УТВЕРЖДЕН
АКСФ.501490.008 ТУ-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС АУТЕНТИФИКАЦИИ И ХРАНЕНИЯ ИНФОРМАЦИИ «РУТОКЕН» версии 4

Технические условия

АКСФ.501490.008 ТУ

Листов 51

Москва, 2021

Оглавление

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ТУ	Технические условия
ЭЦП	Электронная цифровая подпись

ВВЕДЕНИЕ

Настоящие технические условия (ТУ) распространяются на программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4 (далее по тексту - ПАК «Рутокен» v. 4, Изделие).

ПАК «Рутокен» v. 4 является программно-техническим средством аутентификации пользователей и предназначен для выполнения функций по защите информации, может применяться в значимых объектах критической информационной инфраструктуры 1 категории[1], в государственных информационных системах 1 класса защищенности[2], в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности[3], в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных[4], в информационных системах общего пользования II класса[5] для реализации следующих мер:

– многофакторная аутентификация пользователей и\или администраторов в информационных системах (меры ИАФ.1 в части идентификации по имени пользователя и аутентификации по паролю пользователя, ИАФ.2 в части идентификации устройств в информационной системе, ИАФ.4 в части изменения аутентификационной информации (средств аутентификации), ИАФ.6 в части идентификации и аутентификации внешних пользователей, ЗСВ.1 в части идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре и их усиления);

[1] В соответствии со статьей 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, №31, ст. 4736) и Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

[2] В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утверждены приказом ФСТЭК России от 11.02.2013 г. № 17).

[3] В соответствии с «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (приказ ФСТЭК России № 31 от 14.03.2014 г.).

[4] В соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены Приказом ФСТЭК России от 18.02.2013 г. № 21).

[5] В соответствии с «Требования о защите информации, содержащейся в информационных системах общего пользования» (утверждены Приказом ФСТЭК России от 31.08.2010 г. № 416/489).

- управление доступом субъектов доступа к объектам доступа (меры УПД.2 в части реализации ролевого разграничения доступа, УПД.6 в части ограничения количества неуспешных попыток входа в информационную систему).

ПАК «Рутокен» v. 4 состоит из следующих компонентов:

- ПО Панель управления Рутокен
- электронный идентификатор «Рутокен» v. 4 в формате смарт-карты или карты microSD, или токена (usb, type-c, micro, SD) с предустановленной «Карточной операционной системой Рутокен», далее микропрограмма;
- комплект документации.

Электронный идентификатор «Рутокен» v. 4 представлен следующими моделями:

- Рутокен ЭЦП SC;
- Рутокен ЭЦП 2.0;
- Рутокен ЭЦП 2.0 2100;
- Рутокен ЭЦП PKI;
- Рутокен ЭЦП 2.0 Flash;
- Рутокен Lite;
- Рутокен S.

Предприятие-разработчик, изготовитель и заявитель на проведение сертификации: АО «Актив-софт» (юридический адрес: 115088, г. Москва, ул. Шарикоподшипниковская, дом 1, этаж 4, пом. IX, комн. 11; Фактический адрес: 115088, г. Москва, ул. Шарикоподшипниковская, дом 1, этаж 4, пом. IX, комн. 11, сайт: http://www.rutoken.ru/), имеющее лицензию на деятельность по технической защите конфиденциальной информации рег. номер 0415 (выдана ФСТЭК России 5 декабря 2005 года, действительна бессрочно), а также лицензию на деятельность по разработке и (или) производству средств защиты конфиденциальной информации рег. номер 0247 (выдана ФСТЭК России 5 декабря 2005 года, действительна бессрочно).

Пример записи обозначения продукции в документации и при заказе: **программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4.**

Краткое наименование - ПАК «Рутокен» v. 4.

Компонентный состав ПАК «Рутокен» v. 4 представлен на рисунке 1.

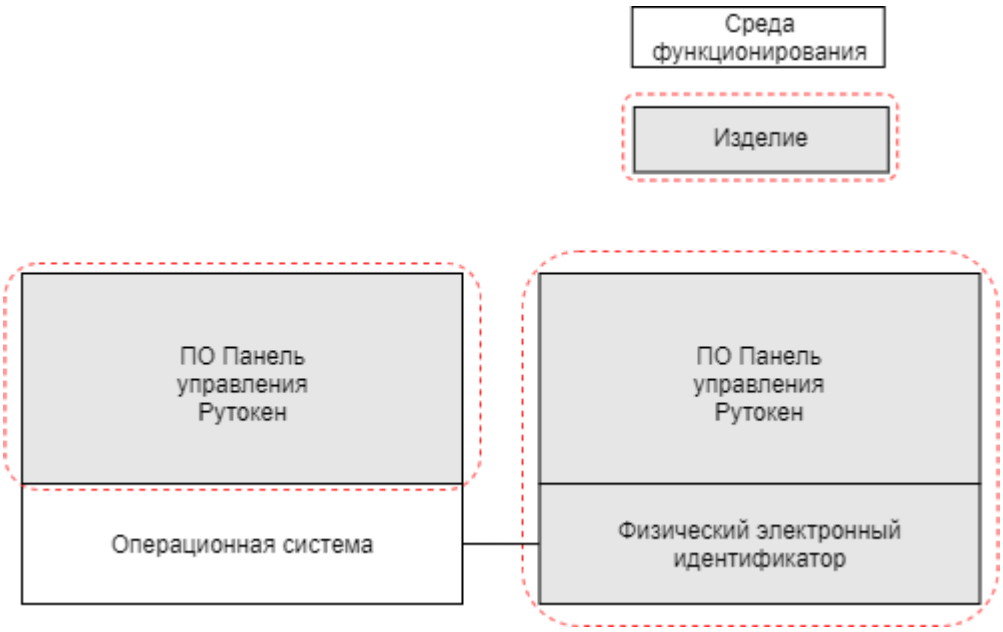


Рисунок 1 – Компонентный состав Изделия

1 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

1.1 Основные параметры и характеристики

1.1.1 ПАК «Рутокен» v. 4 должен соответствовать требованиям настоящих ТУ.

1.2 Основные параметры и характеристики (свойства)[6]

1.2.1 ПАК «Рутокен» v. 4 должен реализовывать следующие факторы аутентификации, необходимые для выполнения многофакторной аутентификации пользователей и\или администраторов в информационных системах (меры ИАФ.1 в части идентификации по имени пользователя и аутентификации по паролю пользователя, ИАФ.2 в части идентификации устройств в информационной системе, ИАФ.4 в части изменения аутентификационной информации (средств аутентификации), ИАФ.6 в части идентификации и аутентификации внешних пользователей, УПД.2 в части реализации ролевого разграничения доступа, ЗСВ.1 в части идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре и их усиления, УПД.6 в части ограничения количества неуспешных попыток входа в информационную систему):

- ПАК «Рутокен» v. 4 должен обеспечивать хранение аутентификационной информации в памяти электронного идентификатора Рутокен; ПАК «Рутокен» v. 4 должен обеспечивать программный интерфейс для выполнения операций чтения, записи и удаления над аутентификационными данными, хранящимися в памяти электронного идентификатора Рутокен[7];
- ПАК «Рутокен» v. 4 должен требовать предъявление PIN-кода пользователя при доступе к аутентификационной информации, хранящейся в памяти электронного идентификатора Рутокен; ПАК «Рутокен» v. 4 должен проверять соответствие значения предъявленного PIN-кода пользователя установленному эталонному значению PIN-кода пользователя; доступ к аутентификационной

[6] Основные параметры и характеристики, которыми должен обладать ПАК «Рутокен» v. 4, указаны в соответствии с требованиями приказов ФСТЭК России № 31 от 14 марта 2014 г. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», № 17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и № 21 от 18 февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, а также методического документа от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»).

[7] Указанная аутентификационная информация, которой владеет пользователь или администратор информационной системы, используется при реализации многофакторной аутентификации в информационной системе (обеспечивается фактор «владения»).

информации, хранящейся в памяти электронного идентификатор Рутокен, должен предоставляться только в случае совпадения значения предъявленного PIN-кода пользователя и эталонного значения PIN-кода пользователя[8].

1.2.2 ПАК «Рутокен» v. 4 должен задавать минимальное и максимальное число символов в PIN-коде в пределах от 1 до 16 символов. В PIN-коде могут использоваться символы английского и русского алфавита нижнего и верхнего регистров, десятичные цифры и символы, не принадлежащие к алфавитно-цифровому набору. При этом должна задаваться минимальная сложность PIN-кода с определяемыми требованиями к сочетанию букв верхнего и нижнего регистра, цифр и специальных символов. (ИАФ.4 в части установления характеристик пароля).

1.2.3 В ПАК «Рутокен» v. 4 должно быть установлено ограничение количества последовательных неуспешных попыток ввода PIN-кода пользователя и\или PIN-кода администратора, должно быть обеспечено блокирование электронного идентификатора «Рутокен» при превышении пользователем или администратором ограничения количества неуспешных попыток ввода PIN-кода (УПД.6 в части ограничения количества неуспешных попыток входа в информационную систему).

1.2.4 ПАК «Рутокен» v. 4 должен обеспечивать управление доступом пользователей и администраторов информационной системы, а также программных средств информационной системы к аутентификационной информации в памяти электронного идентификатора «Рутокен» и средствам управления ПАК «Рутокен» v. 4 на основе специальных наборов символов - PIN-кода пользователя и PIN-кода администратора (мера защиты УПД.2 в части реализации управления доступом на основе ролей). Правила разграничения, в соответствии с которыми ПАК «Рутокен» v. 4 должен предоставлять доступ, представлены в таблице 1.

Таблица 1

Тип учетной записи	Права доступа
Пользователь	1. изменение своего PIN-кода; 2. изменение символьного имени электронного идентификатора «Рутокен»; 3. чтение общей информации относительно электронного идентификатора «Рутокен» из системной области памяти;

[8] PIN-код пользователя применяется для подтверждения факта того, что используемая в процессе аутентификации аутентификационная информация, принадлежит пользователю или администратору информационной системы, который обладает этой информацией (фактор «знания»).

Тип учетной записи	Права доступа
Администратор	1. изменение своего PIN-кода; 2. разблокировка PIN-код пользователя; 3. чтение общей информации относительно электронного идентификатора «Рутокен» из системной области памяти. 4. форматирование электронного идентификатора «Рутокен».

1.2.5 ПАК «Рутокен» v. 4 должен требовать предъявление PIN-кода пользователя в следующих случаях:

- изменение своего PIN-кода;
- изменение символьного имени электронного идентификатора «Рутокен»;

ПАК «Рутокен» v. 4 должен проверять соответствие значения предъявленного PIN-кода пользователя установленному эталонному значению PIN-кода пользователя. Изменение PIN-кода пользователя должен быть осуществлен только в случае совпадения значения предъявленного PIN-кода пользователя и эталонного значения PIN-кода пользователя.

1.2.6 ПАК «Рутокен» v. 4 должен требовать предъявление PIN-кода администратора в следующих случаях:

- изменение своего PIN-кода;
- разблокировка PIN-код пользователя;
- форматирование электронного идентификатора «Рутокен».

