АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО ПОЛЬЗОВАТЕСЯ «РУТОКЕН ЭЦП 2.0»

(АРМ ПОЛЬЗОВАТЕЛЯ «РУТОКЕН ЭЦП 2.0»)

КБДЖ. 468244.073 ПП

Листов 15

2015 г.

Содержание

Аннотация

Данный документ содержит общую информацию по использованию АРМ пользователя «РУТОКЕН ЭЦП 2.0», входящего в состав средства криптографической защиты информации «РУТОКЕН ЭЦП 2.0», предназначенного для шифрования и расшифрования сообщений, создания и проверки электронных подписей, хэширования сообщений.

СКЗИ «РУТОКЕН ЭЦП 2.0» выпускается в двух исполнениях по классам защиты КС1, КС2.

1. Системные требования

Для функционирования ПО требуется:

- наличие библиотеки СКЗИ «РУТОКЕН ЭЦП 2.0» для используемой операционной системы;
- наличие свободного USB-порта;
- СКЗИ функционирует на программно-аппаратных платформах
  Windows XP SP3/2003/Vista/2008/2008R2/7/2012/8/2012R2/8.1 (ia32, x64);
  Linux;
  FreeBSD;
  Mac OS.
- АПМДЗ, сертифицированное по требованиям ФСБ России (для исполнения 2).

Используемые аппаратные модули должны быть инициализированы при помощи АРМ ЗКИ «РУТОКЕН ЭЦП 2.0». Запрещается инициализировать сертифицированные аппаратные модули иными программными и аппаратными средствами, а также использовать такие модули в работе.

2. Описание функционирования

АРМ пользователя позволяет выполнять криптографические операции библиотеки PKCS#11, используя ключевую информацию, хранящуюся на аппаратном модуле.

АРМ пользователя поддерживает выполнение следующих российских криптографических алгоритмов: ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ 28147-89.

АРМ пользователя позволяет работать с СКЗИ только в режиме пользователя.

АРМ пользователя предназначен для выполнения следующих функций:

- шифрование, хэширование, формирование и проверка электронной подписи в областях памяти токена;
- смена PIN-кода пользователя;
- выполнение подписи журнала операций РУТОКЕН ЭЦП 2.0.

АРМ пользователя дает возможность использовать только библиотеку rtPKCS11ECP.dll, входящую в состав сертифицированного продукта СКЗИ «Рутокен ЭЦП 2.0», и не позволяет изменять предустановленные режимы функционирования СКЗИ.

Срок действия PIN-кода пользователя не может превышать 6 месяцев. По истечении срока действия пользователю требуется обратиться к администратору безопасности для смены PIN-кода. Смена PIN-кода осуществляется в соответствии с п. 4.6 или при помощи АРМ ЗКИ «РУТОКЕН ЭЦП 2.0».

3. Ключевые документы

В качестве ключевой информации должны использоваться ключи, полученные при помощи АРМ ЗКИ «РУТОКЕН ЭЦП 2.0», входящего в состав сертифицированного продукта СКЗИ «Рутокен ЭЦП 2.0». Ключевая информация является конфиденциальной.

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

3.1.Сроки действия ключей

Срок действия ключей электронной подписи – не более трёх лет.

Срок действия ключей ключей проверки электронной подписи – не более пятнадцати лет.

Срок действия секретных ключей – не более трёх лет.

По истечении срока действия ключей АМ «РУТОКЕН ЭЦП 2.0» передается администратору безопасности.

4. Использование программы в среде ОС Windows

4.1. Запуск программы и аутентификация

АРМ пользователя реализован в виде исполняемого файла **UserARM.exe**.

Библиотека функций стандарта PKCS#11, входящая в состав СКЗИ, представлена в виде файла **rtPKCS11ECP.dll**, и должна располагаться либо в директории **C:\\Windows\System32**, либо в той же директории, что и исполняемый файл **UserARM.exe.**

Для начала работы с вставьте подсоедините устройство к слоту и запустите утилиту.

При запуске утилиты предлагается ввести PIN-код пользователя для аутентификации на СКЗИ.

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 более 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.

При попытке ввести пустой PIN-код АРМ пользователя прекращает свою работу.

Смена PIN-кода пользователя осуществляется в соответствии с п. 4.6 или при помощи АРМ ЗКИ ««РУТОКЕН ЭЦП 2.0».

Примечание. При 10 неудачных попытках ввода PIN-кода пользователя доступ к токену блокируется и использование его при помощи утилиты становится невозможным. При блокировке токен передается администратору безопасности и переформатируется при помощи АРМ ЗКИ «РУТОКЕН ЭЦП 2.0».

