Утвержден

КБДЖ.468244.065 ПП-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ)

«РУТОКЕН ЭЦП 2.0»

Правила пользования

КБДЖ.468244.065 ПП

Листов 14

Изделие «Средство криптографической защиты информации «РУТОКЕН ЭЦП 2.0»

Формуляр КБДЖ.468244.065 ФО

АННОТАЦИЯ

В данном документе изложены правила пользования средством криптографической защиты информации (СКЗИ) «РУТОКЕН ЭЦП 2.0». При использовании СКЗИ необходимо также следовать требованиям нормативных и эксплуатационных документов, входящих в состав СКЗИ, в частности, следующих документов:

- «АРМ ЗКИ «РУТОКЕН ЭЦП 2.0». Правила пользования»;
- «АРМ Пользователя «РУТОКЕН ЭЦП 2.0». Правила пользования».

В качестве аппаратных средств для выработки ключевой информации используется сертифицированный физический ДСЧ.

В состав СКЗИ «РУТОКЕН ЭЦП 2.0» входит:

- Средство защиты от несанкционированного доступа, сертифицированное по требованиям ФСБ России (для уровня защиты КС2).
- программный модуль АРМ ЗКИ «РУТОКЕН ЭЦП 2.0».
- Аппаратный модуль «РУТОКЕН ЭЦП 2.0» (КБДЖ.468244.065).
- Автоматизированное рабочее место пользователя (АРМ Пользователя) «РУТОКЕН ЭЦП 2.0» в комплектации:
    - программный модуль АРМ Пользователя «РУТОКЕН ЭЦП 2.0»
        - динамическая библиотека PKCS#11;
        - утилита АРМ Пользователя (исполняемый файл)[1];
    - АРМ Пользователя. Модуль контроля целостности.

Примечание 1. Исполняемый файл утилиты АРМ Пользователя «РУТОКЕН ЭЦП 2.0» может не входить в состав СКЗИ.

ОГЛАВЛЕНИЕ

1. Общие положения 5
1.1. Программно-аппаратные среды функционирования 6
1.2. Условия эксплуатации 7
1.3. Аутентификация в СКЗИ «РУТОКЕН ЭЦП 2.0» 7
1.4. Требования безопасности при работе с изделием 7
2. Ключевые документы 7
2.1. Ключевые документы 7
2.2. Хранение ключевых документов 8
2.3. Уничтожение ключевых документов 8
2.4. Плановая смена ключей 8
2.5. Сроки действия ключей 8
3. Учёт СКЗИ 9
4. Компрометация ключевых документов СКЗИ «РУТОКЕН ЭЦП 2.0» 9
5. Журнал операций 9
6. Ведение журналов 10
7. Инициализация АМ «РУТОКЕН ЭЦП 2.0» 11
8. Требования безопасности функционирования рабочих мест 11
Специальные требования 13
9. Ввод СКЗИ в эксплуатацию 13
10. Действия в нештатных ситуациях 14
11. Порядок выполнения технического обслуживания, ремонт и утилизация. 15

1. Общие положения

СКЗИ «РУТОКЕН ЭЦП 2.0» подключается по шине USB к ПЭВМ и предназначено для шифрования, аутентификации, вычисления и проверки электронной подписи (ЭП) и безопасного хранения данных.

СКЗИ «РУТОКЕН ЭЦП 2.0» допускается защищать только несекретную, ограниченного распространения информацию.

СКЗИ «РУТОКЕН ЭЦП 2.0» реализует функции выполнения и проверки электронной подписи только в автоматическом режиме.

Защищаемая и защищенная при помощи СКЗИ «РУТОКЕН ЭЦП 2.0» информация представляется в виде файла.