ПАК «Рутокен» v. 4 должен проверять соответствие значения предъявленного PIN-кода администратора установленному эталонному значению PIN-кода администратора. Изменение PIN-кода пользователя изменение PIN-кода администратора, разблокирование электронного идентификатора «Рутокен», доступ к функциям управления должны быть осуществлены только в случае совпадения значения предъявленного PIN-кода администратора и эталонного значения PIN-кода администратора.

1.2.7 ПАК «Рутокен» v. 4 должен осуществлять идентификацию электронных идентификаторов по их логическим именам. ПАК «Рутокен» v. 4 должен обеспечивать присвоение электронному идентификатору «Рутокен» символьного имени для упрощения его визуальной идентификации (ИАФ.2 в части идентификации устройств в информационной системе).

1.3 Комплектность

1.3.1 ПАК «Рутокен» v. 4 поставляется в составе комплекта, который должен содержать следующие основные части:

- дистрибутив программного обеспечения;
- электронный идентификатор «Рутокен»;
- комплект документации.

1.3.2 Комплектация поставляемой продукции приведена в Таблице 2.

Таблица 2

Наименование	**Кол-во**	**Примечание**
Электронный идентификатор Рутокен		Количество и модель идентификатора определяется условиями договора на поставку ПАК «Рутокен» v. 4. Электронный идентификатор «Рутокен» v. 4 может быть представлен следующими моделями: – Рутокен ЭЦП SC; – Рутокен ЭЦП 2.0; – Рутокен ЭЦП 2.0 2100; – Рутокен ЭЦП PKI; – Рутокен ЭЦП 2.0 Flash; – Рутокен Lite; – Рутокен S.
Компакт-диск размещенным на нем дистрибутивом программного обеспечения: – ПО Панель управления Рутокен для 32-разрядных ОС; – ПО Панель управления Рутокен для 64-раздрядных ОС. и документацией в составе: – «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Руководство администратора, АКСФ.501490.008 90»; – «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Руководство пользователя, АКСФ.501490.008 91»; – «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Технические	1 1 1 1 1	Поставляется в электронном виде (поставляется на компакт-диске опционально, в соответствии с условиями договора на поставку)

Наименование	Кол-во	Примечание
условия АКСФ.501490.008 ТУ» – «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Формуляр АКСФ.501490.008 30»	1	
«Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Формуляр АКСФ.501490.008 30»	1	Поставляется в печатном виде
Защитный конверт компакт-диска	1	
Заверенная копия сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00)	1	Поставляется в электронном виде
Упаковочная тара.	1	Упаковочная тара состоит из коробки
Сертификат подлинности электронного идентификатора (от разработчика и изготовителя – АО «Актив–софт»)	1	Поставляется в печатном виде

Электронные идентификаторы «Рутокен» v. 4 поставляются с предустановленным программным обеспечением, приведенным ниже:

- файл rutokenst.s19, на ЭИ Рутокен ЭЦП SC;
- файл _rutokenst80.s19 на Рутокен ЭЦП 2.0 2100;
- файл USB_Firmware_ARM_17_ECP_CERT_uv3.hex, Рутокен ЭЦП 2.0;
- файл rutokenst80.s19, Рутокен ЭЦП PKI;
- файл USB_Firmware_ARM_43_ECP_CERT_uv3.hex, Рутокен ЭЦП 2.0 Flash;
- файл rutoken.cap, Рутоке Lite SD;
- файл RUTOKEN_S_REL.hex, Рутокен S;
- файл USB_Firmware_ARM_13_lite_FSTEK_uv3.hex, Рутокен Lite.

1.3.3 Контрольные суммы дистрибутива ПАК «Рутокен» v. 4 рассчитаны по алгоритму «Уровень-1, программно» с использованием программы фиксации исходного состояния программного комплекса «ФИКС» (версия 2.0.2), имеющей сертификат соответствия № 1548, выдан ФСТЭК России 15 января 2008 года, действителен до 15 января 2020 г.), приведены в таблице 3.

Таблица 3

№ пп	Имя файла	КС
Каталог \Linux\x86\		
1	rtAdmin	ba93a75d
Каталог \Linux\x86\pkicore\include\rutoken\		
2	pki-core-cpp.h	ea47ffbc
Каталог \Linux\x86\pkicore\lib\		
3	libpki-core.so.1.1.0	713376d2
4	librtpkcs11ecp.so	f73f161f
Каталог \Linux\x86\plugin\		
5	libnpCryptoPlugin.so	df50c6d9
6	librtpkcs11ecp.so	f73f161f
Каталог \Linux\x86\rtpkcs11ecp\		
7	librtpkcs11ecp.so	f73f161f
8	cryptoki.h	25a5c72d
Каталог \Linux\x86\rtpkcs11ecp\include\		
9	pkcs11.h	cf0e4b88
10	pkcs11f.h	ddb513a5
11	pkcs11t.h	31bcf4bf
12	rtpkcs11.h	1fea107c
13	rtpkcs11f.h	0b314af0
14	rtpkcs11t.h	14a6a55d
Каталог \Linux\x86_64\		
15	rtAdmin	6a700e35
Каталог \Linux\x86_64\pkicore\include\rutoken\		
16	pki-core-cpp.h	ea47ffbc
Каталог \Linux\x86_64\pkicore\lib\		
17	libpki-core.so.1.1.0	9d6f7fd0
18	librtpkcs11ecp.so	43c77caa
Каталог \Linux\x86_64\plugin\		
19	libnpCryptoPlugin.so	abaaa076
20	librtpkcs11ecp.so	43c77caa
Каталог \Linux\x86_64\rtpkcs11ecp\		
21	librtpkcs11ecp.so	43c77caa
Каталог \Linux\x86_64\rtpkcs11ecp\include\		
22	cryptoki.h	25a5c72d
23	pkcs11.h	cf0e4b88
24	pkcs11f.h	ddb513a5
25	pkcs11t.h	31bcf4bf
26	rtpkcs11.h	1fea107c
27	rtpkcs11f.h	0b314af0
28	rtpkcs11t.h	14a6a55d
Каталог \Windows\drivers\		
29	rtDrivers.exe	ee28954a
30	rtDrvRemover.exe	38887f3d
Каталог \Windows\plugin\		
31	RutokenPlugin.msi	51501479

Каталог \Windows\x86\		
32	rtAdmin.exe	d6783803
33	rtDrivers.x86.msi	ef2a7785
Каталог \Windows\x86\pkicore\include\rutoken\		
34	pki-core-cpp.h	ea47ffbc
Каталог \Windows\x86\pkicore\lib\		
35	pki-core.dll	3732f92f
36	pki-core.lib	e0ab22bc
37	rtpkcs11ecp.dll	91cf181c
Каталог \Windows\x86\rtpkcs11ecp\		
38	rtpkcs11ecp.dll	91cf181c
Каталог \Windows\x86\rtpkcs11ecp\include\		
39	cryptoki.h	25a5c72d
40	pkcs11.h	cf0e4b88
41	pkcs11f.h	ddb513a5
42	pkcs11t.h	31bcf4bf
43	rtpkcs11.h	1fea107c
44	rtpkcs11f.h	0b314af0
45	rtpkcs11t.h	14a6a55d
Каталог \Windows\x86_64\		
46	rtAdmin.exe	fd77cd03
47	rtDrivers.x64.msi	dcb1ef72
48	rtpkcs11ecp.dll	29727f93
Каталог \Windows\x86_64\pkicore\include\rutoken\		
49	pki-core-cpp.h	ea47ffbc
Каталог \Windows\x86_64\pkicore\lib\		
50	pki-core.dll	44dd7dca
51	pki-core.lib	23730dd2
52	rtpkcs11ecp.dll	29727f93
Каталог \Windows\x86_64\rtpkcs11ecp\		
53	rtpkcs11ecp.dll	29727f93
Каталог \Windows\x86_64\rtpkcs11ecp\include\		
54	cryptoki.h	25a5c72d
55	pkcs11.h	cf0e4b88
56	pkcs11f.h	ddb513a5
57	pkcs11t.h	31bcf4bf
58	rtpkcs11.h	1fea107c
59	rtpkcs11f.h	0b314af0
60	rtpkcs11t.h	14a6a55d

Контрольные суммы файлов программного обеспечения электронных идентификаторов рассчитаны по алгоритму «Уровень-1, программно» с использованием программы фиксации исходного состояния программного комплекса «ФИКС» (версия 2.0.2), имеющей сертификат соответствия № 1548, выдан ФСТЭК России 15 января 2008 года, действителен до 15 января 2020 г.), приведены в таблице 4.

Таблица 4

№ пп	Имя файла	КС
1	rutoken.cap	b5397c06
2	_rutokenst80.s19	782a911a
3	rutokenst.s19	df66d253
4	rutokenst80.s19	0788886f
5	USB_Firmware_ARM_17_ECP_CERT_uv3.hex	1c0fe7af
6	USB_Firmware_ARM_43_ECP_CERT_uv3.hex	130d629e
7	RUTOKEN_S_REL.hex	fe2cc35d
8	USB_Firmware_ARM_13_lite_FSTEK_uv3.hex	fe0edd02

Контрольные суммы неизменяемых файлов установленного ПАК «Рутокен» v. 4, рассчитанные программой фиксации и контроля исходного состояния программного комплекса «ФИКС 2.0.2» по алгоритму «Уровень-1, программно», имеющей сертификат соответствия № 1548, выдан ФСТЭК России 15 января 2008 года, действителен до 15 января 2020 г.), приведены в приложении А.

1.3.4 На ПАК «Рутокен» v. 4 должна быть разработана эксплуатационная документация в следующем составе:

- «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Формуляр», АКСФ.501490.008 30 01;
- «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Описание применения», АКСФ.501490.008 31;
- «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Руководство администратора», АКСФ.501490.008 90;
- «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Руководство пользователя», АКСФ.501490.008 91.

1.3.5 На ПАК «Рутокен» v. 4 должна быть разработана программная документация в следующем составе:

- «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Спецификация», АКСФ.501490.008;
- «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Описание программы», АКСФ.501490.008 13.

1.4 Требования к документации

1.4.1 В состав документации Изделия должны входить:

- Технические условия, содержащие полный комплекс требований к продукции, ее изготовлению, приемке, а также методы, средства и оборудование,

применяемое при контроле. Документ должен быть разработан с учетом требований ГОСТ 2.114-2016.

- Формуляр, содержащий общие сведения о программе, основные характеристики, комплектность, свидетельство о приёмке, свидетельство об упаковке и маркировке, гарантийные обязательства, сведения о рекламациях. Документ должен быть разработан с учетом требований ГОСТ 19.501-78.
- Руководство администратора, содержащее описание действий по приемке Изделия, действий по безопасной установке и настройке Изделия, действий по реализации функций безопасности среды функционирования Изделия.
- Руководство пользователя, содержащее описание режимов работы Изделия, принципов безопасной работы Изделия, описание функций и интерфейсов функций Изделия, доступных каждой роли пользователей, описание параметров (настроек) безопасности Изделия, доступных каждой роли пользователей, и их безопасных значений, описание типов событий безопасности, связанных с доступными пользователю функциями Изделия, описание действий после сбоев и ошибок эксплуатации Изделия.

