|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | **ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ТСС»** |   **средство криптографической защиты информации**  **«Dcrypt 1.0 v.2»**  **Руководство администратора безопасности**  **4012-006-61649217-18 01 91**  Москва  2018 |

**Аннотация**

Настоящий документ является руководством администратора безопасности с**редства 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

[Оглавление 3](#_Toc532475607)

[Список сокращений 5](#_Toc532475608)

[1 Основные технические данные и характеристики СКЗИ «Dcrypt 1.0 v.2» 6](#_Toc532475609)

[2 Инсталляция и конфигурирование Изделия 7](#_Toc532475610)

[2.1 Первоначальная инсталляция СКЗИ «Dcrypt 1.0 v.2» 7](#_Toc532475611)

[2.2 Установка и дальнейшее конфигурирование изделия 7](#_Toc532475612)

[2.2.1 Конфигурационные настройки СКЗИ «Dcrypt 1.0 v.2» для исполнения 16, 17 и 18 7](#_Toc532475613)

[2.2.2 Конфигурационные настройки СКЗИ «Dcrypt 1.0 v.2» для исполнения 19, 20 и 21 9](#_Toc532475614)

[2.3 Запуск СКЗИ «Dcrypt 1.0 v.2» исполнения 19, 20 и 21 для установления защищенного канала 10](#_Toc532475615)

[2.4 Журналирование событий в СКЗИ «Dcrypt 1.0 v.2» исполнение 19,20 и 21 11](#_Toc532475616)

[2.5 Учет ключевой информации 11](#_Toc532475617)

[2.5.1 Виды ключевой информации и ключевые носители 11](#_Toc532475618)

[2.5.2 Способы формирования ключевой информации 12](#_Toc532475619)

[2.5.3 Создание ключевых пар для АП VPN -серверов и АП VPN -клиентов 15](#_Toc532475620)

[2.5.4 Хранение ключевых носителей 16](#_Toc532475621)

[2.5.5 Сроки действия ключей 16](#_Toc532475622)

[2.5.6 Уничтожение ключевой информации на ключевых носителях 17](#_Toc532475623)

[2.5.7 Компрометация ключей 17](#_Toc532475624)

[2.5.8 Учет ключевой информации 17](#_Toc532475625)

[3 Настройка защищенных соединений 19](#_Toc532475626)

[4 Контроль целостности программного обеспечения 20](#_Toc532475627)

[4.1 Обеспечение контроля целостности 20](#_Toc532475628)

[4.1.1 Обеспечение контроля целостности программного обеспечения (для СКЗИ «Dcrypt 1.0 v.2» исп. 1, 4, 31 и 34) 22](#_Toc532475629)

[4.1.2 Обеспечение контроля целостности программного обеспечения (для СКЗИ «Dcrypt 1.0 v.2» исп. 3, 6, 18, 21, 33 и 36) 22](#_Toc532475630)

[4.2 Обеспечение разграничения прав доступа пользователей 23](#_Toc532475631)

[4.3 Обеспечение динамического контроля целостности программного обеспечения посредством ЗПС (для СКЗИ «Dcrypt 1.0 v.2» исп. 3, 6, 18, 21, 33 и 36) 24](#_Toc532475632)

[4.3.1 Обеспечение динамического контроля целостности программного обеспечения СКЗИ «Dcrypt 1.0 v.2» исп. 3, 18 и 33 24](#_Toc532475633)

[5 Обеспечение замкнутой программной среды 26](#_Toc532475634)

[5.1 Описание и настройка замкнутой программной среды в СКЗИ «Dcrypt 1.0 v.2» для вариантов исполнения 6, 21 и 36 26](#_Toc532475635)

[5.1.1 Описание модуля ЗПС 26](#_Toc532475636)

[5.1.2 Настройка модуля ЗПС 27](#_Toc532475637)

[5.1.3 Запуск модуля ЗПС 30](#_Toc532475638)

[5.2 Описание и настройка замкнутой программной среды в СКЗИ «Dcrypt 1.0 v.2» для вариантов исполнения 3, 18 и 33 34](#_Toc532475639)

[5.2.1 Назначение ЗПС 34](#_Toc532475640)

[5.2.2 Установка ЗПС 35](#_Toc532475641)

