транзакцию с помощью закрытого ключа, скопировав после подписанную транзакцию на онлайн-

компьютер. Затем можно осуществить отправку транзакции адресату.

Таким образом компьютер, который постоянно подключен к Интернету, никогда не соприкасается с закрытыми ключами.

К недостаткам этого метода можно отнести неудобства для пользователя во время применения метода при частом проведении большого количества транзакций.

При подписи транзакций офлайн присутствуют возможные риски и налагаются определенные ограничения, а именно:

- причиной потери ключей может стать поломка офлайн-компьютера;
- в целях подстраховки следует делать резервные копии ключей на других защищённых носителях;
- в качестве носителей информации для обмена данными между первым (онлайн) и вторым (офлайн) компьютерами рекомендуется использовать оптические диски или любые другие носители информации, не имеющие вычислительных устройств.

1.2.4 Фрагментирование закрытых ключей

Основой метода является криптографическая схема разделения секрета. Согласно этой схеме закрытый ключ разбивается на определённое количество фрагментов. При этом для восстановления ключа могут требоваться не все фрагменты, а лишь часть из них. Каждый фрагмент сам по себе не имеет никакой ценности и не содержит важной информации. Это позволяет добиться очень высокого уровня безопасности хранения криптовалюты.

На практике данный метод может реализовываться следующим образом:

- закрытый ключ разбивается на фрагменты, каждый из которых передаётся конкретному доверительному лицу;
- определяется минимальное количество частей, необходимое для восстановления ключа.

С точки зрения защищённости от взлома или кражи такой метод эффективен. Во-первых, каждый участник может хранить свой фрагмент ключа в надёжном месте. Во-вторых, даже если один и два фрагмента попадут в руки злоумышленников, они всё равно не смогут получить доступ к полной версии ключа. А остальные участники тем временем смогут перенести средства на новый адрес.

1.2.5 Мультиподпись

При использовании мультиподписи транзакция подписывается несколькими закрытыми ключами.

На практике метод может реализовываться следующим образом:

- определяется общее количество ключей для подписи;
- ключи раздаются разным доверенным лицам;
- устанавливается допустимый минимум для подписи транзакции;
- при создании транзакции средства переведутся по нужному адресу только тогда, когда транзакцию подпишет необходимое количество держателей ключей.

Метод мультиподписи в своей основе схож с методом фрагментирования закрытых ключей (раздел 1.1.3) в части привлечения нескольких доверенных лиц для использования и соответственно хранения закрытого ключа. Рассмотренный метод мультиподписи метод не только обеспечивает высокий уровень защиты хранилища от стороннего вмешательства, но и позволяет организовать ответственное управление крупным капиталом, размещённым в криптовалюте.

1.2.6 Аппаратные кошельки

Аппаратные кошельки появились на рынке относительно недавно, но уже пользуются хорошей популярностью.

Кошельки такого типа представляют собой физическое электронное

устройство небольших размеров. Модели некоторых производителей выполняются в виде флешки.

На устройстве хранятся зашифрованные закрытые ключи. Для проведения транзакций кошелёк подключается к компьютеру, который постоянно подключен к Интернет, а затем создается транзакция. Аппаратный кошелёк подписывает её закрытым ключом и отправляет обратно на компьютер. При этом ключ не может быть скомпрометирован.

Аппаратные кошельки — компактные устройства, которые легко использовать в повседневной работе. К тому же они обеспечивают надёжную защиту хранимых ключей на аппаратном уровне. Доступ к устройству защищается PIN-кодом.

Аппаратные кошельки практически невозможно взломать, даже если устройство попадёт в руки злоумышленников.

1.2.7 Онлайн кошелек

При использовании «горячего» способа хранения криптовалюты выделяют еще один вид кошельков - онлайн кошелек.

Использование онлайн кошелька для криптовалюты предоставляют специальные сервисные сайты обслуживания. Ими могут быть биржи обмена, платёжные системы, сервис хранения данных.

За время существования криптовалюты существующие онлайн-сервисы выработали определенные правила и меры ее защиты — от SMS-подтверждений, мультиподписей и двухфакторной аутентификации до страхования и «холодного» хранения средств пользователей, доверяющих им свои деньги.

Пользование онлайн-кошельками не предусматривает установки определенного программного обеспечения на компьютер, поэтому не используют его ресурсы и оперативную память. Но при этом функциональность

таких ресурсов ничем не хуже аппаратных кошельков для криптовалюты, некоторые из них обладают таким преимуществом, как получение списка адресных книг и истории всех транзакций по e-mail или через SMS.

Плюсы: удобство, доступность.

Минусы: зависимость от третьей стороны.

1.3 Условия функционирования программно-аппаратного криптокошелька

По результатам анализа достоинств и недостатков существующих методов «холодного» хранения криптовалюты следует вывод, что на сегодняшний день самым безопасным методом для хранения криптовалюты является программно-аппаратный криптокошелек.

Рассмотрим программно-аппаратный криптокошелек на примере программно-аппаратного криптокошелька Trezor от чешской компании SatoshiLabs, который можно использовать для подписания транзакций, подтвержденных на небольшом дисплее. Другими словами, чтобы совершить (подтвердить) платеж, необходимо ввести подтверждающие данные на этом устройстве.

Основной уязвимостью программно-аппаратного кошелька является невозможность подтвердить адрес получателя при передаче криптовалюты, то есть фишинг-атака.

Внешний вид программно-аппаратного кошелька Trezor показан на рисунке 1.

Внутри корпуса кошелька находятся плата с расположенным на ней черно-белый OLED дисплей с разрешением 128×64 пикселя, а также различные элементы, среди которых центральное место занимает 120 МГц ARM процессор семейства Cortex M3.



Рисунок 1 — Программно-аппаратный кошелек Trezor

При первоначальном использовании криптокошелька необходимо:

- после подключения устройства к компьютеру через USB-переходник перейти на сайт компании myTrezor.com для выполнения дальнейших инструкций;
- скачать программу, необходимую для взаимодействия компьютера с электронным кошельком;
- установить специальное программное обеспечение;
- на странице личного кабинета выбрать создание нового хранилища или восстановление доступа к существующему депозиту с помощью SEED-фраз.

Затем на дисплее данного кошелька отобразятся 24 SEED-фраз, которые нужно записать на надежный носитель, исключая доступ третьим лицам. SEED-фразы необходимы при восстановлении доступа. В дальнейшем доступ к секретным словам на кошельке будет невозможен.

Последний этап первоначальной настройки «TREZOR» - это создание PIN-кода с целью безопасного входа в личный кабинет.

В программно-аппаратном кошельке «TREZOR» реализованы следующие механизмы защиты: подтверждение транзакции с помощью подписи,

генерируемой закрытым ключом, и восстановление доступа к кошельку по seed-фразе.

А также модели программно-аппаратного кошелька поставляются с защитной голографической наклейкой над портом USB-C, остатки которой очень трудно удалить с корпуса устройства. Наклейка является достаточно хорошим способом защиты от несанкционированного доступа в дополнение к основной мере – вводу PIN-кода.

Для обеспечения дополнительной безопасности расположение кнопок ввода PIN-кода на устройстве меняется при каждом запросе.

Актуальность темы исследования определяется отсутствием надежного механизма защиты программно-аппаратных криптокошельков, что негативно отражается на безопасности хранения своих активов самостоятельно.

Хотя объем крипторынка на сегодня и не сравним с объемом классического рынка финансовых услуг, но, учитывая быстрое развитие криптовалюты, защита программно-аппаратных криптокошельков имеет широкое распространение в области криптоиндустрии. Кража криптоактивов происходит главным образом не через блокчейн технологию, которая безопасна сама по себе, а через другие уязвимые места, а именно — криптокошелек, что определяет необходимость совершенствования его механизма защиты.

На фоне роста конкуренции среди криптокошельков, поставщики этой услуги требуют от пользователей предоставления большего количества персональных данных.

Компании-производители программно-аппаратных криптокошельков сталкиваются с проблемой невозможности обеспечения достаточного уровня защиты средств пользователя. Исследователи активно выдвигают предложения по вопросам основных принципов соблюдения безопасности, но каждая редакция вызывает новую волну дискуссий.

Исследование и разработка проектного решения механизма защиты программно-аппаратного криптокошелька, к примеру, от атак на транзакции

покупки и (или) продажи в криптовалюте, сделают работу программно-аппаратного кошелька наиболее эффективным способом к осуществлению защищенных транзакций при совершении атак злоумышленниками.

Рассмотрим программно-аппаратный кошелек в качестве средства криптографической защиты информации (СКЗИ). Структура СКЗИ определяется функциями, которое разрабатываемое СКЗИ должно реализовывать.

Основными компонентами СКЗИ выступают следующие механизмы: механизм предпускового контроля, механизм шифрования, механизм контроля правильности работы механизма шифрования, механизм защиты от несанкционированного доступа (далее — НСД) и механизм аутентификации.

