

Первое применение	
Справ. №	

УТВЕРЖДЕН
 26.20.40-032-47359501 ТУ-ЛУ

**ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС
 АУТЕНТИФИКАЦИИ И ХРАНЕНИЯ ИНФОРМАЦИИ
 «РУТОКЕН» версии 5**

ТЕХНИЧЕСКИЕ УСЛОВИЯ

26.20.40-032-47359501 ТУ

На 45 листах

Москва, 2021

Подпись и дата	
Име. № дубл.	
Взам. име. №	
Подпись и дата	

26.20.40-032-47359501 ТУ

Име. № подл.	Изм	Лист	№ документа	Подпись	Дата	26.20.40-032-47359501 ТУ		
						Литера	Лист	Листов
Разработ .							1	45
Проверил								
Т.конт р.								
Н.конт р.								
Ут вердил								
<p align="center">Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 5</p>						АО «Акт ИВ-софт»		

СОДЕРЖАНИЕ

	Список используемых сокращений	4
	Введение	5
	1 Технические требования	8
	1.1 Основные параметры и характеристики	8
	1.2 Основные параметры и характеристики (свойства)	8
	1.3 Комплектность	11
	1.4 Требования к документации	14
	1.5 Маркировка и упаковка	14
	1.6 Требования к среде функционирования	15
	2 Требования безопасности	17
	3 Требования охраны окружающей среды	18
	4 Правила приемки	19
	4.1 Общие положения.	19
	4.2 Приемочные испытания.	19
	4.3 Периодические испытания.	20
	5 Методы контроля	22
	5.1 Общие положения.	22
	5.2 Методы проверки комплектности	22
	5.3 Методы проверки упаковки и маркировки	22
	5.4 Проверка документации	23
	5.5 Методы контроля параметров и характеристик (свойств) Изделия	23
	6 Транспортирование и хранение	24
	7 Указания по эксплуатации	25
	7.1 Общие указания	25
	7.2 Устранение недостатков	26
	7.3 Процедура обновления	28
	8 Техническая поддержка	30

Первое применение											
Справ. №											
Подпись и дата											
Име. № дубл.											
Взам. инв. №											
Подпись и дата											
Име. № подл.		26.20.40-032-47359501 ТУ									
Изм	Лист	№ документ а	Подпись	Дат а	Программно-аппарат ный комплекс аут ент ификации и хранения информации «Рут окон» версии 5			Лит ера	Лист	Лист ов	
Разработ .										2	45
Проверил								АО «Акт ив-софт »			
Т.конт р.											
Н.конт р.											
Ут вердил											

9 Гарантийные обязательства..... 31

Первое применение	
Справ. №	

Подпись и дата	
Име. № дубл.	
Взам. име. №	
Подпись и дата	

26.20.40-032-47359501 ТУ

Име. № подл.	Изм	Лист	№ документа	Подпись	Дата	Программно-аппаратный комплекс автоматизации и хранения информации «Рут-окен» версии 5	Литера	Лист	Листов	
	Разработ.							3	45	
	Проверил						АО «Акт ИВ-софт»			
	Т.контр.									
	Н.контр.									
	Утв. вердил									

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

**Термин,
сокращение**

Определение

ОС

Операционная система

ПАК

Программно-аппаратный комплекс

ПО

Программное обеспечение

ТУ

Технические условия

ЭЦП

Электронная цифровая подпись

Име. №подл.	Подпись и дата	Взам. и инв. №	Инв. №дубл.	Подпись и дата					
					26.20.40-032-47359501 ТУ				
Изм.	Лист	№ документ а	Подпись	Дат а					
					Лист				
					4				

– управление доступом субъектов доступа к объектам доступа (УПД.2, УПД.6 и их усиления).

ПАК «Рутокен» v. 5 состоит из следующих компонентов:

- ПО Панель управления Рутокен;
- электронный идентификатор «Рутокен» v. 5 в формате токена и/или смарт-карты (в вариантах исполнения: sc, usb, type-c, micro, SD, nfc) с предустановленной «Карточной операционной системой Рутокен», далее микропрограмма;
- устройство чтения смарт-карт Рутокен SCR 3001;
- комплект документации.