1.4.2 Документация, входящая в комплект поставки потребителю, не должна иметь дефектов после изготовления и должна соответствовать подлинникам документации, хранящимся в архиве разработчика документации.

1.5 Маркировка и упаковка

1.5.1 Маркирование ПАК «Рутокен» v. 4 осуществляется изготовителем с помощью нанесения на корпус изделия и/или нерабочую сторону диска уникального идентификатора средства защиты информации (далее идентификатор СЗИ).

1.5.2 Идентификатор СЗИ является уникальным и имеет следующий вид:
РОСС RU.01.[номер сертификата].[заводской номер]

- [номер сертификата] – номер сертификата соответствия ПАК «Рутокен» v. 4;
- [заводской номер] – уникальная последовательность групп букв и цифр.

1.5.3 Заводской номер электронного идентификатора имеет следующий вид «[серия] [номер] [модификация]», например: «4500 0912345678 32G».

1.5.4 Заводской номер компакт-диска имеет следующий вид «D-[номер]», например: «D-0912345678».

1.5.5 Компакт-диск с размещенным на нём дистрибутивом ПАК «Рутокен» v. 4 и комплектом документации должен упаковываться в защитный конверт, а весь комплект изделия – в коробку.

1.5.6 Маркировка компакт-диска ПАК «Рутокен» v. 4 должна быть нанесена на лицевую (нерабочую) сторону и должна содержать:

- товарный знак предприятия-изготовителя;
- наименование продукции;
- идентификатор СЗИ.

1.5.7 Маркировка электронных идентификаторов из состава ПАК «Рутокен» v. 4 должна содержать идентификатор средства защиты информации.

1.5.8 Идентификатор средства защиты информации Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 размещается в документе «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4». Формуляр».

1.6 Требования к среде функционирования

К аппаратному и программному обеспечению, которые используются для установки Изделия, предъявляются минимальные требования, изложенные в таблице 5.

Таблица 5 – Минимальные требования к программному и аппаратному обеспечению

Таблица 5

Элемент	**Параметр**
Операционная система	ОС Microsoft Windows 8.1 (32/64-bit), ОС Microsoft Windows 10 (32/64-bit), ОС Альт Сервер 8 (32/64-bit), ОС Альт Рабочая станция 8 (32/64-bit), ОС Альт Образование 8 (32/64-bit), ОС Альт Линукс СПТ 7 (32/64-bit), ОС Альт 8 СП (32/64-bit), EMIAS OS 1.0, ОС Astra Linux Special Edition (РУСБ.10015-01) (32/64-bit), ОС Astra Linux Common Edition (32/64-bit)
Процессор	1 ГГц с архитектурой для всех версий ОС,
Оперативная память	2 Гб
Жесткий диск (свободное пространство)	20 МБ

2 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

Специальных требований при изготовлении, испытаниях, транспортировании, хранении, эксплуатации и утилизации ПАК «Рутокен» v. 4 не предъявляется.

3 ТРЕБОВАНИЯ ОХРАНЫ ОКРУЖАЮЩЕЙ СРЕДЫ

Специальных требований при изготовлении, испытаниях, транспортировании, хранении, эксплуатации и утилизации ПАК «Рутокен» v. 4 по допустимым химическим и биологическим воздействиям на окружающую среду не предъявляется.

4 ПРАВИЛА ПРИЕМКИ

4.1 Общие положения.

4.1.1 Для осуществления контроля и приемки ПАК «Рутокен» v. 4 проводятся приемо-сдаточные испытания.

4.1.2 Для осуществления контроля характеристик ПАК «Рутокен» v. 4 в процессе эксплуатации проводятся периодические испытания.

4.1.3 Испытания ПАК «Рутокен» v. 4 проводятся до полного их завершения вне зависимости от результатов промежуточных испытаний. Испытания могут быть прекращены только в случае несоответствия образца требованиям разработанной на него документации. К началу проведения испытаний должны быть завершены мероприятия по подготовке испытаний, предусматривающие:

- полную проверку готовности мест проведения испытаний по обеспечению испытаний;
- полное наличие, годность и готовность средств материально-технического обеспечения, гарантирующих создание условий и режимов испытаний;
- создание необходимых условий для проведения испытаний.

4.1.4 При проведении испытаний ПАК «Рутокен» v. 4 могут применяться следующие методы:

- экспертно-документальный метод;
- проверка отдельных функций ПАК «Рутокен» v. 4 с помощью тестирующих средств, а также путем их пробного запуска и наблюдения за их выполнением.

4.1.5 При проведении испытаний ПАК «Рутокен» v. 4 необходимо пользоваться терминами и определениями в соответствии с ГОСТ 16325-88, ГОСТ 16493-70, ГОСТ Р 51167-98, ГОСТ Р 51168-98, ГОСТ Р 51169-98, ГОСТ Р 51170-98, ГОСТ Р 51171-98, ГОСТ 28806-90.

4.2 Приемо-сдаточные испытания.

4.2.1 Приемо-сдаточные испытания проводятся с целью контроля соответствия ПАК «Рутокен» v. 4 требованиям настоящих ТУ.

4.2.2 Объем и последовательность приемо-сдаточных испытаний приведены в таблице 6.

Таблица 6

№ п/п	Наименования испытаний и проверок	Пункты ТУ		Виды испытаний	
		Технические требования	Методы испытаний	Приемо-сдаточные	Периодические
1	Проверка информации, записанной на компакт-диске	1.3.3	5.1	+	+
2	Проверка упаковки и маркировки	1.5	5.3	+	+
3	Проверка комплектности	1.3	5.2	+	+
4	Проверка функциональных характеристик	1.2	5.4	–	+

Примечание:

В таблице 6 приняты следующие обозначения:

- «+» - испытания проводить;
- «–» - испытания не проводить.

Результаты приемо-сдаточных испытаний можно считать положительными, а Изделие – выдержавшим испытания, если:

- контрольные суммы программных компонент, входящих в Изделие, совпадают с контрольными суммами, приведенными в Формуляре АКСФ.501490.008 30;
- упаковка соответствует требованиям 1.5 настоящих ТУ;
- комплектность поставки соответствует требованиям пункта 1.3 настоящих ТУ.

При отрицательных результатах приемо-сдаточных испытаний необходимо проводить анализ выявленных дефектов, выяснять причины, вызвавшие их появление, и принимать меры по их устранению.

Испытания Изделия проводить силами и средствами предприятия-изготовителя.

Изделие, не прошедшее приемо-сдаточные испытания, возвращать на доработку, после чего его предъявлять на приемку с пометкой «Повторно».

Изделие, не прошедшее приемо-сдаточные испытания повторно, браковать, при этом выявлять причины появления дефектов и принимать меры по их устранению.

4.3 Периодические испытания.

4.3.1 Периодические испытания проводятся с целью контроля образца ПАК «Рутокен» v. 4 на соответствие требованиям настоящих ТУ в процессе его эксплуатации.

4.3.2 Периодические испытания проводить в объеме и последовательности согласно таблице 6.

4.3.3 Периодические испытания Изделий, прошедших приемосдаточные испытания, проводить один раз в год.

4.3.4 Испытания ПАК «Рутокен» v. 4 проводятся на смонтированной аппаратуре при установленном (инсталлированном) программном обеспечении ПАК «Рутокен» v. 4.

4.3.5 Результаты периодических испытаний считают положительными, а Изделие – выдержавшим испытания, если Изделие соответствует в полном объеме требованиям настоящих Технических условий.

4.3.6 В случае неудовлетворительных испытаний Изготовитель анализирует характер дефектов, определяет причины, вызвавшие их появление, и принимает меры по их устранению. По результатам анализа принимается решение о проведении дальнейших испытаний.

5 МЕТОДЫ КОНТРОЛЯ

5.1 Общие положения.

5.1.1 На испытания ПАК «Рутокен» v. 4 должен быть предоставлен в комплектности, приведенной в таблице 2.

5.1.2 Перед проведением испытаний должен быть произведена идентификация объекта испытаний. Идентификация объекта испытаний заключается в проверке соответствия контрольных сумм программного обеспечения ПАК «Рутокен» v. 4 эталонным значениям.

5.1.3 При подготовке стенда для проведения испытаний необходимо произвести установку компонентов согласно требованиям разработанной на него эксплуатационной документации.

5.1.4 Испытания должны проводиться в нормальных климатических условиях эксплуатации средств вычислительной техники (п.1.3.2, ГОСТ 21552-84).

5.1.5 Меры безопасности обслуживающего персонала и экспертов, а также технических средств при проведении испытаний должны соответствовать требованиям ГОСТ 21552-84.

5.2 Методы проверки комплектности

5.2.1 Проверка комплектности объекта испытаний производится сравнением комплектности предъявленного к приемке экземпляра ПАК «Рутокен» v. 4 с комплектностью ПАК «Рутокен» v. 4, указанной в таблице 2 настоящих ТУ.

5.2.2 ПАК «Рутокен» v. 4 считается прошедшим испытания, если его комплектность соответствует комплектности, указанной в таблице 2 настоящих ТУ.

5.3 Методы проверки упаковки и маркировки

5.3.1 Проверку упаковки проводят путем контроля соответствия упаковки компакт-диска, с размещёнными на нём дистрибутивом ПАК «Рутокен» v. 4 и документацией, а также всего комплекта ПАК «Рутокен» v. 4, требованиям, указанным в п. 1.5.

5.3.2 ПАК «Рутокен» v. 4 считается прошедшим проверку в части упаковки, если компакт-диск, с размещёнными на нём дистрибутивом ПАК «Рутокен» v. 4 и документацией, уложен в защитный бумажный конверт, а весь комплект изделия – в коробку, что соответствует требованиям, указанным в п. 1.5 настоящих ТУ.

5.3.3 Проверку маркировки проводят путем контроля соответствия маркировки комплекта ПАК «Рутокен» v. 4, наносимой на нерабочую поверхность оптического диска, а также наличия и размещения знака соответствия требованиям, указанным в п. 1.5 настоящих ТУ.

5.3.4 ПАК «Рутокен» v. 4 считается прошедшим проверку в части маркировки, если маркировка комплекта изделия соответствует требованиям, указанным в п. 1.5 настоящих ТУ.

5.4 Проверка документации

5.4.1 Проверка документации включает:

- проверку соответствия документации требованиям п.1.4 настоящих ТУ;
- проверку комплектности документации на соответствие требованиям п. 2.2 настоящих ТУ.

5.4.2 Изделие считается выдержавшим испытания, если:

- документация разработана в соответствии с требованиями п.1.4 настоящих ТУ;
- документация комплекта поставки соответствует требованиям п. 2.2 настоящих ТУ.

5.5 Методы контроля параметров и характеристик (свойств) Изделия

5.5.1 Проверка параметров и характеристик ПАК «Рутокен» v. 4 проводится в соответствии с методикой проверки функциональных характеристик, изложенной в Приложении Б.

