ООО Фирма «ИнфоКрипт»

УТВЕРЖДЕНО
ИНФК.11485466.4012.021 34 05-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«VPN-Key-TLS»

вариант исполнения 7

Правила пользования

ИНФК.11485466.4012.021 34 05

2022

Предисловие

Настоящие правила пользования распространяются на СКЗИ «VPN-Key-TLS» в варианте исполнения 7 (далее СКЗИ «VPN-Key-TLS») и обязательны для выполнения пользователями СКЗИ «VPN-Key-TLS».

Правила пользования составлены в соответствии с документом ТС 26.2.001–2020 «Состав и содержание правил пользования средств криптографической защиты информации».

Содержание

1 Перечень используемых терминов и сокращений 4

2 Назначение СКЗИ и его основные характеристики 5

3 Ключевая система и ключевые документы 10

3.1 Характеристики ключевой системы 10
3.2 Управление ключевой информацией 11

4 Порядок распространения и учета СКЗИ 13

4.1 Способы передачи и хранения СКЗИ 14
4.2 Поэкземплярный учет СКЗИ 15

5 Требования по обеспечению безопасности при вводе СКЗИ в эксплуатацию 15

5.1 Требования к встраиванию СКЗИ в прикладные системы и к проведению исследований СФ СКЗИ 15
5.2 Требования по размещению 16
5.3 Требования к персоналу, обслуживающему СКЗИ 18
5.4 Инициализация и ввод СКЗИ в эксплуатацию 19

6 Требования по обеспечению безопасности при эксплуатации СКЗИ 20

6.1 Общие требования по защите от НСД 20
6.2 Требования к аутентификации и разграничению доступа 24
6.3 Требования по обеспечению целостности СКЗИ 25
6.4 Порядок обеспечения работоспособности СКЗИ 26

7 Требования по обеспечению безопасности при выводе СКЗИ из эксплуатации 29

1 Перечень используемых терминов и сокращений

В настоящем документе использованы следующие термины с соответствующими определениями:

Термин	Определение
АРМ инициализации	Изделие «АРМ инициализации» из состава СКЗИ «VPN-Key-TLS Администратор»
АРМ управления обновлениями	Изделие «АРМ управления обновлениями» из состава СКЗИ «VPN-Key-TLS Администратор»
PIN-код	Пароль доступа к устройству
PUK-код	Дополнительный код доступа, предназначенный для разблокирования устройства после троекратного неправильного ввода PIN-кода

В настоящем документе используются следующие обозначения и сокращения:

Обозначение	**Описание**
АРМ	Автоматизированное рабочее место
АПМДЗ	Аппаратно-программный модуль доверенной загрузки
АС	Аппаратные средства
НЖМД	Накопитель на жёстком магнитном диске
НСД	Несанкционированный доступ
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
ПЭВМ	Персональная электронная вычислительная машина
СКЗИ	Средство криптографической защиты информации
СФ	Среда функционирования
УЦ	Удостоверяющий центр
ФКН	Функциональный ключевой носитель
ЭП	Электронная подпись

2 Назначение СКЗИ и его основные характеристики

2.1 СКЗИ «VPN-Key-TLS» в варианте исполнения 7 (учётный индекс Н-136Ж) предназначено для шифрования, имитозащиты, электронной подписи и проверки подписи данных, организации клиентской части протокола TLS 1.2 (RFC 5246) и реализации безопасного хранения и использования секретных ключей.

СКЗИ «VPN-Key-TLS» может использоваться:

- в качестве персонального средства криптографической защиты информации;
- в качестве средства электронной подписи;
- для создания на его базе криптографических систем (путём разработки программного обеспечения, обеспечивающего прикладные функции криптографической системы).

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

2.3 Состав СКЗИ:

- микрокод firmware550.bin, функционирующий в специализированном устройстве «VPN-Key-TLS», изготовленном в соответствии с ТУ 11485466.26.20.40.140.028.002;
- программный модуль start, функционирующий на ПЭВМ под управлением ОС Windows (имеет название «start.exe»), Linux (имеет название «Linux_x64»), MacOS (имеет название «\Start.app\Contents\MacOS\Start») (далее start.exe).
- программный модуль hashctrl, функционирующий на ПЭВМ под управлением ОС Windows (имеет название hashctrl.exe), Linux, MacOS (имеет название hashctrl, далее по тексту используется название hashctrl.exe);
- сертифицированный ФСБ России АПМДЗ (для класса КС2);
- СКЗИ «VPN-Key-TLS» вариант исполнения 7. Формуляр.

ИНФК.11485466.4012.021 30 05;

- Правила пользования. ИНФК.11485466.4012.021 34 05;
- СКЗИ «VPN-Key-TLS» вариант исполнения 7. Руководство пользователя. ИНФК.11485466.4012.021 91 05;
- Программа контроля целостности HashCtrl. Инструкция по эксплуатации. 11485466.72.21.12.103-02 91;
- СКЗИ «VPN-Key-TLS» вариант исполнения 7. Инструкция программиста. Описание HTTP-интерфейса устройства. 11485466.72.21.12.124 33 01 (предназначена разработчикам прикладного программного обеспечения, использующего СКЗИ);
- СКЗИ «VPN-Key-TLS» вариант исполнения 7. Инструкция программиста. Описание CCID-интерфейса. 11485466.72.21.12.124 33 02 (предназначена разработчикам средств криптографической защиты информации, непосредственно взаимодействующим с микрокодом из состава СКЗИ).

2.4 К основным функциям СКЗИ «VPN-Key-TLS» относятся:

- реализация клиентской стороны протокола TLS в соответствии с RFC 5246 (TLS 1.2) и Рекомендациями по стандартизации «Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)» ТК26 2014 год;
- реализация абонентского шифрования в формате CMS в соответствии с RFC 5652 и Рекомендациями по стандартизации «Использование наборов алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS» ТК26 2014 год;
- создание ЭП в соответствии с ГОСТ Р 34.10-2012 в том числе в формате CMS в соответствии с RFC 5652 и Рекомендациями по стандартизации «Использование наборов алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях

формата CMS» ТК26 2014 год;

- проверка ЭП в соответствии с ГОСТ Р 34.10-2012 и ГОСТ Р 34.10 2001, в том числе в формате CMS в соответствии с RFC 5652 и Рекомендациями по стандартизации «Использование наборов алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS» ТК26 2014 год;
- создание ключевой информации в соответствии с ГОСТ Р 34.10 2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
- вычисление имитовставки для данных в соответствии с ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая»;
- реализация установки, безопасного хранения и использования секретных ключей, сформированных как внутри устройства, так и внешним приложением.