Сертификация СКЗИ «РУТОКЕН ЭЦП 2.0» распространяется использование отечественных криптографических алгоритмов: ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012, – при обязательном выполнении следующих условий:

- Использующиеся АМ должны быть инициализированы при помощи АРМ ЗКИ «РУТОКЕН ЭЦП 2.0». Запрещается инициализировать сертифицированные АМ иными программными и аппаратными средствами, а также использовать такие АМ в работе.
- Объекты с ключевой информацией, записанные в память АМ при его инициализации на АРМ ЗКИ «РУТОКЕН ЭЦП 2.0», не могут быть перезаписаны или удалены.

Использование алгоритмов ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94 возможно до 31 декабря 2018 года.

Период непрерывной работы СКЗИ «РУТОКЕН ЭЦП 2.0» не должен превышать 1 суток.

СКЗИ «РУТОКЕН ЭЦП» дает возможность:

- формировать на АРМ ЗКИ и экспортировать в АМ «РУТОКЕН ЭЦП 2.0» ключевую информацию;
- формировать в АМ «РУТОКЕН ЭЦП 2.0» ключи шифрования, ключи ЭП, ключи проверки ЭП;
- шифровать/расшифровывать внешние данные, передаваемые в изделие через USB порт ПЭВМ, в режиме гаммирования в соответствии с ГОСТ 28147-89;
- шифровать/расшифровывать внешние данные, передаваемые в изделие через USB порт ПЭВМ, в режиме гаммирования с обратной связью в соответствии с ГОСТ 28147-89;
- вырабатывать имитовставку на данные в соответствии с ГОСТ 28147-89;
- шифровать и хранить во внутренней памяти информацию, передаваемую в изделие через USB порт ПЭВМ;
- шифровать «прозрачно» все содержимое EEPROM-памяти по алгоритму ГОСТ 28147-89;
- формировать и проверять ЭП данных по алгоритму ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 с использованием алгоритмов хэширования ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, соответственно.

Для корректной работы реализованных алгоритмов необходимо выполнить следующие требования.

I. Для обеспечения стойкости и свойств ЭП.

Электронная подпись предназначена для аутентификации лица, подписавшего электронное сообщение. Кроме того, использование ЭП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения:

- осуществить контроль целостности передаваемого подписанного сообщения;
- доказательно подтвердить авторство лица, подписавшего сообщение;
- защитить сообщение от возможной подделки.

Для обеспечения заявленных свойств ЭП при развертывании сети связи, защищенной с использованием СКЗИ, требуется обеспечить:

1. Невозможность отказа абонента, подписавшего сообщение, от своей подписи. Для этого должна быть выполнена процедура закрепления пары ключей ЭП (ключ подписи и ключ проверки подписи) за администратором безопасности и каждым абонентом. Например, каждый абонент должен лично явиться в удостоверяющий центр (УЦ) и расписаться за владение сертификатом своего открытого ключа и сертификатом открытого ключа УЦ.
2. Надежное хранение в тайне своего ключа ЭП.
3. Невозможность подделки справочника сертификатов и стоп-листа абонентов. Выполняется с помощью проверки подписи УЦ под сертификатами и стоп-листом.
4. Ключ ЭП электронных документов не должен использоваться ни для каких иных целей.
5. Ключи проверки ЭП не могут быть переданы по сети связи, к которой имеет доступ противник, без использования механизмов защиты.

II. Для обеспечения стойкости шифрования.

Для обеспечения стойкости шифрования необходимо:

- на открытые данные вычислять имитовставку в соответствии с ГОСТ 28147-89;
- формирование синхропосылки следует производить с использованием ПДСЧ;
- предусмотреть в формате данных, подлежащих шифрованию, информацию, защищающую от повторов ранее переданных сообщений.

III. Для обеспечения стойкости алгоритма выработки общего ключа на базе ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012.

Для обеспечения стойкости алгоритма выработки общего ключа на базе ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 необходимо:

- при передаче синхровектора использовать протокол, подтверждающий корректный прием на стороне получателя, а также обеспечивающий целостность и защиту от повторов;
- кроме того, абонент-отправитель должен каким-либо способом (например, в процессе реализации протокола) убедиться в том, что абонент-получатель выработал ключ, совпадающий с ключом, который выработал абонент-отправитель;
- обеспечить защиту от несанкционированного доступа (НСД) ключа обмена при его передаче в открытом виде.