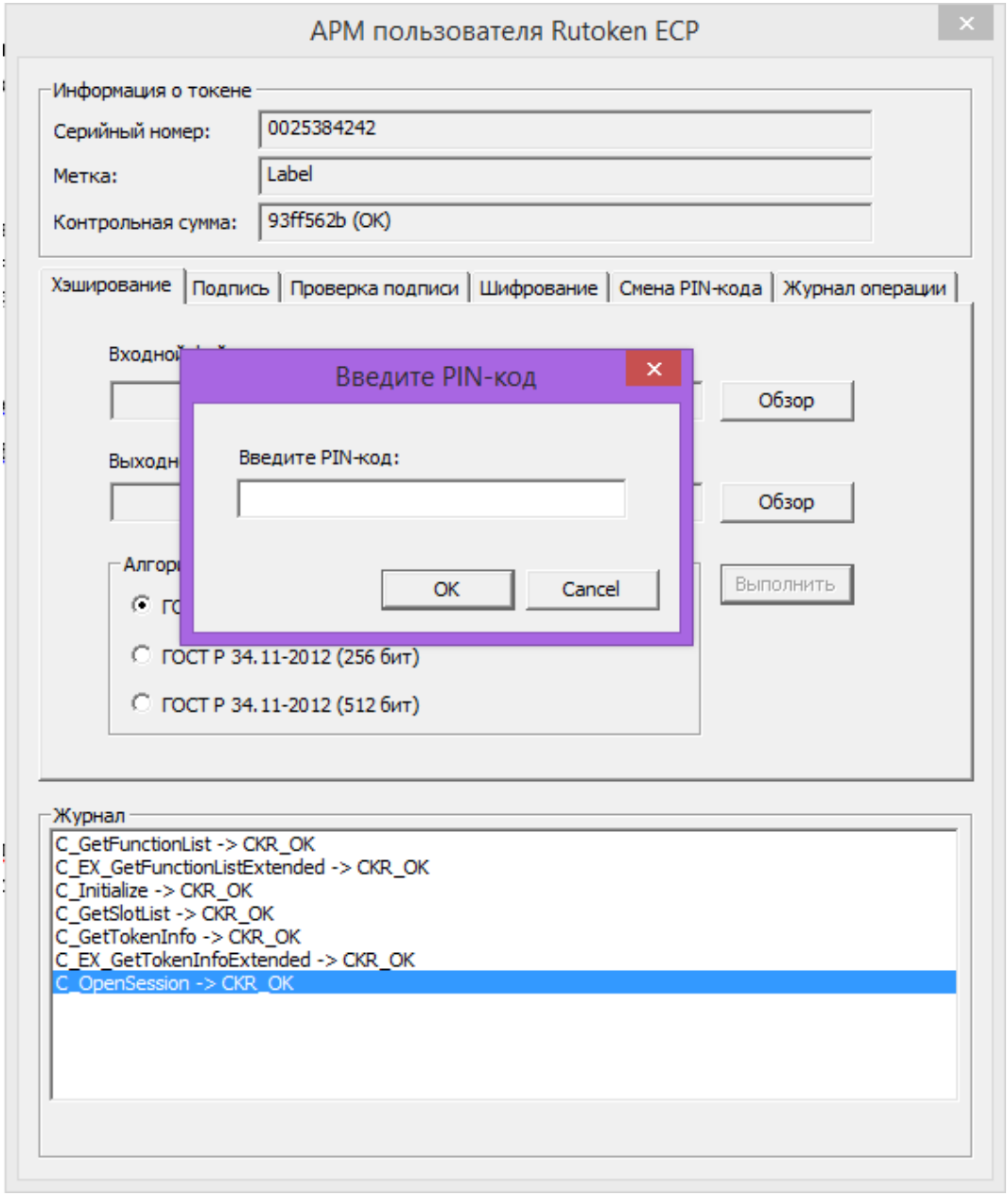


Рисунок 1

В поле **Информация о токене** можно увидеть серийный номер, метку токена и контрольную сумму микропрограммы, вычисляемую при запуске утилиты. В случае корректной суммы микропрограммы, в поле Контрольная сумма будет стоять статус **(ОК)**. При повреждении микропрограммы токена в поле находится значение

0000 (Неверная контрольная сумма).

4.2. Хэширование

Для выполнения функции хэширования сообщения требуется

- выбрать вкладку Хэширование;
- в поле **Входной файл** указать файл, содержащий сообщение;
- в поле **Выходной файл** указать имя файла, в который будет сохранен хэш;
- в поле **Алгоритм** выбрать, по какому стандарту производить вычисление значения хэш-функции: ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 (256), ГОСТ Р 34.11-2012 (512);

- нажать кнопку **Выполнить**.

Результатом выполнения функции хэширования является выходной файл с расширением *.dig, включающий в себя хэш от содержимого входного файла.

АРМ пользователя не позволяет выполнять операцию хэширования для пустого входного файла и выдает ошибку **Некорректная длина данных**.