2.5 СКЗИ «VPN-Key-TLS» удовлетворяет:

- «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну», для классов КС1 и КС2;
- «Требованиям к средствам электронной подписи» для классов КС1 и КС2 при выполнении операций: создания ЭП для пользовательских данных в автоматическом режиме; проверки ЭП для пользовательских данных в режиме автоматической проверки ЭП; создания ключа ЭП, создания ключа проверки ЭП;
- «Специальным требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведения, составляющих государственную тайну, и эксплуатируемых на территории Российской Федерации» по уровню

$КС_Б$;

– «Требованиям по защите линейной передачи средства криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» по уровню защищенности $КС_Б$.

2.6 СКЗИ «VPN-Key-TLS» использует устройства «VPN-Key-TLS», подключаемые к USB-порту ПЭВМ.

2.7 СКЗИ «VPN-Key-TLS» должно функционировать на ПЭВМ, удовлетворяющую следующим программным и аппаратным требованиям:

– процессор не ниже Pentium II, НЖМД ёмкостью не менее 10 Гб, ОЗУ ёмкостью не менее 1 Гб, наличие USB-порта. Для класса КС2 на ПЭВМ должен быть установлен АПМДЗ, сертифицированный в соответствии с требованиями ФСБ России к аппаратно-программным модулям доверенной загрузки ЭВМ;

– ПЭВМ должна работать под управлением одной из следующих ОС:

  - Windows 7;
  - Windows 8.1;
  - Windows 10;
  - Windows 11;
  - MacOS Catalina 10.15;
  - MacOS BigSur 11;
  - MacOS Monterey 12;
  - MacOS Ventura 13;
  - ubuntu 16.04 LTS x64;
  - ubuntu 18.04 LTS x64;
  - ubuntu 20.04 LTS x64;
  - ubuntu 22.04 LTS x64;
  - Alt workstation 9 x64;
  - Alt workstation 10 x64;
  - CentOS Stream 8 x64;
  - Debian 10 x64;

- Debian 11 x64;
- Fedora Linux 36;
- Mcst Elbrus 6;
- REDOS 7.3 MUROM x64;
- Astra Linux C2 x64;
- Astra Linux SE 1.7.0 x64;

– СКЗИ может функционировать под управлением одной из следующих виртуальных сред (гипервизоров):

- Microsoft Hyper-V Server 2012/2012R2/2016/2019;
- Citrix XenServer 7.1;
- Citrix Virtual Apps and Desktops 7;
- VMWare WorkStation 16 (x86, x64);
- VMWare WorkStation Player 16 (x86, x64);
- VMWare Fusion 13;
- QEMU 7;
- VMWare vSphere ESXi (6.7, 7.0);
- Oracle VirtualBox (6.1, 7.0);
- Parallels Desktop (Mac OS) 18 (x64).

2.8 Для указанных ОС и гипервизоров должно быть обеспечено получение обновлений по безопасности. В случае подключения СКЗИ к каналам связи, выходящим за пределы контролируемой территории, не допускается использование ОС и (или) гипервизоров, производителями которых не выпускаются обновления.

2.9 Под управлением виртуальных сред СКЗИ функционирует по уровню защиты КС1.

2.10 Устройства «VPN-Key-TLS» должны физически подключаться к вычислительному средству, на котором функционирует ПО СКЗИ. Допускается удаленное подключение устройств «VPN-Key-TLS» при условии реализации специальных (дополнительных) мер и проведении оценки их влияния на СКЗИ «VPN-Key-TLS» в соответствии с ПКЗ-2005.

2.11 СКЗИ «VPN-Key-TLS» реализует следующие интерфейсы:

- HTTP-интерфейс;
- Интерфейс командной строки;
- Графический интерфейс пользователя (веб-интерфейс);
- APDU-интерфейс.

3 Ключевая система и ключевые документы

3.1 Характеристики ключевой системы

3.1.1 СКЗИ «VPN-Key-TLS» использует ключевую систему типа «открытое распределение ключей».

3.1.2 СКЗИ «VPN-Key-TLS» использует следующие типы ключей:

Ключи	Описание
Корневой ключ проверки подписи УЦ	Входящий в состав корневого сертификата УЦ ключ, с помощью которого проверяется подпись загружаемых в хранилище устройства сертификатов, устанавливается в устройство средствами АРМ инициализации.
Ключ проверки подписи АРМ инициализации	Расположенный на устройстве «VPN-Key-TLS» ключ, с помощью которого проверяется подпись загружаемых средствами **АРМ инициализации** на устройство сертификатов ключей первичного соединения TLS и транспортных ключей. Создается средствами АРМ инициализации, соответствующий ему сертификат выпускается удостоверяющим центром и устанавливается в устройство средствами АРМ инициализации.
Первичный ключ TLS	Ключевая пара, вырабатываемая устройством «VPN-Key-TLS» в процессе инициализации устройства на **АРМ инициализации**. Первичные ключи TLS используются для соединения СКЗИ с TLS-сервером до того момента, пока на СКЗИ не сформируются пользовательские ключи соединения TLS
Транспортный ключ	Ключевая пара, вырабатываемая устройством «VPN-Key-TLS» в процессе инициализации устройства на **АРМ инициализации**. Транспортные ключи используются для заверения запросов на сертификаты пользовательских ключей соединения TLS и ключей ЭП или шифрования
Ключи ЭП	Ключевая пара, вырабатываемая устройством «VPN-Key-TLS», с помощью которой осуществляется создание и/или проверка электронной подписи
Ключи шифрования	Ключевая пара, вырабатываемая устройством «VPN-Key-TLS», с помощью которой формируется ключ шифрования ключа защиты
Ключ шифрования ключа защиты	Ключ, вырабатываемый устройством «VPN-Key-TLS», с помощью которого шифруются ключи защиты (не сохраняется в устройстве)

Ключ защиты	Ключ, вырабатываемый устройством «VPN-Key-TLS» и предназначенный для шифрования данных (не сохраняется в устройстве)
Ключи TLS	Ключевая пара, вырабатываемая устройством «VPN-Key-TLS», с помощью которой осуществляется защищенное соединение СКЗИ с TLS-сервером
Ключ проверки подписи обновлений ПО	Расположенный на устройстве «VPN-Key-TLS» ключ, с помощью которого проверяется подпись загружаемых на устройство обновлений ПО. Создаётся и записывается в устройство средствами АРМ управления обновлениями

3.1.3 Ключевыми носителями являются устройства «VPN-Key-TLS». Секретные ключи из состава ключевых пар «Ключи ЭП», «Ключи шифрования», «Ключи TLS» хранятся в устройстве в защищенном хранилище в зашифрованном виде.