1.1. Программно-аппаратные среды функционирования

СКЗИ «Рутокен ЭЦП 2.0» функционирует на следующих программно-аппаратных платформах:

Windows XP SP3/2003/Vista/2008/2008R2/7/2012/8/2012R2/8.1 (ia32, x64);

Linux;

FreeBSD;

Mac OS (для класса защиты КС1).

1.2. Условия эксплуатации

При эксплуатации АМ «РУТОКЕН ЭЦП 2.0» необходимо соблюдать меры предосторожности и, в том числе, не допускать механических воздействий (падений, сотрясений, вибрации) на АМ «РУТОКЕН ЭЦП 2.0», а также не прилагать излишних усилий при его подсоединении к порту компьютера.

Диапазон рабочих температур	От +5° до +50° С
Диапазон температур хранения	От +5° до +45° С
Допустимая относительная влажность воздуха	От 0 до 80% (без конденсата)

1.3. Аутентификация в СКЗИ «РУТОКЕН ЭЦП 2.0»

Аутентификация в СКЗИ «РУТОКЕН ЭЦП 2.0» основывается на PIN-коде пользователя, который должен состоять не менее, чем из 6 символов (до 32) с длиной алфавита не менее 10 символов. Символы могут включать в себя как буквы и цифры, так и знаки препинания и т. п., т. е. любые символы, которые можно ввести со стандартной клавиатуры. Срок действия пароля до смены не должен превышать 6 месяцев.

В зависимости от введенного PIN-кода, прошедший аутентификацию пользователь получает одну из следующих ролей, различающихся полномочиями в АМ «РУТОКЕН ЭЦП 2.0»:

- «Пользователь АМ», который имеет право менять свой PIN-код; данной ролью должны обладать конечные пользователи АМ «РУТОКЕН ЭЦП 2.0»;
- «Администратор АМ», который имеет право менять как свой PIN-код, так и PIN-код пользователя; права администратора АМ необходимы администратору АРМ ЗКИ «РУТОКЕН ЭЦП 2.0» для выполнения инициализации АМ «РУТОКЕН ЭЦП 2.0» и загрузки в него ключевой информации – см. документ «АРМ ЗКИ «РУТОКЕН ЭЦП 2.0». Правила пользования».

1.4. Требования безопасности при работе с изделием

При эксплуатации изделия категорически запрещается:

- работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный на ПЭВМ;
- оставлять аппаратный модуль «РУТОКЕН ЭЦП 2.0» без контроля, в том числе, при уходе пользователя с рабочего места;
- оставлять ПЭВМ без контроля при включенном питании;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- использовать ключи свыше срока, указанного в настоящих правилах.

2. Ключевые документы

2.1. Ключевые документы

Ключевыми документами СКЗИ являются:

- личные ключевые носители пользователей – аппаратные модули «РУТОКЕН ЭЦП 2.0», содержащие ключи шифрования, ключи ЭП, ключи проверки ЭП;
- ключевые носители для использования программно-аппаратных средств защиты от НСД, содержащие ключи аутентификации.

Информация на выведенных из действия аппаратных модулях «РУТОКЕН ЭЦП 2.0» подлежит уничтожению в соответствии с п. 2.3.

Пароли для доступа к АМ «РУТОКЕН ЭЦП 2.0» (PIN-коды) являются персональными паролями и должны сохраняться в тайне.

2.2. Хранение ключевых документов

Администратор безопасности несет ответственность за хранение ключевых носителей для ПАК защиты от НСД.

Ключевые носители пользователей должны храниться в личных сейфах или непосредственно у пользователей.

2.3. Уничтожение ключевых документов

Уничтожение ключевых документов осуществляется путем разрушения аппаратного модуля «РУТОКЕН ЭЦП 2.0» в области микроконтроллера и флэш-памяти с помощью кусачек или других инструментов.