Электронный идентификатор «Рутокен» v. 5 может быть представлен следующими моделями:

- Рутокен ЭЦП 2.0 3000;
- Рутокен ЭЦП 2.0 Flash;
- Рутокен ЭЦП 3.0 3100;
- Рутокен ЭЦП 3.0 3200;
- Рутокен ЭЦП 3.0 3220;
- Рутокен Lite.

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 5.**

Краткое наименование - ПАК «Рутокен» v. 5.

Компонентный состав ПАК «Рутокен» v. 5 представлен на рисунке 1.

Ине. №подл.	Подпись и дата
Взам. инв. №	Ине. №дубл.
Подпись и дата	Подпись и дата

Изм.	Лист	№ документ а	Подпись	Дат а	26.20.40-032-47359501 ТУ	Лист
						6

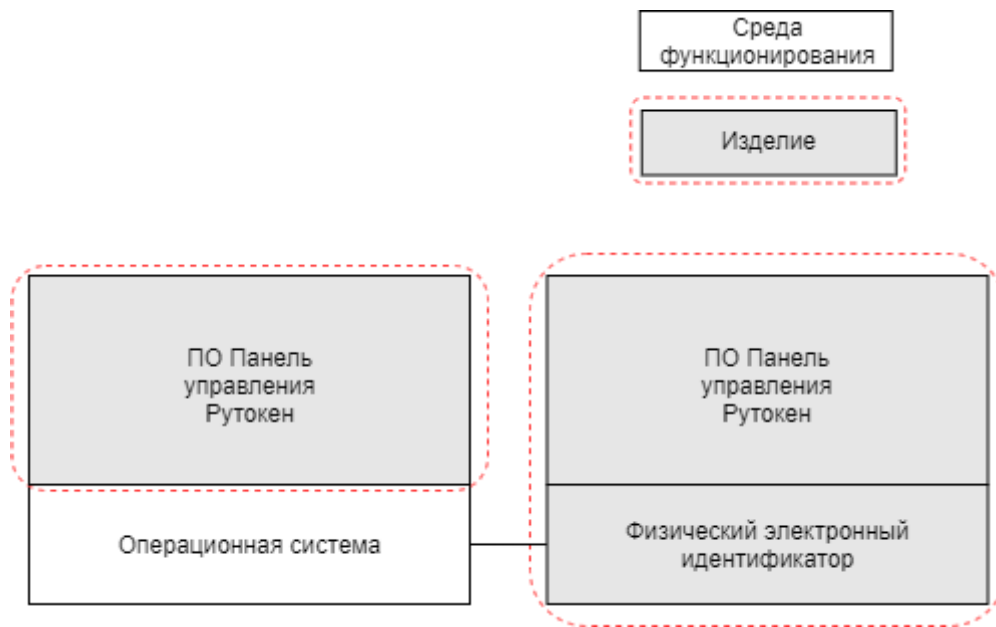


Рисунок 1 – Компонентный состав Изделия

Инв. №подл.	Подпись и дата			
	Инв. №дубл.			
Инв. №подл.	Подпись и дата			
	Взам. инв. №			
Инв. №подл.	Подпись и дата			
	Инв. №дубл.			
Инв. №подл.	Подпись и дата			
	Взам. инв. №			
Инв. №подл.	Подпись и дата			
	Инв. №дубл.			
<p style="text-align: center;">26.20.40-032-47359501 ТУ</p>				Лист
<p>Изм. Лист № документ а Подпись Дат а</p>				7

1 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

1.1 Основные параметры и характеристики

1.1.1 ПАК «Рутокен» v. 5 должен соответствовать требованиям настоящих ТУ.

1.2 Основные параметры и характеристики (свойства)⁶

1.2.1 ПАК «Рутокен» v. 5 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 методов управления доступом, УПД.6 в части ограничения неуспешных попыток входа в информационную систему, ЗСВ.1 в части идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре и их усиления):

– ПАК «Рутокен» v. 5 должен обеспечивать хранение аутентификационной информации в памяти электронного идентификатора Рутокен; ПАК «Рутокен» v. 5 должен обеспечивать программный интерфейс для выполнения операций чтения, записи и удаления над аутентификационными данными, хранящимися в памяти электронного идентификатора Рутокен⁷;

⁶ Основные параметры и характеристики, которыми должен обладать ПАК «Рутокен» v. 5, 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»).