[5.2.3 Удаление ЗПС 37](#_Toc532475642)

[5.2.4 Конфигурационные параметры 37](#_Toc532475643)

[5.2.5 Безопасность конфигурационных параметров 38](#_Toc532475644)

[5.2.6 Подготовка к использованию 39](#_Toc532475645)

[5.2.7 Возможные проблемы, связанные с использованием ЗПС 40](#_Toc532475646)

[6 Регистрация событий 41](#_Toc532475647)

Список сокращений

|  |  |  |  |
| --- | --- | --- | --- |
| CRL | | Список аннулированных (отозванных) сертификатов | |
| VPN | | Virtual Private Network – виртуальная частная сеть | |
| АП | | Абонентский пункт | |
| АПМДЗ | | Аппаратно-программный модуль доверенной загрузки | |
| АРМ | | Автоматизированное рабочее место | |
| ДСЧ | | Датчик случайных чисел | |
| ЗПС | | Замкнутая программная среда | |
| НГМД | | Накопитель на гибких магнитных дисках | |
| НСД | | Несанкционированный доступ | |
| ОС | | Операционная система | |
| ПДСЧ | | Программный датчик случайных чисел | |
| ПО | | Программное обеспечение | |
| СВТ | | Средство вычислительной техники | |
| СКЗИ | | Средство криптографической защиты информации | |
| ЭЦП | | Электронно-цифровая подпись | |
|  |  | |

# Основные технические данные и характеристики СКЗИ «Dcrypt 1.0 v.2»

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 безопасности. 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».

# Инсталляция и конфигурирование Изделия

## Первоначальная инсталляция СКЗИ «Dcrypt 1.0 v.2»

Первоначальная инсталляция СКЗИ «Dcrypt 1.0 v.2» в среде его функционирования осуществляется посредством использования исполняемого файла «install\_dcrypt».

## Установка и дальнейшее конфигурирование изделия

Для установки изделия необходимо:

* на СВТ установить и настроить аппаратно-программный модуль доверенной загрузки (далее – АПМДЗ) для исполнений 2, 3, 5, 6, 17, 18, 20, 21, 32, 33, 35 и 36 СКЗИ «Dcrypt 1.0 v.2»;
* установить/копировать на СВТ исполняемые файлы с установочного компакт-диска соответствующего исполнения СКЗИ «Dcrypt 1.0 v.2»;
* установить и настроить средства доверенной загрузки согласно их эксплуатационной документации или сконфигурировать BIOS в соответствии с требованиями раздела 5 «Требования к программному и аппаратному обеспечению» и подраздела 6.3 «Организационно-технические меры защиты от НСД» раздела 6 «Требования по защите от несанкционированного доступа» документа «Средство криптографической защиты информации СКЗИ «Dcrypt 1.0 v.2». Правила пользования. 4012-006-61649217-18 01 95»;
* настроить замкнутую программную среду (далее – ЗПС) в соответствии с разделом 5 «Обеспечение замкнутой программной среды».

### Конфигурационные настройки СКЗИ «Dcrypt 1.0 v.2» для исполнения 16, 17 и 18

Исполняемый файл «dmvpnd.exe» представляет собой консольное приложение, предназначенное для установления защищенного VPN-соединения с сервером   
СКЗИ «Dcrypt 1.0 v.2».

Аргументы:

* «--adapter "{6A44349F-3AAC-4D17-BF9C-71D0681434BD}"» - идентификатор TAP-адаптера. Идентификаторы адаптеров уникальны в каждой системе. Так же при установке\удалении TAP-адаптера данные идентификаторы изменяются системой. Если параметр отсутствует или имеет пустое значение или содержит невалидный идентификатор, ПО СКЗИ «Dcrypt 1.0 v.2» попытается обнаружить подходящий адаптер в системе и использовать его для установления соединения. Если в системе отсутствуют подходящие TAP-адаптеры, пользователю/ администратору безопасности будет выведено сообщение об ошибке;
* «--seed "D:\Projects\VpnClient\dmvpnd\!testdata\seed.dsc"» - путь к файлу инициализации генератора псевдослучайных чисел. Если указанный файл отсутствует, то пользователю/ администратору безопасности будет выведено сообщение об ошибке;
* «--ca "С:\Users\TestUser\DPki\ca.crt"» - путь к файлу сертификата. Если указанный файл отсутствует, то пользователю/ администратору безопасности будет выведено сообщение об ошибке;
* «--keypair "С:\Users\TestUser\DPki\testuser.dkpc"» - путь к файлу ключевой пары. Если указанный файл отсутствуют, то пользователю/ администратору безопасности будет выведено сообщение об ошибке;
* «--passphrase "1111"» - пароль от ключевой пары. При попытке установления соединения происходит проверка пароля, при неправильном значении будет выведено сообщение об ошибке. Факт неправильного ввода пароля также будет записан в журнал регистрации событий;
* --ip "172.20.15.183" - IP адрес сервера СКЗИ «Dcrypt 1.0 v.2»;
* --port 1024 - порт сервера СКЗИ «Dcrypt 1.0 v.2»;
* --install - ключ, при использовании которого введенные параметры запоминаются в системе. В дальнейшем можно производить установления VPN соединения с сервером простым вызовом «dmvpnd.exe» без указания параметров. Параметры сохраняются для каждого пользователя/ администратора безопасности раздельно.

Пример 1: следующая командная строка запустит попытку установления VPN соединения с сервером СКЗИ «Dcrypt 1.0 v.2» по адресу «--ip "192.168.1.100" --port 1024»:

«

> 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

».

Пример 2: следующая командная строка сохранит настройки для дальнейшего использования:

«

> 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

».

### Конфигурационные настройки СКЗИ «Dcrypt 1.0 v.2» для исполнения 19, 20 и 21

Исполнение 21 СКЗИ «Dcrypt 1.0 v.2» позволяют установить защищенное соединение по сети между двумя и более компьютерами. Администратор безопасности должен создать корневой сертификат и две ключевые пары для клиента и для сервера (процесс создания ключевых пар для АП VPN – серверов и АП VPN – клиентов описан в разделе 2.5.3 «Создание ключевых пар для АП VPN -серверов и АП VPN -клиентов» настоящего документа). Ключевая информация содержит следующие атрибуты:

* seed.dsc – начальное заполнение ПДСЧ;
* ca.crt – корневой сертификат;
* crl.crl – список отозванных сертификатов;
* client1.dkpc – ключевая пара пользователя, защищенная паролем.

Затем создать конфигурационный файл. Пример содержания конфигурационного файла client1.xml:

«

<?xml version="1.1" encoding="UTF-8" ?>

<msg revision="18" type="160" client\_type="0" session\_id="00000000-0000-0000-0000-000000000000">

<params>

<vpnService mode="Client" guid="e79bdce5-8ba5-43c5-9159-972934f5c98f">

<tap name="tapc1" mtu="10000" mac="00:00:00:00:00:00" address="9.0.0.2" netmask="255.255.255.0"/>

<crypto caGuid="" crlGuid="" certGuid="" keyGuid=""/>

<client port="7777">

<remoteServer hostname="172.20.1.52" port="1024"/>

</client>

</vpnService>

</params>

</msg>

»

Пример содержания конфигурационного файла server.xml:

«

<?xml version="1.1" encoding="UTF-8" ?>

<msg revision="18" type="160" client\_type="0" session\_id="00000000-0000-0000-0000-000000000000">

<params>

<vpnService mode="Server" guid="8e25db17-773c-4a51-a566-0d8b091e321f">

<tap name="taps1" mtu="10000" mac="00:00:00:00:00:00" address="9.0.0.1" netmask="255.255.255.0"/>

<crypto caGuid="" crlGuid="" certGuid="" keyGuid=""/>

<server port="1024">

<dhcpServer enabled="true" startAddress="9.0.0.10" endAddress="9.0.0.100" dnsAddress="8.8.8.8" leaseTime="3600"/>

</server>

</vpnService>

</params>

</msg>

»

Где параметр «remoteServer» указывает, на какой IP-адрес и UDP-порт необходимо производить подключение.

Файлы настроек и ключевой информации должны быть защищены от модификации следующей командой:

«

chmod 600 seed.dsc

chmod 600 client1.xml

chmod 600 ca.crt

chmod 600 crl.crl

chmod 600 client1.dkpc

».

