

УТВЕРЖДЕН
ЖТЯИ.00096-01 30 01-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КРИПТОГРАФИЧЕСКИЙ МОДУЛЬ
«КриптоПро HSM» версия 2.0 (КОМПЛЕКТАЦИИ 1 И 2)

Формуляр

ЖТЯИ.00096-01 30 01

Листов 18

2018 г.

СОДЕРЖАНИЕ

1. Общие указания	3
2. Требования к эксплуатации ПАКМ.....	5
3. Общие сведения и Основные технические данные.....	6
4. Комплектность	8
5. Свидетельство о приемке	11
6. Свидетельство об упаковке	12
7. Гарантийные обязательства.....	13
8. Сведения о рекламациях.....	14
9. Сведения о хранении.....	15
10. Сведения о закреплении изделия при эксплуатации.....	16
11. Сведения об изменениях.....	17
12. Особые отметки.....	18

1. ОБЩИЕ УКАЗАНИЯ

1.1. Формуляр на изделие Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0, ПАКМ ЖТЯИ.00096-01, является документом, удостоверяющим гарантированные изготовителем основные характеристики СКЗИ, определяющим комплект поставки, отражающим сведения о производимых изменениях в комплекте поставки и другие данные за весь период эксплуатации.

1.2. Эксплуатация ПАКМ ЖТЯИ.00096-01 должна проводиться в соответствии с эксплуатационной документацией, предусмотренной настоящим Формуляром, и в соответствии с разделом V «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение-2005)».

1.3. Порядок обеспечения информационной безопасности при использовании ПАКМ ЖТЯИ.00096-01 определяется руководителем эксплуатирующей организации на основе требований по организационно-техническим мерам защиты, изложенным в эксплуатационной документации на СКЗИ.

1.4. При эксплуатации ПАКМ ЖТЯИ.00096-01 должны использоваться сертификаты открытых ключей, выпущенные Удостоверяющим центром, сертифицированным ФСБ России по классу защиты не ниже класса защиты используемого СКЗИ.

1.5. При встраивании ПАКМ ЖТЯИ.00096-01 (собственно ПАКМ, клиентская компонента ПАКМ «КриптоПро HSM Client») в прикладные системы необходимо по Техническому заданию, согласованному с 8 центром ФСБ России, проводить оценку среды функционирования ПАКМ на выполнение предъявленных к ПАКМ требований в случаях:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации (далее – государственные органы);
- при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд (далее – организации, выполняющие государственные заказы);
- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;
- при обработке информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;
- при обработке информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

В остальных случаях рекомендуется проводить установленным порядком проверку корректности встраивания СКЗИ в прикладные системы с целью оценки обоснованности и достаточности мер, принятых для защиты информации, обрабатываемой СКЗИ.

В случае использования вызовов, не входящих в перечень Приложения 1 документа ЖТЯИ.00096-01 95 01. Правила пользования, необходимо производить разработку отдельного СКЗИ на базе ПАКМ «КриптоПро HSM» версия 2.0 в соответствии с действующей нормативной базой (в частности, с Постановлением Правительства Российской Федерации от

16 апреля 2012 г. №313 и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)).

1.6. Формуляр входит в комплект поставки ПАКМ ЖТЯИ.00096-01 и должен постоянно храниться в органе (подразделении), ответственном за эксплуатацию ПАКМ, в печатном виде.

1.7. Все записи, вносимые в формуляр, должны быть заверены лицами, ответственными за эксплуатацию ПАКМ.

1.8. ПАКМ «КриптоПро HSM» версия 2.0 соответствует «Требованиям к средствам электронной подписи» (Приложение 1 к Приказу ФСБ РФ от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»).

2. ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ ПАКМ

При эксплуатации ПАКМ ЖТЯИ.00096-01 должны выполняться следующие требования:

2.1. Средствами ПАКМ не допускается обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

2.2. Допускается использование ПАКМ для криптографической защиты персональных данных.

2.3. Ключевая информация является конфиденциальной.

2.4. Срок действия ключа проверки ЭП – не более 15 лет после окончания срока действия соответствующего ключа ЭП.

2.5. Клиентские компоненты ПАКМ должны использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. В случае их отсутствия рекомендуется по возможности использовать существующие антивирусные средства защиты. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

2.6. Размещение компонент ПАКМ в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

2.7. При эксплуатации ПАКМ (ПАКМ, клиентские компоненты ПАКМ) необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К).

2.8. Установка программных компонент может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ и эксплуатационной документации (в соответствии с п. 7 ЖТЯИ.00096-01 90 02 Использование интерфейсных модулей).

3. ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

3.1. ПАКМ ЖТЯИ.00096-01 предназначен для защиты информации, не содержащей сведений, составляющих государственную тайну, в информационных системах с выполнением следующих функций:

- создание/проверка электронной подписи;
- вычисление значения хэш-функции областей памяти и файлов;
- шифрование/расшифрование областей памяти и файлов;
- вычисление имитовставки областей памяти и файлов;
- генерация и хранение ключей;
- уничтожение ключей:
 - при работе с российскими криптографическими алгоритмами;
 - при работе с алгоритмами SHA1, RSA, 3DES.
- сопряжение с устройством доступа по криптографически защищенным каналам «К»¹, «К2», «К2s»;
- удаленное выполнение операций создания/проверки электронной подписи и шифрования/расшифрования файлов.

Примечание 1: Канал «К» используется только в рамках Головного удостоверяющего центра.

3.2. ПАКМ «КриптоПро HSM» обеспечивает:

- реализацию криптографических функций и интерфейс взаимодействия ПАКМ с серверами и клиентскими компонентами ПАКМ пользователей;
- хранение более 500 000 ключевых контейнеров пользователей в зашифрованном виде;
- интерфейс к прикладным криптографическим функциям в соответствии со спецификацией интерфейса СКЗИ «КриптоПро CSP» версии 4.0;
- возможность использования функций ПАКМ через интерфейсы Microsoft CryptoAPI;
- возможность использования функций ПАКМ через интерфейс PKCS#11;
- идентификацию и аутентификацию пользователей при локальном и удаленном доступе к ПАКМ;
- проверку целостности критичного к безопасному функционированию ПО при инициализации ПАКМ;
- генерацию случайных чисел с использованием аппаратного ДСЧ;
- генерацию закрытого ключа с использованием исходного материала, предоставленного уполномоченной организацией;
- сопряжение ПАКМ с сервером/группой серверов по отдельному сегменту Ethernet;
- сопряжение ПАКМ с удаленным рабочим местом Web администрирования ПАКМ;
- ввод закрытого разделенного ключа активации ПАКМ с ключевых носителей на интеллектуальных картах;
- выполнение функций создания и проверки электронной подписи (ЭП) согласно ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, вычисление хэш-функции согласно ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2012;
- шифрование и имитозащита согласно ГОСТ 28147-89;
- возможность встречной работы ПАКМ «КриптоПро HSM» с СКЗИ «КриптоПро CSP»;

3.3. При встраивании ПАКМ уровень защиты данных, обрабатываемых результирующей системой с применением ПАКМ, определяется в рамках оценки влияния (см. п.1.5) среды функционирования ПАКМ на выполнение предъявленных к ПАКМ требований по классу KB/KB2 (при встраивании аппаратного модуля в соответствии с Комплектацией 1 Исполнением 1) или КСЗ (для аппаратного модуля в соответствии с иными исполнениями Комплектации 1).

3.4. Срок действия ключей ЭП, являющихся неэкспортируемыми, составляет не более 3-х лет. Максимальный срок действия ключей проверки ЭП - 15 лет. Максимальный срок действия открытых ключей обмена – не более 3-х лет. Максимальный срок действия неэкспортируемых закрытых ключей обмена составляет не более 3-х лет. Срок действия иных ключей не превышает 1 года 3 месяцев.

Примечание. Сроки действия ключей электронной подписи и закрытых ключей обмена могут уточняться при проведении работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПАКМ, на выполнение предъявленных к ПАКМ требований по ТЗ, согласованному с 8 Центром ФСБ России.

3.5. В ПАКМ «КриптоПро HSM» реализованы следующие российские криптографические алгоритмы:

- Алгоритм зашифрования/расшифрования данных и вычисление имитовставки реализован в соответствии с документом «ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
- Алгоритм формирования и проверки ЭП реализован в соответствии с документами «ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и «ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
- Алгоритм выработки значения хэш-функции реализован в соответствии с документами «ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования» и «ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования».

3.6. В ПАКМ «КриптоПро HSM» обеспечена возможность использования криптографических алгоритмов SHA1, RSA, 3DES.

3.7. Сетевая аутентификация реализована на базе протокола TLS v.1.0 (RFC 2246) с использованием алгоритмов п. 3.4 в соответствии с документом «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS). Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)».