Име. №подл.	Подпись и дата	Взам. и инв. №	Име. №дубл.	Подпись и дата
-------------	----------------	----------------	-------------	----------------

Изм.	Лист	№ документ а	Подпись	Дат а	26.20.40-032-47359501 ТУ	Лист
						8

–ПАК «Рутокен» v. 5 должен требовать предъявление PIN-кода пользователя при доступе к аутентификационной информации, хранящейся в памяти электронного идентификатора Рутокен; ПАК «Рутокен» v. 5 должен проверять соответствие значения предъявленного PIN-кода пользователя установленному эталонному значению PIN-кода пользователя; доступ к аутентификационной информации, хранящейся в памяти электронного идентификатора Рутокен, должен предоставляться только в случае совпадения значения предъявленного PIN-кода пользователя и эталонного значения PIN-кода пользователя⁸.

1.2.2 ПАК «Рутокен» v. 5 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. 5 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. 5 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. 5 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. 5 должен предоставлять доступ, представлены в таблице 1.

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»).

Ине. №подл.	Подпись и дата
Взам. инв. №	Ине. №дубл.
Подпись и дата	Подпись и дата

Таблица 1 - роли ПАК «Рутокен» v. 5

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;
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. 5 должен требовать предъявление PIN-кода пользователя в следующих случаях:

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

ПАК «Рутокен» v. 5 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. 5 должен требовать предъявление PIN-кода администратора в следующих случаях:

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

ПАК «Рутокен» v. 5 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

Име. №подл.	Подпись и дата
Взам. и инв. №	Име. №дубл.
Подпись и дата	Подпись и дата

значения предъявленного PIN-кода администратора и эталонного значения PIN-кода администратора.

1.2.7 ПАК «Рутокен» v. 5 должен осуществлять идентификацию электронных идентификаторов по их логическим именам. ПАК «Рутокен» v. 5 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. 5 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 – комплект поставляемой продукции

Наименование	Кол-во	Примечание
Электронный идентификатор Рутокен		Количество и модель идентификатора определяется условиями договора на поставку ПАК «Рутокен» v. 5. Электронный идентификатор «Рутокен» v. 5 может быть представлен следующими моделями: – Рутокен ЭЦП 2.0 3000; – Рутокен ЭЦП 2.0 Flash; – Рутокен ЭЦП 3.0 3100; – Рутокен ЭЦП 3.0 3200; – Рутокен ЭЦП 3.0 3220; – Рутокен Lite.
Компакт-диск размещенным на нем дистрибутивом программного обеспечения: – ПО Панель управления Рутокен 32-bit; – ПО Панель управления Рутокен 64-bit. и документацией в составе: – «Программно-аппаратный комплекс	1 1 1	Поставляется в электронном виде (поставляется на компакт-диске опционально, в соответствии с условиями договора на поставку)

Ине. № подл.	Подпись и дата
Взам. инв. №	Ине. № дубл.
Подпись и дата	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата
------	------	-------------	---------	------

26.20.40-032-47359501 ТУ

Лист

11

Наименование	Кол-во	Примечание
аутентификации и хранения информации «Рутокен» версии 5. Руководство администратора, 26.20.40-032-47359501 90»;	1	
– «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 5. Руководство пользователя, 26.20.40-032-47359501 91»;	1	
– «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 5. Технические условия 26.20.40-032-47359501 ТУ»	1	
Устройство чтения смарт-карт Рутокен SCR 3001;	1	Поставляется опционально (количество определяется условиями договора на поставку ПАК «Рутокен» v. 5.)
«Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 5. Формуляр 26.20.40-032-47359501 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. 5 поставляются с предустановленным программным обеспечением, приведенным ниже:

- файл ECP_54_FSB_FKN2_Release.hex Рутокен ЭЦП 2.0 3000;
- файл ECP_54_FSB_TM2_FKN2_Release.hex Рутокен ЭЦП 2.0 Flash
- файл ECP_ST31G480_FSB_Release.hex Рутокен ЭЦП 3.0 3100;
- файл ECP_54_FSB_Release_9F9F6482.hex Рутокен ЭЦП 3.0 3200;
- файл ECP_54_FSB_Release_9F9F6482.hex Рутокен ЭЦП 3.0 3220;

Ине. №подл.	Подпись и дата
Взам. инв. №	Ине. №дубл.
Подпись и дата	
Ине. №подл.	