5.5.2 ПАК «Рутокен» v. 4 считается прошедшим испытания, если функциональные характеристики соответствуют функциональным характеристикам, указанным в п. 1.2 настоящих ТУ.

6 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ

6.1 ПАК «Рутокен» v. 4 можно транспортировать на неограниченные расстояния автомобильным, железнодорожным и авиационным видами транспорта при температуре окружающей среды от -20°С до +50°С. ПАК «Рутокен» v. 4 должен транспортироваться в упаковке Изготовителя в соответствии с требованиями ГОСТ 21552-84. Упаковка ПАК «Рутокен» v. 4 при транспортировке должна быть закреплена любым способом, исключающим ее перемещение.

6.2 ПАК «Рутокен» v. 4 должен храниться в упаковке в отапливаемых помещениях при температуре воздуха от +5°С до +40°С и относительной влажности воздуха не более 80%. В помещениях для хранения ПАК «Рутокен» v. 4 необходимо исключить возможность попадания в воздух паров агрессивных веществ (кислот, щелочей).

7 УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

7.1 Общие указания

При эксплуатации ПАК «Рутокен» v. 4 на объектах информатизации, обрабатывающих информацию ограниченного доступа, необходимо выполнение следующих ограничений:

- использование операционных систем, приведенных в пункте 1.6 настоящего документа, имеющих сертификат соответствия ФСТЭК России, или, в случае его отсутствия, дополнительно использовать средства защиты информации от несанкционированного доступа, для защиты информации ограниченного доступа;
- запрет на использования ПАК «Рутокен» v. 4 для обработки информации, содержащей сведения, составляющие государственную тайну;
- ПАК «Рутокен» v. 4» должен устанавливаться на оборудование, соответствующее требованиям, определенным в настоящем документе;
- наличие администратора безопасности, отвечающего за правильную эксплуатацию ПАК «Рутокен» v. 4;
- обеспечение физической сохранности средств вычислительной техники с установленным ПАК «Рутокен» v. 4 и исключение возможности доступа к ним посторонних лиц;
- доступ к каталогу с установленным программным обеспечением ПАК «Рутокен» v. 4 «%WINDIR%\System32\Aktiv Co\» в операционных системах семейства Windows должен быть разрешён только администратору;
- сохранение в секрете идентификаторов, PIN-кодов и паролей администраторов и пользователей ПАК «Рутокен» v. 4;
- обязательная смена PIN-кода «по умолчанию» электронных идентификаторов после их инициализации;
- проведение периодического контроля целостности ПАК «Рутокен» v. 4 с помощью программ контроля целостности (не реже одного раза в месяц);
- проведение периодической проверки на наличие актуальных уязвимостей (недостатков) в ПАК «Рутокен» v. 4 и среде его функционирования с использованием средств анализа защищенности (не реже одного раза в месяц);
- проведение периодической проверки ПАК «Рутокен» v. 4 и среды его функционирования на наличие компьютерных вирусов с использованием средств антивирусной защиты (не реже одного раза в месяц).

Для всех компонентов среды функционирования ПАК «Рутокен» v. 4 должны быть установлены все актуальные обновления программного обеспечения, а также выполнены рекомендации разработчиков по безопасному конфигурированию, либо приняты меры по защите информации, нейтрализующие уязвимости.

Установка ПАК «Рутокен» v. 4 должна осуществляться в соответствии с эксплуатационной документацией.

Каналы передачи данных ПАК «Рутокен» v. 4, расположенные в пределах контролируемой зоны, должны быть защищены организационно-техническими мерами. Для защиты каналов передачи данных ПАК «Рутокен» v. 4, выходящих за пределы контролируемой зоны, должны применяться средства криптографической защиты информации, имеющие действующий сертификат ФСБ России.

При использовании ПАК «Рутокен» v. 4 в государственных информационных системах и информационных системах персональных данных оператором информационной системы должны быть выполнены все требования к усилениям мер защиты.

Должно быть обеспечено использование протокола IPv6 или использование статической ARP-таблицы (мера направлена на нейтрализацию уязвимости BDU:2014-00018 из банка данных угроз безопасности информации ФСТЭК России).

7.2 Устранение недостатков

Предприятие-изготовитель принимает на себя обязательства по поиску и устранению недостатков в ПАК «Рутокен» v. 4 на протяжении всего жизненного цикла Изделия.

Предприятие-изготовитель осуществляет прием сообщений о недостатках от потребителей на сайте http://www.rutoken.ru/ и по телефону 8 (495) 925-7790.

Предприятие-изготовитель периодически, не реже одного раза в месяц, должно проводить поиск известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях. В качестве общедоступных источников в первую очередь должны использоваться база данных уязвимостей (далее - БДУ) в составе банка данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), а также следующие дополнительные источники:

- https://cve.mitre.org/ ,
- https://nvd.nist.gov/ ,
- https://www.exploit-db.com/ ,
- http://www.rapid7.com/db/ ,

- http://www.cvedetails.com/ ,
- http://www.securitylab.ru/ и другие.

Предприятие-изготовитель должен провести анализ выявленных уязвимостей на предмет возможности их использования для нарушения безопасности. При анализе уязвимостей необходимо учитывать следующие критерии:

- тип ошибки;
- версию программного обеспечения, подверженную уязвимости;
- уровни опасности уязвимости (критическая, высокая, средняя, низкая);
- информацию об устранении.

Процедура устранения уязвимостей ПАК «Рутокен» v. 4 должна обеспечивать возможность обновления ПО для устранения актуальных уязвимостей.

В случае выявления информации об уязвимости ПАК «Рутокен» v. 4 и сред его функционирования из различных источников и отсутствия информации об этой уязвимости в БДУ, предприятие-изготовитель предоставляет информацию о данной уязвимости в ФСТЭК России для размещения в БДУ.

Устранение недостатков должно предусматривать доведение информации о недостатках ПАК «Рутокен» v. 4, а также о компенсирующих мерах по защите информации или ограничениях по применению, а также доработку ПАК «Рутокен» v. 4, в том числе разработку обновлений ПАК «Рутокен» v. 4 или разработку мер по защите информации, нейтрализующих недостаток. Общий срок устранения недостатка ПАК «Рутокен» v. 4 не должен превышать 60 дней с момента выявления недостатка.

При выявлении уязвимостей ПАК «Рутокен» v. 4 предприятие-изготовитель должен осуществить следующие мероприятия:

- в случае отсутствия, на момент проверки информации по выявленным уязвимостям ПАК «Рутокен» v. 4, доступных релизов ПАК «Рутокен» v. 4 с устраненными уязвимостями, разработать компенсирующие меры по защите информации или ограничения по применению ПАК «Рутокен» v. 4, снижающие возможность эксплуатации уязвимостей;
- довести информацию о компенсирующих мерах и ограничениях по применению до потребителей в срок не более 48 часов с момента выявления недостатка;
- доработать ПАК «Рутокен» v. 4 или его отдельные компоненты, в том числе выпустить обновление ПАК «Рутокен» v. 4 или, в случае невозможности устранения уязвимостей ПАК «Рутокен» v. 4 путем применения обновления,

выпустить меры по защите информации, нейтрализующие недостаток и внести необходимые изменения в эксплуатационную документацию;

- провести тестирование доработанного ПАК «Рутокен» v. 4 или его отдельных компонентов на предмет влияния обновлений ПАК «Рутокен» v. 4 на его функции безопасности, подтверждения устранения уязвимостей, невнесения новых уязвимостей в ПАК «Рутокен» v. 4;
- довести информацию о недостатках ПАК «Рутокен» v. 4, о компенсирующих мерах по защите информации или ограничениях по применению, а также о выпуске обновлений ПАК «Рутокен» v. 4 или мерах по защите информации, нейтрализующих недостаток, до каждого потребителя сертифицированного ПАК «Рутокен» v. 4 путем отправки сообщений на электронные адреса потребителей;
- обеспечить гарантированную доставку обновлений ПАК «Рутокен» v. 4 потребителям;
- если уязвимость не устраняется обновлением ПАК «Рутокен» v. 4 или реализацией мер по защите информации, нейтрализующих недостаток, предприятие-изготовитель незамедлительно и гарантированно, с подтверждением, сообщает об этом всем потребителям и в ФСТЭК России. Потребители прекращают применение ПАК «Рутокен» v. 4.

Если потребитель не может выполнить установку обновления ПАК «Рутокен» v. 4 и/или реализовать меры по защите информации, нейтрализующие недостаток ПАК «Рутокен» v. 4, он прекращает его применение.

7.3 Процедура обновления

При внесении изменений в ПАК «Рутокен» v. 4 предприятие-изготовитель проводит испытания в связи с внесением изменений (при необходимости для проведения испытаний привлекается испытательная лаборатория). В случае внесения в ПАК «Рутокен» v. 4 изменений, связанных с устранением уязвимостей, процедура обновления ПАК «Рутокен» v. 4 потребителем проводится до проведения испытаний. В случае внесения в ПАК «Рутокен» v. 4 иных изменений процедура обновления ПАК «Рутокен» v. 4 потребителем возможна только при положительных результатах испытаний.

Процедура обновления должна предусматривать доведение информации о необходимости обновления ПАК «Рутокен» v. 4 и обеспечение гарантированной доставки обновлений ПАК «Рутокен» v. 4 потребителям. Доведение информации о выпуске обновлений ПАК «Рутокен» v. 4 должно осуществляться до каждого

потребителя, сертифицированного ПАК «Рутокен» v. 4 путем отправки сообщений на электронные адреса потребителей. Предприятие-изготовитель предоставляет потребителям обновления ПАК «Рутокен» v. 4 на оптическом диске.

При получении обновлений ПАК «Рутокен» v. 4 перед их установкой необходимо проверить подлинность и целостность полученных файлов обновлений. Для установки обновлений администратор безопасности должен выполнить следующие действия:

- добавить корневой сертификат, скаченный с сайта изготовителя https://ra.rutoken.ru/rootcerts, добавить его в список доверенных сертификатов ОС;
- проверить подлинность файлов обновлений при помощи присылаемой с обновлением сигнатуры, а также программным обеспечением КриптоПро или при помощи веб-сервиса https://crypto.kontur.ru/verify. Если подлинность файлов обновлений не подтверждена, необходимо обратиться в службу поддержки предприятия-изготовителя;
- провести расчет контрольных сумм файлов обновлений с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС» (версии 2.0.2) по алгоритму «Уровень-1, программно». Сравнить контрольные суммы файлов обновлений с указанными на оптическом диске. При расхождении контрольных сумм с эталонными значениями необходимо обратиться в службу поддержки предприятия-изготовителя;
- произвести установку актуальных обновлений.

8 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Предприятие-изготовитель оказывает базовую техническую поддержку ПАК «Рутокен» v. 4. В рамках базовой технической поддержки предприятие-изготовитель обеспечивает поиск, анализ и устранение недостатков ПАК «Рутокен» v. 4 на протяжении срока действия базовой технической поддержки.

Базовая техническая поддержка входит в стоимость поставляемого ПАК «Рутокен» v. 4 и обеспечивается предприятием-изготовителем. Срок базовой технической поддержки определяется сроком действия сертификата соответствия ФСТЭК России и может быть продлен по окончании срока действия сертификата соответствия.