Механизм предпускового контроля предназначен для проверки корректности работы стека, ОЗУ, исполнительной части микроконтроллера программно-аппаратного криптокошелька при подключении к персональному компьютеру и целостности программного обеспечения.

Механизм шифрования предназначен для шифрования/расшифрования информации, а также для контроля и блокировки шифратора при его неисправностях и сбоях в ПО.

Механизм защиты от НСД предназначен для исключения доступа к внутренним элементам программно-аппаратного криптокошелька

Механизм аутентификации предназначен для подтверждения аутентифицируемого процесса с физическим лицом, от имени которого он действует.

Основным элементом, на основе которого предлагается реализовывать СКЗИ, является flash-память на базе микроконтроллера с архитектурой Cortex-M3. Основные характеристики flash-памяти приведены в таблице 2.

Устройство представляет собой автономное устройство для хранения цифровой валюты на базе микроконтроллера и flash-памяти, а также имеет последовательный стык ввода/вывода USB 3.0. С целью защиты от НСД

конструкции на корпусе устройства расположена защитная голограмма, которой запечатан USB-порт, установленная организацией-изготовителем.

Структура средств криптографической защиты информации, выполненных на базе программно-аппаратного криптокошелька показана на рисунке 2 и на плакате «Структура средств криптографической защиты информации, выполненных на базе программно-аппаратного криптокошелька».



Рисунок 2 — Структура СКЗИ

В квадрате СКЗИ показаны механизмы для пояснения последовательности их выполнения. Сначала пользователь проверяет голографическую наклейку на НСД, потом подключает программно-аппаратный криптокошелек с СКЗИ к персональному компьютеру и СКЗИ автоматически проводит предпусковой контроль. Затем пользователь вводит пароль и аутентифицируется, после чего уже может быть осуществлено шифрование.

Таблица 2 — Характеристики flash-памяти

Архитектура	Накопитель на базе flash-памяти, работающий под управлением микроконтроллера
Исполнение	Малогабаритный корпус с разъемом Micro-USB типа C

Продолжение таблицы 2

Архитектура	Накопитель на базе flash-памяти, работающий под управлением микроконтроллера
Емкость оперативной памяти	1,024 Мб
Протокол обмена с внешними устройствами	USB 2.0 и USB 3.0
Рабочая температура	От минус 20 °С до плюс 60 °С
Масса	12 грамм

3 Разработка модели нарушителя и модели угроз безопасности информации, обрабатываемой с использованием программно-аппаратного криптокошелька

3.1 Модель обеспечения информационной безопасности

3.1.1 Типы угроз безопасности информации и их источники

Так как ни одним нормативным документом не регламентирована методика создания модели угроз безопасности носителей информации, поэтому было принято решение разработать модель угроз безопасности для информационной системы, в которой есть помещение, в рамках которого у определенного лица имеется возможность работы с программно-аппаратным криптокошельком — далее ИС.

Программно-аппаратный криптокошелек предназначен для защиты конфиденциальной информации, обрабатываемой на персональных компьютерах. Программно-аппаратный криптокошелек может быть разработан для организаций, где ведется работа с конфиденциальной информацией и существует необходимость обеспечения ее сохранности.

Программно-аппаратный криптокошелек состоит из следующих составляющих объектов информационной безопасности:

- аппаратная составляющая, потенциальный вред которой может быть нанесен непосредственным физическим воздействием на объект;
- информационная составляющая, потенциальный вред которой может быть нанесен с использованием возможностей технических и программных средств.

В качестве источников угроз безопасности информации выступают следующие типы:

- антропогенные источники (антропогенные угрозы);
- техногенные источники (техногенные угрозы);

- стихийные источники (угрозы стихийных бедствий, иных природных явлений);
- атаки.

Источниками антропогенных угроз безопасности информации выступают следующие субъекты:

- лица, имеющие права на получение информации из программно-аппаратного криптокошелька (пользователи криптокошелька);
- лица, обслуживающие программно-аппаратный криптокошелек (администраторы информационной безопасности);
- лица, группы лиц или организации, имеющие доступ к объектам информационной безопасности с полномочиями, предоставляемыми неограниченному кругу лиц;
- лица, представляющие организацию-изготовителя системы и осуществляющие разработку и обслуживание программно-аппаратного криптокошелька (разработчики программно-аппаратного криптокошелька и СКЗИ), но при этом не принимающие участие в непосредственной обработке конфиденциальной информации.

Источниками техногенных угроз безопасности информации являются нарушения свойств работоспособности программно-аппаратного криптокошелька, связанные с неустранимыми отказами или сбоями в работе технических средств или программного обеспечения. Такие угрозы могут быть обусловлены:

- низким качеством (надежностью) технических, программных или программно-технических средств;
- низким качеством (надежностью) сетей связи и (или) услуг связи;
- низким качеством обслуживания со стороны обслуживающих лиц.

Природные явления и стихийные бедствия, являющиеся источниками стихийного характера, также могут приводить к нарушению свойств работоспособности программно-аппаратного криптокошелька.

Атаки наиболее опасные угрозы безопасности информации, что обусловлено их тщательной подготовкой, скрытностью проведения, целенаправленным выбором объектов и целей атак. Атаки готовятся и проводятся нарушителем. При этом возможности проведения атак определяются соответствующими возможностями нарушителя. Анализ возможностей, которыми может обладать нарушитель, проводится в рамках разработки модели нарушителя.

Основной задачей обеспечения информационной безопасности является противодействие атакам нарушителя на объекты информационной безопасности (далее — ИБ). Для источников угроз разработана модель нарушителей ИБ.

3.1.2 Условия размещения и особенности функционирования ИС

В информационной системе организации-заказчика была выделена одна однотипная информационная система, где обрабатывается конфиденциальная информация, необходимая для реализации информационного процесса, заключающегося в подписании транзакций, подтвержденных на небольшом дисплее программно-аппаратного криптокошелька.

Назначение системы — подтверждение платежей с использованием банковского счета.

Для обрабатываемой конфиденциальной информации системы необходимо обеспечивать сохранность таких свойств информации, как: конфиденциальность, целостность и доступность.

Ресурсы системы размещены на автоматизированном рабочем месте пользователя (далее — АРМ), где установлено специальное программное обеспечение, необходимое для взаимодействия компьютера с электронным

кошельком, и программно-аппаратный криптокошелек (далее - физический носитель конфиденциальной информации).

Физические меры защиты объектов, где размещены ресурсы системы: АРМ и физический носитель конфиденциальной информации размещены в офисных помещениях, оборудованных межкомнатными дверьми с замками и системой поддержания климата.

Меры по обеспечению контролируемой зоны – все технические средства расположены в пределах офисного здания. Здание оборудовано системой видеонаблюдения и сигнализацией на дверях. Контролируемой зоной являются периметр охраняемой территории предприятия, ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

В подсистеме используются только кабельные соединения. Все кабели проложены в пределах контролируемой зоны, следовательно к ним применяются меры ограничения несанкционированного доступа, относящиеся к контролируемой зоне (видео-наблюдение, сигнализация на дверях, замки на дверях).

Данная подсистема осуществляет информационное взаимодействие с информационно-телекоммуникационной сетью (далее - ИТКС) общего пользования. В силу того, что данная ИС для выполнения своего основного назначения подключается к сети Интернет, повышается вероятность несанкционированного доступа к обрабатываемой конфиденциальной информации, следовательно требуется организация защиты с помощью СКЗИ.

3.1.3 Объекты защиты и их описание

В информационной системе организации-заказчика защите подлежат следующие объекты:

- технические средства и компоненты информационной системы;
- АРМ пользователя программно-аппаратного криптокошелька;

- кабельные соединения;
- программное обеспечение:
 - специальное программное обеспечение для взаимодействия физического носителя конфиденциальной информации и компьютера с электронным кошельком;
- носители информации и документация, используемая в информационной системе:
 - ключевая, парольная и аутентификационная информация СКЗИ;
 - носитель ключевой, парольной и аутентификационной информации СКЗИ;
 - эксплуатационная документация программно-аппаратного криптокошелька;
- используемые информационной системой каналы (линии) связи, включая кабельные системы:
 - кабели локально вычислительной сети (далее - ЛВС) и телефонной линии;
 - информационно-телекоммуникационная сеть;
- помещения, в которых находятся ресурсы информационной системы:
 - выделенное помещение для работы пользователей.

3.2 Модель нарушителя

3.2.1 Режим и степень участия персонала в обработке конфиденциальной информации

Обработка конфиденциальной информации осуществляется в однопользовательском режиме.

В информационной системе присутствует разграничение прав доступа.

Сотрудники, имеющие доступ к ИС:

- администратор ИБ – обеспечивает разграничение прав доступа, занимается обслуживанием и конфигурированием СКЗИ, а также настройкой технических и программных средств, поддержанием их работоспособности, резервным копированием данных;
- пользователь программно-аппаратного криптокошелька – имеет полномочия на чтение, запись и изменение данных, не имеют полномочий по модификации аппаратного и программного обеспечения;
- сотрудники частной охранной организации;
- обслуживающий персонал информационной системы, в том числе ее разработчики.

