|  |  |  |
| --- | --- | --- |
|  |

|  |
| --- |
| **ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ТСС»** |

**средство криптографической защиты информации****«Dcrypt 1.0 v.2»****Руководство пользователя****4012-006-61649217-18 01 34**Москва2018 |

**Аннотация**

Настоящий документ является руководством пользователя **средства криптографической защиты информации «Dcrypt 1.0 v.2»** (далее – СКЗИ «Dcrypt 1.0 v.2», изделие) для исполнений 1, 2, 3, 4, 5, 6, 16, 17, 18, 19, 20 21, 31, 32, 33, 34, 35 и 36.

Оглавление

[Список сокращений 4](#_Toc526862436)

[1 Основные технические данные и характеристики изделия 5](#_Toc526862437)

[1.1 Условные обозначения 5](#_Toc526862438)

[2 Учет ключевой информации 6](#_Toc526862439)

[2.1 Виды ключевой информации и ключевые носители 6](#_Toc526862440)

[2.2 Хранение ключевых носителей 6](#_Toc526862441)

[2.3 Сроки действия ключей 6](#_Toc526862442)

[2.4 Действия пользователя при возникновении необходимости уничтожения ключевой информации на ключевых носителях 7](#_Toc526862443)

[2.5 Компрометация ключевой информации 7](#_Toc526862444)

[3 СКЗИ «Dcrypt 1.0 v.2» исп. 18: Установка защищенного соединения 8](#_Toc526862445)

[4 СКЗИ «Dcrypt 1.0 v.2» исп. 21: Установка защищенного соединения 9](#_Toc526862446)

Список сокращений

|  |  |
| --- | --- |
| VPN | Virtual Private Network |
| АП | Абонентский пункт |
| АРМ | Автоматизированное рабочее место |
| СВТ | Средство вычислительной техники |
| СКЗИ | Средство криптографической защиты информации |
| ЭЦП | Электронно-цифровая подпись |

# Основные технические данные и характеристики изделия

Основные технические данные и характеристики, а также требования к программному и аппаратному обеспечению средства криптографической защиты информации «Dcrypt 1.0 v.2» (далее – СКЗИ «Dcrypt 1.0 v.2», изделие) приведены в документе «Средство криптографической защиты информации «Dcrypt 1.0 v.2. Правила пользования. 4012-006-61649217-18 01 95».

При использовании СКЗИ «Dcrypt 1.0 v.2» в программных продуктах необходимо следовать требованиям эксплуатационной документации, входящей в состав комплекта поставки СКЗИ «Dcrypt 1.0 v.2», включающий следующие эксплуатационные документы: «Средство криптографической защиты информации «Dcrypt 1.0 v.2». Формуляр. 4012-006-61649217-18 01 30», «Средство криптографической защиты информации «Dcrypt 1.0 v.2». Правила пользования. 4012-006-61649217-18 01 95», «Средство криптографической защиты информации «Dcrypt 1.0 v.2». Руководство администратора. 4012-006-61649217-18 01 91», «Средство криптографической защиты информации «Dcrypt 1.0 v.2». Руководство разработчика. 4012-006-61649217-18 01 92», «Средство криптографической защиты информации «Dcrypt 1.0 v.2». Руководство пользователя. 4012-006-61649217-18 01 34».

## Условные обозначения

АП VPN – условное обозначение СКЗИ «Dcrypt 1.0 v.2» для исполнений 16, 17, 18, 19, 20 и 21. АП VPN устанавливается на СВТ и выполняет функции, определенные в разделе 2 формуляра 4012-006-61649217-18 01 30, обеспечивая защиту TLS-соединений, в соответствии с ГОСТ 28147-89, ГОСТ Р 34.11-2012 и может использоваться для криптографической защиты (шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти) информации, не содержащей сведений, составляющих государственную тайну.

АП VPN обеспечивает выполнение следующей целевой функции:

* защита каналов связи посредством протокола защищенного обмена по сети по схеме DTLS 1.2.

# Учет ключевой информации

## Виды ключевой информации и ключевые носители

Ключевая информации и ключевые носители подразделяются следующие виды:

* закрытый персональный ключ пользователя;
* открытый персональный ключ пользователя;
* закрытый корневой ключ;
* открытый корневой ключ.

Подробное описание видов ключевой информации и ключевых носителей приведено в таблице Таблица 1.