4. КОМПЛЕКТНОСТЬ

Таблица 4.1 – Комплектация 1 «ПАКМ» (Исполнения 1,2,3,4)

Наименование	Количество, децимальный номер
Аппаратные компоненты	
ПАКМ «КриптоПро HSM». Системный блок	1 В соответствии с приложениями ЖТЯИ.00096-01 ТУ
Ключи электронного замка ПАКМ - идентификаторы Touch Memory. Один идентификатор (с маркировкой «А»), предназначен для проведения технического обслуживания предприятием-изготовителем; остальные служат для активации ПАКМ.	
Карта канала К/К2	4
Ключевой носитель – смарт-карта	16
Кабель электропитания	1
Считыватель смарт-карт	Опционально
Сетевой адаптер с оптическим интерфейсом SC	Опционально
Соединительный оптический патч-корд SC-SC, 3 м	Опционально
Программные компоненты	
ПАКМ «КриптоПро HSM». Базовые программные модули.	ЖТЯИ.00096-01 99 01
ПАКМ «КриптоПро HSM». Интерфейсные программные модули.	ЖТЯИ.00096-01 99 02
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-01 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-01 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-01 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-01 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-01 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-01 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-01 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-01 ТУ
Заверенная копия сертификата	

Таблица 4.2 – Комплектация 2 Исполнение 1 – «ПАКМ» и «КриптоПро HSM Client», уровень защиты КС1

Наименование	Децимальный номер
Аппаратные компоненты	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1
Программные компоненты	
ПО «КриптоПро HSM Client». Базовые программные модули.	ЖТЯИ.00096-01 99 03
ПО «КриптоПро CSP» версии 4.0 Исполнение 1-Base	ЖТЯИ.00087-01
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-01 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-01 90 02

Наименование	Децимальный номер
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-01 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-01 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-01 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-01 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-01 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-01 ТУ
Заверенная копия сертификата	

Таблица 4.3 – Комплектация 2 Исполнение 2 – «ПАКМ» и «КриптоПро HSM Client», уровень защиты КС2

Наименование	Децимальный номер
Аппаратные компоненты	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1
Средство защиты от несанкционированного доступа	См. Примечания п. 4
Программные компоненты	
ПО «КриптоПро HSM Client». Базовые программные модули.	ЖТЯИ.00096-01 99 03
ПО «КриптоПро CSP» версии 4.0 Исполнение 2-Base	ЖТЯИ.00088-01
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-01 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-01 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-01 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-01 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-01 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-01 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-01 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-01 ТУ
Заверенная копия сертификата	

Таблица 4.4 – Комплектация 2 Исполнение 3 – «ПАКМ» и «КриптоПро HSM Client», уровень защиты КС3

Наименование	Децимальный номер
Аппаратные компоненты	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1
Средство защиты от несанкционированного доступа	См. Примечания п. 4
Программные компоненты	
ПО «КриптоПро HSM Client». Базовые программные модули.	ЖТЯИ.00096-01 99 03
ПО «КриптоПро CSP» версии 4.0 Исполнение 3-Base	ЖТЯИ.00089-01
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-01 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-01 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-01 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-01 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-01 94 01

Наименование	Децимальный номер
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-01 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-01 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-01 ТУ
Secure Pack Rus версия 3.0.	ЕАРМ.5090005.032-03
Secure Pack Rus версия 3.0. Формуляр.	ЕАРМ.5090005.032-03 30 01
Заверенная копия сертификата	

Примечания:

1. Клиентская компонента «КриптоПро HSM Client» уровня защиты КС1 и КС2 функционирует в программно-аппаратных средах:

- Windows включает программно-аппаратные среды:
 - 7/8/8.1/10/Server 2003/2008 (x86, x64);
 - Server 2008 R2/2012/2012 R2/2016 (x64).
- Linux Standard Base ISO/IEC 23360 (ia32, x64), программно-аппаратные среды, удовлетворяющие стандарту LSB 4.x:
 - Cent OS (ia32, x64);
 - Fedora (ia32, x64);
 - Linpus (ia32);
 - Mandriva (ia32, x64);
 - MontaVista Linux (ia32, x64);
 - Oracle Enterprise Linux (ia32, x64);
 - Open SUSE (ia32, x64);
 - Red Hat Enterprise Linux (ia32, x64);
 - SUSE Linux Enterprise (ia32, x64);
 - SUSE LINUX (ia32);
 - Ubuntu (ia32, x64);
 - Xandros (ia32);
 - Trustverse Linux XP (ia32);
 - Debian (ia32, x64);
- Unix включает программно-аппаратные среды:
 - ALT Linux (ia32, x64);
 - FreeBSD (ia32, x64);
 - AIX (Power PC).

2. Клиентская компонента «КриптоПро HSM Client» уровня защиты КС3 функционирует в следующих программно-аппаратных средах

- Windows 7/8/8.1/10/Server 2003/2008 (x86, x64);
- Windows Server 2008 R2/2012/2012 R2/2016 (x64).

с пакетом Secure Pack Rus версия 3.0.