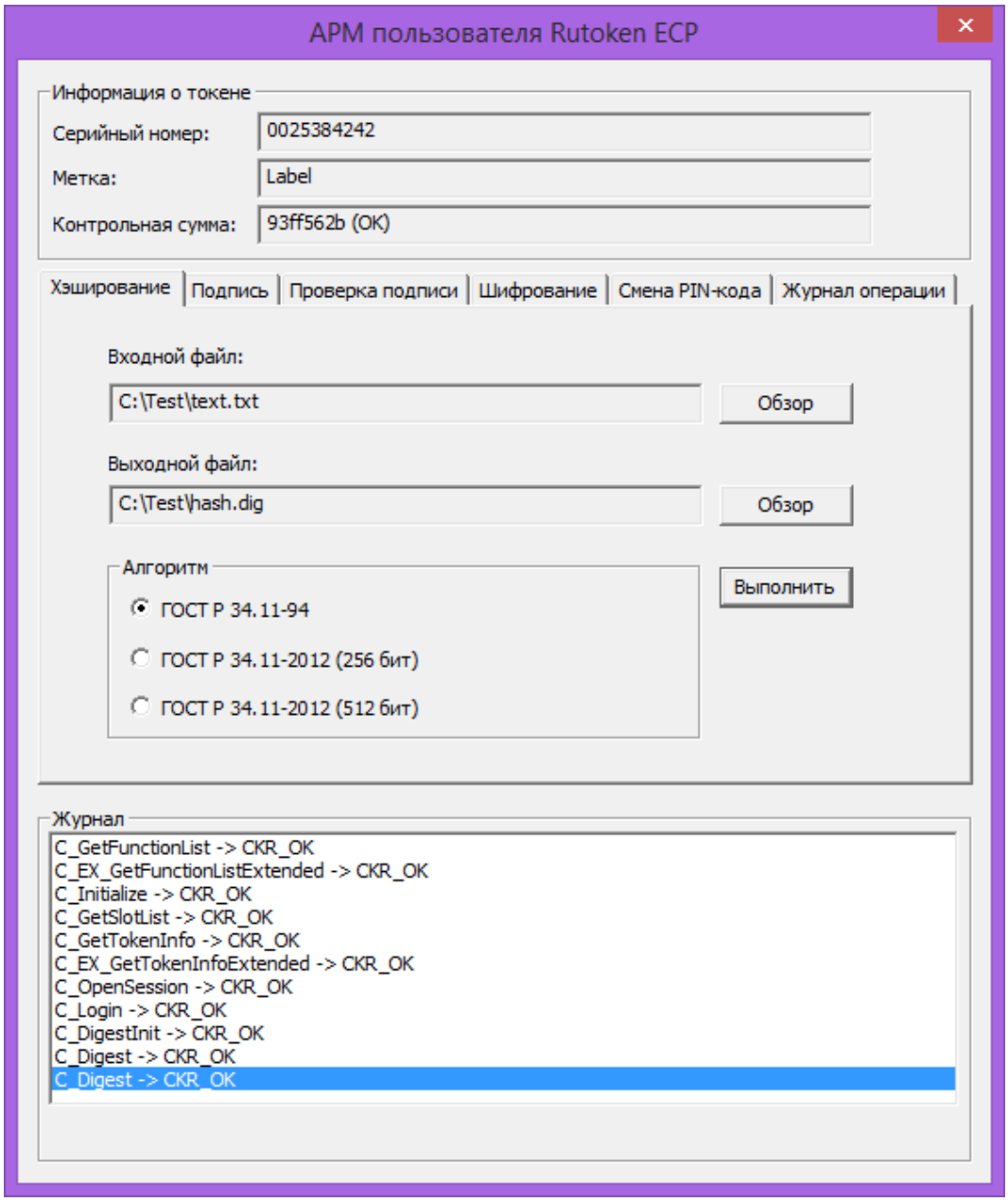


Рисунок 2

4.3. Электронная подпись

Для выполнения электронной подписи файла требуется

- выбрать вкладку **Подпись**;
- в поле **Алгоритм** выбрать ГОСТ 34.10-2001 или ГОСТ 34.10-2012;
- в поле **Ключ** выбрать ключ электронной подписи, хранящийся на токене;
- в поле **Входной файл** указать файл, содержимое которого следует подписать;
- в поле **Выходной файл** ввести имя файла, в который будет сохранена подпись;

- в поле **Алгоритм** выбрать алгоритм, по которому будет подписан файл: ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012;
- подтвердить операцию на экране устройства доверенной визуализации;
- нажать кнопку **Подписать**.

Результатом операции электронной подписи является выходной файл с расширением *.sig, включающий в себя подпись содержимого входного файла.

