

УТВЕРЖДЕН
АКСФ.501490.008 30 ЛУ

**Программно-аппаратный комплекс аутентификации и хранения
информации «Рутокен» версии 4
Формуляр**

АКСФ.501490.008 30

Листов 34

Москва, 2021

ОГЛАВЛЕНИЕ

Список используемых сокращений	3
Аннотация	3
1 Общие сведения	4
Общие указания	6
2 Основные характеристики	7
3 Комплектность	10
4 Среда функционирования	16
5 Указания по эксплуатации	17
6 Техническая поддержка	22
7 Гарантии изготовителя	23
8 Периодический контроль основных характеристик при эксплуатации и хранении	24
9 Свидетельство о приёмке	25
10 Свидетельство об упаковке и маркировке	26
11 Сведения о рекламациях	27
12 Сведения о хранении	28
13 Сведения об изменениях	29
14 Особые отметки	30
Лист регистрации изменений	31
Приложение А. КОНТРОЛЬНЫЕ СУММЫ НЕИЗМЕНЯЕМЫХ ФАЙЛОВ	32

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

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

АННОТАЦИЯ

Настоящий документ содержит основные сведения о программно-аппаратном комплексе аутентификации и хранения информации «Рутокен» версии 4 АКСФ.501490.008 30. В формуляре отражается техническое состояние изделия после его изготовления и в процессе эксплуатации.

1 ОБЩИЕ СВЕДЕНИЯ

- 1.1 Наименование изделия – программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» v. 4.
- 1.2 Тип продукта: программно-аппаратный комплекс.
- 1.3 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).
- 1.4 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 категории¹, в государственных информационных системах 1 класса защищенности², в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности³, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных⁴, в информационных системах общего пользования II класса⁵:

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).

- многофакторная аутентификация пользователей и\или администраторов в информационных системах (меры УПД.2 в части реализации ролевого разграничения доступа, УПД.6 в части ограничения количества неуспешных попыток входа в информационную систему);
- управление доступом субъектов доступа к объектам доступа (меры УПД.2 в части реализации ролевого разграничения доступа).

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.

- 1.5 ПАК «Рутокен» v. 4 сертифицирован в Системе сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00) и имеет сертификат соответствия № 3753 (выдан ФСТЭК России «30» мая 2017 года, действителен до «30» мая 2025 года). Согласно сертификату, Изделие соответствует требованиям технических условий АКСФ.501490.008 ТУ при выполнении указаний по эксплуатации, указанных в разделе 5 настоящего формуляра

ОБЩИЕ УКАЗАНИЯ

- 1.6 Настоящий формуляр удостоверяет комплектность программно-аппаратного комплекса аутентификации и хранения ключевой информации «Рутокен» версии 4 (далее по тексту – ПАК «Рутокен» v. 4, Изделие) и содержит указания по его эксплуатации.
- 1.7 Перед началом эксплуатации ПАК «Рутокен» v. 4 необходимо внимательно ознакомиться с настоящим формуляром и поставляемой документацией.
- 1.8 Порядок подготовки ПАК «Рутокен» v. 4 к работе подробно изложен в эксплуатационной документации.
- 1.9 Формуляр должен постоянно находиться в подразделении, ответственном за эксплуатацию ПАК «Рутокен» v. 4.
- 1.10 Все записи в формуляре производят только чернилами, отчетливо и аккуратно. Допускается использовать при записях шариковые ручки с черной или фиолетовой (синей) пастой. Подчистки, помарки и незаверенные исправления не допускаются. Правильность и своевременность заполнения формуляра контролируют должностные лица.
- 1.11 Настоящий формуляр заполняется представителями службы, ответственной за эксплуатацию ПАК «Рутокен» v. 4.

2 ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

2.1 Основные параметры и характеристики (свойства)⁶

2.2 ПАК «Рутокен» v. 4 реализовывает 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 обеспечивает хранение аутентификационной информации в памяти электронного идентификатор Рутокен; ПАК «Рутокен» v. 4 обеспечивает программный интерфейс для выполнения операций чтения, записи и удаления над аутентификационными данными, хранящимися в памяти электронного идентификатора Рутокен⁷;
- ПАК «Рутокен» v. 4 требует предъявление PIN-кода пользователя при доступе к аутентификационной информации, хранящейся в памяти электронного идентификатор Рутокен; ПАК «Рутокен» v. 4 проверяет соответствие значения предъявленного PIN-кода пользователя установленному эталонному значению PIN-кода пользователя; доступ к аутентификационной информации, хранящейся в памяти электронного идентификатор Рутокен, предоставляется

⁶ Основные параметры и характеристики, которыми обладает 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 Состав 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»).