Администратор ИБ осуществляет техническое обслуживание технических и программных средств СКЗИ и среды функционирования (далее - СФ), включая их настройку и конфигурирование.

Пользователь программно-аппаратного криптокошелька имеет доступ к объектам защиты в виде их АРМ, программного обеспечения, а также к защищаемой конфиденциальной информации.

Право разового доступа к ИС имеют работники обслуживающих организаций. Они могут осуществлять физический доступ к аппаратному обеспечению ИС, но только в присутствии сопровождающих лиц.

3.2.2 Классификация нарушителей и источников атак

Нарушители могут обладать следующим потенциалом:

- средний потенциал – наличие возможностей уровня группы лиц/организации по разработке и использованию специальных средств эксплуатации уязвимостей;

— низкий потенциал – наличие возможностей уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей.

Угрозы безопасности информации, обрабатываемой в информационной системе организации-заказчика, могут реализовываться как внешними, так и внутренними нарушителями.

Возможные внутренние нарушители с указанием их потенциала:

- пользователь программно-аппаратного криптокошелька – низкий потенциал;
- сотрудники частной охранной организации – низкий потенциал;
- обслуживающий персонал информационной системы – средний потенциал.

Возможные внешние нарушители с указанием их потенциала:

- бывшие сотрудники организации-заказчика – низкий потенциал;
- разработчики ИС – средний потенциал;
- «хакеры» – средний потенциал.

Внешние нарушители могут получить доступ к объектам защиты путем проведения атак через сеть Интернет.

Обобщенные возможности источников атак следующие:

- возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны;
- возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования;
- возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования.

3.3 Угрозы безопасности информации

На основании обобщенных возможностей источников атак составлена таблица 3.

Таблица 3 – Актуальные источники атак

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	Актуально	
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ	Актуально	
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	Актуально	
1.4	Использование штатных средств ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	Актуально	

Продолжение таблицы 3

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Актуально	
2.2	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	Не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
3.2	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
3.3	Проведение работ по созданию способов и средств атак в научноисследовательских центрах, специализирующихся в области	Не актуально	не осуществляется обработка сведений, составляющих

Продолжение таблицы 3

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ		государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	Не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.
4.3	Возможность воздействовать на любые компоненты СКЗИ и СФ	Не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые

Продолжение таблицы 3

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.

Данные актуальные источники атак делают актуальными следующие угрозы:

- угроза несанкционированного копирования защищаемой информации;
- угроза модификации информации и навязывания ложной информации;
- перехват конфиденциальной информации, позволяющий осуществить доступ к ее содержимому;
- хищение программно-аппаратного криптокошелька;
- физическое повреждение программно-аппаратного криптокошелька.

На основании возможностей нарушителей, направления атак и раздела 3.2 «Модель нарушителя» данного документа определен класс средств криптографической защиты информации — КСЗ.

4 Выбор организационных, физических и технических мер защиты информации, обрабатываемой с использованием программно-аппаратного криптокошелька

По результатам проведенного анализа возможных угроз безопасности информации, обрабатываемой с использованием программно-аппаратного криптокошелька, сформулирован перечень основных задач, которые должны решаться системой информационной безопасности:

- управление доступом пользователей к программно-аппаратному криптокошельку с целью защиты от неправомерного случайного или умышленного вмешательства в его работу и несанкционированного доступа к его информационным, программным и аппаратным ресурсам со стороны посторонних лиц, а также лиц из числа персонала организации;
- регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в ИС и имеющих отношение к ее безопасности;
- контроль работы пользователей программно-аппаратного криптокошелька и оперативное оповещение администратора безопасности о попытках несанкционированного доступа к нему.

По способам осуществления меры обеспечения безопасности информации выделены на:

- организационные (административные);
- физические и технические (аппаратные и программные).

В таблице 4 приведены меры противодействия угрозам безопасности информации, использующие уязвимости системы защиты программно-аппаратного криптокошелька.

Таблица 4 — Меры противодействия угрозам безопасности информации

№ п/п	Уязвимость	Угроза безопасности информации	Защитные меры
1	Недостатки или отсутствие механизмов аудита, связанные с возможностью бесконтрольного несанкционированного блокирования доступности целевой информации	Вмешательство в работу программно-аппаратного криптокошелька, связанное с модификацией информации, навязыванием ложной информации и к полному или частичному отказу в обслуживании	Контроль подключения программно-аппаратного криптокошелька Реализация антивирусной защиты Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
2	Недостатки или отсутствие механизмов аудита, связанные с возможностью не обнаруженной модификации (подмены) целевой информации не уполномоченными на это лицами	Вмешательство в работу программно-аппаратного криптокошелька, связанное с модификацией информации, навязыванием ложной информации и к полному или частичному отказу в обслуживании Перехват конфиденциальной информации, позволяющий осуществить доступ к ее содержимому	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации Контроль подключения программно-аппаратного криптокошелька Установка градации сотрудников и их уровней доступа к конфиденциальной информации
3	Недостатки реализации необходимых организационно-режимных мероприятий, связанные с возможностью несанкционированного визуального просмотра защищаемой информации на дисплее программно-аппаратного криптокошелька, а так же несанкционированного ознакомления с распечатываемыми документами, содержащими конфиденциальную информацию	Угроза несанкционированного копирования защищаемой информации Перехват конфиденциальной информации, позволяющий осуществить доступ к ее содержимому Хищение программно-аппаратного криптокошелька	Организация охраны и надежного пропускного режима Технические средства визуального наблюдения, связи и охранной сигнализации Установка градации сотрудников и их уровней доступа к конфиденциальной информации

Продолжение таблицы 4

№ п/п	Уязвимость	Угроза безопасности информации	Защитные меры
4	Недостатки или отсутствие механизмов защиты информационных ресурсов ИС от компьютерных вирусов	Перехват конфиденциальной информации, позволяющий осуществить доступ к ее содержимому Вмешательство в работу программно-аппаратного криптокошелька, связанное с модификацией информации, навязыванием ложной информации и к полному или частичному отказу в обслуживании	Использование лицензионного программного обеспечения Реализация антивирусной защиты Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
5	Наличие недокументированных (недекларированных) возможностей, внесенных на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию, ремонта и обслуживания программных и технических средств ИС	Вмешательство в работу программно-аппаратного криптокошелька, связанное с модификацией информации, навязыванием ложной информации и к полному или частичному отказу в обслуживании	Контроль исходного состояния программного обеспечения Контроль полноты и отсутствия избыточности исходных текстов программного обеспечения Использование автономных АРМ, обрабатывающих конфиденциальную информацию, без подключения сетей связи
6	Недостатки реализации необходимых организационно-режимных мероприятий на территории обслуживающей организации, связанные с возможностью перехвата разглашаемой защищаемой информации	Перехват конфиденциальной информации, позволяющий осуществить доступ к ее содержимому Хищение программно-аппаратного криптокошелька	Организация охраны и надежного пропускного режима Технические средства визуального наблюдения, связи и охранной сигнализации Организация мероприятий по тестированию подготовки персонала к работе в критических ситуациях
7	Непреднамеренные действия персонала, обслуживающие рабочие места	Физическое повреждение программно-аппаратного криптокошелька	Визуальный контроль собственных действий пользователя Допуск к работе со средствами ИС

Продолжение таблицы 4

№ п/п	Уязвимость	Угроза безопасности информации	Защитные меры
		Хищение программно-аппаратного криптокошелька	квалифицированного персонала, прошедшего обучение и обладающего соответствующими навыками
8	Доступ лиц, имеющих право на техническое обслуживание, к рабочим местам и программно-аппаратному криптокошельку в момент обработки с использованием этих средств конфиденциальной информации	Вмешательство в работу программно-аппаратного криптокошелька, связанное с модификацией информации, навязыванием ложной информации и к полному или частичному отказу в обслуживании Физическое повреждение программно-аппаратного криптокошелька Угроза несанкционированного копирования защищаемой информации	Технические средства визуального наблюдения, связи и охранной сигнализации Установка градации сотрудников и их уровней доступа к конфиденциальной информации Организация доступа обслуживающего персонала к средствам ИС только в сопровождении доверенных лиц

5 Анализ и оценка соответствия механизмов защиты Рекомендации по стандартизации с учетом класса КСЗ

5.1 Принципы применения криптографических механизмов в СКЗИ

Руководствуясь рекомендациями по стандартизации [1], применение криптографических механизмов в СКЗИ основано на следующих принципах:

- использование криптографических механизмов, утвержденных в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографических механизмов, имеющих положительное заключение ФСБ России по результатам их экспертных криптографических исследований;
- значения параметров криптографических механизмов должны удовлетворять условиям, определяемым в рекомендациях по выбору параметров криптографических механизмов, утверждаемых ФСБ России;
- криптографические механизмы, а также преобразования, реализующие обработку ключевой информации, ее выработку и удаление, следует реализовывать непосредственно в СКЗИ.