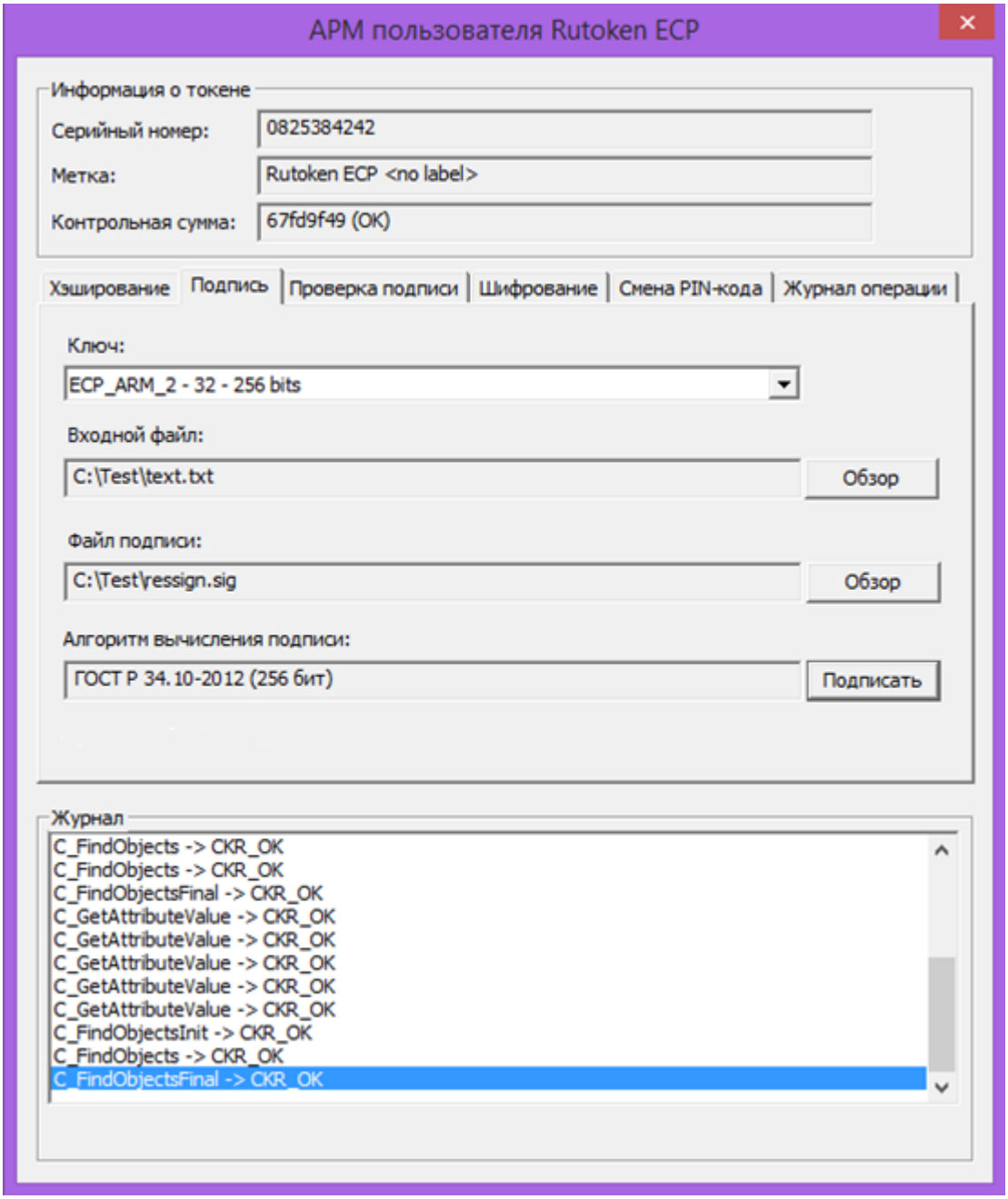


Рисунок 3

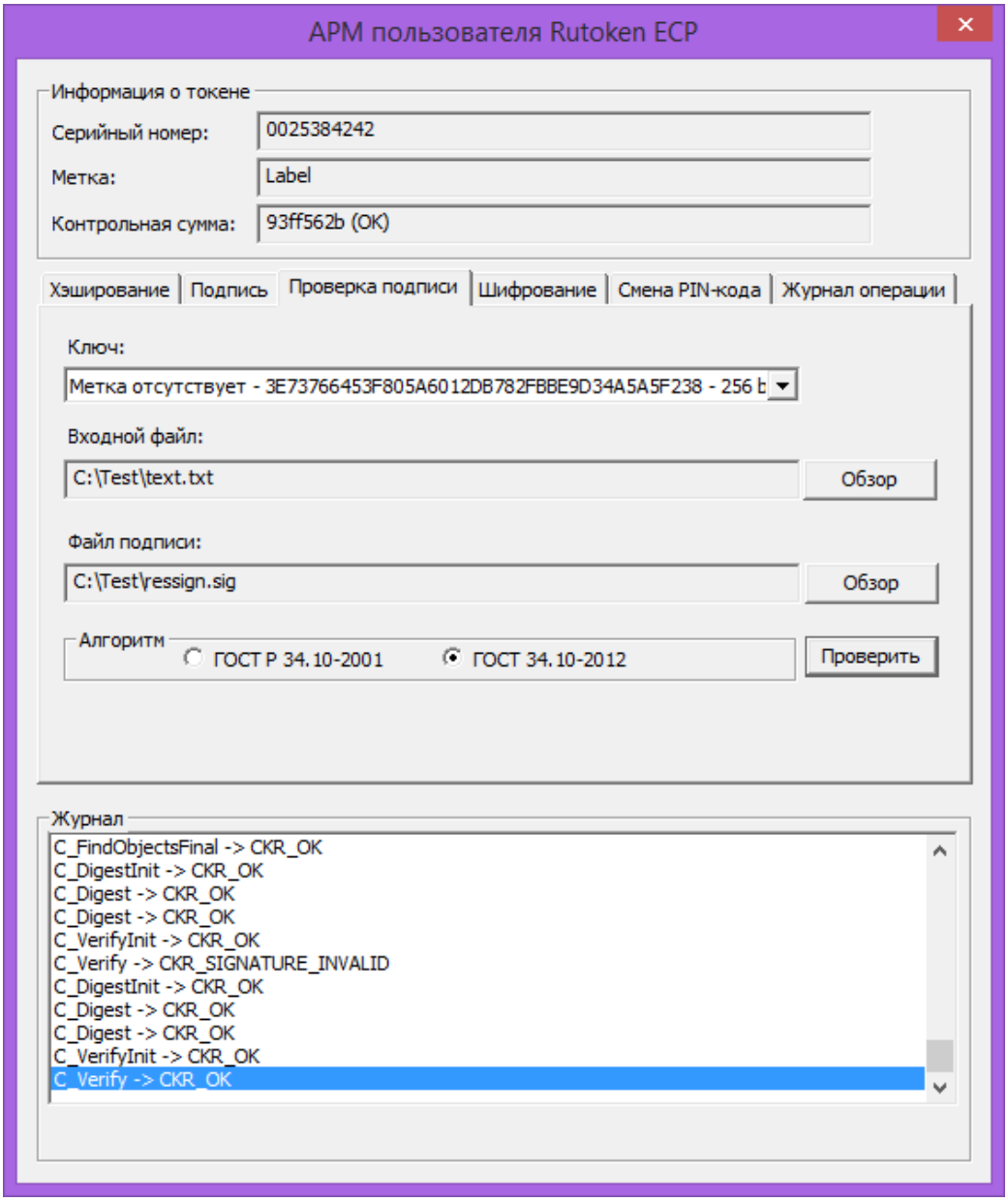
4.4. Проверка электронной подписи

Для проверки электронной подписи требуется

- выбрать вкладку **Проверка подписи**;

- в поле **Ключ** выбрать ключ проверки электронной подписи, хранящийся на токене;
- в поле **Входной файл** указать файл сообщения, для которого формировалась электронная подпись;
- в поле **Файл подписи** указать файл с расширением, содержащий подпись входного файла;
- в поле **Алгоритм** выбрать алгоритм проверки ЭП: ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012.

В результате выполнения операции проверки электронной подписи пользователю выдается сообщение с результатом проверки.



4.5. Шифрование/расшифрование

Шифрование выполняется по алгоритму ГОСТ 28147-89 в режиме гаммирования с обратной связью.

Для того, чтобы зашифровать файл по алгоритму ГОСТ 28147-89 требуется

- выбрать вкладку **Шифрование**;

- в поле **Ключ** выбрать ключ шифрования, хранящийся на токене;
- в поле **Входной файл** указать файл, который содержит исходный текст;
- в поле **Выходной файл** указать файл, в который будет записан результат операции шифрования;
- нажать кнопку **Зашифровать**.

Результатом операции шифрования является файл с расширением *.enc с зашифрованным содержимым входного файла.

Для того, чтобы расшифровать файла по алгоритму ГОСТ 28147-89 требуется

- выбрать вкладку **Шифрование**;
- в поле **Ключ** выбрать ключ шифрования, хранящийся на токене;
- в поле **Входной файл** указать файл, который содержит шифрованный текст;
- в поле **Выходной файл** указать имя файла, в который будет записан результат операции расшифрования;
- нажать кнопку **Расшифровать**.

Результатом операции расшифрования является файл, содержащий результат расшифрования входного файла.