только в случае совпадения значения предъявленного PIN-кода пользователя и эталонного значения PIN-кода пользователя⁸.

- 2.2.1 ПАК «Рутокен» v. 4 задает 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 задается 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)
- 2.2.2 В ПАК «Рутокен» v. 4 установлено ограничение количества последовательных неуспешных попыток ввода PIN-кода пользователя и\или PIN-кода администратора, 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).
- 2.2.3 ПАК «Рутокен» v. 4 обеспечивает 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 предоставляет доступ, представлены в таблице 1.

Таблица 1

Тип учетной записи	Права доступа
Пользователь	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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».

2.2.4 ПАК «Рутокен» v. 4 требует предъявление PIN-кода пользователя в следующих случаях:

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

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

2.2.5 ПАК «Рутокен» v. 4 требует предъявление PIN-кода администратора в следующих случаях:

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

ПАК «Рутокен» v. 4 проверяет 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 осуществлены только в случае совпадения значения предъявленного PIN-кода администратора и эталонного значения PIN-кода администратора.

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

3 КОМПЛЕКТНОСТЬ

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

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

3.2 Комплектность 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: <ul style="list-style-type: none"> – 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 с размещенным на нем дистрибутивом программного обеспечения: <ul style="list-style-type: none"> – ПО Панель управления Рутокен для 32-разрядных ОС; – ПО Панель управления Рутокен для 64-разрядных ОС. и документацией в составе: <ul style="list-style-type: none"> – «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Руководство администратора, АКСФ.501490.008 90»; – «Программно-аппаратный комплекс аутентификации и хранения информации 	<p>1</p> <p>1</p> <p>1</p> <p>1</p>	Поставляется в электронном виде (поставляется на компакт-диске опционально, в соответствии с условиями договора на поставку)

Наименование	Кол-во	Примечание
«Рутокен» версии 4. Руководство пользователя, АКСФ.501490.008 91»;	1	
– «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4. Технические условия АКСФ.501490.008 ТУ».	1	
– «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

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

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.

3.4 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», приведены в приложении А настоящего формуляра.

3.5 Эксплуатационная документация на ПАК «Рутокен» v. 4 поставляется 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

- «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.

4 СРЕДА ФУНКЦИОНИРОВАНИЯ

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 (ПУСБ.10015-01) (32/64-bit), ОС Astra Linux Common Edition (32/64-bit)
Процессор	1 ГГц
Оперативная память	2 Гб
Жесткий диск (свободное пространство)	20 МБ (свободного пространства)

5 УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

5.1 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).

5.2 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.

5.3 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

Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 4 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 встроенных утилит ОС 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.

6 ТЕХНИЧЕСКАЯ ПОДДРЕЖКА

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.

7 ГАРАНТИИ ИЗГОТОВИТЕЛЯ

- 7.1 Предприятие-изготовитель гарантирует соответствие ПАК «Рутокен» v. 4 требованиям ТУ при соблюдении потребителем условий и правил эксплуатации, транспортирования и хранения, установленных в эксплуатационной документации.
- 7.2 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.
- 7.3 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.

8 ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ

Результаты контроля основных характеристик ПАК «Рутокен» v. 4 заносятся в таблицу 6.

Таблица 6

Проверяемая характеристика	Дата проведения испытаний					
	20__ г.		20__ г.		20__ г.	
	Отметка о соответствии	Проводил испытания (должность, подпись)	Отметка о соответствии	Проводил испытания (должность, подпись)	Отметка о соответствии	Проводил испытания (должность, подпись)
Контрольная сумма дистрибутива						
Контрольная сумма программных модулей						

Проверяемая характеристика	Дата проведения испытаний					
	20__ г.		20__ г.		20__ г.	
	Отметка о соответствии	Проводил испытания (должность, подпись)	Отметка о соответствии	Проводил испытания (должность, подпись)	Отметка о соответствии	Проводил испытания (должность, подпись)
Контрольная сумма дистрибутива						
Контрольная сумма программных модулей						

9 СВИДЕТЕЛЬСТВО О ПРИЁМКЕ

Программно-аппаратный комплекс аутентификации
и хранения информации «Рутокен» версии 4

идентификатор СЗИ

соответствует требованиям технических условий АКСФ.501490.008 ТУ.