Изм.	Лист	№ документ а	Подпись	Дат а
------	------	--------------	---------	-------

–«Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 5. Описание программы», 26.20.40-032-47359501 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. 5 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. 5 содержащий число от 00001 до 99999;

Име. №подл.	Подпись и дата	Взам. инв. №	Име. №дубл.	Подпись и дата
Изм.	Лист	№ документ а	Подпись	Дат а

26.20.40-032-47359501 ТУ

Лист

14

Элемент	Параметр
	ОС Astra Linux Special Edition (32/64-bit), ОС Astra Linux Common Edition (32/64-bit), ОС «Аврора», ОС «РЕД ОС» (32/64-bit)
Процессор	1 ГГц с архитектурой для всех версий ОС,
Оперативная память	2 Гб
Жесткий диск (свободное пространство)	20 МБ

Име. №подл.	Подпись и дата	Взам. и инв. №	Инв. №дубл.	Подпись и дата
Изм.	Лист	№ документа	Подпись	Дата

26.20.40-032-47359501 ТУ

Лист

16

4 ПРАВИЛА ПРИЕМКИ

4.1 Общие положения.

4.1.1 Для осуществления контроля и приемки ПАК «Рутокен» v. 5 проводятся приемо-сдаточные испытания.

4.1.2 Для осуществления контроля характеристик ПАК «Рутокен» v. 5 в процессе эксплуатации проводятся периодические испытания.

4.1.3 Испытания ПАК «Рутокен» v. 5 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. 5 могут применяться следующие методы:

- экспертно-документальный метод;
- проверка отдельных функций ПАК «Рутокен» v. 5 с помощью тестирующих средств, а также путем их пробного запуска и наблюдения за их выполнением.

4.1.5 При проведении испытаний ПАК «Рутокен» v. 5 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 Приемно-сдаточные испытания.

4.2.1 Приемно-сдаточные испытания проводятся с целью контроля соответствия ПАК «Рутокен» v. 5 требованиям настоящих ТУ.

4.2.2 Объем и последовательность приемо-сдаточных испытаний приведены в таблице 4.

Таблица 4 – приемо-сдаточные испытания

№ п/п	Наименования испытаний и проверок	Пункты ТУ		Виды испытаний	
		Технические требования	Методы испытаний	Приемо-сдаточные	Периодические

Ине. №подл.	Подпись и дата	Взам. инв. №	Ине. №дубл.	Подпись и дата
-------------	----------------	--------------	-------------	----------------

Изм.	Лист	№ документ а	Подпись	Дат а	26.20.40-032-47359501 ТУ	Лист
						19

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 4 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 26.20.40-032-47359501 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.

4.3Периодические испытания.

4.3.1Периодические испытания проводятся с целью контроля образца ПАК «Рутокен» v. 5 на соответствие требованиям настоящих ТУ в процессе его эксплуатации.

Ине. №подл.	Подпись и дата
Взам. инв. №	Подпись и дата
Ине. №дубл.	Подпись и дата
Подпись и дата	

Изм.	Лист	№ документ а	Подпись	Дат а

26.20.40-032-47359501 ТУ

Лист

20

4.3.2 Периодические испытания проводить в объеме и последовательности согласно таблице 4.

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

4.3.4 Испытания ПАК «Рутокен» v. 5 проводятся на смонтированной аппаратуре при установленном (инсталлированном) программном обеспечении ПАК «Рутокен» v. 5.

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.

Име. №подл.	Подпись и дата	Взам. и инв. №	Инв. №дубл.	Подпись и дата					
Изм.	Лист	№ документ а	Подпись	Дат а	26.20.40-032-47359501 ТУ				Лист
									21

5 МЕТОДЫ КОНТРОЛЯ

5.1 Общие положения.

5.1.1 На испытания ПАК «Рутокен» v. 5 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. 5 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. 5 с комплектностью ПАК «Рутокен» v. 5, указанной в таблице 2 настоящих ТУ.