5.2 Механизм шифрования

ФСБ России был введен в действие межгосударственный стандарт 34.12-2018 [12] взамен ГОСТ 28147-89 [2], поэтому предлагается использовать алгоритм криптографического преобразования по ГОСТ 34.12-2018 (вариант «Магма») [12], который предназначен для аппаратной и программной реализации. Одним из достоинств является то, что ГОСТ 34.12-2018 [12] удовлетворяет современным криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации.

В программно-аппаратном криптокошельке использован протокол вычисления SHA-256 [9]. Данный протокол работает с информацией, раздробленной на части по 512 бит (или другими словами 64 байта). Он производит ее криптографическое «смешивание», а затем выдаёт 256-битный хеш-код. В состав алгоритма входит простой раунд, который повторяется 64 раза.

Алгоритм SHA-256 [9] не используется по своему прямому назначению в российских информационных системах, оснащаемых сертифицированными средствами криптографической защиты.

Технология блокчейн, на основе которой работает программно-аппаратный криптокошелек, изначально не подразумевает шифрование какой-либо информации. Поэтому предложено скорректировать наименование механизма — механизм криптографического преобразования информации.

5.3 Механизм предпускового контроля

Контроль работоспособности программно-аппаратного криптокошелька должен включать:

- обнаружение неисправностей в работе со стеком;
- обнаружение неисправностей в работе с ОЗУ;
- проверку работоспособности исполнительной части микроконтроллера;
- контроль целостности программного обеспечения.

Механизм обнаружения неисправности в работе со стеком производит после назначения портам начальных адресов памяти и записи в стек памяти проверку присвоения адресов. При несовпадении номера порта и адреса в стеке памяти производится перевод программы на выполнение вечного цикла, и дальнейшая работа устройства блокируется до перезапуска и проведения

повторной проверки.

Механизм обнаружения неисправности в работе с ОЗУ производит запись в каждую из ячеек памяти ее собственного адреса с последующим сравнением адреса и значения по данному адресу и при отрицательном результате производится перевод программы на выполнение вечного цикла, и дальнейшая работа устройства блокируется до перезапуска и проведения повторной проверки.

Контроль работоспособности исполнительской части микроконтроллера осуществляется путем проверки корректности работы арифметических, логических операций, установки флагов, срабатывания переходов, вызова подпрограмм. При отрицательном результате производится перевод программы на выполнение вечного цикла, и дальнейшая работа устройства блокируется до перезапуска и проведения повторной проверки.

Механизм проверки целостности программного обеспечения в процессе запуска устройства осуществляет расчёт контрольной суммы по predetermined алгоритму, после чего рассчитанное значение сравнивается с эталонным значением. При несовпадении значений процесс запуска устройства прекращается.

При неуспешном прохождении хотя бы одного из пунктов механизма предпускового контроля дальнейшая штатная работа устройства невозможна. Для продолжения работы необходимо устранить неисправность.

В программно-аппаратном криптокошельке должен быть реализован механизм предпускового контроля.

Информация, обрабатываемая программно-аппаратным криптокошельком, хранится в виде цепочки блоков, где каждому блоку присваивается цифровая подпись – хеш-сумма, являющаяся уникальным идентификатором.

Так как каждый блок имеет контрольную сумму хранения, в течение предпускового контроля контрольные суммы должны проверяться. В случаях

повреждения блока должен производиться цикл восстановления блока, после чего проверка повторяется и выносится решение о целостности блока.

5.4 Механизм защиты от НСД

СКЗИ должно обеспечивать безопасность защищаемой информации при условии несанкционированного доступа к защищенной СКЗИ информации в процессе ее хранения или передачи по каналам связи.

В рассмотренном программно-аппаратном криптокошельке защитой от несанкционированного доступа выступает голографическая наклейка над портом USB-C, остатки которой очень трудно удалить с корпуса устройства, что является достаточно хорошим способом только при первоначальном приобретении программно-аппаратного криптокошелька, при этом в процессе эксплуатации защита от НСД к разъему отсутствует. Защита от НСД к меню обеспечивается вводом PIN-кода.

5.5 Механизм аутентификации

Основной угрозой при использовании механизма аутентификации является угроза кражи носителя аутентификационных данных с последующим доступом к программно-аппаратному криптокошельку.

В программно-аппаратном криптокошельке аутентификационными данными выступает PIN-код пользователя, который он вводит для подтверждения транзакции.

При получении доступа к аутентификационным данным нарушитель будет иметь возможность восстановить доступ к программно-аппаратному криптокошельку и входа в личный кабинет, что позволит злоумышленнику заполучить цифровую валюту, которая хранится в кошельке.

В связи с чем в дополнение к механизму аутентификации организационными мерами должен быть исключен доступ посторонних лиц к носителям аутентифицирующей информации.

5.6 Механизм контроля правильности работы механизма шифрования программно-аппаратного криптокошелька

В пункте 5.1 настоящего документа было обосновано отсутствие механизма шифрования, поэтому механизм контроля правильности предназначен для выявления ошибок в работе криптографических механизмов программно-аппаратного криптокошелька.

Для подтверждения работоспособности криптографических механизмов предлагается проверять их на контрольном примере путем подачи эталонных значений на вход криптоалгоритма и последующего сравнения полученного результата с эталонным значением. В случае отрицательного результата сравнения работа с ключами и конфиденциальной информацией должна быть прекращена, а выдача информации – заблокирована.

Кроме того в программно-аппаратном кошельке должны быть реализованы алгоритмы расчета и проверки контрольных сумм.

Алгоритм вычисления контрольной суммы (проверка избыточности циклической суммы) — способ цифровой идентификации некоторой последовательности данных, который заключается в вычислении контрольного значения её циклического избыточного кода.

С точки зрения математики контрольная сумма является типом хэш-функции, используемой для вычисления контрольного кода, применяемого для обнаружения ошибок при передаче или хранении информации. Результат вычисления контрольной суммы добавляется в конец блока данных непосредственно перед началом передачи или сохранения данных на каком-либо носителе информации. Впоследствии он проверяется для подтверждения

её целостности. Применение контрольной суммы обусловлено тем, что подобная проверка хорошо подходит для обнаружения общих ошибок, вызванных наличием шума в каналах передачи данных.

6 Разработка и описание алгоритмов работы механизмов защиты информации, обрабатываемой с использованием программно-аппаратного криптокошелька

6.1 Алгоритм механизма криптографического преобразования информации

В СКЗИ криптографическое преобразование информации реализуется в соответствии с алгоритмом ГОСТ 34.12-2018 (вариант «Магма») [12] (далее — алгоритм). Обоснованием для этого является то, что данный алгоритм является стандартом шифрования Российской Федерации и является обязательным для организаций, компаний РФ, которые используют шифровальную защиту для данных, загружаемых или передаваемых через компьютерные сети, отдельные компьютерные комплексы.

Данный алгоритм предназначен как для аппаратной реализации, так и для программных реализаций, а также не определяет ограничений на уровень секретности защищаемой информации.

Алгоритм содержит 32 цикла преобразования, где каждый цикл состоит из простых операций. Длина ключа алгоритма - 256 бит.

В состав ключевого блокнота программно-аппаратного криптокошелька входят:

- открытый ключ конфиденциальной связи Кк;
- закрытый ключ конфиденциальной связи Кк;
- вектор инициализации программного датчика случайных чисел (далее - ПДСЧ) КДСЧ.

Открытый ключ конфиденциальной связи Кк предназначен для формирования адреса пользователя программно-аппаратного криптокошелька, который известен третьим лицам.

Закрытый ключ конфиденциальной связи K_k предназначен для формирования электронно-цифровой подписи транзакций программно-аппаратного криптокошелька.

Вектор КДСЧ предназначен для первоначальной инициализации программного датчика случайных чисел. Возможен вариант, когда в состав ключевого блокнота будет входить исключительно вектор ПДСЧ, из шума полученного с его помощью уже будет формироваться пара ключей «открытый-закрытый».

Обмен информацией между парой программно-аппаратных криптокошельков организуется в виде сеансов связи. Под сеансом связи понимается интервал времени от момента установления соединения до момента разрыва соединения. В процессе установления сеанса программно-аппаратный криптокошелек создает сеансовые ключи на основе ключа K_k , при этом каждый пакет информации, передаваемый в процессе одного сеанса связи, подписывается ЭП, после чего при разрыве соединения данные ключи уничтожаются и осуществляется выработка новой ключевой информации.

Формирование электронной цифровой подписи осуществляется в соответствии с ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» [10].

В данном ГОСТ Р 34.10-2012 [10] определены процессы формирования и проверки цифровой подписи под сообщением пользователя.

Алгоритм механизма криптографического преобразования информации показан на рисунке 3 и на плакате «Алгоритмы работы механизмов защиты информации программно-аппаратного криптокошелька, лист 1».

