ООО Фирма «ИнфоКрипт»

УТВЕРЖДЕН

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «VPN-Key-TLS»

вариант исполнения 7

ФОРМУЛЯР
ИНФК.11485466.4012.021 30 05

2022

СОДЕРЖАНИЕ

Содержание 2
1. Общие указания 3
2. Общие сведения и основные характеристики 4
3. Комплектность 5
4. Свидетельство о приемке 7
5. Свидетельство об упаковке 7
6. Гарантии изготовителя 8
7. Сведения о рекламациях 9
8. Сведения о хранении 10
9. Сведения о закреплении изделия при эксплуатации 11
10. Сведения об изменениях 11
11. Особые отметки 12

1. ОБЩИЕ УКАЗАНИЯ

Перед эксплуатацией изделия необходимо внимательно ознакомиться с эксплуатационной документацией на средство криптографической защиты информации (СКЗИ), приведенной в разделе «Комплектность», и обеспечить выполнение комплекса организационно-технических мероприятий, определенных в документации.

Формуляр должен постоянно находиться в подразделении, ответственном за эксплуатацию изделия.

Все записи в формуляре производятся отчетливо и аккуратно. Незаверенные исправления не допускаются.

2. ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

Изделие – программное и программно-аппаратное средство криптографической защиты информации «VPN-Key-TLS», ИНФК.11485466.4012.021.

СКЗИ «VPN-Key-TLS» предназначено для обеспечения защиты конфиденциальной информации, не составляющей государственной тайны.

Данный формуляр распространяется на СКЗИ «VPN-Key-TLS» в варианте исполнения 7.

СКЗИ «VPN-Key-TLS» в данном варианте исполнения соответствует

- «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» для классов КС1-КС2;
- «Требованиям к средствам электронной подписи» для классов КС1/КС2 (утверждены приказом ФСБ России №796 от 27 декабря 2011 г.);
- «Специальным требованиям к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации (СТ-Р)» по уровню $КС_Б$;
- «Требованиям по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» по уровню защищенности $КС_Б$.

СКЗИ «VPN-Key-TLS» в данном варианте исполнения обеспечивает выработку данных для реализации двухсторонней аутентификации, контроля целостности и конфиденциальности информационного обмена исполнений СКЗИ в соответствии с протоколом TLS 1.2 (RFC 5246), шифрование и создание/проверку электронной подписи блоков данных, поступающих в устройство «VPN-Key-TLS», генерацию ключевой информации, в соответствии с:

- ГОСТ 28147-89 «СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ»;
- ГОСТ Р 34.11-2012 «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ФУНКЦИЯ ХЭШИРОВАНИЯ»;
- ГОСТ Р 34.10-2012 «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ПРОЦЕССЫ ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ».

Хранение ключевой информации осуществляется в устройстве «VPN-Key-TLS» в защищенной области памяти.

3. КОМПЛЕКТНОСТЬ

СКЗИ **«VPN-Key-TLS»** поставляется в следующих комплектациях:

Комплектация варианта исполнения 7

Наименование	Обозначение	Количество
firmware550.bin	11485466.72.21.12.124	1****
start	11485466.72.21.12.125	1****
HashCtrl.exe (Windows)	11485466.72.21.12.103	1*****
hashctrl.lin64 (Linux)	11485466.72.21.12.103-04	1*****
hashctrl (MacOS)	11485466.72.21.12.103-05	1*****
АПМДЗ (обязателен к использованию для класса КС2)		1*
СКЗИ «VPN-Key-TLS» вариант исполнения 7. Формуляр	ИНФК.11485466.4012.021 30 05	1***
СКЗИ «VPN-Key-TLS» вариант исполнения 7. Правила пользования	ИНФК.11485466.4012.021 34 05	1***
СКЗИ «VPN-Key-TLS» вариант исполнения 7. Руководство пользователя	ИНФК.11485466.4012.021 91 05	1***
Инструкция по эксплуатации программы контроля целостности	11485466.72.21.12.103-02 91	1***, *****
СКЗИ «VPN-Key-TLS» вариант исполнения 7. Инструкция программиста. Описание HTTP-интерфейса устройства	11485466.72.21.12.124 33 01	1**, ***
СКЗИ «VPN-Key-TLS» вариант исполнения 7. Инструкция программиста. Описание CCID интерфейса	111485466.72.21.12.124 33 02	1******, ***
Сертификат ФСБ (копия)		1***