Вместо уничтожения АМ может возвращаться производителю для низкоуровневого форматирования и последующей загрузки в АМ программного обеспечения.

На ключевые документы, подлежащие уничтожению, составляется акт.

2.4. Плановая смена ключей

Плановая смена ключевых документов производится не реже одного раза в 3 года.

Администратор безопасности не позднее, чем за месяц до плановой смены ключей, извещает пользователей о предстоящей плановой смене ключей.

Администратор безопасности на АРМ ЗКИ «РУТОКЕН ЭЦП 2.0» с помощью программного модуля АРМ ЗКИ (rtECP_ARM_MFC.exe) записывает в память АМ «РУТОКЕН ЭЦП 2.0» новую ключевую информацию и делает соответствующую отметку в «Журнале пользователей». Порядок записи ключевой информации в АМ «РУТОКЕН ЭЦП 2.0» подробно описан в документе «Программный модуль АРМ ЗКИ «РУТОКЕН ЭЦП 2.0». Правила пользования».

Пользователь должен периодически (не реже 1 раза в 6 месяцев) менять PIN-код АМ «РУТОКЕН ЭЦП 2.0».

Кроме того, периодически (не реже 1 раза в 6 месяцев) должны меняться пароли, используемые для ограничения доступа к АРМ ЗКИ «РУТОКЕН ЭЦП 2.0».

2.5. Сроки действия ключей

Срок действия

ключа ЭП – 3 года;

ключа проверки ЭП – 15 лет;

закрытого ключа обмена – 3 года;

открытого ключа обмена – 3 года.

3. Учёт СКЗИ

Учёт СКЗИ ведется по регистрационным номерам, присваиваемым каждому экземпляру СКЗИ. Для учёт СКЗИ следует фиксировать события в следующих журналах:

1. Журнал регистрации СКЗИ. В данном журнале фиксируются все регистрационные номера используемых СКЗИ, их состав, идентификационные номера автоматизированных модулей.
2. Журнал учёта ключевых документов. В данном журнале фиксируется, какие ключевые документы записываются на автоматизированный модуль.
3. Журнал назначения СКЗИ. В данном журнале указываются имена пользователей и номера соответствующих СКЗИ, выданных пользователям.

4. Компрометация ключевых документов СКЗИ «РУТОКЕН ЭЦП 2.0»

Под компрометацией ключевых документов СКЗИ «РУТОКЕН ЭЦП 2.0» понимается разглашение PIN-кодов аппаратных модулей «РУТОКЕН ЭЦП 2.0».

При компрометации СКЗИ «РУТОКЕН ЭЦП 2.0» пользователь должен немедленно прекратить работу с данным устройством и поставить в известность администратора безопасности.

По факту компрометации должно быть проведено служебное расследование с участием Администратора безопасности.

После проведения служебного расследования выполняется установленным порядком переинициализация АМ «РУТОКЕН ЭЦП 2.0». Переинициализация выполняется так же, как и при плановой смене ключей.

5. Журнал операций

Журнал операций позволяет хранить в оперативной памяти устройства информацию о последней операции электронной подписи. На специальном ключе подписи журнала операций формируется подпись журнала. Данная ЭП дает возможность удостовериться, что операция формирования подписи была проведена на данном СКЗИ.

Ключ подписи журнала операций хранится в СКЗИ «РУТОКЕН ЭЦП 2.0» и не удаляется при стандартном форматировании устройства.

6. Ведение журналов

В данном разделе приводится рекомендуемый перечень и содержание документов для Администраторов безопасности.