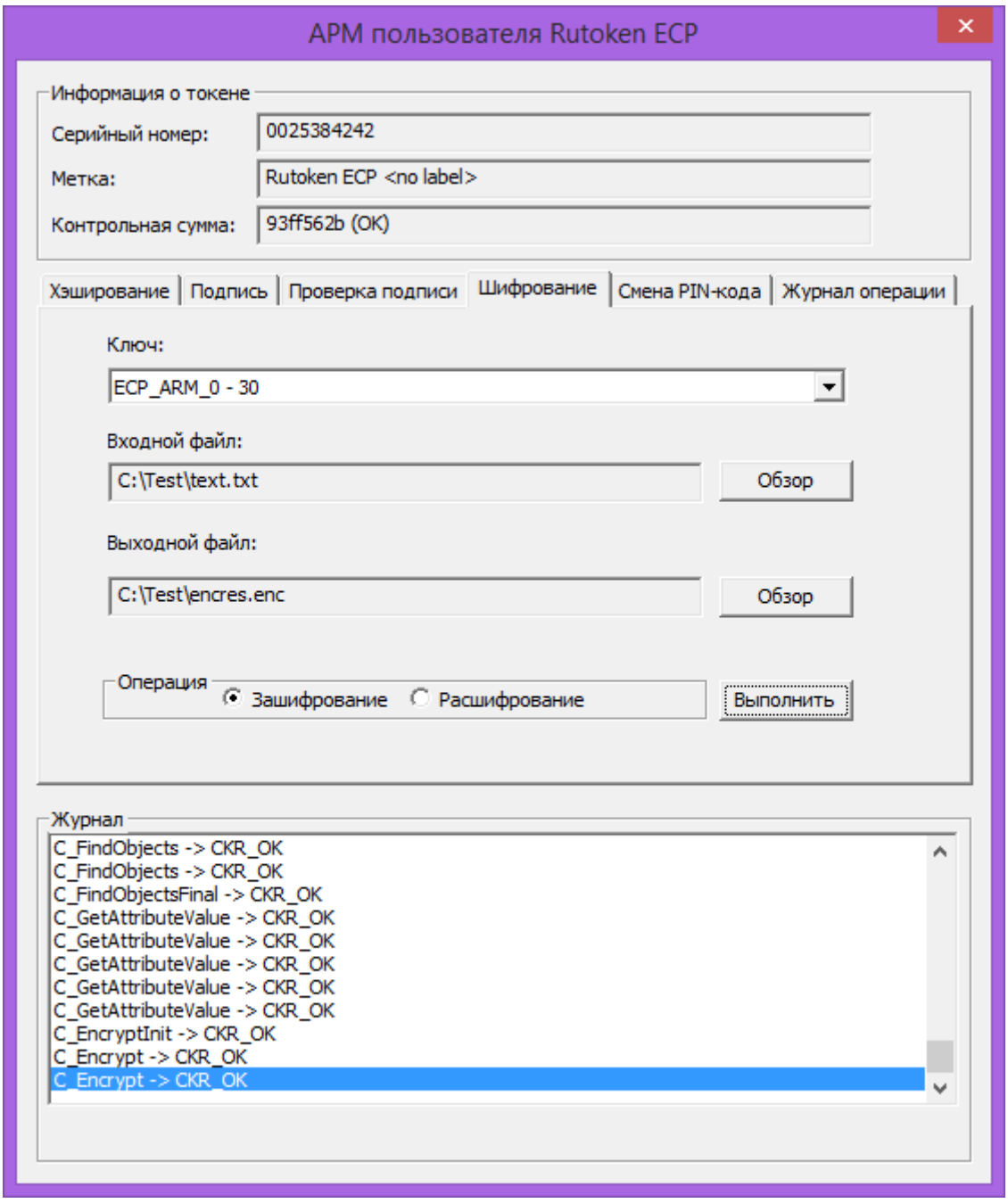
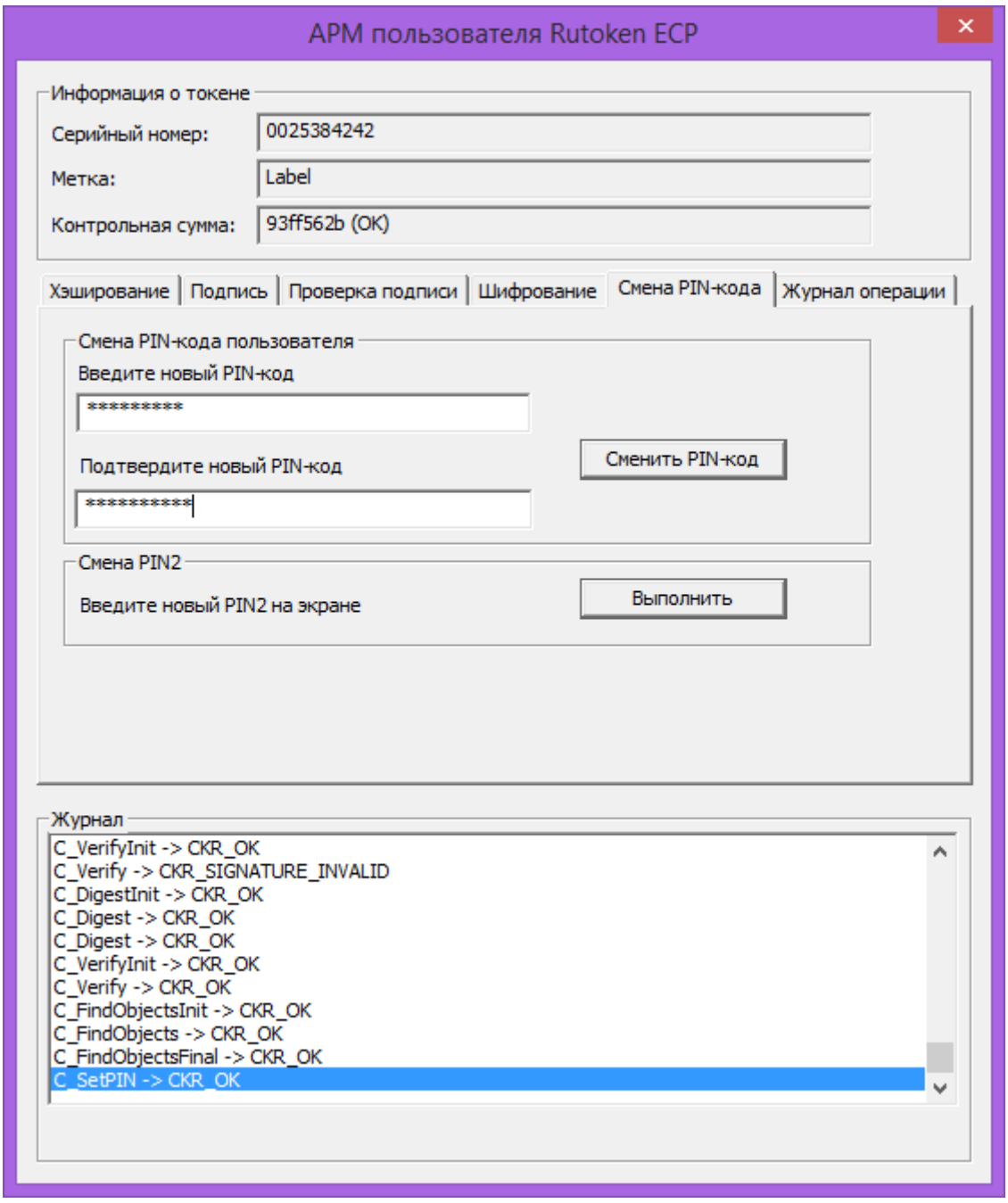