*: поставляется по согласованию с покупателем, допускается использование АПМДЗ, имеющего действующий сертификат ФСБ России по требованиям к аппаратно-программным модулям доверенной загрузки ПЭВМ.
**: предназначено разработчикам прикладного программного обеспечения, использующего СКЗИ в варианте исполнения 7, поставка осуществляется по отдельному запросу на договорных условиях.
***: документация, включая заполненный формуляр, поставляется в электронном виде, поставка на бумажном носителе возможна по отдельному запросу на договорных условиях.
****: может поставляться в установленном в устройства, изготовленные в соответствии с ТУ 11485466.26.20.40.140.028.002, виде.
*****: поставляется по отдельному запросу в зависимости от эксплуатируемой ОС.
******: предназначено разработчикам средств криптографической защиты информации, встраивающим СКЗИ «VPN-Key-TLS» в варианте исполнения 7, поставка осуществляется по отдельному запросу на договорных условиях.

Контрольное значение на программный модуль "firmware550.bin", рассчитанное программой HashCtrl.exe с ключом "/h3":
9E 8E 55 30 6D 70 F1 7E 66 91 FB FC 9F C9 02 C4 1D 91 CD 5D 82 DC 68 AE 7A C7 7C C0 3B B3 82 35

Контрольное значение на все программные модули приложения "start", рассчитанное программой HashCtrl.exe с ключом "/h256" в потоковом режиме:
3D C1 B7 9F 80 70 B6 99 98 57 79 40 01 3F 43 90 C4 C3 92 F9 1F 36 66 88 14 DF F8 73 9E 80 51 68

Контрольное значение на программный модуль "HashCtrl.exe" (Windows), рассчитанное программой HashCtrl.exe с ключом "/h256":
B7 69 86 F7 97 05 30 B7 D7 FB 7E 2F 05 C9 67 D9 8D 9D 34 84 1D 5F B3 96 06 6C B8 65 05 87 AB 79

Контрольное значение на программный модуль "hashctrl.lin64" (Linux 64 бита), рассчитанное программой HashCtrl.exe с ключом "/h256":
1B DC 6C FF 5C 5E 32 AC 02 89 18 DA A7 B7 A2 A4 E3 43 74 43 1E F4 CE 8B E1 9C 76 B6 0C D8 9D 99

Контрольное значение на программный модуль "hashctrl" (MacOS), рассчитанное программой HashCtrl.exe с ключом "/h256":
80 A4 DD 4C 6A 54 D4 77 62 8A 34 30 47 3F A9 C4 00 55 0B 08 91 50 F0 6B 6F D7 F4 C3 C2 CA 3A 30

4. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие СКЗИ **«VPN-Key-TLS»** ИНФК.11485466.4012.021, вариант исполнения 7, учетный индекс Н-136Ж, регистрационный номер 879Ж-_____

вид носителя:

☐ CD-ROM	_____ шт.
☐ Flash Memory	_____ шт.
☐ аппаратный модуль	_____ шт.
☐ «VPN-Key 6.0una»	серийный номер _____
☐ «CCAG14000»	серийный номер _____

соответствует эталону, хранящемуся в _____, и признано годным для эксплуатации.

Дата выпуска: «_____»_____ 20__ г.

М.П.

_____

5. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие СКЗИ **«VPN-Key-TLS»** ИНФК.11485466.4012.021, вариант исполнения 7, учетный индекс Н-136Ж, регистрационный номер 879Ж-_____ маркировано и упаковано _____.