3.1.4 СКЗИ «VPN-Key-TLS» поддерживает размеры секретных ключей 256 и 512 битов, открытых ключей 512 и 1024 бита соответственно.

3.1.5 Сроки действия ключевой информации не должны превышать 3 лет, за исключением открытых ключей ЭП, срок их действия не должен превышать 15 лет, и ключей защиты, срок их действия определяется ограничениями, установленными на такие ключи в СКЗИ, с которым взаимодействует СКЗИ «VPN-Key-TLS», но не должен превышать 3 лет.

3.1.6 Пользователь СКЗИ должен не реже 1 раза в 3 года обращаться на АРМ инициализации для замены корневого сертификата, транспортных ключей и первичных ключей TLS с последующим формированием новых ключей ЭП, ключей шифрования и ключей TLS.

3.1.7 Пользователь СКЗИ должен не реже 1 раза в 3 года формировать новые ключи ЭП, ключи шифрования и ключи TLS в устройстве «VPN-Key-TLS».

3.2 Управление ключевой информацией

3.2.1 Транспортировка ключевых носителей на рабочее место пользователя СКЗИ должна осуществляться доверенным образом. Ключевые носители пользователей должны храниться непосредственно у пользователей, если иное не предусмотрено политикой безопасности эксплуатирующей организации.

3.2.2 Резервирование ключевой информации не предусмотрено.

3.2.3 СКЗИ должно быть инициализировано средствами АРМ инициализации в соответствии с документом «СКЗИ “VPN-Key-TLS Администратор”. Изделие “АРМ инициализации”. Руководство пользователя. 11485466.72.21.12.075 91», при этом в устройство «VPN-Key-TLS» будут установлены корневой сертификат, транспортные ключи и первичные ключи TLS. Одновременно с этим в устройство записывается инициализирующая последовательность для программного датчика случайных чисел, реализованного в СКЗИ.

3.2.4 Формирование ключей ЭП, ключей шифрования и ключей TLS должно производиться в соответствии с документом «СКЗИ “VPN-Key-TLS” вариант исполнения 7. Руководство пользователя. ИНФК.11485466.4012.021 91 05».

3.2.5 Использование ключевой информации должно производиться в соответствии с документом «СКЗИ “VPN-Key-TLS” вариант исполнения 7. Руководство пользователя. ИНФК.11485466.4012.021 91 05».

3.2.6 Под явной компрометацией ключевой информации в настоящем документе понимается разглашение PIN- и PUK-кодов, хищение, утрата или временная потеря ключевого носителя, несанкционированный доступ к ключевому носителю, обнаружение следов взлома ключевого носителя при эксплуатации или транспортировке.

3.2.7 В случае явной компрометации ключевой информации необходимо немедленно после выявления факта компрометации прекратить использование устройства «VPN-Key-TLS», уведомить об этом ответственных лиц с целью помещения сертификатов скомпрометированных ключей в список отозванных сертификатов и выполнить в отношении имеющегося устройства (при разглашении PIN- или PUK-кодов) или нового устройства (в остальных случаях явной компрометации) требования пунктов 3.2.3 и 3.2.4 настоящих Правил.

3.2.8 Под неявной компрометацией ключевой информации в настоящем документе понимается увольнение работников, имевших доступ к ключевым

документам, выявление нарушений правил эксплуатации или транспортировки ключевых носителей, предусмотренных политикой безопасности эксплуатирующей организации, любые случаи неработоспособности ключевых носителей.

3.2.9 Случаи неявной компрометации ключевой информации необходимо рассматривать в каждом случае отдельно и принимать решение о наличии или отсутствии компрометации исходя из результатов проведения разбирательства, проводимого в соответствии с требованиями политики безопасности, принятой в организации, в области неявной компрометации ключевой информации.

3.2.10 При обнаружении попытки несанкционированного доступа к техническим средствам, на которых эксплуатируется СКЗИ, необходимо переустановить операционную систему и ПО СКЗИ, устанавливаемого на ПЭВМ.

3.2.11 Ключевая информация на ключевых носителях, срок действия которой истек, уничтожается средствами АРМ инициализации (необходимо выполнить в отношении носителя требования пунктов 3.2.3 и 3.2.4 настоящих Правил).

Уничтожение ключевых носителей, в том числе вышедших из строя, осуществляется путем их разрушения с помощью кусачек или других инструментов с уничтожением микросхем.

3.2.12 Стороннее средство «удостоверяющий центр» используется для создания корневых сертификатов, сертификатов по запросам, созданным с помощью СКЗИ «VPN-Key-TLS», и списков аннулированных сертификатов. В качестве такого средства должно использоваться сертифицированное СКЗИ.

4 Порядок распространения и учета СКЗИ

Транспортировка, учет, хранение, размещение, техническое обслуживание, эксплуатация, уничтожение СКЗИ «VPN-Key-TLS» и технической документации к нему, а также допуск к ключевым документам должны осуществляться в строгом соответствии с:

– Положением о разработке, производстве, реализации и эксплуатации

шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005, зарегистрировано в Минюсте РФ 3 марта 2005 г. № 6382);

- Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (приложение к Приказу ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152, зарегистрировано в Минюсте РФ 6 августа 2001 г. № 2848);
- формуляром «СКЗИ “VPN-Key-TLS” вариант исполнения 7. Формуляр. ИНФК.11485466.4012.021 30 05»;
- настоящими Правилами пользования.