Ведутся следующие журналы:

1. *«Журнал регистрации администраторов безопасности»*, в котором фиксируются зарегистрированные администраторы безопасности, их заместители и доверенные представители.
2. *«Журнал событий»*, где отражаются все важные события: плановая смена ключей, факты компрометации ключевых документов, нештатные ситуации.
3. Администраторы безопасности должны также вести «*Журнал пользователей*», в котором записываются данные о выданных пользователю ключевых носителях (аппаратные модули «РУТОКЕН ЭЦП 2.0») и о нештатных ситуациях, произошедших на рабочих местах с установленными СКЗИ.

7. Инициализация АМ «РУТОКЕН ЭЦП 2.0»

Инициализация выполняется администратором безопасности на АРМ ЗКИ ««РУТОКЕН ЭЦП 2.0»».

Порядок инициализации АМ «РУТОКЕН ЭЦП 2.0» подробно описан в документе «Программный модуль АРМ ЗКИ «РУТОКЕН ЭЦП 2.0». Правила пользования».

8. Требования безопасности функционирования рабочих мест

1. Использующиеся АМ должны быть инициализированы при помощи АРМ ЗКИ «РУТОКЕН ЭЦП 2.0». Запрещается инициализировать сертифицированные АМ иными программными и аппаратными средствами, а также использовать такие АМ в работе
2. На АРМ пользователя должно использоваться только лицензионное ПО фирм-производителей. В случае необходимости использования иного программного обеспечения, его применение должно быть санкционировано администратором безопасности. В любом случае стороннее ПО не должно содержать средств разработки и отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование ПО СКЗИ.
3. Установленное на АРМ пользователя ПО не должно содержать средств разработки или отладки.
4. Для библиотеки rtPKCS11ECP.dll и исполняемого модуля АРМ (в случае его использования) пользователя должен быть обеспечен контроль целостности при помощи утилиты КБДЖ.01182.«АРМ Пользователя. Модуль контроля целостности» (Checksum). Контроль целостности должен выполняться перед каждым использованием СКЗИ. Если в процессе работы программы КБДЖ.01182.«АРМ Пользователя. Модуль контроля целостности» (Checksum) будет обнаружено несовпадение контрольных сумм, то работа с СКЗИ запрещается, до прохождения процедуры восстановления целостности ПО.
5. Восстановление целостности ПО возможно путем удаления динамической библиотеки и исполняемых файлов и драйверов, входящих в состав КБЖД.468244.073. АРМ Пользователя, КБЖД.468244.072. АРМ ЗКИ и их повторной установки с эталонного носителя.
6. Программное обеспечение СКЗИ используемое на ПЭВМ должно контролироваться с помощью сертифицированного по требованиям ФСБ России АПМДЗ, который производит расчет контрольных сумм объектов контроля до загрузки операционной системы. АПМДЗ должен вычислять контрольные суммы файлов, указанные администратором и сравнивать их с эталонными значениями (в соответствии с документом КБДЖ.468244.065 ФО) (для класса КС2).

   В случае использования для инициализации АМ программного обеспечения КБЖД.468244.072. АРМ ЗКИ (при поставке АМ, не инициализированных на производстве), целостность модуле АРМ ЗКИ также должны контролироваться при помощи сертифицированного АПМДЗ.

   В состав модулей программного обеспечения, подлежащих проверке должны быть включены исполняемые модули операционной системы, модули ПО СКЗИ, а также драйвера ПО АПМДЗ. В случае обнаружении искажений

объектов контроля работа с СКЗИ запрещается, и должна быть выполнена процедура восстановления целостности ПО в соответствии с п. 5.

7. Регламентный контроль ПО СКЗИ должен выполняться каждый раз перед включением СКЗИ, но не реже, чем один раз в сутки.
8. В случае нарушения целостности системного программного обеспечения (СПО) автоматизированного модуля (АМ) СКЗИ при работе внутренней системы контроля, пользователь должен:
    - немедленно прекратить эксплуатацию данного АМ «РУТОКЕН ЭЦП 2.0»;
    - сообщить администратору безопасности о факте нарушения целостности внутреннего ПО.