## Запуск СКЗИ «Dcrypt 1.0 v.2» исполнения 19, 20 и 21 для установления защищенного канала

Уполномоченный пользователь, 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 команд будет являться установленное защищенное соединение (см. рисунок Рисунок 1).

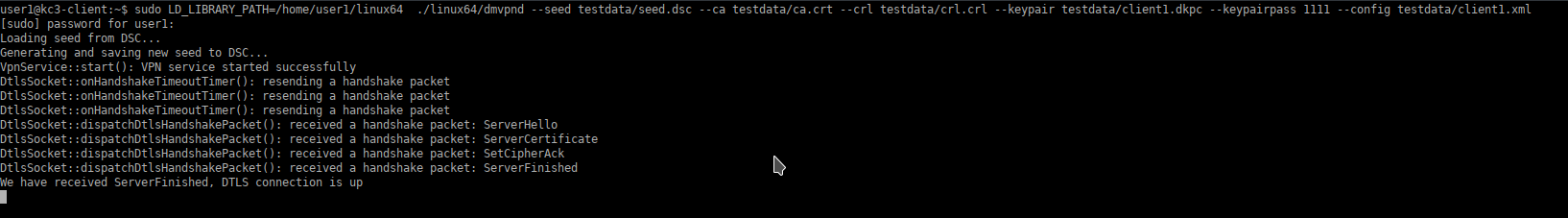


Рисунок 1 – Успешно построенное защищенное соединение

Команды для запуска приведены в качестве примера и могут отличаться от типовых в силу отличий пути к тем или иным файлам.

## Журналирование событий в СКЗИ «Dcrypt 1.0 v.2» исполнение 19,20 и 21

СКЗИ «Dcrypt 1.0 v.2» исполнение 19, 20 и 21 регистрируют следующие события:

* ввод, смена, стирание ключевой информации;
* попытки неудачного ввода ключевой информации;
* факты использование ключевой информации дольше заданного срока;
* факты проведения регламентных работ.

Пример инициации данных событий приведен на рисунке Рисунок 2.

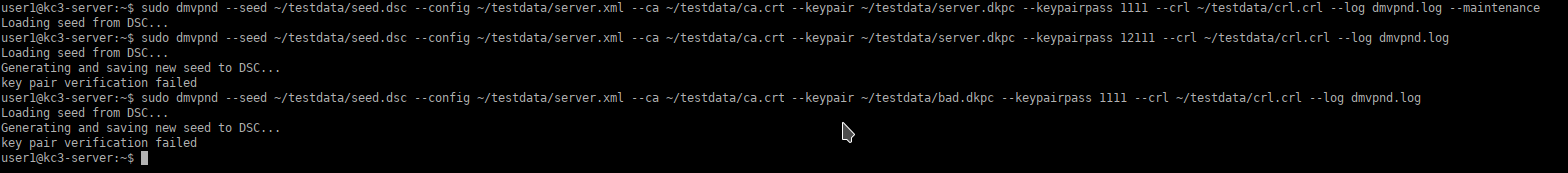


Рисунок 2 – Инициация событий, подвергаемых аудиту

Журнал событий при этом будет содержать записи, приведенные на рисункеРисунок 3.

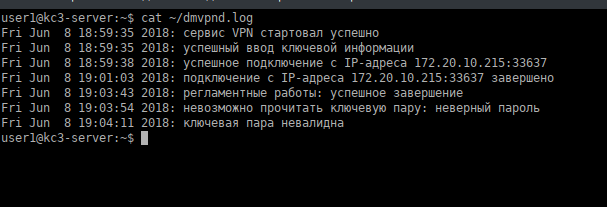


Рисунок 3 – Журнал событий

## 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.

Закрытые ключи хранятся в зашифрованном виде в формате ключевого контейнера. Открытые ключи хранятся в открытом виде в соответствии с RFC5280, RFC4491. Способы формирования ключевой информации описаны в эксплуатационных документах, входящих в состав комплекта поставки СКЗИ «Dcrypt 1.0 v.2». 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 электронно-цифровой подписи (далее – ЭЦП) электронных документов, установление канала защищенного обмена по сети |
| Открытый персональный ключ пользователя | КриптоАРМ | Шифрование / расшифрование электронных документов, проверка ЭЦП электронных документов, установление канала защищенного обмена по сети |
| Закрытый корневой ключ | КриптоАРМ | Выдача (формирование ЭЦП) открытого ключа пользователя, отзыв открытого ключа пользователя |
| Открытый корневой ключ | КриптоАРМ | Проверка валидности открытого ключа пользователя |

### Способы формирования ключевой информации

Для двусторонней аутентификации при установлении канала VPN (Virtual Private Network) используются ключевые пары в соответствии с ГОСТ Р 34.10-2012. Для генерации ключевых пар и соответствующих им сертификатов X.509 возможно использование утилиты «dmcrypt-util». Главное окно программы показано на рисунке Рисунок 4.