5.2.2 ПАК «Рутокен» v. 5 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. 5 и документацией, а также всего комплекта ПАК «Рутокен» v. 5, требованиям, указанным в п. 1.5.

5.3.2 ПАК «Рутокен» v. 5 считается прошедшим проверку в части упаковки, если компакт-диск, с размещёнными на нём дистрибутивом ПАК «Рутокен» v. 5 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. 5, наносимой на нерабочую поверхность оптического диска, а

Ине. №подл.	Подпись и дата
Взам. инв. №	Ине. №дубл.
Подпись и дата	Подпись и дата

Изм.	Лист	№ документ а	Подпись	Дат а
------	------	--------------	---------	-------

26.20.40-032-47359501 ТУ

Лист

22

также наличия и размещения идентификатора по требованиям, указанным в п. 1.5 настоящих ТУ.

5.3.4 ПАК «Рутокен» v. 5 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. 5 проводится в соответствии с методикой проверки функциональных характеристик, изложенной в Приложении А.

5.5.2 ПАК «Рутокен» v. 5 считается прошедшим испытания, если функциональные характеристики соответствуют функциональным характеристикам, указанным в п. 1.2 настоящих ТУ.

Име. №подл.	Подпись и дата	Взам. инв. №	Инв. №дубл.	Подпись и дата	26.20.40-032-47359501 ТУ				Лист
									23
Изм.	Лист	№ документ а	Подпись	Дат а					

6 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ

6.1 ПАК «Рутокен» v. 5 можно транспортировать на неограниченные расстояния автомобильным, железнодорожным и авиационным видами транспорта при температуре окружающей среды от -20°C до +50°C. ПАК «Рутокен» v. 5 должен транспортироваться в упаковке Изготовителя в соответствии с требованиями ГОСТ 21552-84. Упаковка ПАК «Рутокен» v. 5 при транспортировке должна быть закреплена любым способом, исключающим ее перемещение

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

Име. №подл.	Подпись и дата	Взам. и инв. №	Инв. №дубл.	Подпись и дата	26.20.40-032-47359501 ТУ				Лист
									24
Изм.	Лист	№ документ а	Подпись	Дат а					

7 УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

7.1 Общие указания

При эксплуатации ПАК «Рутокен» v. 5 на объектах информатизации, обрабатывающих информацию ограниченного доступа, необходимо выполнение следующих ограничений:

- использование средств защиты информации от несанкционированного доступа, имеющих сертификат соответствия ФСТЭК России, для защиты информации ограниченного доступа, а также операционных систем;
- запрет на использования ПАК «Рутокен» v. 5 для обработки информации, содержащей сведения, составляющие государственную тайну;
- ПАК «Рутокен» v. 5 должен устанавливаться на оборудование, соответствующее требованиям, определенным в настоящем документе;
- наличие администратора безопасности, отвечающего за правильную эксплуатацию ПАК «Рутокен» v. 5;
- обеспечение физической сохранности средств вычислительной техники с установленным ПАК «Рутокен» v. 5 и исключение возможности доступа к ним посторонних лиц;
- доступ к каталогу с установленным программным обеспечением ПАК «Рутокен» v. 5 «%WINDIR%\System32\Aktiv Co\» должен быть разрешён только администратору;
- сохранение в секрете идентификаторов, PIN-кодов и паролей администраторов и пользователей ПАК «Рутокен» v. 5;
- обязательная смена PIN-кода «по умолчанию» электронных идентификаторов после их инициализации;
- проведение периодического контроля целостности ПАК «Рутокен» v. 5 с помощью программ контроля целостности (не реже одного раза в месяц);
- проведение периодической проверки на наличие актуальных уязвимостей (недостатков) в ПАК «Рутокен» v. 5 и среде его функционирования с использованием средств анализа защищенности (не реже одного раза в месяц);
- проведение периодической проверки ПАК «Рутокен» v. 5 и среды его функционирования на наличие компьютерных вирусов с использованием средств антивирусной защиты (не реже одного раза в месяц).
- отсутствие средств разработки и отладки ПО в среде функционирования ПАК «Рутокен» v. 5;

Име. №подл.	Подпись и дата	Взам. инв. №	Инв. №дубл.	Подпись и дата
Изм.	Лист	№ документ а	Подпись	Дат а

26.20.40-032-47359501 ТУ

Лист

25

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. 5 должна обеспечивать возможность обновления ПО для устранения актуальных уязвимостей.