Ответственный за приемку

М.П.

личная подпись

расшифровка подписи

10 СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

Программно-аппаратный комплекс аутентификации
и хранения информации «Рутокен» версии 4

идентификатор СЗИ

Упакован АО «Актив-софт» согласно требованиям, предусмотренным в действующей технической документации.

Ответственный за упаковку

М.П.

личная подпись

расшифровка подписи

Маркировано в соответствии с требованиями технических условий идентификатором Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00

Маркировку произвёл

личная подпись

расшифровка подписи

11 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

11.1 Рекламация может быть предъявлена предприятию-изготовителю – компании АО «Актив-софт» (115088, г. Москва, ул. Шарикоподшипниковская, дом 1, этаж 4, пом. IX, комн. 11) в период гарантийного срока, как при приемке ПАК «Рутокен» v. 4, так и в процессе его хранения и эксплуатации.

11.2 Факт несоответствия ПАК «Рутокен» v. 4 требованиям эксплуатационной документации должен быть оформлен актом. Акт должен содержать сведения о характере неисправностей, условиях их возникновения и обеспечивать возможность точного воспроизведения ситуации, при которой неисправности были обнаружены. Акт подписывается лицами, эксплуатирующими ПАК «Рутокен» v. 4, утверждается руководителем предприятия (организации) Потребителя и направляется Изготовителю ПАК «Рутокен» v. 4, который принимает меры по устранению выявленных неисправностей, если они подтверждаются.

11.3 Содержание рекламаций и меры, принятые по ним, записываются в таблицу 7.

Таблица 7

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

12 СВЕДЕНИЯ О ХРАНЕНИИ

- 12.1 Изделие хранится в упаковке изготовителя при температуре окружающего воздуха от +5°C до +35°C, относительной влажности воздуха не более 65%.
- 12.2 В помещении для хранения Изделия не должно быть агрессивных примесей (паров кислот, щелочей).
- 12.3 При хранении не допускаются резкие изменения температуры окружающего воздуха (более 20 градусов Цельсия в час) и воздействия внешних магнитных полей напряженностью более 4000 А/м.
- 12.4 Сведения о хранении заносятся в таблицу 8.

Таблица 8

Дата		Условия хранения	Должность, фамилия и подпись лица, ответственного за хранение
установки на хранение	снятия с хранения		

13 СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

Сведения об изменениях заносятся в таблицу 9.

Таблица 9

Основание (входящий номер сопроводи- тельного документа и дата)	Дата проведения изменения	Содержание изменения	Порядковый номер изменения	Должность, фамилия и подпись лица, ответственного за проведение изменения	Подпись лица, ответст- венного за эксплуата- цию изделия

14 ОСОБЫЕ ОТМЕТКИ

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]

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	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
FireWyrnNativeMessageHost.exe	68b34764
rtpkcs11ecp.dll	695d49fd
rtpkcs11.dll	254c7bfe
pki-core.dll	44dd7dca
pki-core.lib	23730dd2
rtCSP.dll	a06d15cf
rtGrTools.dll	650723d7
rtAPIlt.dll	d26387d2
rtMiniDrv.dll	75316778
rtAPI.dll	de641c8f
rtAPIex.dll	9e3bdf94
rtcontrol_Panel.exe	54afdb88
rterr.dll	10ad518b
rtAPIi.dll	4ba38c10
rtlib.dll	2491fc37
rtGrTools.dll	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
FireWyrnNativeMessageHost.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
rtAPIlex.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	fe2cc35d
USB_Firmware_ARM_13_lite_FSTEK_uv3.hex	fe0edd02
libnpCryptoPlugin.so	abaaa076
librtpkcs11ecp.so	43c77caa
libpki-core.so.1.1.0	9d6f7fd0
rtAdmin	6a700e35

Контрольные суммы неизменяемых файлов ОО для среды функционирования Unix x86

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
libnpCryptoPlugin.so	df50c6d9
librtpkcs11ecp.so	f73f161f
libpki-core.so.1.1.0	713376d2
rtAdmin	ba93a75d