Рисунок 4

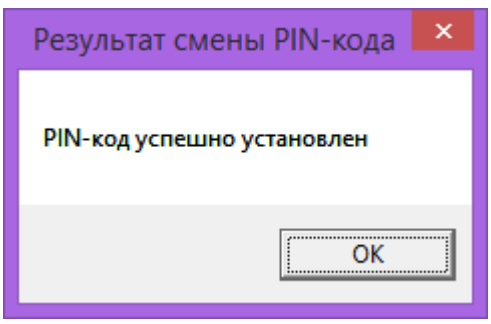
4.6. Смена PIN-кода

Для смены PIN-кода пользователя требуется:

- перейти во вкладку Смена PIN-кода;
- в поле Смена PIN-кода пользователя вести новый PIN-код в окно Введите новый PIN-код и Подтвердите новый PIN-код;
- нажать кнопку Сменить PIN-код.



При удачном выполнении операции откроется окно с сообщением



Для смены PIN2 требуется

- открыть вкладку Смена PIN-кода;

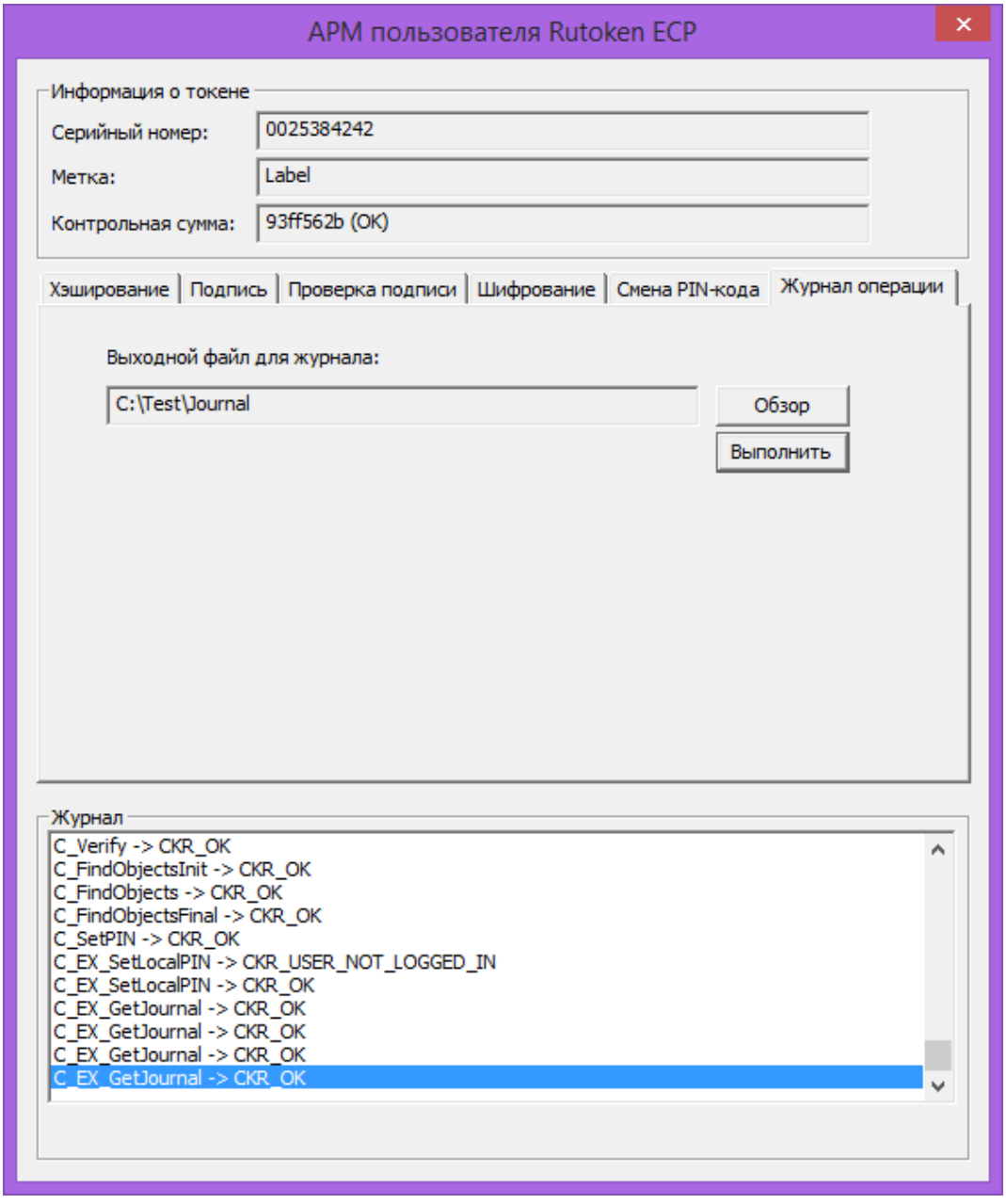
- в поле Смена PIN2 нажать кнопку Выполнить.