4.1 Способы передачи и хранения СКЗИ

4.1.1 Передача СКЗИ «VPN-Key-TLS» и эксплуатационной документации к нему на бумажном носителе между различными организациями должна происходить с оформлением актов передачи в двух экземплярах, в которых должны быть указаны названия, количество, учетные номера передаваемых изделий; аппаратные средства, документация на СКЗИ на бумажном носителе, носители информации, входящие в комплект поставки, должны быть упакованы способами, обеспечивающими контроль вскрытия упаковки. Передача СКЗИ «VPN-Key-TLS» и эксплуатационной документации к нему в пределах эксплуатирующей организации может быть определена политикой безопасности эксплуатирующей организации.

Эксплуатационная документация в электронном виде должна сопровождаться электронной подписью, сформированной с использованием ключей подписи организации-производителя СКЗИ.

4.1.2 Допускается транспортирование СКЗИ «VPN-Key-TLS» и эксплуатационной документации к нему на бумажном носителе в тарной упаковке автотранспортом и железнодорожным транспортом, хранение в

упаковке в отапливаемых помещениях в соответствии с требованиями ГОСТ 21552-84.

Хранение СКЗИ «VPN-Key-TLS» и эксплуатационной документации к нему в эксплуатирующей организации должно осуществляться способами, обеспечивающими невозможность подмены (например, в сейфе).

4.1.3 Ответственное лицо в эксплуатирующей организации в процессе приемки СКЗИ «VPN-Key-TLS» и эксплуатационной документации к нему должно осуществить проверку комплектности СКЗИ и документации в соответствии с разделом «Комплектность» в формуляре на изделие, маркировку изделия. При получении эксплуатационной документации в электронном виде должна быть проверена правильность электронной подписи документации с использованием средства ЭП или с использованием службы проверки электронной подписи справочно-информационного интернет-портала сервиса Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)» https://www.gosuslugi.ru/eds.

4.2 Поэкземплярный учет СКЗИ

4.2.1 Используемые или хранимые СКЗИ «VPN-Key-TLS» и эксплуатационная документация к ним подлежат поэкземплярному учету с использованием условных наименований и регистрационных номеров.

5 Требования по обеспечению безопасности при вводе СКЗИ в эксплуатацию

5.1 Требования к встраиванию СКЗИ в прикладные системы и к проведению исследований СФ СКЗИ

5.1.1 Для СКЗИ «VPN-Key-TLS» предусмотрены следующие варианты использования:

1. самостоятельное использование для выполнения криптографических операций (ЭП и проверка ЭП, зашифрование и расшифрование данных) средствами:

– графического интерфейса пользователя СКЗИ («СКЗИ “VPN-Key-

TLS” вариант исполнения 7. Руководство пользователя. ИНФК.11485466.4012.021 91 05»);

– интерфейса командной строки и HTTP-интерфейса («СКЗИ “VPN-Key-TLS” вариант исполнения 7. Описание HTTP-интерфейса. 111485466.72.21.12.124 33 01»);

2. самостоятельное использование для организации TLS-соединения с использованием веб-браузера;

3. эксплуатация прикладного программного обеспечения, использующего HTTP-интерфейс СКЗИ («СКЗИ “VPN-Key-TLS” вариант исполнения 7. Описание HTTP-интерфейса. 111485466.72.21.12.124 33 01») (разработка ППО должна вести с использованием функций, указанных в Приложении 1 к настоящим Правилам, при разработке ППО должна быть проведена оценка его влияния на СКЗИ);

4. эксплуатация другим СКЗИ устройства «VPN-Key-TLS» в качестве функционального ключевого носителя с использованием APDU-интерфейса (разработка указанного СКЗИ должна проводиться в соответствии с ПКЗ-2005), перечень команд APDU-интерфейса приведен в документе «СКЗИ “VPN-Key-TLS” вариант исполнения 7. Инструкция программиста. Описание CCID-интерфейса. 11485466.72.21.12.124 33 02»).

5.1.2 Результаты работы СКЗИ «VPN-Key-TLS» во всех вариантах должны использоваться в соответствии с политикой безопасности эксплуатирующей организации.

5.1.3 При использовании СКЗИ «VPN-Key-TLS» в четвертом варианте, установка ключей в устройство «VPN-Key-TLS» должна осуществляться только после проверки разрешения на такую установку, полученного от СКЗИ «VPN-Key-TLS».

5.2 Требования по размещению

5.2.1 Устройство «VPN-Key-TLS» по воздействию климатических факторов относится к группе 1 ГОСТ 21552-84 и предназначено для установки в

отапливаемых помещениях и эксплуатации в условиях круглосуточной или сменной работы.

Нормальными климатическими условиями эксплуатации устройства являются:

- температура окружающего воздуха - 20 ± 5ºС;
- относительная влажность окружающего воздуха - 60 ± 15 %;
- атмосферное давление - от 84 до 107 кПа (630–800 мм рт. ст.).

5.2.2 Должны быть приняты организационно-технические меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства, оснащенные СКЗИ «VPN-Key-TLS», посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.

5.2.3 Должны быть приняты организационно-технические меры по исключению несанкционированного доступа к техническим средствам, оснащенным СКЗИ «VPN-Key-TLS», лиц, не являющихся пользователями СКЗИ (при использовании СКЗИ по классу КС2).

5.2.4 Должны выполняться требования политики безопасности, принятой в организации в области размещения технических средств, обрабатывающих конфиденциальную информацию.

5.2.5 Для обеспечения специальной защиты СКЗИ должны выполняться следующие требования:

1. Для обеспечения защиты ключевой и открытой информации СКЗИ по уровню $КС_Б$ от утечки по каналу связи при подключении объектов информатизации (ПЭВМ, аппаратно-программные комплексы и др.), в которые устанавливается СКЗИ «VPN-Key-TLS», к каналам связи, выходящим за пределы контролируемой территории, необходимо чтобы канал связи был реализован в виде:

- радиоканалов GSM, GPRS, 3G\4G, WiFi, а также других современных каналов мобильной или беспроводной связи;
- волоконно-оптической линии связи, уходящей за пределы контролируемой зоны.

2. Использование СКЗИ «VPN-Key-TLS» в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, без проведения специальных исследований и специальной проверки АС СКЗИ и АС СФ СКЗИ запрещается.

3. В случае планирования размещения СКЗИ «VPN-Key-TLS» в помещениях, в которых присутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и (или) установлены АС и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, АС иностранного производства, входящие в состав СКЗИ и СФ СКЗИ «VPN-Key-TLS», должны быть подвергнуты проверкам по выявлению устройств, предназначенных для негласного получения информации.