   Администратор должен вернуть АМ на производство до низкоуровнего форматирования в соответствии с п. 11 Порядок выполнения технического обслуживания, ремонт и утилизация.

   Дальнейшая эксплуатация СКЗИ «РУТОКЕН ЭЦП 2.0» с нарушенной целостностью внутреннего СПО не допускается.
9. Должны выполняться требования политики безопасности, принятой в организации, в области размещения технических средств, обрабатывающих конфиденциальную информацию.
10. На ПЭВМ с установленной программой АРМ Пользователя должны быть выполнены следующие требования:
    - на ПЭВМ должны быть установлены сертифицированные ФСБ России антивирусные средства;
    - необходимо регулярно устанавливать пакеты обновления безопасности, обновлять антивирусные базы;
    - при подключении к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX) без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов;
    - должна быть установлена только одна операционная система, правом установки и настройки которой должен обладать только администратор;
    - должна быть отключена возможность удаленного управления ОС;
    - средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты;
    - необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (системному реестру, файлам и каталогам, временным файлам, журналам системы, файлам подкачки, кэшируемой информации), неиспользуемые протоколы, сервисы и службы рекомендуется отключить;
    - средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты;
    - в BIOS ПЭВМ определяются установки, исключающие возможность сетевой загрузки. Не должны применяться ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС;
    - в настройках ПО BIOS ПЭВМ должны быть определены установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске (для класса КС2);
    - в настройках АПМДЗ необходимо включить ограничение времени на его инициализацию (минимальное время от включения ПЭВМ до получения управления АПМДЗ) (для класса КС2);

- вход в BIOS ПЭВМ должен быть защищен паролем с длиной не менее 6 символов (для класса КС2). Смена пароля должна производиться администратором не реже, чем 1 раз в 6 месяцев;
- должно быть проведено опечатывание ПЭВМ с АРМ Пользователя, исключающее возможность несанкционированного изменения его аппаратной части (для класса КС2).

Специальные требования

Должны выполняться следующие специальные требования:

1. СКЗИ «РУТОКЕН ЭЦП 2.0» необходимо устанавливать на ПЭВМ, разрешенные по требованиям информационной безопасности для обработки несекретной информации (конфиденциального характера), согласно принятой в информационной системе модели угроз (нарушителя).
2. В случае наличия в модели нарушителя возможностей по осуществлению перехвата обрабатываемой криптосредствами информации с использованием каналов побочных излучений и наводок, защита СКЗИ может быть обеспечена при установке СКЗИ на ПЭВМ, удовлетворяющие требованиям информационной безопасности СТР-К или аналогичным. При этом защита может быть обеспечена использованием оптических развязывающих устройств, устанавливаемых в тракте передачи информации (при его наличии) – линии связи, выходящей за пределы контролируемой зоны, например, конвертора среды передачи интерфейса Fast Ethernet «ANCUD MC-FX/TX-100» Фирмы «АНКАД» (КБДЖ.467113.023 ТУ).
3. В случае отсутствия в модели нарушителя возможностей по осуществлению перехвата обрабатываемой криптосредствами информации с использованием каналов побочных излучений и наводок, данное требование носит рекомендательный характер.
4. При размещении ПЭВМ с СКЗИ в помещениях, в которых присутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну и (или) установлены АС и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, АС иностранного производства, входящие в состав «Рутокен ЭЦП 2.0», должны быть подвергнуты проверкам по выявлению устройств, предназначенных для негласного получения информации.

9. Ввод СКЗИ в эксплуатацию

1. Рабочее место Администратора и Пользователя должны удовлетворять требованиям, изложенным в п. 8 данного документа.
2. Администратор и Пользователь СКЗИ должны пройти соответствующую подготовку по правилам работы с СКЗИ и изучить эксплуатационную документацию на СКЗИ.
3. В случае инициализации АМ «Рутокен ЭЦП 2.0» не на производстве, а на АРМ ЗКИ, программный модуль АРМ ЗКИ, динамическая библиотека rtPKCS11ECP.dll/librtpkcs11ecp.so устанавливаются на ПЭВМ в соответствии с документом КБДЖ.468244.072 ПП «АРМ ЗКИ «РУТОКЕН ЭЦП 2.0». Правила пользования».