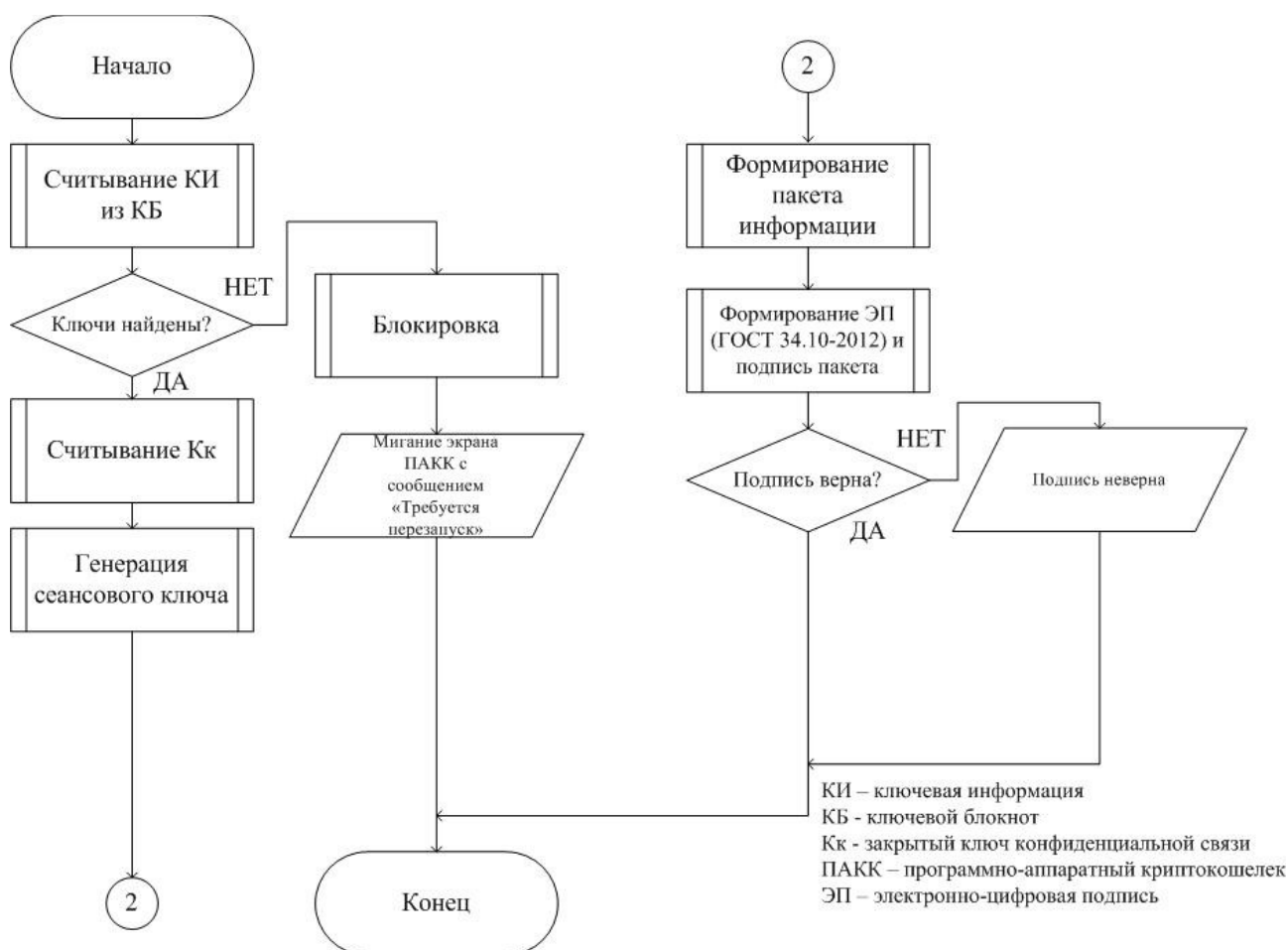


Рисунок 3 — Алгоритм механизма криптографического преобразования информации

6.2 Алгоритм механизма предпускового контроля

Предпусковой контроль предназначен для первоначальной диагностики отдельных модулей программно-аппаратного криптокошелька.

Предпусковой контроль программно-аппаратного криптокошелька включает в себя:

- тестирование исполнительной части микроконтроллера (процессора);
- тестирование внутреннего оперативно-запоминающего устройства (ОЗУ);

- тестирование работы стека ;
- проверка целостности программного обеспечения.

При получении неправильных результатов любого из вышеперечисленных тестов работа СКЗИ блокируется. Алгоритм предпускового контроля представлен на рисунке 4 и плакате «Алгоритмы работы механизмов защиты информации программно-аппаратного криптокошелька, лист 2».

Согласно пункту 6.1.3 рекомендаций по стандартизации «Р 1323565.1.012-2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации» [1] в СКЗИ класса КСЗ должна быть предусмотрена реализация блокировки работы СКЗИ в случаях диагностики неисправности СКЗИ, при достижении предельных значений технических характеристик СКЗИ (механизм, сигнализирующий или блокирующий работу СКЗИ при достижении предельных значений технических характеристик СКЗИ) и нарушении целостности ПО СКЗИ.

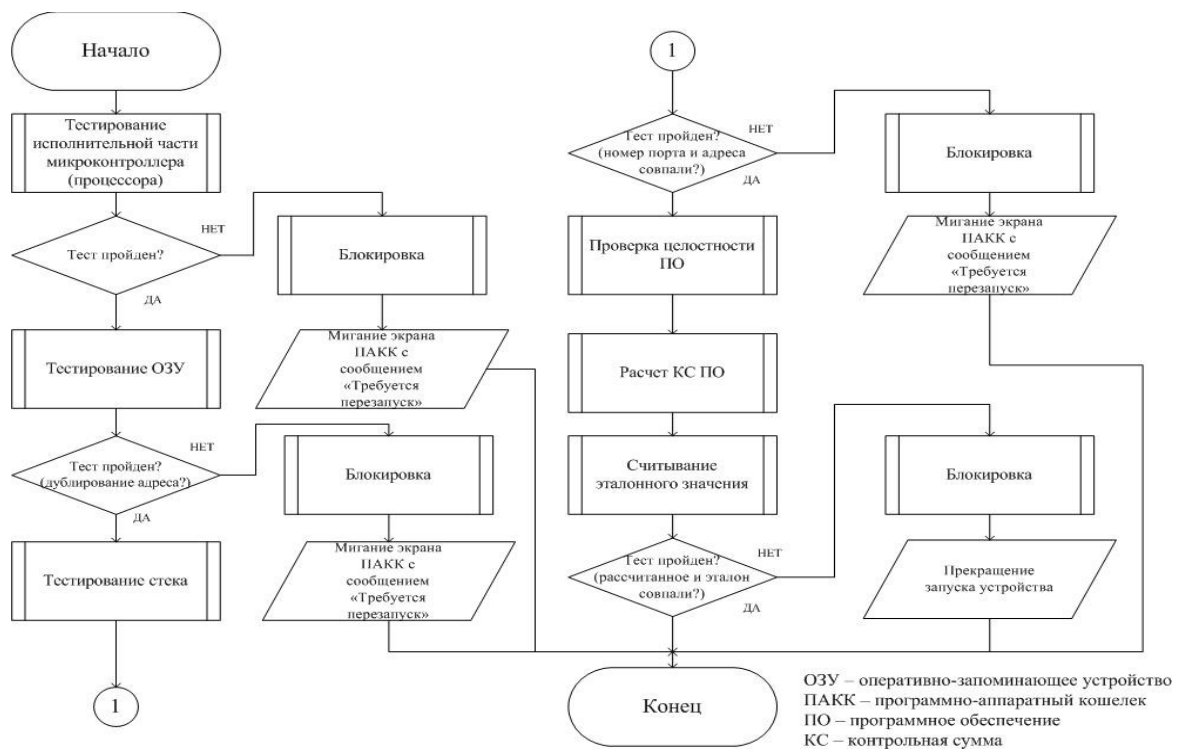


Рисунок 4 — Алгоритм механизма предпускового контроля

6.3 Алгоритм механизма защиты от НСД

Согласно пункту 6.1.3 рекомендаций по стандартизации «Р 1323565.1.012-2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации» [1] в качестве составной части СКЗИ класса КСЗ должна быть реализована система защиты от несанкционированного доступа к защищаемой СКЗИ информации.

Так как в программно-аппаратном криптокошельке уже существуют следующие способы защиты от несанкционированного доступа:

- голографическая наклейка над портом USB-C (при первоначальном приобретении программно-аппаратного криптокошелька);
- ввод PIN-кода (доступ к меню от НСД).

В процессе эксплуатации предлагается реализовывать к имеющимся механизмам защиты от НСД отключение питания разъема USB до получения положительного результата аутентификации пользователя по PIN-коду.