3. ПАКМ и клиентская компонента уровня защиты КВ функционируют в программно-аппаратных средах, согласованных с 8 центром ФСБ России.

4. В качестве средства защиты от несанкционированного доступа используется Программно-аппаратный комплекс с физическим датчиком случайных чисел «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180) или Аппаратно-программный модуль доверенной загрузки универсальный М-526Б (КРИПТОН ЗАМОК/У) КБДЖ.468243.067 ТУ. Поставка - по согласованию с пользователем.

5. Комплект документации предназначен администраторам безопасности и разработчикам прикладного программного обеспечения, использующего СКЗИ.

6. Программное обеспечение и документация в электронном виде в формате PDF (Adobe Acrobat Reader) на CD-ROM для всех исполнений СКЗИ поставляется единым дистрибутивом, формуляр и копия сертификата, заверенная ООО «КРИПТО-ПРО», - в печатном виде.

7. Использование СКЗИ в конкретной программно-аппаратной среде ограничивается лицензией.

5. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие ПАКМ «КриптоПро HSM» ЖТЯИ.00096-01 версия _____

серийный № дистрибутива _____

вид носителя:

CD-ROM _____ шт.

CD-ROM _____ шт.

_____ шт.

соответствует эталону и признано годным для эксплуатации.

Дата производства: «_____» _____ 20__ г.

Дата модернизации: «_____» _____ 20__ г.

М.П.

Генеральный директор

(подпись)

6. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие ПАКМ «КриптоПро HSM» ЖТЯИ.00096-01 версия _____

серийный № дистрибутива _____

упаковано в

коробку типа _____

Дата упаковки: "_____" _____ 20__ г.

М. П.

Упаковку произвел

(подпись)

7. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

- 7.1. Пользователь приобретает изделие ПАКМ «КриптоПро HSM» и должен использовать его в соответствии с рекомендациями, изложенными в эксплуатационной документации.
- 7.2. Предприятие-изготовитель гарантирует работоспособность изделия в соответствии с объявленными характеристиками в течение Гарантийного срока при соблюдении пользователем требований эксплуатационной документации на изделие.
- 7.3. Гарантийный срок изделия — 12 (двенадцать) месяцев. Датой начала гарантийного срока является дата производства изделия (см. п. 5).
- 7.4. В случае выявления в изделии дефектов, не связанных с нарушением правил эксплуатации, транспортирования и хранения (в соответствии с требованиями, предъявляемыми изготовителем носителей информации), в течение Гарантийного срока изделие подлежит рекламации, и предприятие-изготовитель обязуется по получении рекламации в возможно короткий срок устранить дефекты своими силами и средствами вплоть до поставки нового изделия, а также принять меры, исключающие эти дефекты во всех остальных экземплярах изделия.
- 7.5. Замена в изделии неисправных частей (деталей, узлов, сборочных единиц) в период гарантийного срока не ведет к установлению нового гарантийного срока на все изделие, либо на замененные части изделия. При этом гарантийный срок изделия продлевается на время, в течение которого изделие не использовалось из-за обнаруженных в нем недостатков.
- 7.6. Условия и порядок гарантийного обслуживания изделия приведены в Регламенте обслуживания оборудования, опубликованном на Интернет-сайте предприятия-изготовителя по адресу <https://www.cryptopro.ru>.
- 7.7. Действие гарантийных обязательств прекращается при истечении гарантийного срока.
- 7.8. Изготовитель предоставляет возможность продления сервисного обслуживания ПАКМ «КриптоПро HSM» в течение не менее 5 лет с даты производства изделия (см. п. 5) в соответствии с Регламентом обслуживания оборудования, опубликованном на Интернет-сайте предприятия-изготовителя по адресу <https://www.cryptopro.ru>.
- 7.9. Данные о поставке (продаже) изделия:

(наименование организации-поставщика (продавца) изделия)

М.П.

(подпись)

8. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

- 8.1. Рекламации, связанные с эксплуатацией изделия, должны направляться предприятию-изготовителю в письменном виде по адресу:
127018, Москва, ул. Сущёвский вал, д. 18.
- 8.2. Срок рассмотрения рекламации — 1 (один) месяц со дня получения рекламации.
- 8.3. При несоответствии поставляемого изделия, его тары, упаковки, консервации, маркировки и комплектности требованиям сопроводительной документации, пользователь обязан направить рекламацию предприятию-изготовителю в течении 60 дней со дня поставки изделия.
- 8.4. Предприятие-изготовитель принимает рекламацию, если не установлена вина получателя в возникновении дефекта в изделии.
- 8.5. Сведения о рекламациях представлены в табл. 1.

Таблица 1. Учет предъявленных рекламаций

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