Рисунок 4 – Главное окно утилиты «dmcrypt-util»

Во время своей работы утилита использует встроенный ПДСЧ, который необходимо инициализировать случайной последовательностью, взятой с физического датчика случайных чисел (далее – ДСЧ) аппаратно-программного модуля доверенной загрузки. Встроенный ПДСЧ так же возможно инициализировать из файла со случайной последовательностью, заранее сгенерированной аппаратно-программным модулем доверенной загрузки. Перечень поставляемых аппаратно-программных модулей доверенной загрузки приведен в таблице 4 «Состав комплекта поставки СКЗИ «Dcrypt 1.0 v.2» раздела 4 «Комплектность» документа «Средство криптографической защиты информации «Dcrypt 1.0 v.2». Формуляр. 4012-006-61649217-18 01 30».

После инициализации ПДСЧ необходимо сгенерировать корневую ключевую пару и экспортировать корневой сертификат в отдельный файл, а для этого необходимо выполнить следующие действия:

* выбрать пункт меню «CA -> Setup CA»;
* в открывшемся мастере создания корневой ключевой пары и списка отозванных сертификатов (далее – CRL) требуется выбрать путь к файлу, в котором будет сохранена корневая ключевая пара, и задать пароль для шифрования этого контейнера, при этом следует иметь в виду, что обычно ключевая пара имеет расширение файла «.dkpc» (см. рисунокРисунок 5);
* заполнить поля создаваемого корневого сертификата (см. рисунок Рисунок 6);
* выбрать файл, в котором будет сохранен пустой сгенерированный CRL (см. рисунок Рисунок 7);
* нажать кнопку «Завершить» (см. рисунок Рисунок 7).

При нажатии кнопки «Завершить» будет создана корневая ключевая пара и CRL, информация о которых будет отображена в главном окне утилиты «dmcrypt-util» (см. рисунок Рисунок 8).

При установлении VPN-соединения необходимо указать корневой сертификат, при помощи которого будут проверяться сертификаты и сервера, а также клиенты. В этой связи, сразу после создания ключевой пары необходимо экспортировать корневой сертификат в отдельный файл. Для этого необходимо выбрать пункт меню «CA -> Export CA certificate» и путь к месту его сохранения.