Алгоритм механизма защиты от НСД представлен на рисунке 5 и плакате «Алгоритмы работы механизмов защиты информации программно-аппаратного криптокошелька, лист 3».

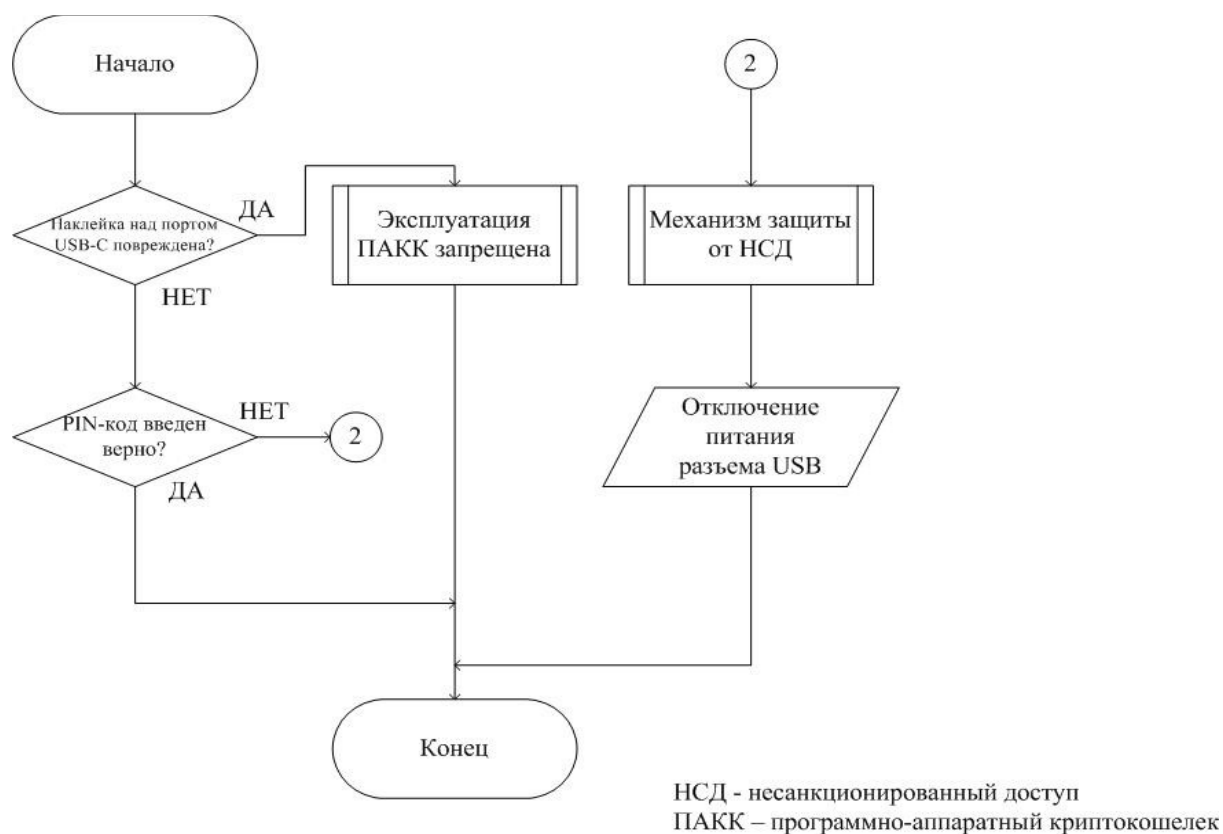


Рисунок 5 — Алгоритм механизма защиты от НСД

6.4 Алгоритм механизма аутентификации

Согласно пунктам 5.5.5, 5.5.7, 5.5.8 и 5.5.11 рекомендаций по стандартизации «Р 1323565.1.012-2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации» [1] в качестве составной части СКЗИ класса КСЗ при аутентификации субъектов доступа, являющихся процессами и осуществляющих взаимодействие с СКЗИ, должен быть реализован механизм, позволяющий ассоциировать аутентифицируемый процесс с физическим лицом, от имени которого он действует, а именно:

— ограничение числа следующих подряд неудачных попыток аутентификации одного субъекта доступа ($i=3$, где i - число следующих подряд неудачных попыток аутентификации);

— при превышении числа следующих подряд неудачных попыток аутентификации одного субъекта доступа установленного предельно допустимого значения доступ этого субъекта доступа к СКЗИ следует блокировать на заданный промежуток времени;

— установление предельно допустимого числа следующих подряд неудачных попыток аутентификации одного субъекта доступа в значение, не превышающее десяти.

Алгоритм механизма аутентификации представлен на рисунке 6 и плакате «Алгоритмы работы механизмов защиты информации программно-аппаратного криптокошелька, лист 4».

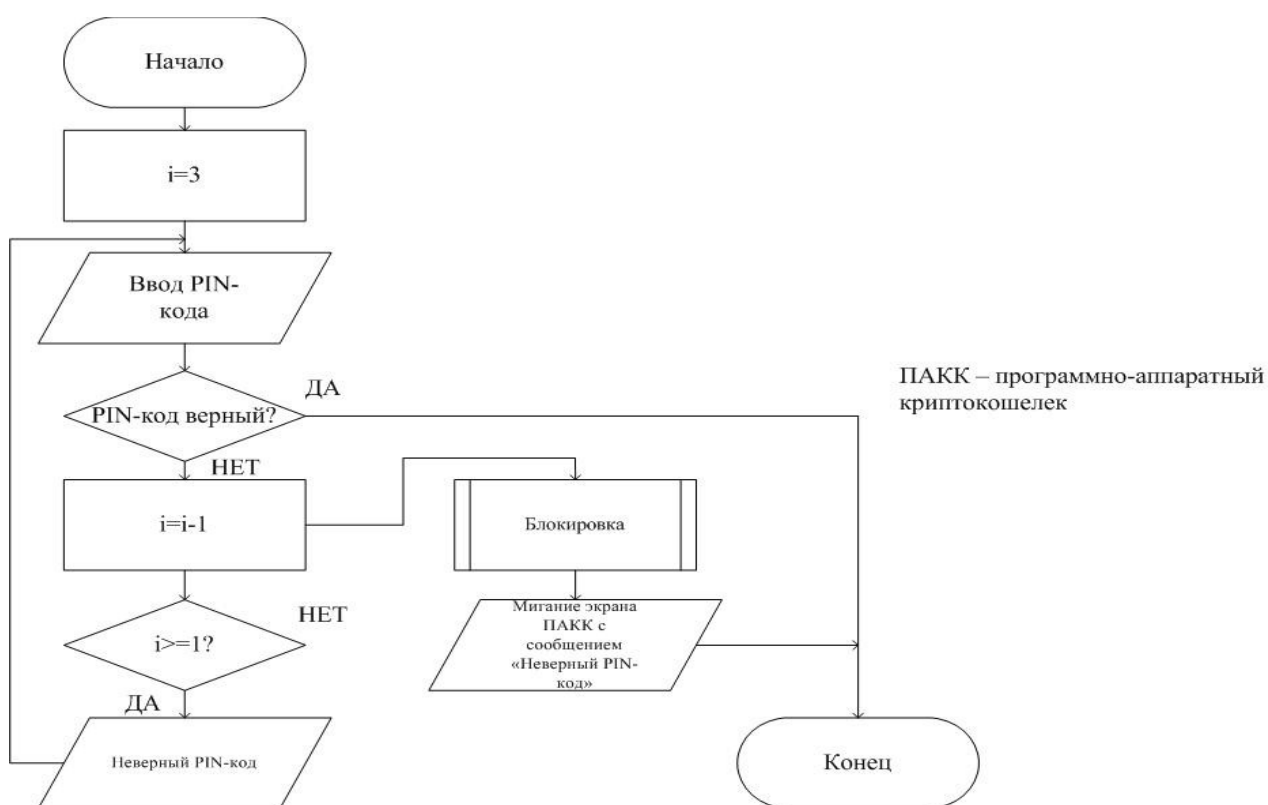


Рисунок 6 — Алгоритм механизма аутентификации

6.5 Алгоритм механизма контроля правильности работы криптографических механизмов программно-аппаратного криптокошелька

Данный механизм предназначен для выявления ошибок в процессе работы криптографических механизмов программно-аппаратного криптокошелька. Для этого формируется некоторое число, называемое контрольной суммой и являющееся функцией блока данных, и добавляет его к этому блоку данных. Таким образом, используя данный алгоритм, рассчитывается контрольная сумма блока данных и сравнивается с эталонным значением.

Алгоритм контрольного суммирования CRC (Cyclic redundancy code) [11] предназначен для контроля целостности данных и используется в проводных, беспроводных сетях и в устройствах хранения данных, для проверки информации на подлинность и защиты от несанкционированного изменения. Алгоритм основан на свойствах деления с остатком многочлена на многочлен. Результатом контрольного суммирования CRC является остаток от деления многочлена, соответствующего исходным данным, на порождающий многочлен фиксированной длины.