В случае планирования размещения СКЗИ «VPN-Key-TLS» в помещениях, в которых отсутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и не установлены АС и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, решение о проведении проверок АС иностранного производства, входящих в состав СКЗИ и СФ СКЗИ «VPN-Key-TLS», принимается организацией, обеспечивающей эксплуатацию данных средств ЭП.

5.2.6 Требования к размеру контролируемой зоны отсутствуют.

5.2.7 Хранение СКЗИ «VPN-Key-TLS» и носителей с документацией на СКЗИ «VPN-Key-TLS» должно осуществляться непосредственно на местах пользования, если иное не предусмотрено политикой безопасности эксплуатирующей организации, при этом должна быть обеспечена невозможность подмены документации (например, в сейфе пользователя).

5.3 Требования к персоналу, обслуживающему СКЗИ

5.3.1 В ролевой модели СКЗИ «VPN-Key-TLS» предусмотрена роль пользователя, который осуществляет самостоятельно формирование ключевой информации и администрирование: установку сертификатов, списка отозванных сертификатов и обновлений ПО устройства, выбор класса СКЗИ.

5.3.2 В ролевой модели СКЗИ «VPN-Key-TLS» предусмотрена роль администратора, который осуществляет инициализацию СКЗИ.

5.3.3 Назначение и смена пользователей СКЗИ, а также ознакомление с эксплуатационной документацией на СКЗИ производится по письменному распоряжению ответственного лица с отметкой в журнале поэкземплярного учета, если иное не предусмотрено политикой безопасности эксплуатирующей организации.

5.3.4 Право пользования СКЗИ может предоставляться только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на СКЗИ.

5.4 Инициализация и ввод СКЗИ в эксплуатацию

5.4.1 Инициализация СКЗИ «VPN-Key-TLS» должна производиться в соответствии с документом «СКЗИ “VPN-Key-TLS Администратор”. Изделие “АРМ инициализации”. Руководство пользователя. 11485466.72.21.12.075 91».

5.4.2 При вводе СКЗИ «VPN-Key-TLS» в эксплуатацию пользователь должен осмотреть устройство, подключить его с соблюдением требований, изложенных в документе «СКЗИ “VPN-Key-TLS” вариант исполнения 7. Руководство пользователя. ИНФК.11485466.4012.021 91 05». Перед первым запуском СКЗИ необходимо сверить серийный номер СКЗИ и контрольную сумму микрокода, находящиеся в файле device.cfg на CD-дисководе, соответствующем устройству, а также контрольную сумму модулей «Start», находящуюся в файле tlsapp.hsh, с серийным номером и эталонными контрольными суммами, указанными в формуляре, сменить PIN-код и PUK-код, создать ключи ЭП, шифрования и TLS и соответствующие запросы на сертификаты, направить созданные запросы в УЦ и по получении сертификатов установить их. Модулем HashCtrl в соответствии с документом «Программа контроля целостности HashCtrl. Инструкция по эксплуатации. 11485466.72.21.12.103-02 91» должны быть рассчитаны контрольные суммы на модули «Start» и саму утилиту контроля целостности и сверены с эталонными контрольными суммами, указанными в формуляре.

При несовпадении контрольных сумм ввод СКЗИ в эксплуатацию запрещается.

6 Требования по обеспечению безопасности при эксплуатации СКЗИ

6.1 Общие требования по защите от НСД

6.1.1 Устройство «VPN-Key-TLS» при уходе пользователя с рабочего места необходимо отключать от ПЭВМ.

6.1.2 Устройство «VPN-Key-TLS» запрещается оставлять без контроля, при этом оно должно храниться в сейфе или непосредственно у пользователя.

6.1.3 Запрещается передача устройств «VPN-Key-TLS» лицам, к ним не допущенным.

6.1.4 PIN и PUK-коды для доступа к устройству «VPN-Key-TLS» являются персональными паролями и должны сохраняться в тайне.

6.1.5 Пользователь должен периодически (не реже 1 раза в 6 месяцев) менять PIN и PUK-коды в устройстве «VPN-Key-TLS» в соответствии с документом «СКЗИ “VPN-Key-TLS” вариант исполнения 7. Руководство пользователя. ИНФК.11485466.4012.021 91 05».

6.1.6 При работе с СКЗИ «VPN-Key-TLS» средствами веб-браузеров, пользователь должен запретить предлагаемое браузерами сохранение PIN и PUK-кода.

6.1.7 Должна быть выполнена процедура закрепления ключей ЭП, шифрования и TLS за пользователем (например, лично обратиться в УЦ и зарегистрировать свой открытый ключ).

6.1.8 Запрещается подключать к ПЭВМ с установленным ПО СКЗИ «VPN-Key-TLS» не предусмотренные производителем ПЭВМ устройства и соединители.

6.1.9 Запрещается использовать СКЗИ или подключать устройство «VPN-Key-TLS» к ПЭВМ, если выявлено нарушение функционирования (в т. ч. функционирование в нештатном режиме) хотя бы одного из компонентов аппаратного окружения или выявлены следы вскрытия на системном блоке (корпусе) ПЭВМ или устройства «VPN-Key-TLS», осуществлять несанкционированное вскрытие или иным образом нарушать целостность

системного блока (корпуса) ПЭВМ, корпуса устройства «VPN-Key-TLS».

6.1.10 На технических средствах, оснащенных СКЗИ «VPN-Key-TLS», должны быть реализованы следующие меры:

- должны использоваться антивирусные средства;
- должно использоваться только лицензионное ПО фирм-производителей. В случае необходимости использования иного программного обеспечения, его применение должно быть санкционировано ответственным лицом. В любом случае стороннее ПО не должно содержать средств разработки и отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование ПО СКЗИ «VPN-Key-TLS»;
- необходимо регулярно устанавливать пакеты обновления безопасности (Service Packs), обновлять антивирусные базы;
- при подключении к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX) без проведения соответствующих проверок на предмет содержания в них вирусов;
- правом установки и настройки операционных систем и гипервизоров (при их наличии) должен обладать только пользователь СКЗИ с правами администратора операционной системы;
- должна быть отключена возможность удаленного управления операционной системой;
- необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (системному реестру, файлам и каталогам, временным файлам, журналам системы, файлам подкачки, кэшируемой информации), неиспользуемые протоколы, сервисы и службы рекомендуется отключить;
- запрещено оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ после ввода ключевой информации;

- в BIOS ПЭВМ следует определить установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске, отключить возможность загрузки с гибкого магнитного диска, привода CD-ROM, USB-носителей, сетевой загрузки; не должны применяться ПЭВМ с ПО BIOS, исключающим возможность отключения сетевой загрузки ОС и загрузки с USB-носителей;
- вход в BIOS ПЭВМ (для классов КС1 и КС2), вход в ОС и заставку ОС (для класса КС2) должен быть защищен паролем с длиной не менее 6 символов, при этом он должен содержать буквы в верхнем и нижнем регистрах, цифры и специальные символы (знаки пунктуации, скобки, знаки арифметических действий), пароль должен меняться не реже одного раза в 6 месяцев, пароли для входа в BIOS и в ОС должны быть разными;
- средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты.