Таблица 1 – Виды ключевой информации и ключевые носители

|  |  |  |
| --- | --- | --- |
| Наименование | Место создания | Область применения |
| Закрытый персональный ключ пользователя | КриптоАРМ | Шифрование/расшифрование электронных документов, формирование ЭП электронных документов, установление канала защищенного обмена по сети. |
| Открытый персональный ключ пользователя | КриптоАРМ | Шифрование/расшифрование электронных документов, проверка ЭП электронных документов, установление канала защищенного обмена по сети. |
| Закрытый корневой ключ | КриптоАРМ | Выдача (формирование ЭП) открытого ключа пользователя, отзыв открытого ключа пользователя. |
| Открытый корневой ключ | КриптоАРМ | Проверка валидности открытого ключа пользователя. |

## Хранение ключевых носителей

Пользователь несет персональную ответственность за хранение своих ключевых носителей, которые рекомендуется хранить в сейфе.

При наличии в организации, эксплуатирующей СКЗИ «Dcrypt 1.0 v.2», администратора безопасности и организованном централизованном хранении ключевых носителей, администратор безопасности организации несет персональную ответственность за хранение ключевых носителей пользователей.

## Сроки действия ключей

Допустимый срок действия закрытых ключей – не более 1 года 3 месяцев без использования ключа «Рутокен ЭЦП 2.0» или другого сертифицированного по требованиям ФСБ России аналога, и не более 3 лет при использовании ключа «Рутокен ЭЦП 2.0» или другого сертифицированного по требованиям ФСБ России аналога, а открытых ключей – не более 15 лет.

## Действия пользователя при возникновении необходимости уничтожения ключевой информации на ключевых носителях

Ключевые носители с ключевой информацией, срок действия которой истек, не могут использоваться ни в каком другом качестве, кроме ключевого носителя СКЗИ «Dcrypt 1.0 v.2». Пользователю, у которого имеется ключевой носитель с истекшим сроком действия, следует обратиться к администратору безопасности.

## Компрометация ключевой информации

Под компрометацией ключевой информации понимается утрата или временная потеря ключевого носителя, копирование и разглашение ключевой информации, а также несанкционированный доступ к ней. При компрометации закрытого ключа пользователю необходимо обратится к администратору безопасности.

При компрометации закрытого ключа предусматривается следующий порядок действий:

1. о факте компрометации немедленно ставится в известность администратор безопасности;
2. производится генерация новых ключей и замена скомпрометированных ключей на новые с их последующей регистрацией;
3. скомпрометированные ключи на носителе информации уничтожается путем физического воздействия на ключевой носитель или перезаписи на носитель нового закрытого ключа.

# СКЗИ «Dcrypt 1.0 v.2» исп. 16, 17 и 18: Установка защищенного соединения

Для установления VPN соединения с сервером СКЗИ «Dcrypt 1.0 v.2» по адресу «--ip "192.168.1.100" --port 1024» необходимо в интерпретаторе командной строки «cmd» ввести следующую команду:

«

> С:\Program Files\TSS Ltd\DVPN\bin\dmvpnd.exe --seed "С:\Users\TestUser\DPki\seed.dsc" --ca "С:\Users\TestUser\DPki\ca.crt" --keypair "С:\Users\TestUser\DPki\testuser.dkpc" --ip "192.168.1.100" --port 1024

».

Для сохранения текущих настроек соединений необходимо ввести следующую команду:

«

> С:\Program Files\TSS Ltd\DVPN\bin\dmvpnd.exe --seed "С:\Users\TestUser\DPki\seed.dsc" --ca "С:\Users\TestUser\DPki\ca.crt" --keypair "С:\Users\TestUser\DPki\testuser.dkpc" --ip "192.168.1.100" --port 1024 –install

».

При возникновении вопросов касающихся параметров соединения необходимо обратиться к администратору безопасности.

# СКЗИ «Dcrypt 1.0 v.2» исп. 19, 20 и 21: Установка защищенного соединения

Для установки защищенного соединения необходимо получить от администратора безопасности заранее сгенерированный корневой сертификат, ключевую пару и конфигурационный файл.

Затем имея файлы с ключевой информацией и настройками для запуска СКЗИ «Dcrypt 1.0 v.2» исп. 19,20 и 21 должен запустить следующую команду: «dmvpnd --seed seed.dsc --ca ca.crt --crl crl.crl --keypair client1.dkpc --keypairpass 1111 --config client1.xml ---log dmvpd.log», где «keypairpass» – пароль к файлу с ключевой парой, log – файл журнала.

Результатом выполнения команды будет являться установленное защищенное соединение (см. рисунок Рисунок 1).



Рисунок 1 – Успешно построенное защищенное соединение

ВНИМАНИЕ: Команда, в силу отличий пути к тем или иным файлам, может отличаться от приведенной в настоящем документе. Уточнять команду для установки защищенного соединения необходимо у администратора безопасности.