Дата маркировки _____.

Маркировку произвел _____.

Дата упаковки _____.

Упаковку произвел _____.

Изделие после упаковки принял _____.

М.П.

6. ГАРАНТИИ ИЗГОТОВИТЕЛЯ

6.1. Изготовитель гарантирует работоспособность Изделия в соответствии с объявленными характеристиками при условии соблюдения Пользователем правил и условий хранения, транспортировки, монтажа, установки и эксплуатации в течение __ месяцев со дня поставки.

Под неисправностью Изделия понимается неудовлетворительное качество функционирования или отказ от функционирования в оговоренных в эксплуатационной документации условиях, обусловленные устойчивым (регулярным) выходом параметров программных и (или) аппаратных компонент за границы допустимых значений, предписанных их Изготовителем.

6.2. В течение гарантийного срока Изготовитель безвозмездно устраняет дефекты Изделия при условии соблюдения Пользователем правил и условий хранения, транспортировки, монтажа, установки и эксплуатации.

6.3. Изготовитель производит гарантийный ремонт при условии возврата Изделия (компоненты Изделия) в упаковке.

6.4. Если в период гарантийного срока Изделие вышло из строя по вине Пользователя вследствие неправильного хранения, транспортировки, монтажа, установки, эксплуатации Изделия, внесения изменений в Изделие без согласования с Изготовителем или других причин, то ремонт производится за счет Пользователя.

6.5. Консультации осуществляются по "горячей" линии с 9-30 до 18-00 по Московскому времени по телефонам (495) _____ или E-mail _____.

6.6. По мере модернизации Изделия Изготовитель обязуется информировать Пользователя о новых версиях Изделия.

7. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

7.1. Порядок предъявления рекламаций

7.1.1. Рекламация может быть предъявлена Изготовителю в период гарантийного срока как при приемке Изделия, так и в процессе его хранения и эксплуатации.

7.1.2. Факт несоответствия Изделия эксплуатационной документации должен быть оформлен актом. Акт должен содержать сведения об условиях эксплуатации Изделия и о выявленном несоответствии и обеспечивать возможность точного повторения ситуации, при которой оно было обнаружено. Акт подписывается лицами, эксплуатирующими Изделие, утверждается руководителем предприятия (организации) Пользователя и направляется Изготовителю, который принимает меры по устранению выявленного несоответствия, если оно подтверждается.

7.2. Устранение неисправности производится Изготовителем изделия. Адрес предприятия-изготовителя: _____.

7.3. Содержание рекламаций и меры, принятые по ним, записываются в таблице:

Учет предъявленных рекламаций

Дата обнаружения неисправности	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

8. СВЕДЕНИЯ О ХРАНЕНИИ

8.1. Изделие должно храниться в помещении при температуре от +4 до +50 °С и относительной влажности воздуха от 30% до 80%.

8.2. При хранении Изделия должны быть исключены резкие изменения температуры и влажности воздуха, а также воздействие прямых солнечных лучей.

8.3. В помещениях для хранения Изделия необходимо исключить возможность попадания в воздух паров агрессивных веществ (кислот, щелочей), вызывающих коррозию изделия.

8.4. Не допускается хранение Изделия вблизи сильных электромагнитных полей, а также на расстоянии менее, чем один метр от нагревательных приборов.

8.5. Контроль условий хранения проводится пользователем ежеквартально. Сведения о хранении заносятся в таблицу:

Таблица

Дата установки на хранение		Дата снятия с хранения	Условия хранения

9. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ

Должность ответственного лица	Фамилия ответственного лица	Номер и дата приказа об назначении	Номер и дата приказа об освобождении	Подпись ответственного лица

10. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

№ п/п	Основание (№ сопроводитель-ного документа и дата)	Дата проведения изменения	Содержание изменения	Должность, фамилия и подпись лица, ответственного за изменения	Подпись лица, ответственного за эксплуатацию изделия

11. ОСОБЫЕ ОТМЕТКИ