Количество различных остатков от деления многочлена на многочлен меньше, чем количество различных исходных многочленов. Таким образом, контрольное суммирование CRC однозначно определяет, что два массива данных отличаются друг от друга, если отличаются их контрольные суммы. Но, если две контрольные суммы совпали, невозможно однозначно утверждать, что для их формирования использовался один и тот же исходный массив данных.

В зависимости от вида порождающего многочлена и его длины, изменяется вероятность совпадения контрольных сумм для различных исходных данных и время контрольного суммирования.

Контрольное суммирование, работающее с порождающими многочленами 32 степени (CRC-32), в пределе позволяет получить надежность порядка: $2^{32} = 4.294.967.296$. Что позволяет, практически со 100% вероятностью, обнаруживать сбои при хранении и передаче данных.

Исходная битовая последовательность блока данных представляется в виде двоичного многочлена. При этом каждый бит такой последовательности соответствует одному из полиномиальных коэффициентов. Контрольный код по методу контрольной суммы рассчитывается, как остаток от деления по модулю 2 многочлена, полученного из исходной битовой последовательности, на некоторый другой заранее определённый многочлен (такой многочлен называется порождающим или примитивным).

Алгоритм механизма контроля правильности работы криптографических механизмов представлен на рисунке 7 и плакате «Алгоритмы работы механизмов защиты информации программно-аппаратного криптокошелька, лист 5».

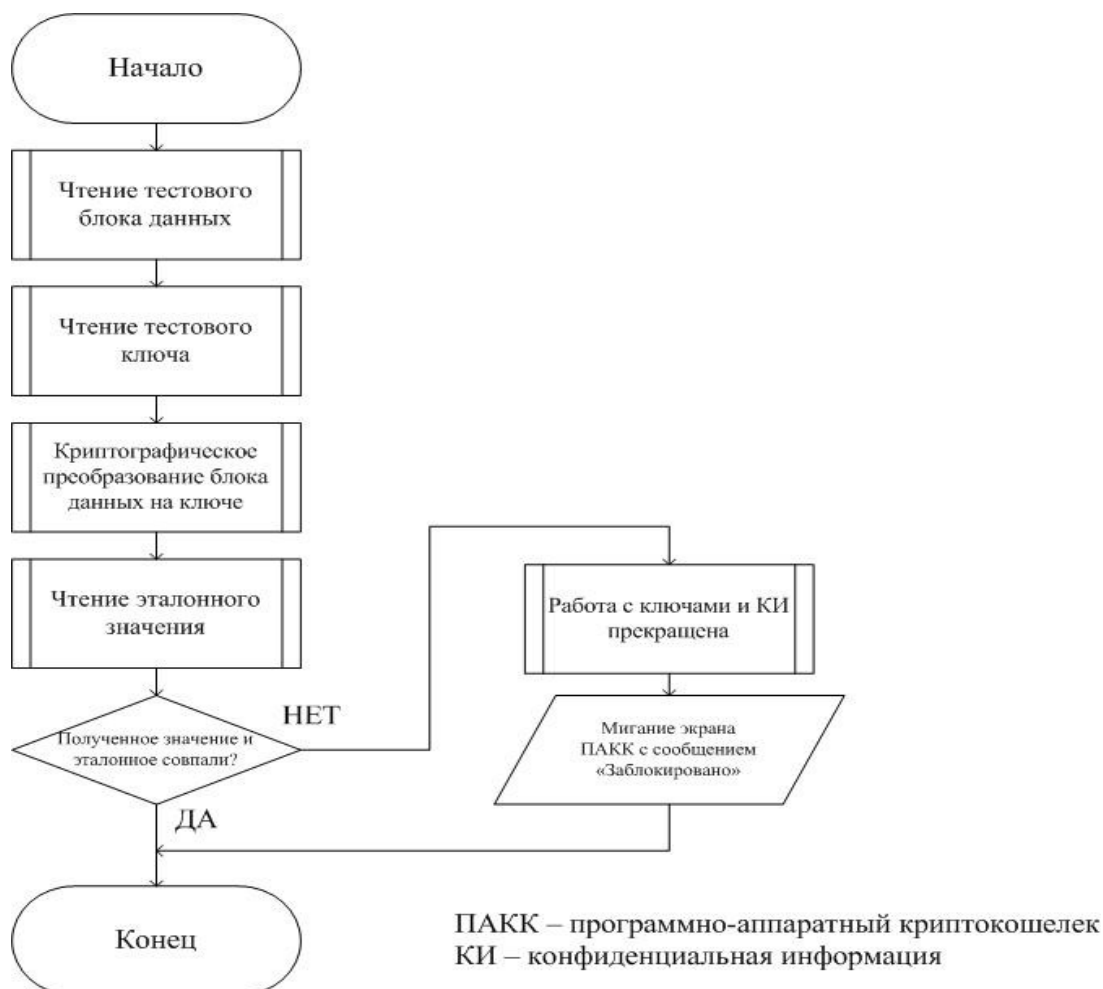


Рисунок 7 — Алгоритм механизма контроля правильности работы криптографических механизмов

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

7.1 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации

По официальной статистике, ежегодно в России от сердечно-сосудистых заболеваний умирает около 1 млн. 300 тысяч человек, смертность по этой причине превышает половину числа всех смертей в стране. Россия лидирует по этому показателю среди развитых стран.

Одной из причин сердечно-сосудистых заболеваний является сидячий образ жизни, а работа специалиста по защите информации подразумевает долгое сидение за рабочим местом. Сидячий образ жизни вреден, потому что положение сидя (или лежа) уменьшает нагрузку на сердечно-сосудистую систему, а также позволяет сердцу и кровеносным сосудам «расслабиться». В отличие от него, положение стоя вынуждает сердечно-сосудистую систему работать активнее, просто для поддержания нормального уровня артериального давления. Снижение исходного уровня сердечно-сосудистой деятельности, связанного с длительным сидением, может привести к относительной сердечной дезадаптации. Резкая перемена сидячего положения на стоячее может вызвать повышение артериального давления, что в некоторых случаях приводит к потере сознания.

Зачастую, люди, чья работа связана с сидячим образом жизни, страдают от плохой циркуляции крови в нижних конечностях, что приводит к развитию варикозного заболевания вен. При долгом сидении без смены положения сосуды пережимаются, кровь в них застаивается и не может двигаться как положено — вверх. Из-за этого стенки сосудов испытывают давление и когда оно становится избыточно высоким, кровь выталкивается и ее излишки растягивают вены. Но не столь опасно варикозное расширение вен, как являющийся её следствием

тромбофлебит, который ведет к образованию тромбов. Тромбы могут закупоривать вены, образуя флемботромбоз, либо оторвавшись от стенки сосуда по кровотоку попасть в легкие. Это в большинстве случаев приводит к тяжёлым осложнениям, а иногда и к летальному исходу.

Помимо варикозного расширения вен сидячий образ жизни специалиста по защите информации опасен тем, что продолжительное отсутствие физической активности приводит к гипотоническим (пониженное артериальное давление) и гипертоническим (повышенное артериальное давление) заболеваниям.

7.2 Методы и средства физической культуры, снижающие их воздействие

Для снижения рисков при ведении сидячего образа жизни необходимо заниматься физическими упражнениями, которые являются научно обоснованным методом профилактики заболеваний сердечно-сосудистой системы. Регулярные занятия физическими упражнениями уменьшают вероятность возникновения заболеваний органов кровообращения.

Для предотвращения и профилактики заболеваний сердечно-сосудистой системы физические упражнения рекомендуются всем, но особенно тем, у кого есть факторы риска, такие как сидячий образ жизни. В основном рекомендуются такие виды занятий, как гимнастические упражнения, бег, ходьба, плавание, ходьба на лыжах, туризм.

Гимнастические упражнения развивают мышечную силу, укрепляют связки, делают суставы более подвижными, совершенствуют координацию движений. Например, при гипотонической болезни силовые, скоростно-силовые и статические упражнения повышают артериальное давление, а при гипертонической болезни дыхательные упражнения и упражнения для мелких мышечных групп способствуют его снижению. Дыхательные упражнения и

упражнения в расслаблении мышц также оказывают общее оздоровительное действие для всего организма.

Ходьба — основное средство в оздоровительной и лечебной физической культуре. Является естественной для организма человека формой мышечной деятельности. Во время ходьбы в работу включается большинство мышц туловища, ног и рук. Поэтому людям, ведущим сидячий образ жизни, рекомендуется больше передвигаться пешком, так как это самый доступный способ оздоровления организма, также не требующий практически никаких затрат. В лечебных целях рекомендуется ходьба в медленном (от 60 до 70 шагов в минуту, скорость продвижения не более 3 км/ч), в среднем (от 80 до 100 шагов в минуту, скорость 4 км/ч) и в быстром (от 100 до 110 шагов в минуту, скорость 5 км/ч). Нежелательно ходить в более быстром темпе. В начале ходьбы следует делать более короткие шаги и держать медленный темп, затем шаг нужно удлинять, а темп увеличивать. Во время ходьбы необходимо следить за дыханием, а именно согласовывать его с шагами — выдох немного длиннее, чем вдох.