Иные виды технической поддержки (расширения сервисов технической поддержки) предоставляются предприятием-изготовителем на возмездной основе, в соответствии с действующими политиками и правилами оказания технической поддержки продуктов предприятия-изготовителя.

Техническая поддержка ПАК «Рутокен» v. 4 осуществляется предприятием-изготовителем по адресу/телефону/электронной почте: 115088, г. Москва, ул. Шарикоподшипниковская, дом 1, этаж 4, пом. IX, комн. 11 / 8 (495) 925-7790 / info@rutoken.ru.

Об окончании производства и базовой технической поддержки ПАК «Рутокен» v. 4 предприятие-изготовитель информирует потребителей не позднее, чем за 1 год до окончания производства и поддержки следующими способами:

- публикацией соответствующей информации на сайте предприятия-изготовителя;
- направлением электронных писем на электронные почтовые адреса потребителей.

9 ГАРАНТИИ ИЗГОТОВИТЕЛЯ

9.1 Предприятие-изготовитель гарантирует соответствие ПАК «Рутокен» v. 4 требованиям ТУ при соблюдении потребителем условий и правил эксплуатации, транспортирования и хранения, установленных в эксплуатационной документации.

9.2 В случае выявления в ПАК «Рутокен» v. 4 дефектов, не связанных с нарушением правил эксплуатации, транспортирования и хранения, ПАК «Рутокен» v. 4 подлежит рекламации. Рекламации предъявляются предприятию-изготовителю. Предприятие-изготовитель обязуется при получении рекламации в возможно короткий срок принять меры по устранению дефектов.

9.3 Гарантийный срок эксплуатации ПАК «Рутокен» v. 4 – 12 месяцев (или больший срок, если это определено договором на поставку или лицензионным соглашением) со дня передачи его потребителю.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Из-менен-ие	Номера листов				Всего листов в доку-менте	Номер доку-мента	Вх. № сопровод итель-ного доку-мента и дата	Под-пись	Дата
	изме-нен-ных	заме-нен-ных	но-вых	изъ-ятых					
1	2	3	4	5	6	7	8	9	10

ПРИЛОЖЕНИЕ А. КОНТРОЛЬНЫЕ СУММЫ НЕИЗМЕНЯЕМЫХ ФАЙЛОВ

Контрольные суммы неизменяемых файлов установленного ПАК «Рутокен» v. 4.

Контрольные суммы неизменяемых файлов ОО для среды функционирования Windows x64

Неизменяемые файлы	**Значение контрольной суммы**
rutoken.cap _rutokenst80.s19 rutokenst.s19 rutokenst80.s19 USB_Firmware_ARM_17_ECP_CERT_uv3.hex USB_Firmware_ARM_43_ECP_CERT_uv3.hex RUTOKEN_S_REL.hex USB_Firmware_ARM_13_lite_FSTEK_uv3.hex	b5397c06 782a911a df66d253 0788886f 1c0fe7af 130d629e fe2cc35d fe0edd02
npCryptoPlugin.dll npRutokenPlugin.dll FireWyrmNativeMessageHost.exe	2e03a149 eadf37e8 68b34764
rtpkcs11ecp.dll rtpkcs11.dll pki-core.dll pki-core.lib rtCSP.dll rtGrTools.dll rtAPIlt.dll rtMiniDrv.dll rtAPI.dll rtAPIex.dll	695d49fd 254c7bfe 44dd7dca 23730dd2 a06d15cf 650723d7 d26387d2 75316778 de641c8f 9e3bdf94
rtcontrol_Panel.exe rterr.dll rtAPIi.dll rtlib.dll rtGrTools.dll	54afdb88 10ad518b 4ba38c10 2491fc37 650723d7
rtcontrol_Panel_Tools.exe	6e59e41b
rtDrvRemover.exe	38887f3d
rtAdmin.exe	fd77cd03

Контрольные суммы неизменяемых файлов ОО для среды функционирования Windows x32

Неизменяемые файлы	**Значение контрольной суммы**
rutoken.cap	b5397c06
_rutokenst80.s19	782a911a
rutokenst.s19	df66d253
rutokenst80.s19	0788886f
USB_Firmware_ARM_17_ECP_CERT_uv3.hex	1c0fe7af
USB_Firmware_ARM_43_ECP_CERT_uv3.hex	130d629e
RUTOKEN_S_REL.hex	fe2cc35d
USB_Firmware_ARM_13_lite_FSTEK_uv3.hex	fe0edd02
npCryptoPlugin.dll	2e03a149
npRutokenPlugin.dll	eadf37e8
FireWyrmNativeMessageHost.exe	68b34764
rtpkcs11ecp.dll	91cf181c
rtpkcs11.dll	55d83d1e
pki-core.dll	3732f92f
pki-core.lib	e0ab22bc
rtCSP.dll	7fad27aa
rtGrTools.dll	64e62e96
rtAPIlt.dll	3b3775bb
rtAPI.dll	3e42709c
rtAPIex.dll	63b05fd5
rtcontrol_Panel.exe	82d921a9
rterr.dll	4e23a182
rtAPIi.dll	80100bb3
rtlib.dll	a9bd4691
rtGrTools.dll	64e62e96
rtcontrol_Panel_Tools.exe	5feab24e
rtDrvRemover.exe	38887f3d
rtAdmin.exe	d6783803

Контрольные суммы неизменяемых файлов ОО для среды функционирования Unix x86_64

Неизменяемые файлы	**Значение контрольной суммы**
rutoken.cap	b5397c06
_rutokenst80.s19	782a911a
rutokenst.s19	df66d253
rutokenst80.s19	0788886f
USB_Firmware_ARM_17_ECP_CERT_uv3.hex	1c0fe7af
USB_Firmware_ARM_43_ECP_CERT_uv3.hex	130d629e

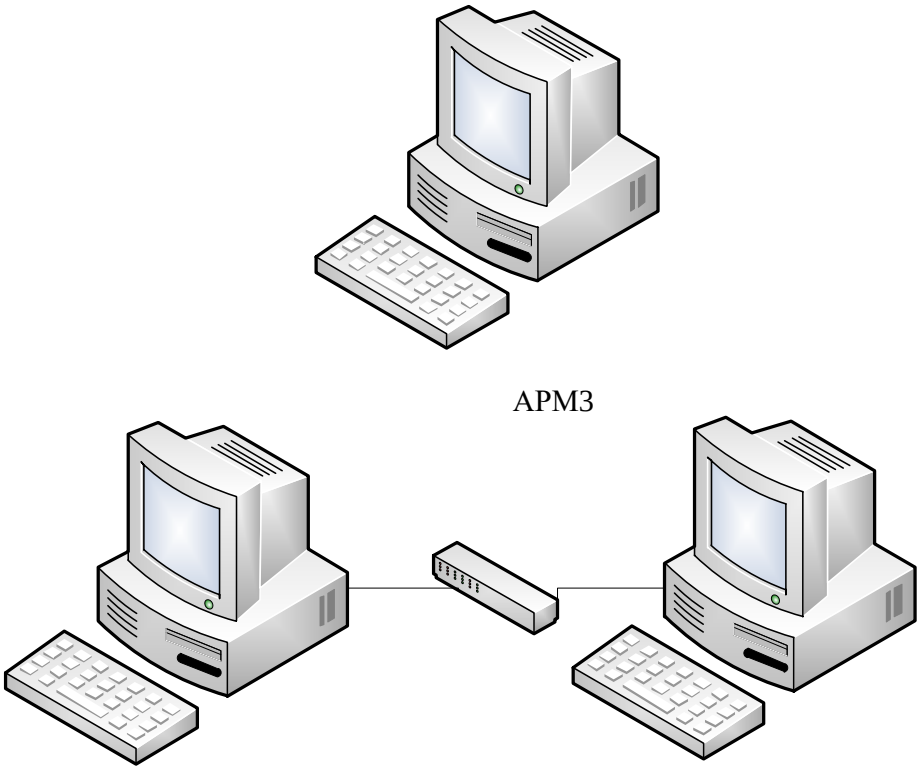
Неизменяемые файлы	**Значение контрольной суммы**
RUTOKEN_S_REL.hex USB_Firmware_ARM_13_lite_FSTEK_uv3.hex	fe2cc35d fe0edd02
libnpCryptoPlugin.so	abaaa076
librtpkcs11ecp.so libpki-core.so.1.1.0	43c77caa 9d6f7fd0
rtAdmin	6a700e35

Контрольные суммы неизменяемых файлов ОО для среды функционирования Unix x86

Неизменяемые файлы	**Значение контрольной суммы**
rutoken.cap _rutokenst80.s19 rutokenst.s19 rutokenst80.s19 USB_Firmware_ARM_17_ECP_CERT_uv3.hex USB_Firmware_ARM_43_ECP_CERT_uv3.hex RUTOKEN_S_REL.hex USB_Firmware_ARM_13_lite_FSTEK_uv3.hex	b5397c06 782a911a df66d253 0788886f 1c0fe7af 130d629e fe2cc35d fe0edd02
libnpCryptoPlugin.so	df50c6d9
librtpkcs11ecp.so libpki-core.so.1.1.0	f73f161f 713376d2
rtAdmin	ba93a75d

ПРИЛОЖЕНИЕ Б. МЕТОДИКА ПРОВЕРКИ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК

Схема испытательного стенда



В состав испытательного стенда должны входить технические средства, приведенные в таблице А.1.

Таблица А.1

Обозначение на схеме	Техническая конфигурация	Компоненты общего и тестового программного обеспечения
АРМ1	Intel(R) Core (TM) 2 Duo CPU E7200, 2,54 ГГц, 2 ГБ ОЗУ	ОС Microsoft Windows 8.1 (32/64-bit), ОС Microsoft Windows 10 (32/64-bit), ПО Панель управления Рутокен Программа фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.2)

АРМ2	Intel(R) Core (TM) 2 Duo CPU E7200, 2,54 ГГц, 2 ГБ ОЗУ	ОС Microsoft Windows Server 2012 x64
АРМ3	Intel(R) Core (TM) 2 Duo CPU E7200, 2,54 ГГц, 2 ГБ ОЗУ	ОС Альт Сервер 8 (32/64-bit), ОС Альт Рабочая станция 8 (32/64-bit), ОС Альт Образование 8 (32/64-bit), ОС Альт Линукс СПТ 7 (32/64-bit), ОС Альт 8 СП (32/64-bit), EMIAS OS 1.0, ОС Astra Linux Special Edition (РУСБ.10015-01) (32/64-bit), ОС Astra Linux Common Edition (32/64-bit) ПО Панель управления Рутокен
Электронный идентификатор		Рутокен ЭЦП SC; Рутокен ЭЦП 2.0 2100 Рутокен ЭЦП 2.0 64КБ; Рутокен ЭЦП 2.0 micro 64КБ; Рутокен ЭЦП 64КБ, PKI версия; Рутокен ЭЦП micro 64КБ, PKI версия; Рутокен ЭЦП 2.0 64КБ Flash 4ГБ; Рутокен Lite SD «Rutoken lite» (Рутокен lite); «Rutoken S» (Рутокен S).
Коммутатор	–	–

Порядок проверки пункта 1.2.1 технических условий АКСФ.501410.008 ТУ

Для проведения проверки по данному пункту необходимо выполнить действия, представленные далее по тексту (для Рутокен S и Lite вместо шагов 1 – 13 выполнить аналогичные шаги, представленные в Приложении В).