6.1.11 На технических средствах, оснащенных СКЗИ «VPN-Key-TLS», предназначенных для использования по классу КС2, дополнительно должен быть установлен АПМДЗ с действующим сертификатом соответствия и реализован следующий комплекс мероприятий по его установке и наладке:

- должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность бесконтрольного изменения аппаратной части рабочей станции;
- установка и настройка АПМДЗ должна производиться в соответствии с эксплуатационной документацией на АПМДЗ. Перед эксплуатацией АПМДЗ необходимо ознакомиться с комплектом документации на данный комплекс и принять рекомендуемые в документации защитные организационные меры;
- должно быть установлено ограничение времени (минимальное

время) на инициализацию АПМДЗ, для обеспечения невозможности отключить АПМДЗ средствами BIOS;

- должно быть установлено ограничение на максимальное количество неудачных попыток аутентификации – не более 10;
- средствами АПМДЗ должна блокироваться загрузка операционных систем со съёмных носителей и по сети;
- средствами АПМДЗ должен быть обеспечен контроль целостности системных файлов операционной системы и программных модулей СКЗИ, установленных на ПЭВМ;
- в случае обнаружения нарушения целостности программного обеспечения работа должна быть прекращена, для восстановления целостности программного обеспечения, установленного на ПЭВМ, необходимо его переустановить.

6.1.12 Дополнительно на технических средствах, оснащенных СКЗИ, функционирующим под управлением ОС Windows 10, Windows 11, необходимо реализовать следующие меры:

1. Запустить командную строку от имени администратора.
2. Остановить службу «Функциональные возможности для подключенных пользователей и телеметрия» (DiagTrack) путем ввода команды sc stop DiagTrack.
3. Удалить службу «Функциональные возможности для подключенных пользователей и телеметрия» (DiagTrack) путем ввода команды sc delete DiagTrack.
4. Удалить файлы с расширением *.rbs в директории %ProgramData%/Microsoft/Diagnosis, в которых хранятся подготовленные к отправке данные, при их наличии. При возникновении проблем с удалением данных файлов необходимо в свойствах на вкладке «Безопасность» разрешить полный доступ к файлу, а затем удалить.
5. Удалить службу маршрутизации push-сообщений WAP путем ввода команды sc delete dmwappushservice.

6. Запустить программу regedit.exe и, с использованием поиска в реестре по слову «DiagTrack-Listener», определить файл, в котором накапливается информация сессии AutoLogger-DiagTrackListener автоматической службы трассировки Windows (Event Tracing for Windows, ETW) – полный путь к файлу хранится в поле FileName соответствующей записи реестра. Перейти в окне командной строки в папку с файлом при помощи команды cd %путь к папке% (где %путь к папке% - путь из поля «FileName» без указания имени файла).

7. Очистить содержимое файла путем ввода команды echo "" > AutoLogger-Diagtrack-Listener.etl.

8. Запретить доступ к файлу путем ввода команды icacls %FileName% /deny *S-1-1-0:F. На экран будет выдано сообщение об обработке файла.

Данные действия необходимо выполнять после каждого кумулятивного обновления.

6.1.13 Контроль настроек, организационно-технических мероприятий и соблюдения правил эксплуатации должен осуществляться не реже раза в полгода специально назначенным лицом, являющимся пользователем СКЗИ «VPN-Key-TLS», если иное не предусмотрено политикой безопасности эксплуатирующей организации.

6.2 Требования к аутентификации и разграничению доступа

6.2.1 При использовании СКЗИ «VPN-Key-TLS» по классу КС1 предусмотрена однофакторная аутентификация: ввод PIN-кода, по классу КС2 дополнительно предусмотрена аутентификация средствами АПМДЗ, смена пароля АПМДЗ должна производиться не реже одного раза в 6 месяцев.

6.2.2 Длина PIN-кода равна 6 символам. Допустимыми символами являются заглавные и строчные английские буквы, цифры и спецсимволы.

6.2.3 Допускается не более 2 попыток ввода неверного PIN-кода подряд. При третьем подряд неверном вводе PIN-кода, соответствующая учётная запись блокируется. Для разблокирования учётной записи необходимо ввести PUK-код.

6.2.4 Длина PUK-кода равна 12 символам. Допустимыми символами

являются заглавные и строчные английские буквы, цифры и спецсимволы. В случае трёх и более попыток ввода неверного PUK-кода подряд начинается период принудительной задержки, зависящий от количества предыдущих попыток ввода неверного PUK-кода подряд (см. Приложение 2). Допускается не более 9 попыток ввода неверного PUK-кода подряд. После десятого подряд неверного ввода PUK-кода разблокирование учётной записи невозможно.

6.2.5 Смена PIN-кода и PUK-кода должна производиться в соответствии с документом «СКЗИ “VPN-Key-TLS” вариант исполнения 7. Руководство пользователя. ИНФК.11485466.4012.021 91 05».

6.2.6 Ввод PIN-кода для доступа к СКЗИ требуется при каждом подключении устройства.

6.3 Требования по обеспечению целостности СКЗИ

6.3.1 Должен производиться контроль основных характеристик при эксплуатации и после хранения изделий путем проверки целостности ПО СКЗИ, в том числе микрокода устройства, в соответствии с документацией на СКЗИ.