При удачном выполнении операции откроется окно с сообщением об успешном выполнении операции.

4.7. Журнал операций

Для получения файла журнала операций требуется:

- открыть вкладку Журнал операций;
- в поле Выходной файл для журнала ввести имя файла, в который будет сохранен журнал операций;
- нажать кнопку Выполнить.



Подпись журнала операций осуществляется в соответствии с п. 4.3.

5. Использование программы в среде ОС Linux, FreeBSD, Mac OS

5.1.Запуск программы

Для ОС Linux, FreeBSD, Mac OS АРМ Пользователя Рутокен ЭЦП 2.0 реализован в виде исполняемого файла userARM. Для его запуска необходимо перейти в папку, содержащую исполняемый файл и выполнить следующую команду:

```
./userARM [<команда> [<опции и файлы>]]
```

userARM – имя исполняемого файла;

команда – одна из возможных команд, описанных ниже, начинающаяся с «--» (ЭП, проверка ЭП, хэширование, шифрование/расшифрование, смена пин-кода);

опции – параметры команды, начинающиеся с «-»; порядок опций должен быть строго такой, как указано в описании команды;

файлы – файлы, зависящие от команды. Порядок файлов должен быть строго таким, как указано в описании команды.

Примечание: 1. Библиотека PKCS#11 должна находиться в той же директории, что и исполняемый файл АРМ Пользователя.
2. На устройстве может находиться только один ключ подписи/шифрования и один ключ подписи журнала.

5.2. Информация об устройстве

Для получения информации об устройстве необходимо выполнить команду:

```
./userARM --info
```

Результатов данной команды будет выведен на экране:

ID – уникальный идентификатор устройства;

label – метка устройства;

Checksum – контрольная сумма микропрограммы.

5.3.Хэширование

Вычисление значение хэш-функции по алгоритму ГОСТ Р 34.11-94 выполняется при помощи команды

```
./userARM --hash94 -in <infile> -out <outfile>
```

Вычисление значение хэш-функции по алгоритму ГОСТ Р 34.11-2012 длины 256 выполняется при помощи команды

```
./userARM --hash2012_256 -in <infile> -out <outfile>
```

Вычисление значение хэш-функции по алгоритму ГОСТ Р 34.11-2012 длины 512 выполняется при помощи команды

```
./userARM --hash2012_512 -in <infile> -out <outfile>
```

где

<infile> - имя входного файла, для которого необходимо вычислить значение хэш-фунции,

<outfile> - имя выходного файла с результатом работы функции с раширением *.dig.

5.4.Электронная подпись

Подпись на ключе документа на экране устройства выполняется при помощи команды

```
./userARM --signInvisible -in <infile> -out <outfile>
```

где

<infile> - имя входного файла, для которого необходимо сформировать ЭП,

<outfile> - имя выходного файла с результатом работы функции с раширением *.sig.

После ввода команды **signInvisible** необходимо ввести PIN-код пользователя.

5.5.Проверка электронной подписи

Проверка ЭП выполняется при помощи команды

```
./userARM --verify -in <infile> -out <outfile>
```

где

<infile> - имя входного файла для которого формировалась ЭП,

<outfile> - имя входного файла подписи с расширением *.sig для которого необходимо проверить ЭП,

Шифрование/расшифрование

Шифрование выполняется при помощи команды

```
./userARM --encrypt -in <infile> -out <outfile>
```

где

<infile> - имя входного файла, который необходимо зашифровать,

<outfile> - имя выходного файла с результатом работы функции.

Расшифрование выполняется при помощи команды

```
./userARM --decrypt -in <infile> -out <outfile>
```

где

<infile> - имя входного файла, который необходимо расшифровать,

<outfile> - имя выходного файла с результатом работы функции.

После ввода команды **encrypt/decrypt** необходимо ввести PIN-код пользователя.

5.6.Смена PIN-кода

5.6.1. Смена PIN-кода пользователя

Для смены PIN-кода пользователя необходимо выполнить команду

```
./userARM --changePIN
```

затем, ввести текущий PIN-код пользователя в поле:

```
Enter PIN:
```

ввести новый PIN-код пользователя в поле:

```
Enter new PIN:
```

5.7.Журнал операций

1. Получение журнала операций выполняется командой

```
./userARM --journal –out <outfile>
```

где

<outfile> - имя выходного файла, содержащего журнал.

После ввода команды необходимо ввести PIN-код пользователя в поле

```
Enter PIN:
```

2. Подпись журнала осуществляется при помощи команды

```
./userARM --signInvisible –in <infile> -out <outfile> -journal
```

где

<infile> - файл журнала, полученного на предыдущем шаге;

<outfile> - выходной файл с результатом операции подписи.

После ввода команды необходимо ввести PIN-код пользователя в поле

```
Enter PIN:
```

3. Проверка подписи журнала осуществляется при помощи команды

```
./userARM --verify -in <infile> -out <outfile>
```

где

<infile> - имя входного файла журнала, полученного при помощи команды **journal,**

<outfile> - имя файла с результатом работы функции подписи журнала.

После ввода команды необходимо ввести PIN-код пользователя в поле

```
Enter PIN:
```

6. Возвращаемые коды ошибок

Сообщения об ошибках при работе с программой выдаются пользователю в MessageBox, ниже приведена таблица соответствия данных сообщений возвращаемым значениям функций интерфейса PKCS#11.