1. Осуществление подключения электронного ключа Рутокен к АРМ3 из состава стенда.

2. Осуществление проверки корректного подключения электронного ключа Рутокен. Выполнение команды:

$ su

$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -T

3. Осуществление генерации ключевой пары. Выполнение команды:

$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so --keypairgen --key-type rsa:2048 -l --id 45

4. Осуществление открытия openssl и осуществление загрузки модуля поддержки pkcs11.Выполение команды:

$ openssl

OpenSSL> engine dynamic -pre SO_PATH:/usr/lib64/openssl/engines/engine_pkcs11.so -pre ID:pkcs11 -pre LIST_ADD:1 -pre LOAD -pre MODULE_PATH:/usr/lib64/librtpkcs11ecp.so

5. Осуществление создания сертификата в PEM—формате. Выполнение команды:

OpenSSL> req -engine pkcs11 -new -key 0:45 -keyform engine -x509 -out cert.pem -text

6. Осуществление конвертации сертификата из формата PEM в формат CRT. Выполнение команды:

OpenSSL> x509 -in cert.pem -out cert.crt -outform DER

7. Осуществление закрытия openssl. Сохранение сертификата CRT на электронный ключ Рутокен. Выполнение команды:

openssl> exit

$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l -y cert -w cert.crt --id 45

8. Осуществление проверки успешной записи сертификата на электронный ключ Рутокен. Выполнение команды:

$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -O -l

9. Осуществление создания файла конфигурации pam_pkcs11. Выполнение команды:

cp /usr/share/pam_pkcs11/pam_pkcs11.conf.example /etc/security/pam_pkcs11/pam_pkcs11.conf

cp /usr/share/pam_pkcs11/subject_mapping.example /etc/security/pam_pkcs11/subject_mapping

10. Включение аутентификации по внешнему носителю на АРМ3. Выполнение команды:

rm /etc/pam.d/system-auth

ln -s /etc/pam.d/system-auth-pkcs11 /etc/pam.d/system-auth

11. Осуществление редактирования конфигурации аутентификации в системе. Изменение второй строчки файла конфигурации на строчку «auth [success=1 default=ignore] pam_pkcs11.so pkcs11_module=/usr/lib64/librtpkcs11ecp.so». Выполнение команды:

mcedit /etc/pam.d/system-auth

12. Осуществление редактирования файла /etc/security/pam_pkcs11/pam_pkcs11.conf . Выполнение команды:

mcedit /etc/security/pam_pkcs11/pam_pkcs11.conf

pam_pkcs11 {

```
  nullok = false;
  debug = false;
  use_first_pass = false;
  use_authtok = false;
  card_only = false;
  wait_for_card = false;
  use_pkcs11_module = rutokenecp;

  # Aktiv
  pkcs11_module rutokenecp {
    module = /usr/lib64/librtpkcs11ecp.so
    slot_num = 0;
    support_thread = true;
    ca_dir = /etc/pam_pkcs11/cacerts;
    crl_dir = /etc/pam_pkcs11/crls;
    cert_policy = signature;
  }

  use_mappers = subject;
  mapper_search_path = /lib64/pam_pkcs11;

  mapper subject {
       debug = false;
       module = internal;
       ignorecase = false;
       mapfile = file:///etc/security/pam_pkcs11/subject_mapping;
    }
}
```

13. Добавление связки сертификата на электронном ключе с использованием ОС, установленной на АРМ3 из состава стенда. Выполнение команды:

```
# pkcs11_inspect > /etc/security/pam_pkcs11/subject_mapping
# mcedit  /etc/security/pam_pkcs11/subject_mapping
# Printing data for mapper subject:
/C=RU/ST=Moscow/L=Moscow/O=test/OU=test/CN=user/emailAddress=user1@mail.ru
-> user
```

14. На АРМ2 из состава стенда осуществление нажатия кнопок «Win+R», в открывшемся окне осуществление ввода «mmc» и нажатие на клавиатуре кнопки «Enter».

15. В открывшемся окне «Консоль 1 – Корень консоли» осуществление последовательного перехода к следующим элементам графического интерфейса «Файл – Добавить или удалить оснастку – Центр сертификации – Шаблоны сертификатов».

16. Открытие «Шаблоны сертификатов». Выполнение последовательного перехода «Пользователь со смарт-картой – Скопировать шаблон».

17. В открывшемся окне «Свойства нового шаблона» осуществление выбора вкладки «Общие». Осуществление ввода в поле «Отображаемое имя шаблона» имя для нового шаблона «rut3».

18. Осуществление перехода на вкладку «Обработка запроса». Установление метки в пункте «Подавать заявку для субъекта, не требуя ввода данных». Нажатие кнопки «ОК».

19. В окне «Консоль1 – Корень консоли» осуществление последовательного перехода к следующим элементам графического интерфейса «Шаблоны сертификатов – Создать – Выдаваемый шаблон сертификата». Добавление шаблона «rut3».

20. Осуществление последовательного перехода к следующим элементам графического интерфейса «Active Directory – пользователи и компьютеры – Users – user - Свойства». Установление метки в окне Параметры учетной записи «Для интерактивного входа в сеть нужна смарт-карта». Нажатие кнопки «ОК».

21. На АРМ1 из состава стенда осуществление подключения электронного ключа Рутокен.

22. Осуществление нажатия кнопок «Win+R», в открывшемся окне осуществление ввода «mmc» и нажатие на клавиатуре кнопки «Enter».

23. В открывшемся окне «Консоль 1 – Корень консоли» осуществление последовательного перехода к следующим элементам графического интерфейса «Файл – Добавить или удалить оснастку – Сертификаты».

24. Осуществление последовательного перехода к следующим элементам графического интерфейса «Сертификаты – Личное – Все задачи – Запросить новый сертификат».

25. В открывшемся окне установление метки «rut3», нажатие кнопки «Подробности – Свойства».

26. Осуществление последовательного перехода к следующим элементам графического интерфейса «Закрытый ключ – Поставщик службы шифрования». Установление метки в пункте «Aktiv ruToken CSP v1.0». Удаление метки в пункте «Microsoft Strong Cryptographic Provider». Нажатие кнопки «ОК – Заявка». В появившемся окне осуществление ввода PIN-кода пользователя. Нажатие кнопки «ОК».

27. На АРМ1 из состава испытательного стенда осуществление проверки записанного сертификата. Осуществление последовательного перехода к следующим элементам графического интерфейса «Пуск – Все программы – Рутокен – Панель управления Рутокен – Ввести PIN-код - Сертификаты».

28. Осуществление попыток регистрации в операционной системе АРМ1 из состава стенда без использования электронного ключа.

29. Осуществление попыток регистрации в операционной системе АРМ3 из состава стенда без использования электронного ключа.

30. Подключение электронного ключа Рутокен к АРМ 1 из состава стенда. Осуществление перехода к интерфейсу для ввода аутентификационных данных операционной системы АРМ 1. Осуществление ввода неверного PIN-кода пользователя подключенного электронного ключа Рутокен. Анализ реакции объекта испытаний на попытку пройти процедуру аутентификации с использованием неверного PIN-кода.

31. Подключение электронного ключа Рутокен к АРМ3 из состава стенда. Осуществление перехода к интерфейсу для ввода аутентификационных данных операционной системы АРМ3. Осуществление ввода неверного PIN-кода пользователя подключенного электронного ключа Рутокен. Анализ реакции объекта испытаний на попытку пройти процедуру аутентификации с использованием неверного PIN-кода.

32. Осуществление ввода верного PIN-кода пользователя подключенного электронного ключа Рутокен на АРМ1. Анализ реакции объекта испытаний на попытку пройти процедуру аутентификации с использованием верного PIN-кода.

33. Осуществление ввода верного PIN-кода пользователя подключенного электронного ключа Рутокен на АРМ3. Анализ реакции объекта испытаний на попытку пройти процедуру аутентификации с использованием верного PIN-кода.

34. Осуществление последовательного перехода к следующим элементам графического интерфейса «Панель управления Рутокен – Администрирование – Ввести PIN-код». Осуществление ввода неверного PIN-кода пользователя для получения доступа к информации, хранящейся в памяти Рутокен.

35. В открывшемся окне «Панель управления Рутокен», осуществление ввода верного PIN-кода пользователя для получения доступа к информации, хранящейся в памяти электронного ключа Рутокен.

36. Осуществление импорта аутентификационной информации. Осуществление перехода «Панель управления Рутокен – Сертификаты». Осуществление выбора сертификата и нажатие кнопки «Импортировать».

37. Осуществление перехода «Панель управления Рутокен – Сертификаты – Экспортировать». Осуществление экспорта аутентификационной информации.

38. Осуществление просмотра информации о сертификате Осуществление перехода «Панель управления Рутокен – Сертификаты – Свойства».

39. Осуществление попытки удаления аутентификационной информации хранящейся в памяти электронного ключа. Осуществление перехода «Панель управления Рутокен – Сертификаты – Удалить».

Критерий принятия положительного решения

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. В результате выполнения действий по п. 2 была осуществлена проверка корректного подключения электронного ключа Рутокен.

2. В результате выполнения действий по п.3 была успешно осуществлена генерация ключевой пары.

3. В результате выполнения действий по п.4 был успешно загружен модуль поддержки pkcs11.

4. В результате выполнения действий по п. 5 был успешно создан сертификат в PEM-формате.

5. В результате выполнения действий по п. 7 было успешно произведено сохранение сертификата в формате CRT на электронный ключ Рутокен.

6. В результате выполнения действий по п. 8 была успешно произведена проверка записи сертификата на электронный ключ Рутокен.

7. В результате выполнения действий по п. 10 была успешно включена аутентификация по внешнему носителю.

8. В результате выполнения действий по п. 13 была успешно добавлена связка сертификата на электронном ключе Рутокен с использованием ОС, установленной на АРМ3 из состава стенда.

9. В результате выполнения действий по п.п.14 – 17 был успешно скопирован шаблон «Пользователь со смарт-картой» на АРМ2 из состава стенда.

10. В результате выполнения действий по п. 20 была успешно произведена настройка входа пользователя со смарт-картой.

11. В результате выполнения действий по п.п. 21 – 26 была успешно произведена запись сертификата на электронный ключ Рутокен на АРМ1 из состава стенда.

12. В результате выполнения действий по п. 28 пользователю АРМ1 было отказано в доступе к операционной системе без использования электронного ключа Рутокен.

13. В результате выполнения действий по п. 29 пользователю АРМ3 было отказано в доступе к операционной системе без использования электронного ключа Рутокен.

14. В результате выполнения действий по п. 30 было установлено, что при вводе неверного PIN-кода пользователя АРМ1 в доступе к операционной системе было отказано.