6.3.2 Перед началом работы СКЗИ пользователь должен осуществить расчет контрольных сумм для модулей «Start» и модуля HashCtrl, а также исполняемых модулей операционной системы, средствами модуля HashCtrl, в соответствии с документом «Программа контроля целостности HashCtrl. Инструкция по эксплуатации. 11485466.72.21.12.103-02 91» и сверить их с эталонными контрольными суммами, указанными в формуляре. При обнаружении несовпадения контрольных сумм, работа с СКЗИ запрещается до прохождения процедуры восстановления целостности ПО. Также должен осуществляться контроль целостности микрокода СКЗИ в соответствии с документом «СКЗИ “VPN-Key-TLS” вариант исполнения 7. Руководство пользователя. ИНФК.11485466.4012.021 91 05» и сверка рассчитанных контрольных сумм с эталонными, указанными в формуляре. При обнаружении несовпадения контрольных сумм, средствами АРМ инициализации в устройство «VPN-Key-TLS» должна быть установлена сертифицированная версия микрокода.

6.3.3 Для класса КС2 пользователь может перед началом работы СКЗИ осуществлять контроль целостности с помощью сертифицированного по требованиям ФСБ России АПМДЗ вместо программы контроля целостности hashctrl из состава СКЗИ. В состав модулей программного обеспечения, подлежащих проверке, должны быть включены модули «Start» из состава СКЗИ, исполняемые модули операционной системы, а также драйверы ПО АПМДЗ. Если будет обнаружено несовпадение контрольных сумм, то работа с СКЗИ запрещается до прохождения процедуры восстановления целостности ПО.

6.3.4 При внесении изменений в программное обеспечение СКЗИ «VPN-Key-TLS» пользователь должен установить обновление ПО, сформированное средствами АРМ управления обновлениями, в соответствии с документом «СКЗИ “VPN-Key-TLS” вариант исполнения 7. Руководство пользователя. ИНФК.11485466.4012.021 91 05».

6.3.5 Запуск приложений start.exe, Linux_x64, Start.app должен производиться исключительно из области памяти устройства «VPN-Key-TLS», видимой средствами ОС как носитель информации типа CD-ROM.

6.4 Порядок обеспечения работоспособности СКЗИ

6.4.1 В процессе функционирования устройств «VPN-Key-TLS» расположенные внутри светодиоды сигнализируют о внутреннем состоянии устройства и режимах работы, в которых оно находится. В процессе эксплуатации СКЗИ пользователь должен руководствоваться следующим описанием состояний устройства:

Состояние устройства	**Световая сигнализация**
В устройстве отсутствует микрокод	Постоянно горит красный светодиод
Выполнение команды от ПЭВМ при отсутствующем микрокоде	От момента принятия команды до момента отправки на ПЭВМ ответа красный светодиод гаснет
Загрузка в устройство микрокода	При включенном зелёном светодиоде примерно раз в секунду вспыхивает красный

Состояние устройства	**Световая сигнализация**
Установка загруженного с ПЭВМ микрокода в устройство	~2 раза в секунду мигает зелёный светодиод; красный выключен
Происходит миграция (конвертация внутренних данных из форматов предыдущих версий) после обновления микрокода	После подключения к ПК несколько секунд (до нескольких десятков) неритмично и часто мерцает красный светодиод; зелёный выключен
Первый этап инициализации не произведён или произошла ошибка инициализации критически важной подсистемы устройства при запуске	Попеременно моргают красный и зеленый светодиоды, примерно по полсекунды каждый. Переключение происходит мгновенно
Второй этап инициализация не произведён (не установлены первичный и (или) транспортный сертификаты)	Попеременно моргают красный-зеленый-зеленый светодиоды. Переключения разделены паузой примерно по 0,2 секунды
Инициализация произведена, ошибок не выявлено	В первые примерно 2 секунды после подключения к ПК горят оба светодиода. После их выключения возможна нормальная работа
Фатальная ошибка инициализации (например, контрольная сумма на внутренний микрокод не соответствует эталонному значению)	Оба светодиода мигают одновременно примерно 2 раза в секунду
От ПЭВМ пришла критичная команда (например, инициализация уже инициализированного устройства)	В течение 3 секунд часто мигает красный светодиод; зелёный выключен. Для подтверждения выполнения команды нужно в течение этого времени отключить устройство от ПЭВМ. Если отключение не будет

Состояние устройства	Световая сигнализация
	произведено за это время, то устройством будет выдан на ПЭВМ код отказа от выполнения команды

6.4.2 Не допускается непрерывное функционирование СКЗИ более суток (24 часов) без физического отключения устройства «VPN-Key-TLS» и перезагрузки ПЭВМ.

6.4.3 Действия в нештатных ситуациях, связанных с использованием СКЗИ:

- при не обнаружении устройства средствами операционной системы следует обратиться в службу технической поддержки организации-производителя СКЗИ;
- при полном отсутствии свечения светодиодов на корпусе устройства после подключения следует обратиться в службу технической поддержки организации-производителя СКЗИ;
- при попеременном мигании красного и зеленого светодиодов, примерно по полсекунды каждый, на корпусе устройства следует обратится с устройством на АРМ инициализации для повторной инициализации (при этом из памяти устройства будут удалены все ключевые пары, запросы и сертификаты);
- при отображении на экране изображений, не соответствующих приведенным в документе «СКЗИ “VPN-Key-TLS” вариант исполнения 7. Руководство пользователя. ИНФК.11485466.4012.021 91 05», следует обратиться в службу технической поддержки организации-производителя СКЗИ;
- при обнаружении нарушения целостности программного обеспечения в устройстве «VPN-Key-TLS» необходимо средствами АРМ инициализации осуществить перезапись программного обеспечения или утилизировать его порядком, описанным в настоящих правилах.

6.4.4 Восстановление целостности:

Перед первым запуском СКЗИ, рекомендуется сформировать набор программного обеспечения, используемого при функционировании СКЗИ, сохранить его на отдельном накопителе с расчетом на него контрольных значений утилитой контроля целостности, входящей в состав СКЗИ, в соответствии с документом «Программа контроля целостности HashCtrl. Инструкция по эксплуатации. 11485466.72.21.12.103-02 91».

Данный набор должен использоваться для восстановления работоспособности СКЗИ.

Следует предусмотреть периодический контроль целостности этого ПО. Если будет обнаружено несовпадение контрольных сумм, следует принять меры по обновлению набора ПО.

7 Требования по обеспечению безопасности при выводе СКЗИ из эксплуатации

7.1 При завершении жизненного цикла СКЗИ «VPN-Key-TLS» выводятся из эксплуатации:

- устройство «VPN-Key-TLS»;
- эксплуатационная документация.