В случае выявления информации об уязвимости ПАК «Рутокен» v. 5 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. 5, а также о компенсирующих мерах по защите информации или ограничениях по применению, а также доработку ПАК «Рутокен» v. 5, в том числе разработку обновлений ПАК «Рутокен» v. 5 или разработку мер по защите информации, нейтрализующих недостаток. Общий срок устранения недостатка ПАК «Рутокен» v. 5 не должен превышать 60 дней с момента выявления недостатка.

При выявлении уязвимостей ПАК «Рутокен» v. 5 предприятие-изготовитель должен осуществить следующие мероприятия:

- в случае отсутствия, на момент проверки информации по выявленным уязвимостям ПАК «Рутокен» v. 5, доступных релизов ПАК «Рутокен» v. 5 с устраненными уязвимостями, разработать компенсирующие меры по защите информации или ограничения по применению ПАК «Рутокен» v. 5, 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. 5 или его отдельные компоненты, в том числе выпустить обновление ПАК «Рутокен» v. 5 или, в случае невозможности устранения уязвимостей ПАК «Рутокен» v. 5 путем применения обновления, выпустить меры по защите информации, нейтрализующие недостаток и внести необходимые изменения в эксплуатационную документацию;

Име. №подл.	Подпись и дата
Взам. инв. №	Име. №дубл.
Подпись и дата	Подпись и дата

При получении обновлений ПАК «Рутокен» v. 5 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.

Име. №подл.	Подпись и дата	Взам. инв. №	Инв. №дубл.	Подпись и дата					Лист
									29
Изм.	Лист	№ документ а	Подпись	Дат а	26.20.40-032-47359501 ТУ				

8 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Предприятие-изготовитель оказывает базовую техническую поддержку ПАК «Рутокен» v. 5. В рамках базовой технической поддержки предприятие-изготовитель обеспечивает поиск, анализ и устранение недостатков ПАК «Рутокен» v. 5 на протяжении срока действия базовой технической поддержки.

Базовая техническая поддержка входит в стоимость поставляемого ПАК «Рутокен» v. 5 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. 5 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. 5 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.

Име. №подл.	Подпись и дата	Взам. инв. №	Инв. №дубл.	Подпись и дата
-------------	----------------	--------------	-------------	----------------

Изм.	Лист	№ документ а	Подпись	Дат а	26.20.40-032-47359501 ТУ	Лист
						30

9 ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

9.1 Предприятие-изготовитель гарантирует соответствие ПАК «Рутокен» v. 5 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. 5 дефектов, не связанных с нарушением правил эксплуатации, транспортирования и хранения, ПАК «Рутокен» v. 5 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. 5 – 12 месяцев (или больший срок, если это определено договором на поставку или лицензионным соглашением) со дня передачи его потребителю.

Име. №подл.	Подпись и дата	Взам. и инв. №	Инв. №дубл.	Подпись и дата					Лист
									31
Изм.	Лист	№ документ а	Подпись	Дат а	26.20.40-032-47359501 ТУ				

		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 (32/64-bit), ОС Astra Linux Common Edition (32/64-bit), ОС «РЕД ОС» (32/64-bit) ОС «Аврора» ПО Панель управления Рутокен
Электронный идентификатор		Рутокен ЭЦП 2.0 3000; Рутокен ЭЦП 2.0 Flash; Рутокен ЭЦП 3.0 3100; Рутокен ЭЦП 3.0 3200; Рутокен ЭЦП 3.0 3220; Рутокен Lite.
Коммутатор	–	–

Порядок проверки пункта 1.2.1 технических условий 26.20.40-032-47359501 ТУ

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.
- Выполнение команды:

Име. №подл.	Подпись и дата	Взам. инв. №	Инв. №дубл.	Подпись и дата
Изм.	Лист	№ документ а	Подпись	Дат а

26.20.40-032-47359501 ТУ

Лист

34

```
$ sudo 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. Выполнение команды:

```
$ openssl
```

```
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1/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
```

8. Записываем сертификат на токен

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

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

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

10. Осуществление создания файла конфигурации pam_p11. Выполнение команды:

```
$ sudo nano /usr/share/pam-configs/p11
```

Name: Pam_p11

Default: yes

Priority: 800

Auth-Type: Primary

Auth: sufficient /usr/lib/x86_64-linux-gnu/security/pam_p11.so /usr/lib64/librtpkcs11ecp.so

11. Добавление сертификата в список доверенных

```
$ mkdir ~/.eid
```

```
$ chmod 0775 ~/.eid
```

```
$ cat cert.pem >> ~/.eid/authorized_certificates
```

```
$ chmod 0664 ~/.eid/authorized_certificates
```

12. Включение аутентификации

```
$ sudo pam-auth-update
```

Далее выбрать pam_p11 если отключено и сохранить

Подпись и дата
Инв. №дубл.
Взам. инв. №
Подпись и дата
Инв. №подл.

Изм.	Лист	№ документ а	Подпись	Дат а	26.20.40-032-47359501 ТУ	Лист
						35

13. Настройка pkcs11_eventmgr

```
$ sudo nano /etc/pam_pkcs11/pkcs11_eventmgr.conf
```

```
pkcs11_eventmgr
```

```
{
```

```
# Запуск в бэграунде
```

```
daemon = true;
```

```
# Настройка сообщений отладки
```

```
debug = false;
```

```
# Время опроса в секундах
```

```
polling_time = 1;
```

```
# Установка тайм-аута на удаление карты
```

```
# По-умолчанию 0
```

```
expire_time = 0;
```

```
# Выбор pkcs11 библиотеки для работы с Рутокен
```

```
pkcs11_module = /usr/lib/librtpkcs11esp.so;
```

```
# Действия с картой
```

```
# Карта вставлена:
```

```
event card_insert {
```

```
    # Оставляем значения по умолчанию (ничего не происходит)
```

```
    on_error = ignore ;
```

```
    action = "/bin/false";
```

```
}
```

```
# Карта извлечена
```

```
event card_remove {
```

```
    on_error = ignore;
```

```
    # Вызываем функцию блокировки экрана
```

```
    action = "fly-wmfunc FLYWM_LOCK";
```

Име. №подл.	Подпись и дата	Взам. и инв. №	Име. №дубл.	Подпись и дата
Изм.	Лист	№ документ а	Подпись	Дат а

```

}

# Карта долгое время извлечена

event expire_time {

    # Оставляем значения по умолчанию (ничего не происходит)

    on_error = ignore;

    action = "/bin/false";

}
}

```

14. Добавление pkcs11_eventmgr в автозапуск

Создать ярлык на /usr/bin/pkcs11_eventmgr (правый клик на рабочем столе, создать ярлык, в окне указать путь к pkcs11 event manager /usr/bin/pkcs11_eventmgr)

И поместить его в автозапуск

```
$ sudo cp /home/tester/Desktop/shortcut.desktop /etc/xdg/autostart/
```

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

16. В открывшемся окне «Консоль 1 – Корень консоли» осуществление последовательного перехода к следующим элементам графического интерфейса «Файл – Добавить или удалить оснастку – Центр сертификации», выбрать локальный.

17. Правой кнопкой мыши щелкните по названию папки Шаблоны сертификатов и выберите пункт Управление.

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

19. В открывшемся окне «Свойства нового шаблона» осуществление выбора вкладки «Общие». Осуществление ввода в поле «Отображаемое имя шаблона» имя для нового шаблона «Пользователь с Рутокен».

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

21. В окне «Консоль 1 – Корень консоли» осуществление последовательного перехода к следующим элементам графического интерфейса «Шаблоны сертификатов – Создать – Выдаваемый шаблон сертификата». Добавление шаблона «Пользователь с Рутокен».

22. Осуществление последовательного перехода к следующим элементам графического интерфейса «Active Directory – пользователи и компьютеры – Users – user -

Име. №подл.	Подпись и дата
Взам. и инв. №	Име. №дубл.
Подпись и дата	Подпись и дата

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 длина PIN-кода пользователя – 2, минимальная длина 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.

Име. №подл.	Подпись и дата	Взам. и инв. №	Инв. №дубл.	Подпись и дата

Изм.	Лист	№ документ а	Подпись	Дат а

26.20.40-032-47359501 ТУ

Лист

45