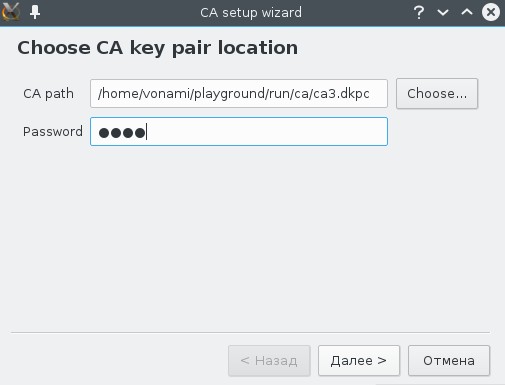


Рисунок 5 – Выбор файла для сохранения корневой ключевой пары

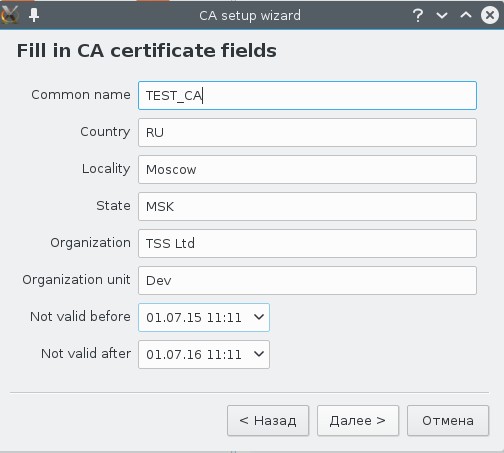


Рисунок 6 – Заполнение полей корневого сертификата

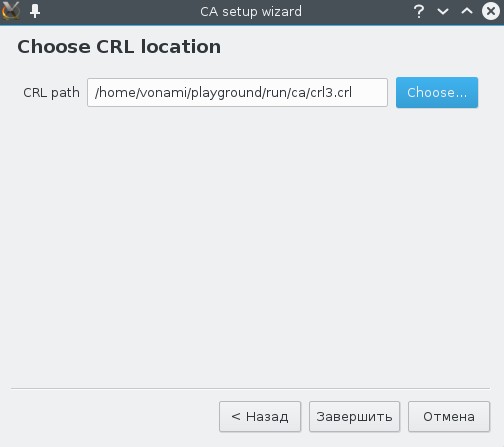


Рисунок 7 – Выбор файла для сохранения CRL

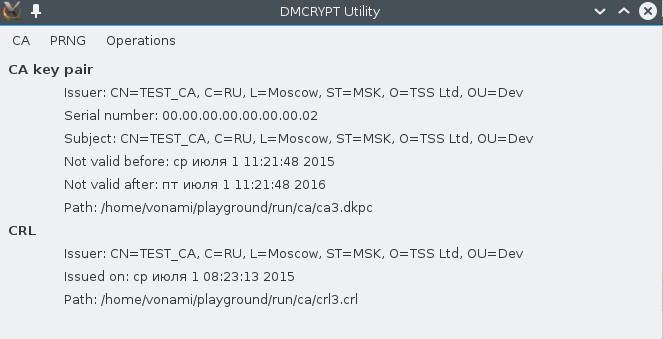


Рисунок 8 – Информация о корневом сертификате и CRL

Генерация ключевой информации также поддерживается сторонними криптопровайдерами (например, производства компании ООО «КРИПТО-ПРО») с применением RFC 4357, 4491, 5830, 5831, 5832, 7836 и прочих.

### Создание ключевых пар для АП VPN -серверов и АП VPN -клиентов

При создании ключевых пар для АП VPN -серверов и АП VPN -клиентов необходимо выбрать в главном меню пункт «CA -> Issue a new X509 certificate» и произвести следующие действия:

* заполнить все поля создаваемого сертификата (см. рисунок Рисунок 6);
* указать путь к сохраняемому файлу с ключевой парой и пароль шифрования (см. рисунокРисунок 5);
* указать путь, в котором будет сохранен отдельно сертификат X509.

При следующем запуске утилиты «dmcrypt-util» она автоматически загрузит созданную корневую ключевую пару, CRL и, таким образом, будет обеспечена возможность продолжить создание дочерних сертификатов. Если же необходимо создать новую ключевую пару, то необходимо повторить процедуру, воспользовавшись меню «CA -> Setup CA».

Кроме того, существует возможность инициализировать сертификат CA из внешних файлов, например, созданных на другом компьютере. Для этого потребуется на том же компьютере еще и экспортировать текущий серийный номер (при каждой операции создания сертификата этот номер увеличивается на единицу) через меню «CA -> Export serial number». Далее необходимо скопировать экспортированный серийный номер, файлы корневой ключевой пары и CRL на данный компьютер, а затем выбрать пункт меню «CA -> Load CA». Утилита предложит указать пути к загружаемым файлам с корневой ключевой парой, CRL и серийным номером. После этого можно продолжить выдачу дочерних сертификатов.

### Хранение ключевых носителей

Ключевые носители пользователей рекомендуется хранить в сейфе. Пользователь несет персональную ответственность за хранение своих ключевых носителей.

При наличии в организации, эксплуатирующей СКЗИ «Dcrypt 1.0 v.2», администратора безопасности и при организованном централизованном хранении ключевых носителей, администратор безопасности несет персональную ответственность за хранение ключевых носителей пользователей. Личные ключевые носители администратора безопасности должны храниться в его личном сейфе.

### 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. Контроль срока использования ключевой информации для СКЗИ «Dcrypt 1.0 v.2» исп. 31, 32, 33, 34, 35 и 36 возложен на администратора безопасности нового СКЗИ.