7.2 Устройства «VPN-Key-TLS» уничтожаются путем их разрушения с помощью кусачек или других инструментов с уничтожением микросхем.

7.3 Факт уничтожения устройства «VPN-Key-TLS» оформляется актом с отметкой в журнале поэкземплярного учета.

Настоящие правила пользования согласованы с ФСБ России.

Приложение 1

Перечень вызовов, использование которых возможно при разработке прикладного ПО с применением СКЗИ «VPN-Key-TLS»

Функция	ОС*			Описание	Ограничение на использование, комментарии
	ОС1	ОС2	ОС3		
Управление сессией пользователя					
GET_PIN_LIST	+	+	+	Получение списка доступных учетных записей	-
LOGIN	+	+	+	Открытие сессии с прерыванием текущей сессии	-
LOGIN1	+	+	+	Открытие сессии с сохранением текущей сессии	-
LOGOUT	+	+	+	Завершение сессии	-
Управление сессиями TLS					
GET_BS_LIST	+	+	+	Получение списка доступных бизнес-систем	-
SET_BS_USE	+	+	+	Открытие сессии с основной бизнес-системой	-
START_NEW_SYSTEM	+	+	+	Открытие сессии с резервной бизнес-системой	-
GET_SID_URL_ID	+	+	+	Получить URL для перехода из бизнес-системы	-
Администрирование учётных записей					
CH_PIN_BY_PUK_ID	+	+	+	Смена PIN по PUK коду	-
CH_PIN_BY_PIN_ID	+	+	+	Смена PIN по PIN коду	-
CH_PUK_BY_PUK_ID	+	+	+	Смена PUK по PUK коду	-
FORMAT_PIN_ID	+	+	+	Форматирование учётной записи с подтверждением отключением	-
FORMAT_PIN_EX_ID	+	+	+	Форматирование учётной записи без подтверждения отключением	-
Обновление микрокода устройства					
INIT_UPD_ID	+	+	+	Начало процедуры обновления микрокода устройства	-
SET_UPD_D_ID	+	+	+	Передача части обновления микрокода	-
FIN_UPD_ID	+	+	+	Окончание процедуры обновления микрокода устройства	-
Модификация хранилища сертификатов					
CREATE_PAIR_EX_ID	+	+	+	Генерировать ключевую пару и квалифицированный запрос на сертификат PKCS10	-

Функция	**ОС***			**Описание**	**Ограничение на использование, комментарии**
	ОС1	ОС2	ОС3		
DELETE_OBJ_ID	+	+	+	Удалить ключевую пару и соответствующие ей сертификаты или один личный сертификат	-
SET_CERT_D_ID	+	+	+	Установить сертификат	-
SET_CRL_D_ID	+	+	+	Установить список отозванных сертификатов (CRL)	-
Использование хранилища сертификатов					
GET_OBJ_LIST_ID	+	+	+	Получить список объектов	-
GET_CERT_ID	+	+	+	Найти объект по полям	-
GET_OBJ_CERT_D_ID	+	+	+	Получить данные объекта	-
Служебные функции					
GET_SYS_INFO_ID	+	+	+	Получить информацию об устройстве	-
SET_ACT_OBJ_ID	+	+	+	Установить сертификат по умолчанию	-
SET_MC_D_ID	+	+	+	Установить конфигурацию бизнес-систем	-
BREAK_CRYPTOOP_H_ID	+	+	+	Прерывание криптоопераций	-
Подписание данных в формате CMS					
INIT_SIGN_H_ID	+	+	+	Инициализация ЭП в формате CMS	Только при значении аргумента "signed_attrs=1" или отсутствии данного аргумента
SET_SIGN_DATA_H_ID	+	+	+	Данные для ЭП в формате CMS	-
CALC_SIGN_H_ID	+	+	+	Вычисление ЭП в формате CMS	Только при отсутствии аргумента "direct_diggest"
GET_SIGN_CMS_H_ID	+	+	+	Получить ЭП в формате CMS	-
GET_CTX_INFO_H_ID	+	+	+	Информация о контексте в формате CMS	-
SIGN_PACKET	+	+	+	Подписание пакета документов	-
Проверка подписи в формате CMS					
INIT_CHECK_H_ID	+	+	+	Инициализация проверки ЭП в формате CMS	-
SET_CHECK_DATA_H_ID	+	+	+	Данные для проверки ЭП в формате CMS	-
CHECK_SIGN_H_ID	+	+	+	Проверка ЭП в формате CMS	Только при отсутствии аргумента "direct_diggest"
Зашифрование в формате CMS					
INIT_ENCIPHER_ID	+	+	+	Инициализация шифрования в формате CMS	-
ADD_RECIPIENT_Y_ID	+	+	+	Добавление стороннего	-

Функция	ОС*			Описание	Ограничение на использование, комментарии
	ОС1	ОС2	ОС3		
				сертификата получателя	
ADD_RECIPIENT_X_ID	+	+	+	Добавление собственного сертификата получателя	-
ENCIPHER_ID	+	+	+	Шифрование данных в формате CMS	-
GET_ENCIPHER_CMS_ID	+	+	+	Получить части для зашифрованного CMS	-
Расшифрование в формате CMS					
INIT_DECIPHER_ID	+	+	+	Инициализация расшифрования в формате CMS	-
DECIPHER_ID	+	+	+	Расшифрование данных в формате CMS	-
END_DECIPHER_ID	+	+	+	Завершение расшифрования данных в формате CMS	-
Наследные функции (ГОСТ 2001)					
GET_CTX_INFO_ID	+	+	+	Информация о контексте	-
INIT_CHECK_ID	+	+	+	Инициализация проверки ЭП	-
SET_CHECK_DATA_ID	+	+	+	Загрузить порцию данных для проверки ЭП	-
CHECK_SIGN_ID	+	+	+	Проверить ЭП	-

*: ОС1 - MS Windows
ОС2 - Linux64
ОС3 - MacOs

Приложение 2

Периоды принудительной задержки в зависимости от числа попыток ввода неверного PUK-кода подряд

Предыдущее число попыток ввода неверного PUK-кода подряд	0	1	2	3	4	5	6	7	8	9
Принудительная задержка до следующей попытки (в минутах)	0	0	0	15	30	60	120	180	1440	1440

Лист регистрации изменений

№ изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводи-тельного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					