Следующее оздоровительное средство — бег. Бег помогает предупредить заболевания сердечно-сосудистой системы и нормализовать функции при начальных проявлениях болезни, повысить резервы организма. Однако это очень сильное средство, которое предъявляет значительные требования к опорно-двигательному аппарату, сердечно-сосудистой и дыхательной системам, поэтому при серьезных заболеваниях этих систем занятия бегом стоит отложить.

При многих заболеваниях сердечно-сосудистой системы можно подобрать такие скорость и длительность бега, которые не будут перегружать, но в то же время будут тренировать эту систему. Регулярные занятия бегом улучшают деятельность и других систем организма. Его лечебное действие заключается в том, что совершенствуются регулирующие системы (центральная и вегетативная нервные системы, эндокринная система). Помимо этого беговые

тренировки повышают тонус парасимпатической системы (в покое снижается артериальное давление). В условиях жизни специалиста по защите информации волнения и стресс являются неотъемлемой частью его профессиональной деятельности и повышают тонус симпатической нервной системы, а беговые тренировки уравнивают взаимодействие этих систем.

Начинать занятия с лечебной целью следует с очень медленного бега — почти со скоростью ходьбы. Только через несколько месяцев занятий можно увеличивать темп, иначе можно вместо оздоровления причинить организму непоправимый вред. После бега рекомендуется выполнять ходьбу, упражнения на расслабление и растягивание мышц туловища и конечностей, а также дыхательные упражнения.

Ходьба на лыжах оказывает разнообразное воздействие на организм и включает в работу все мышечные группы, способствуя их укреплению, ускорению обмена веществ, улучшению функций дыхательной, сердечно-сосудистой и нервной систем, повышению физической работоспособности и закаливанию организма.

При занятиях ходьбой на лыжах стоит варьировать объем занятий в зависимости от температуры воздуха и силы ветра. При морозе и ветре продолжительность пребывания на воздухе необходимо сокращать. Наиболее благоприятными условиями занятий на лыжах является температура воздуха от минус 1 до минус 12 градусов по Цельсию и сила ветра более 10 м/с.

При любом из вышеперечисленных занятий величину нагрузок необходимо дозировать по субъективным ощущениям занимающегося. Нагрузка не должна вызывать сильное утомление, а также необходимо следить за частотой сердечных сокращений, по которой можно судить о доступности физических нагрузок. Допустимый максимум частоты сердечных сокращений в зависимости от возраста определяется расчетом:

— для здоровых людей возраст вычитается из 220;

- для людей с факторами риска — из 200;
- для людей, уже перенесших заболевания сердечно-сосудистой системы, — из 190.

Людам с активной фазой сердечно-сосудистых заболеваний не рекомендуются все вышеперечисленные занятия до момента выздоровления, а после выздоровления необходимо дозировать нагрузки, чтобы не нанести вред ослабленному болезнью организму.

Результатом выполнения физических упражнений является повышение эффективности работы сердечно-сосудистой системы, повышение липопротеидов высокой плотности, или «хорошего» холестерина, и уменьшение триглицеридов в крови человека.

Из вышесказанного можно сделать вывод, что имеет смысл уменьшить время, проводимое сидя, и перераспределить его на время, проводимое на ногах. Практически все люди могут извлечь пользу из регулярных занятий спортом, независимо от того, занимаются ли они спортом интенсивно или придерживаются умеренной оздоровительной нагрузки. Систематизированная физическая деятельность благотворно влияет на весь организм человека и, следовательно, помогает предотвратить большое количество проблем со здоровьем, в том числе снижает риск смертности от сердечно-сосудистых заболеваний.

Заключение

В начале дипломного проектирования, целью которого являлось проектирование механизмов защиты для программно-аппаратного криптокошелька, был проведен обзор существующих криптокошельков «холодного» хранения, позволяющие снизить риск кражи средств до минимума, по итогам которого в качестве наиболее подходящего был выбран программно-аппаратный криптокошелек Trezor от чешской компании SatoshiLabs и рассмотрены условия его функционирования.

Далее был рассмотрен программно-аппаратный кошелек в качестве средства криптографической защиты информации. Были определены функции, которое разрабатываемое СКЗИ должно реализовывать. Разработана структура СКЗИ для пояснения последовательности выполнения функций. Также были представлены характеристики flash-памяти, на основе которого предлагается реализовывать СКЗИ.

На следующем этапе дипломного проектирования были разработаны модель нарушителя и модель угроз безопасности информации, обрабатываемой с использованием программно-аппаратного криптокошелька. Были выделены объекты информационной безопасности и типы источников угроз безопасности информации. Затем определены источники по каждому типу угроз. Учитывая источники угроз, разработана модель нарушителей информационной безопасности, где были рассмотрены следующие вопросы:

- режим и степень участия персонала в обработке конфиденциальной информации;
- классификация нарушителей и источников атак.

По результатам разработки модели нарушителя и на основании обобщенных возможностей источников атак составлены таблица актуальные

источники атак. В результате определены угрозы, актуальными которыми делают актуальные источники.

Далее были определены организационные, физические и технические меры защиты информации, обрабатываемой с использованием программно-аппаратного криптокошелька. Составлена итоговая таблица, где проведена взаимосвязь уязвимостей системы защиты программно-аппаратного криптокошелька, использующих угрозами безопасности информации, и соответствующих им защитных мер.

На следующем этапе дипломного проектирования были проведены анализ уже имеющихся механизмов защиты программно-аппаратного криптокошелька и оценка соответствия механизмов защиты согласно рекомендациям по стандартизации [1] с учетом класса КСЗ.

На завершающем этапе дипломного проектирования разработаны и описаны алгоритмы работы механизмов защиты информации, обрабатываемой с использованием программно-аппаратного криптокошелька.

Таким образом, задание на дипломное проектирование было выполнено в полном объеме.

Список используемых источников

- 1 Рекомендации по стандартизации Р 1323565.1.012-2017. Информационная технология. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. Приняты и введены в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2017 г. № 2068-ст. - М.: Стандартинформ, 2018. - 28 с.
- 2 ГОСТ 28147-89. Системы обработки информации. защита криптографическая. Алгоритм криптографического преобразования. Принят и введен в действие Постановлением Государственного комитета СССР по стандартам от 02.06.89 г. № 1409. - М.: ИПК Издательство стандартов, 1989. - 28 с.
- 3 Что такое приватный ключ биткоин и как его узнать. - [Электронный ресурс]. - URL: <https://prostocoin.com/blog/private-key>. - Режим доступа: свободный. - (Дата обращения: 20.02.2020).
- 4 Минимизация рисков в кредитно-финансовой сфере (блокчейн). - [Электронный ресурс]. - URL: <https://cyberleninka.ru/article/n/minimizatsiya-riskov-v-kreditno-finansovoy-sfere-blokcheyn/viewer>. - Режим доступа: свободный. - (Дата обращения: 23.02.2020).
- 5 Стратегии хранения криптовалюты и ключей. - [Электронный ресурс]. - URL: <https://cryptocartel.club/ru/kriptovalyuta/strategii-hraneniya-kriptovalyuty-i-klyuchey-holodnoe-hranenie-lokalnoe-hranenie>. - Режим доступа: свободный. - (Дата обращения: 27.02.2020).
- 6 Как взломать аппаратный криптокошелек. - [Электронный ресурс]. - URL: <https://www.kaspersky.ru/blog/hardware-wallets-hacked/22183/>. - Режим доступа: свободный. - (Дата обращения: 27.02.2020).

7 Насколько надежны аппаратные криптокошельки? - [Электронный ресурс]. - URL: <https://buy-bitcoin.pro/news/naskolko-nadezhnyi-apparatnyie-kriptokoshelki/>. - Режим доступа: свободный. - (Дата обращения: 28.02.2020).

8 Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. Приняты и введены в действие руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432. - 22 с.

9 Алгоритм хеширования SHA-256 простыми словами. - [Электронный ресурс]. - URL: <https://cryptofound.com/ru/guide/blockchain/simple-words-about-the-hash-algorithm-sha-256/>. - Режим доступа: свободный. - (Дата обращения: 03.04.2020).

10 ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Принят и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. N 215-ст. - М.: Стандартинформ, 2012. - 33 с.

11 Алгоритм контрольного суммирования CRC. - [Электронный ресурс]. - URL: http://all-ht.ru/inf/systems/p_0_13.html. - Режим доступа: свободный. - (Дата обращения: 01.05.2020).

12 ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. Принят и введен в действие Межгосударственным советом по метрологии, стандартизации и сертификации (протокол от 29 ноября 2018 г. № 54). - М.: Стандартинформ, 2018. - 18 с.