### Уничтожение ключевой информации на ключевых носителях

Ключевые носители с ключевой информацией, срок действия которой истек, не могут использоваться ни в каком другом качестве, кроме как в качестве ключевого носителя СКЗИ «Dcrypt 1.0 v.2». Уничтожение ключевых носителей, за исключением накопителей на гибких магнитных дисках (далее – НГМД), осуществляется путем физического воздействия на них (например, посредством их расплющивания молотком на наковальне). НГМД также уничтожаются путем физического воздействия на них (например, посредством их оплавления до бесформенной массы).

### Компрометация ключей

Под компрометацией ключевой информации понимается утрата или временная потеря ключевого носителя, разглашение и/или копирование ключевой информации, а также несанкционированный доступ к ней.

При компрометации закрытого ключа предусматривается следующий порядок действий:

1. о факте компрометации немедленно ставятся 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.

### Учет ключевой информации

При функционировании КриптоАРМ должен вестись «Журнал учета ключей», в которых следует отображать следующую информацию:

* Ф.И.О. лица, производящего запись;
* дата создания ключа;
* идентификаторы ключа (таблицы ключей) (например: серия, номер, комплект и т.п.);
* дата передачи/получения ключа;
* Ф.И.О. получателя/отправителя ключа;
* номер акта о передаче ключа или подпись получателя;
* запись о компрометации ключа.

На абонентский пункт (далее – АП) также должен вестись «Журнал учета ключей» (возможно ведение одного журнала для нескольких АП), в котором следует отображать следующую информацию:

* дата получения/создания ключа;
* идентификатор АП (в случае ведения одного журнала для нескольких АП);
* дата установки сетевых ключей или ключей ЭЦП;
* дата вывода ключа из действия;
* номер акта о передаче (возврате на КриптоАРМ) ключа или об уничтожении ключевой информации;
* запись о компрометации ключа;
* записи, отражающие выдачу на руки пользователям (ответственным исполнителям) и сдачу ими на хранение ключевых носителей (в случае централизованного хранения).

# Настройка защищенных соединений

Для настройки защищенный соединений администратор безопасности должен:

1. Создать корневой сертификат и две ключевые пары для клиента и для сервера (процесс создания ключевых пар для АП VPN – серверов и АП VPN – клиентов описан в разделе 2.5.3 «Создание ключевых пар для АП VPN -серверов и АП VPN -клиентов» настоящего документа).
2. Задать конфигурационные настройки согласно пункту 2.2.1 «Конфигурационные настройки СКЗИ «Dcrypt 1.0 v.2» для исполнения 16, 17 и 18» или согласно пункту 2.2.2 «Конфигурационные настройки СКЗИ «Dcrypt 1.0 v.2» для исполнения 19, 20 и 21» настоящего документа в зависимости от соответствующего исполнения СКЗИ «Dcrypt 1.0 v.2».
3. Обеспечить функционирования ЗПС согласно разделу 5 «Обеспечения замкнутой программной среды»

Администратор безопасности обязан выдавать сертификаты, ключевые пары и конфигурационные файлы необходимые для работы пользователей.

# Контроль целостности программного обеспечения

## Обеспечение контроля целостности

Для обеспечения контроля целостности программных модулей (файлов) СКЗИ «Dcrypt 1.0 v.2» и ОС администратору безопасности необходимо поставить на контроль целостности программные модули (файлы), приведенные в таблице Таблица 2.

Таблица 2 – Перечень программных модулей (файлов)