Сообщение MessageBox	**Возвращаемое значение функции стандарта PKCS#11**	**Комментарии**
Ошибка токена	CKR_DEVICE_ERROR	Ошибка токена в процессе выполнения операции.
Некорректная длина данных	CKR_DATA_LEN_RANGE CKR_ENCRYPTED_DATA_LEN_RANGE	На вход поданы данные некорректной длины.
Неправильные данные	CKR_DATA_INVALID CKR_ENCRYPTED_DATA_INVALID	Подписываемые данные не соответствуют формату выбранного ключа
Функция не разрешена для данного ключа	CKR_KEY_FUNCTION_NOT_PERMITTED	Атрибуты ключа не позволяют использовать его для данной функции.
Подпись неверна	CKR_SIGNATURE_INVALID	Проверяемая подпись не соответствует выбранному сообщению
Неправильный пин-код	CKR_PIN_INCORRECT	Пин-код введен неверно.
Пин-код заблокирован	CKR_PIN_LOCKED	Пользователь превысил допустимое число ввода неверного пароля.
Некорректная длина подписи	CKR_SIGNATURE_LEN_RANGE	Файл, содержащий подпись, которую требуется проверить, выбран неверно.
Токен отсутствует	CKR_TOKEN_NOT_PRESENT	Токен не вставлен в слот.
Внутренняя ошибка	CKR_SESSION_HANDLE_INVALID CKR_ARGUMENTS_BAD	Токен был удален из слота до выполнения операции / Ошибка аргументов.
Не обнаружено ни одного токена		Токен не вставлен в слот.

Не удалось прочитать файл		Файл недоступен для чтения, либо файл пустой.
Не удалось записать файл		Файл недоступен для записи.

7. Журнал событий

В журнале сохраняется детальная информация о событиях, связанных с работой токена, результаты данных событий: выполняемая функция интерфейса PKCS#11, возвращаемое значение функции. Запись в журнал ведется в фоновом режиме и выводится на панель АРМ пользователя.

8. Требования безопасности функционирования утилиты

Пользователь несет персональную ответственность за сохранность ключевой информации, содержащейся на токене.

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.

На АРМ пользователя с установленной утилитой должно быть установлено только лицензионное программное обеспечение и обеспечено их своевременное обновление.

Установленное на АРМ пользователя ПО не должно содержать средств разработки или отладки.

На АРМ пользователя с установленной утилитой должно быть установлено средство антивирусной защиты, сертифицированное по требованиям ФСБ России.

При эксплуатации АРМ пользователя на ПЭВМ должна быть организована аутентификация пользователя средствами операционной системы. Должна быть разработана политика назначения с смены паролей для входа в операционную систему.

Для библиотеки rtPKCS11ECP.dll и исполняемого модуля АРМ пользователя должен быть обеспечен контроль целостности: перед первым запуском ПО СКЗИ необходимо сверить контрольные суммы, находящиеся в файле установленного ПО Checksum.exe с эталонными контрольными суммами, указанными в формуляре. Если в процессе работы программы Checksum.exe будет обнаружено несовпадение контрольных сумм, то работа с СКЗИ запрещается, до прохождения процедуры восстановления целостности ПО. Контроль целостности должен выполняться при каждом запуске ПО.

Восстановление целостности ПО возможно при помощи повторной установки.

Должны выполняться требования политики безопасности, принятой в организации, в области размещения технических средств, обрабатывающих конфиденциальную информацию.

8.1. Специальные требования

Должны выполняться следующие специальные требования:

1. СКЗИ необходимо устанавливать на ПЭВМ, допущенные 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 пользовательской информации с использованием каналов побочных излучений и наводок, защита СКЗИ по уровню КС требований [5] может быть обеспечена при установке СКЗИ на ПЭВМ, удовлетворяющие требованиям информационной безопасности, например, СТР-К. При этом защита, например, может быть обеспечена при использовании 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).
   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.
3. Запрещается использование СКЗИ в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну или конфиденциального характера, без проведения его специальных исследований и специальной проверки.

9. Контроль целостности

Для обеспечения контроля целостности модулей (для уровня защиты КС1) используется утилита контроля целостности Checksum.exe, входящая в состав дистрибутива СКЗИ «Рутокен ЭЦП 2.0». Проверка осуществляется в соответствии с алгоритмом хэширования ГОСТ Р 34.11-94.

Утилита контроля целостности представляет собой приложение командной строки .

Перед запуском утилиты необходимо создать файл, содержащий хэш-значения контролируемых файлов (UserARM.exe, rtPKCS11ECP.dll, Checksum.exe) и пути к ним: в начале строки указывается предварительно вычисленное значение хэш-функции, печатается два пробела, затем указывается путь к файлу, для которого вычислялся хэш, например:

```
50c7ef376e75368fccafa00d197ef93bb9bcb5c0571d4ed31776f6d7401ace35
C:\\Windows\System32\rtPKCS11ECP.dll
```

Для выполнения проверки утилита Checksum.exe запускается в командной строке ОС Windows при помощи команды

```
>Checksum.exe file
```

Где **file** – путь к файлу, содержащему значения хэш-функций и пути к файлам.

Результатом будет заново вычисленное значение хэш-функции для указанных модулей и результат его сравнения со значением, прописанным в созданном файле.

В случае использования утилиты под ОС типа *nix **file** должен формироваться редактором, поддерживающим unix-переносы строк. На таких ОС утилита имеет имя

checksum. Путь в файле **file** должен прописываться с учётом программно-аппаратной платформы.

Для уровня защиты КС2 исполняемый модуль UserARM.exe/UserARM и динамическая библиотека rtPKCS11ECP.dll/librtpkcs11ecp.so должны быть охвачены контролем целостности с помощью АПМДЗ, сертифицированного по требованиям ФСБ России, в соответствии с требованиями эксплуатационной документации на АПМДЗ.