15. В результате выполнения действий по п. 31 было установлено, что при вводе неверного PIN-кода пользователя АРМ3 в доступе к операционной системе было отказано.

16. В результате выполнения действий по п. 32 было установлено, что при вводе верного PIN-кода пользователя пользователь user 5 получил доступ к операционной системе АРМ1.

17. В результате выполнения действий по п. 33 было установлено, что при вводе верного PIN-кода пользователя пользователь user получил доступ к операционной системе АРМ3.

18. В результате выполнения действий по п. 34 пользователь не получил доступ к аутентификационной информации, хранящейся в памяти электронного ключа, по результатам ввода неверного PIN-кода пользователя.

19. В результате выполнения действий по п. 35 пользователь получил доступ к аутентификационной информации, хранящейся в памяти электронного ключа, по результатам ввода верного PIN-кода пользователя.

20. В результате выполнения действий по п. 36 был успешно произведен импорт аутентификационной информации.

21. В результате выполнения действий по п. 37 был успешно произведен экспортаутентификационной информации.

22. В результате выполнения действий по п. 38 была успешно просмотрена информация о сертификате.

23. В результате выполнения действий по п. 39 была успешно удалена аутентификационная информация, хранящаяся в памяти электронного ключа.

Порядок проверки пункта 1.2.4, 1.2.5 и 1.2.6 технических условий АКСФ.501410.008 ТУ

Для проведения проверки по данному пункту необходимо выполнить действия, представленные далее по тексту.

1. Осуществление подключения электронного ключа Рутокен к АРМ1 из состава стенда.

2. Осуществление перехода «Панель управления Рутокен – Администрирование – Ввести PIN-код». В открывшемся окне Панель управления Рутокен установление метки «Пользователь» и осуществление ввода неверного и верного PIN-кода пользователя.

3. В поле «Управление PIN-кодами» осуществление нажатия кнопки «Изменить…». В открывшемся окне Панель управления Рутокен осуществление ввода нового PIN-кода пользователя. Нажатие кнопки «ОК».

4. Осуществление нажатия кнопки «Выйти». Осуществление перехода «Администрирование – Ввести PIN-код». В открывшемся окне осуществление ввода нового PIN-кода пользователя. Нажатие кнопки ОК.

5. Осуществление перехода «Панель управления Рутокен – Администрирование». Осуществление нажатия кнопки «Изменить». В открывшемся окне Имя Рутокен осуществление ввода имя «test». Нажатие кнопки «ОК».

6. В окне Панель управления Рутокен осуществление нажатия кнопки «Информация» и осуществление просмотра информации о Рутокен.

7. В окне Панель управления Рутокен осуществление нажатия кнопки «Выйти». Осуществление нажатия кнопки «Ввести PIN-код». В открывшемся окне Панель управления Рутокен установление метки Пользователь и осуществление ввода неверного PIN-кода пользователя 10 раз. Анализ реакции ОО на проведенные действия.

8. Осуществление нажатия кнопки «Ввести PIN-код». В открывшемся окне Панель управления Рутокен установление метки Пользователь и осуществление ввода верного PIN-кода пользователя. Анализ реакции ОО на проведенные действия.

9. Осуществление перехода «Панель управления Рутокен – Администрирование – Ввести PIN-код». В открывшемся окне Панель управления Рутокен установление метки «Администратор» и осуществление ввода неверного и верного PIN-кода администратора.

10. В окне «Панель управления Рутокен» в поле «управление PIN-кодами» осуществление нажатия кнопки «Разблокировать».

11. В окне Панель управления Рутокен в поле Управление PIN-кодами осуществление нажатия кнопки «Изменить». Осуществление ввода нового PIN-кода администратора.

12. Нажатие кнопки «Выйти». Осуществление нажатия кнопки «Ввести PIN-код». В открывшемся окне «Панель управления Рутокен» установление метки «Администратор» и осуществление ввода нового PIN-кода администратора.

13. В окне «Панель управления Рутокен» в поле «Информация» осуществление нажатия кнопки «Информация» и осуществление просмотра информации о Рутокен.

14. Осуществление перехода «Панель управления Рутокен – Администрирование – Ввести PIN-код». В открывшемся окне «Панель управления Рутокен» установление метки «Пользователь» и осуществление ввода неверного PIN-кода пользователя 10 раз. В окне «Панель управления Рутокен» в поле «управление PIN-кодами» осуществление нажатия кнопки «Разблокировать». Анализ реакции ОО на проведенные действия.

Критерий принятия положительного решения

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. В результате выполнения действий по п. 2 был успешно введен PIN-код пользователя.

2. В результате выполнения действий по п.3 был успешно изменен PIN-код пользователя.

3. В результате выполнения действий по п.5 было успешно задано новое имя электронному ключу Рутокен.

4. В результате выполнения действий по п.6 была успешно просмотрена информация о Рутокен.

5. В результате выполнения действий по п.7 был неверно введен PIN-код пользователя 10 раз.

6. В результате выполнение действий по п.8 был введен верный PIN-код пользователя.

7. В результате выполнение действий по п.9 был неверно и верно введен PIN-код администратора.

8. В результате выполнения действий по п.10 PIN-код пользователя был успешно разблокирован.

9. В результате выполнения действий по п.11 PIN-код администратора был успешно изменен.

10. В результате выполнения действий по п.12 был успешно произведен вход администратора по новому PIN-коду.

11. В результате выполнения действий по п.13 была успешно просмотрена информация о Рутокен.

12. В результате выполнения действий по п.14 было установлено, что разблокировку PIN-кода пользователя невозможно выполнить пользователем, кнопка «Разблокировать» неактивна.

Порядок проверки пункта 1.2.7 технических условий АКСФ.501410.008 ТУ

Для проведения проверки по данному пункту необходимо выполнить действия, представленные далее по тексту. (для Рутокен S вместо шагов 4 – 5 выполнить аналогичные шаги, представленные в Приложении В)

1. Осуществление открытия на АРМ1 из состава стенда «Панель управления Рутокен – Администрирование – Ввести PIN-код». Осуществление ввода верного PIN-кода пользователя.

2. В поле Имя токена нажатие кнопки «Изменить». В открывшемся окне Имя Рутокен осуществление ввода имя токена «user». Нажатие ОК.

3. В поле Информация, нажатие кнопки «Информация» и осуществление просмотра информации о Рутокен.

4. Осуществление открытия на АРМ3 из состава стенда «Приложения – Стандартные – Терминал». Осуществление ввода команды:

```
./rtAdmin –L Rutoken
#(для Рутокен Lite добавить: c12345678)
```

5. Осуществление просмотра информации и Рутокен. Выполнение команды:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -T
```

Критерий принятия положительного решения

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. В результате выполнения действий по п. 2 было успешно задано имя Рутокен.

2. В результате выполнения действий по п. 3 была просмотрена информация о Рутокен.

3. В результате выполнения действий по п. 4 было успешно задано имя Рутокен.

4. В результате выполнения действий по п. 5 была просмотрена информация о Рутокен.

Порядок проверки пункта 1.2.2 технических условий АКСФ.501410.008 ТУ

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. Осуществление открытия «Панель управления Рутокен – Администрирование – Ввести PIN-код». Осуществление ввода верного PIN-кода администратора.

2. Осуществление перехода «Панель управления Рутокен – Настройки – Политики качества PIN-кода - Настройка».

3. В открывшемся окне Политика качества PIN-кодов осуществление снятия меток в полях: Разрешить использование PIN-кода по умолчанию, Разрешить PIN-код, состоящий из одного повторяющегося символа, Разрешить PIN-код, состоящий только из цифр, Разрешить PIN-код, состоящий только из букв, Разрешить PIN-код, совпадающий с предыдущим. В поле Поведение при смене PIN-кода осуществление выбора «Запретить использование» и «Предупреждать». В поле Считать PIN-код «слабым» при длине меньшей, чем установление значения «3». Нажатие кнопки «Применить».

4. Осуществление перехода «Панель управления Рутокен - Администрирование». В поле Управление PIN-кодами осуществление нажатия кнопки «Изменить…».

5. В открывшемся окне «Панель управления Рутокен» в поле Введите новый PIN-код осуществление ввода PIN-кода:

- с повторяющимся символом – ****;
- состоящего только из букв – qwerty;
- слишком короткого PIN-кода – 12;
- совпадающего с текущим PIN-кодом;
- состоящий только из цифр – 123;
- по умолчанию;
- осуществление среднего PIN-кода – q1w2e3r4t5.

Анализ реакции ОО на проведенные действия.

6. Осуществление подключения электронного ключа Рутокен на АРМ3 из состава стенда. (для Рутокен S выполнить аналогичные шаги, представленные в Приложении В)

7. Осуществление открытия «Приложения – Стандартные – Терминал». Указание минимальной длинны PIN-кода администратора и PIN-кода пользователя – 6. Указание значений PIN-кода пользователя и PIN-кода администратора – 12345. Выполнение команды:

./rtAdmin –f –M6 –m6 –a12345 –u12345

Анализ реакции ОО на проведенные действия.

8. Осуществление открытия «Приложения – Стандартные – Терминал». Указание максимальной длинны PIN-кода администратора и PIN-кода пользователя – 32. Осуществление ввода значений PIN-кода пользователя и PIN-кода администратора равных тридцати трём символам. Выполнение команды:

./rtAdmin –f –M32 –m32 –a12345123456789012345678901234567890123456789012 –u12345123456789012345678901234567890123456789012

Анализ реакции ОО на проведенные действия.

9. Осуществление открытия «Приложения – Стандартные – Терминал». Указание длинны PIN-кода администратора и PIN-кода пользователя удовлетворяющие политики качества PIN-кодов. Выполнение команды:

./rtAdmin –f –M6 –m6 –a87654321 –u12345678

Анализ реакции ОО на проведенные действия.

Критерий принятия положительного решения

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. В результате выполнения действий по п. 1 была успешно произведена аутентификация администратора.
2. В результате выполнения действий по п. 3 была успешно изменена политика качества PIN-кода.
3. В результате выполнения действий по п. 5 был осуществлен ввод PIN-кода:

- с повторяющимся символом – ****;
- состоящего только из букв – qwerty;
- осуществление ввода слишком короткого PIN-кода;
- осуществление ввода PIN-кода совпадающего с текущим PIN-кодом;
- осуществление ввода PIN-кода состоящего только из цифр – 123;
- осуществление ввода PIN-кода заданного по умолчанию;
- осуществление ввода «среднего» PIN-кода.

4. В результате выполнения действий по п. 7 был осуществлен ввод некорректного PIN-кода (менее 6 символов).
5. В результате выполнения действий по п. 8 был осуществлен ввод некорректного PIN-кода (более 32 символов).
6. В результате выполнения действий по п. 9 был осуществлен ввод корректного PIN-кода.

Порядок проверки пункта 1.2.3 технических условий АКСФ.501410.008 ТУ

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. Осуществление подключения инициализированного электронного ключа Рутокен к АРМ 1 из состава стенда.
2. Осуществление открытия «Панель управления Рутокен – Администрирование – Ввести PIN-код». В открывшемся окне осуществление ввода неверного PIN-кода пользователя 10 раз. Анализ реакции объекта испытаний на каждое использование неверного PIN-кода пользователя.
3. Осуществление перехода «Панель управления Рутокен – Администрирование – Ввести PIN-код». В открывшемся окне осуществление ввода неверного PIN-кода администратора 10 раз. Анализ реакции объекта испытаний на каждое использование неверного PIN-кода администратора.
4. Осуществление подключения электронного ключа Рутокен на АРМ3 из состава стенда. (для Рутокен S выполнить аналогичные шаги, представленные в Приложении В)
5. Осуществление открытия «Приложения – Стандартные – Терминал». Выполнение команды:

./rtAdmin –f –r2 –R3

6. Используя команду смены PIN-кода администратора осуществление ввода PIN-кода администратора 4 раза. Анализ реакции объекта испытаний на каждое использование неверного PIN-кода администратора. Выполнение команды:

./rtAdmin –o666666 –a87654321

7. Используя команду смены PIN-кода пользователя осуществление ввода PIN-кода пользователя 3 раза. Анализ реакции объекта испытаний на каждое использование неверного PIN-кода администратора. Выполнение команды:

./rtAdmin –c666666 –u87654321

Критерий принятия положительного решения

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. В результате выполнения действий по п. 2 было установлено, что при последовательных неуспешных попытках ввода PIN-код пользователя электронный ключ Рутокен был заблокирован.
2. В результате выполнения действий по п. 3 было установлено, что при последовательных неуспешных попытках ввода PIN-код администратора электронный ключ был заблокирован.
3. В результате выполнения действий по п. 5 был успешно форматирован электронный ключ Рутокен с заданными параметрами: минимальная длинна PIN-кода пользователя – 2, минимальная длинна PIN-кода администратора – 3 .
4. В результате выполнения действий по п. 6 было установлено, что при последовательных неуспешных попытках ввода PIN-код администратора электронный ключ был заблокирован.
5. В результате выполнения действий по п. 7 было установлено, что при последовательных неуспешных попытках ввода PIN-код пользователя электронный ключ был заблокирован.

ПРИЛОЖЕНИЕ В. МЕТОДИКА ПРОВЕРКИ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК РУТОКЕН S И LITE

Порядок проверки пункта 1.2.1 технических условий АКСФ.501410.008 ТУ для Рутокен S.

Для проведения проверки по данному пункту необходимо выполнить действия, представленные далее по тексту:

1. Осуществление подключения электронного ключа Рутокен к АРМ3 из состава стенда.

2. Осуществление инициализации электронного ключа Рутокен S средствами драйвера. Выполнение команд:

```
$ pkcs15-init --erase-card
$ pkcs15-init --create-pkcs15 --so-pin "87654321" --so-puk "" --pin "12345678"
$ pkcs15-init --store-pin --label "User PIN" --auth-id 02 --pin "12345678" --puk ""
```

3. Осуществление проверки корректного подключения электронного ключа Рутокен S, выполнение команды:

```
$ pkcs11-tool --module=opensc-pkcs11.so –T
```

4. Выполнение копирования PAM-модуль на АРМ3 из состава испытательного стенда.

5. Включение аутентификации по внешнему носителю на АРМ3. Выполнение команды:

```
$ rm /etc/pam.d/system-auth
$ ln -s /etc/pam.d/system-auth-pkcs11 /etc/pam.d/system-auth
```

6. Выполнение редактирования файла /etc/pam.d/system-auth. Выполнение команды:

```
# mcedit /etc/pam.d/system-auth
```

В открывшемся окне заменить первую строку на:

auth[TAB]sufficient[TAB]{путь до PAM-модуля} {путь до нужной библиотеки pkcs11 – opensc-pkcs11.so (по умолчанию: /usr/lib64/opensc-pkcs11.so)} {serial токена}

[TAB] - символ табуляции.

7. Осуществить открытие новой сессии в терминале. Выполнение команды:

```
$ su
```

Критерий принятия положительного решения

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. В результате выполнения действий по п. 3-4 выполнена инициализация электронного ключа Рутокен S.

2. В результате выполнения действий по п.п. 5-6 успешно включена аутентификация по внешнему носителю.

3. В результате выполнения действий по п.6-7 успешно выполнено редактирование файла system-auth.

4. В результате выполнения действий по п. 8 успешно открыта новая сессия.

Порядок проверки пункта 1.2.1 технических условий АКСФ.501410.008 ТУ для Рутокен Lite.

Для проведения проверки по данному пункту необходимо выполнить действия, представленные далее по тексту:

1. Осуществление подключения электронного ключа Рутокен к АРМ3 из состава стенда.

2. Осуществление проверки корректного подключения электронного ключа Рутокен Lite, выполнение команды:

```
$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so –T
```

3. Выполнение копирования PAM-модуль на АРМ3 из состава испытательного стенда.

4. Включение аутентификации по внешнему носителю на АРМ3. Выполнение команды:

```
# rm /etc/pam.d/system-auth
# ln -s /etc/pam.d/system-auth-pkcs11 /etc/pam.d/system-auth
```

5. Выполнение редактирования файла /etc/pam.d/system-auth. Выполнение команды:

```
# mcedit /etc/pam.d/system-auth
```

В открывшемся окне заменить первую строку на:

auth[TAB]sufficient[TAB]{путь до PAM-модуля} {путь до нужной библиотеки pkcs11 – librtpkcs11ecp.so} {serial токена }

[TAB] - символ табуляции в этом контексте.

6. Осуществить открытие новой сессии в терминале. Выполнение команды:

```
$ su
```

Критерий принятия положительного решения

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. В результате выполнения действий по п. 2 выполнена инициализация электронного ключа Рутокен S.

2. В результате выполнения действий по п. 4 успешно включена аутентификация по внешнему носителю.

3. В результате выполнения действий по п.5 успешно выполнено редактирование файла system-auth.

4. В результате выполнения действий по п. 6 успешно открыта новая сессия.

Порядок проверки пункта 1.2.7 технических условий АКСФ.501410.008 ТУ для Рутокен S, Рутокен Lite

Для проведения проверки по данному пункту необходимо выполнить действия, представленные далее по тексту:

1. Осуществление подключения электронного ключа Рутокен к АРМ3 из состава стенда.

2. Осуществление открытия на АРМ3 из состава стенда «Приложения – Стандартные – Терминал». Осуществление ввода команды:

```
./rtAdmin –L Rutoken c12345678
```

3. Осуществление просмотра информации и Рутокен. Выполнение команды:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -T
```

Критерий принятия положительного решения

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. В результате выполнения действий по п. 2 успешно задано имя Рутокен.

2. В результате выполнения действий по п. 3 была просмотрена информация о Рутокен.

Порядок проверки пункта 1.2.3 технических условий АКСФ.501410.008 ТУ для Рутокен S

Для проведения проверки по данному пункту необходимо выполнить действия, представленные далее по тексту:

1. Осуществление подключения электронного ключа Рутокен на АРМ3 из состава стенда.

2. PIN-коды пользователя и администратора и количество попыток доступа задаются в файле со списком APDU команд "format_rutokens". Содержимое файла format_rutokens (количество попыток ввода PIN-кода: 3 для администратора и 2 для пользователя).

```
apdu 80:8A:00:00
apdu
00:E0:00:00:38:62:36:80:02:00:00:82:02:38:00:83:02:00:00:86:28:43:01:01:00:00:00:00:FF:02:00:00:00:02:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
apdu
00:DA:01:62:41:80:02:08:00:83:02:01:02:85:03:22:01:33:86:28:43:01:01:00:00:00:00:FF:01:00:00:00:01:00:00:00
:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:A5:08:31:32:33:34:35:36:37:38
apdu 00:A4:08:04:04:00:00:00:00
apdu
00:DA:01:62:41:80:02:08:00:83:02:01:01:85:03:01:01:44:86:28:43:FF:01:00:00:00:00:FF:00:00:00:00:01:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:A5:08:38:37:36:35:34:33:32:31
apdu 80:7B:00:00
```

3. Осуществление инициализации электронного ключа Рутокен S с APDU командами:

```
# opensc-explorer
```

Выполнение копирования APDU команды из файла format_rutokens.

4. Создание внутренней структуры (указать PIN пользователя и администратора).

```
# pkcs15-init -C --pin 12345678 --so-pin 87654321 --so-puk ""
# pkcs15-init –store-pin –a 02 label 123 --pin 12345678 --so-pin 87654321 --puk ""
```

5. Используя команду смены PIN-кода пользователя осуществление ввода PIN-кода пользователя 3 раза. Анализ реакции объекта испытаний на каждое использование неверного PIN-кода администратора. Выполнение команды:

```
pkcs15-tool --change-pin -a 02 --pin 1234567118 --new-pin 12345678
```

6. Используя команду смены PIN-кода администратора осуществление ввода PIN-кода администратора 4 раза. Анализ реакции объекта испытаний на каждое использование неверного PIN-кода администратора. Выполнение команды:

```
pkcs15-tool --change-pin -a 01 --pin 8765432111 --new-pin 87654321
```

Критерий принятия положительного решения

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. В результате выполнения действий по п.2 осуществлен просмотр файла со списком APDU команд «format_rutokens».

2. В результате выполнения действий по п.3 успешно выполнена инициализация электронного ключа Рутокен с APDU командами.

3. В результате выполнения действий по п.4 успешно выполнено создание внутренней структуры электронного ключа Рутокен S.

4. В результате выполнения действий по п. 5 установлено, что при последовательных неуспешных попытках ввода PIN-код администратора электронный ключ был заблокирован.

5. В результате выполнения действий по п. 6 установлено, что при последовательных неуспешных попытках ввода PIN-код пользователя электронный ключ был заблокирован.

Порядок проверки пункта 1.2.2 технических условий АКСФ.501410.008 ТУ для Рутокен S

Для проведения проверки по данному пункту необходимо выполнить действия, представленные далее по тексту:

1. Осуществление открытия «Приложения – Стандартные – Терминал». Указание минимальной длинны PIN-кода администратора и PIN-кода пользователя – 8. Указание значений PIN-кода пользователя и PIN-кода администратора – 1234567. Выполнение команды:

pkcs15-tool --change-pin -a 02 --pin 1234567118 --new-pin 1234567

Анализ реакции ОО на проведенные действия.

2. Осуществление открытия «Приложения – Стандартные – Терминал». Указание максимальной длинны PIN-кода администратора и PIN-кода пользователя – 16. Осуществление ввода значений PIN-кода пользователя и PIN-кода администратора равных тридцати трём символам. Выполнение команды:

pkcs15-tool --change-pin -a 02 --pin 1234567118 --new-pin 12345678901234567890123456789012

Критерий принятия положительного решения

Проверка считается успешно выполненной, если выполнены все условия, представленные далее по тексту.

1. В результате выполнения действий по п. 1 осуществлен ввод некорректного PIN-кода (менее 7 символов).

2. В результате выполнения действий по п. 2 осуществлен ввод некорректного PIN-кода (более 16 символов).