4. В случае инициализации АМ «Рутокен ЭЦП 2.0» не на производстве, а на АРМ ЗКИ, Администратор выполняет инициализацию АМ «Рутокен ЭЦП 2.0» в соответствии с документом КБДЖ.468244.072 ПП «АРМ ЗКИ «РУТОКЕН ЭЦП 2.0». Правила пользования». Затем АМ «Рутокен ЭЦП 2.0» передается пользователю.
5. На рабочем месте пользователя должна быть установлена динамическая библиотека rtPKCS11ECP.dll/librtpkcs11ecp.so, утилита КБДЖ.468244.073.«АРМ Пользователя» (при необходимости использования) и утилита контроля целостности КБДЖ. 01182. «АРМ Пользователя. Модуль контроля целостности».
6. Перед первым использованием СКЗИ требуется сравнить контрольную сумму программного модуля КБДЖ. 01182. «АРМ Пользователя. Модуль контроля целостности» с эталонным значением.
7. Динамическая библиотека rtPKCS11ECP.dll/librtpkcs11ecp.so и утилита КБДЖ.468244.073.«АРМ Пользователя» должны подвергаться контролю целостности в соответствии с п. 9 документа КБДЖ.468244.073 ПП «АРМ Пользователя «Рутокен ЭЦП 2.0». Правила пользования».

10. Действия в нештатных ситуациях

Ниже приведена таблица с основным перечнем нештатных ситуаций и действиями в случае возникновения таких ситуаций.

№ п/п	Нештатная ситуация	Действия при нештатной ситуации
1.	Компрометация устройства	В случае компрометации устройства необходимо следовать действиям, описанным в п. 3 данного документа.
2.	Выход автоматизированного модуля из строя	Необходимо сообщить администратору безопасности о выходе из строя автоматизированного модуля и обеспечить его доставку администратору безопасности для выяснения причин выхода из строя.
3.	Отказы и сбои в работе средств защиты от НСД.	При отказах и сбоях в работе средств защиты от НСД, администратор безопасности, должен восстановить работоспособность средств НСД. При необходимости переустановить программно-аппаратные средства НСД.
4.	Утеря личного автоматизированного модуля.	Утеря личного автоматизированного модуля приводит к компрометации устройства.
5.	Отказы и сбои в работе программных средств вследствие не выявленных ранее ошибок в программном обеспечении.	При отказах и сбоях в работе программных средств, в следствии не выявленных ранее ошибок в программном обеспечении, необходимо остановить работу, локализовать по возможности причину отказов и сбоев и вызвать разработчика данного ПО или его представителя для устранения причин, вызывающих отказы и сбои.
6.	Отказы в работе программных средств вследствие случайного или умышленного их	При отказах в работе программных средств, в следствии случайного или умышленного их повреждения, лицо, ответственное за безопасность функционирования программных и аппаратных

	повреждения.	средств, обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке.

11. Порядок выполнения технического обслуживания, ремонт и утилизация.

АМ СКЗИ «РУТОКЕН ЭЦП 2.0» нельзя оставлять с включённым питанием дольше, чем на сутки.

В случае возникновения ситуации, требующей проведения технического обслуживания, требуется

- обратиться к представителю предприятия-изготовителя;
- уничтожить ключи пользователей, хранящиеся в АМ «Рутокен ЭЦП 2.0» при помощи форматирования утилитой «АРМ ЗКИ».
- передать неисправное устройство представителю предприятия-изготовителя;
- совместно с представителем предприятия-изготовителя определить и по возможности устранить причину отказа АМ.
- в случае невозможности устранить причину отказа АМ, следует утилизировать ключевой носитель в соответствии с п. 2.2. данного документа.