|  |  |  |  |
| --- | --- | --- | --- |
| Исполнение СКЗИ  «Dcrypt 1.0 v.2» | Архитектура процессора | Программные модули (файлы) СКЗИ  «Dcrypt 1.0 v.2» | Программные модули (файлы) ОС |
| СКЗИ «Dcrypt 1.0 v.2», исп. 1 | Intel IA-32 | «DcryptLogSvc.exe», «DmCrypt.dll», «Ddmcrypt-util.exe». | Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 2 | Intel IA-32 | «DcryptLogSvc.exe», «DmCrypt.dll», «Ddmcrypt-util.exe». | Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 3 | Intel IA-32 | «DcryptLogSvc.exe», «DmCrypt.dll», «Ddmcrypt-util.exe», «DmCSEDI.dll», «DmCSE.inf», «DmCSEManager.exe», «DmCSEService.exe», «DmCSE.sys». | Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 4 | Intel IA-32 | «dcryptlogsvc», «dmcrypt-util», «libdmcrypt.so.1». | Ядро ОС Linux и начальный загрузочный образ[[1]](#footnote-1). |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 5 | Intel IA-32 | «dcryptlogsvc», «dmcrypt-util», «libdmcrypt.so.1». | Ядро ОС Linux и начальный загрузочный. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 6 | Intel IA-32 | «dcryptlogsvc», «dmcrypt-util», «dmiced», «libdmcrypt.so.1», «tss\_sys\_hook.ko». | Ядро ОС Linux и начальный загрузочный. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 16 | Intel IA-32 | «DiamondVpn.exe», «DmCrypt.dl»l. | Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 17 | Intel IA-32 | «DiamondVpn.exe», «DmCrypt.dll». | Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 18 | Intel IA-32 | «DiamondVpn.exe», «DmCrypt.dll»,  «DmCSEDI.dll», «DmCSE.inf», «DmCSEManager.exe», «DmCSEService.exe», «DmCSE.sys». | Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 19 | Intel IA-32 | « DcryptLogSvc.exe »,  «dmvpnd.ddl»,  «libdmcrypt.so.1»,  «libdmvpn.so.1». | Ядро ОС Linux и начальный загрузочный. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 20 | Intel IA-32 | « DcryptLogSvc.exe »,  «dmvpnd.ddl»,  «libdmcrypt.so.1»,  «libdmvpn.so.1». | Ядро ОС Linux и начальный загрузочный. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 21 | Intel IA-32 | «dcryptlogsvc», «dmiced», «dmvpnd», «libdmcrypt.so.1», «libdmvpn.so.1», «tss\_sys\_hook.ko». | Ядро ОС Linux и начальный загрузочный. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 31 | Intel IA-32 | «DmCrypt.dll». | Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 32 | Intel IA-32 | «DmCrypt.dll»,  «Dmvpn.dll». | Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 33 | Intel IA-32 | «DmCrypt.dll», «DmCSEDI.dll», «DmCSE.inf», «DmCSEManager.exe», «DmCSEService.exe», «DmCSE.sys». | Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 34 | Intel IA-32 | «libdmcrypt.so.1». | Ядро ОС Linux и начальный загрузочный. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 35 | Intel IA-32 | «libdmcrypt.so.1»,  «libdmvpn.so.1». | Ядро ОС Linux и начальный загрузочный. |
| EM64T |
| СКЗИ «Dcrypt 1.0 v.2», исп. 36 | Intel IA-32 | «dmiced», «libdmcrypt.so.1», «tss\_sys\_hook.ko». | Ядро ОС Linux и начальный загрузочный. |
| EM64T |

### Обеспечение контроля целостности программного обеспечения (для СКЗИ «Dcrypt 1.0 v.2» исп. 1, 4, 16, 19, 31 и 34)

Утилита «dmcrypt-ic» предназначена для контроля целостности программных модулей (файлов) СКЗИ «Dcrypt 1.0 v.2», а также программных модулей (файлов) ОС и исполняется после загрузки самой ОС. Для обеспечения возможности контроля целостности программных модулей (файлов), указанных в таблице Таблица 2 для каждого исполнения СКЗИ «Dcrypt 1.0 v.2», запуск программы «dmcrypt-ic» должен осуществляться с аргументами командной строки.

Для вычисления контрольных сумм вначале создается файл, в котором перечислены пути ко всем контролируемым файлам (например, «list.txt», в котором каждая новая строка является новым путем к контролируемому файлу), а затем вызывается утилита «dmcrypt-ic» посредством команды: «dmcrypt-ic --calc-ic /path/to/list.txt /path/to/ic.txt».

Утилита для каждого указанного файла посчитает контрольную сумму и запишет их в файл «ic.txt».

Вызов утилиты для проверки контрольных сумм осуществляется следующим образом: «dmcrypt-ic --check-ic /path/to/ic.txt».

Кроме того, утилита выведет сообщение, был ли пройден контроль целостности.

### Обеспечение контроля целостности программного обеспечения (для СКЗИ «Dcrypt 1.0 v.2» исп. 2, 3, 5, 6, 17, 18, 20, 21, 32, 33, 35 и 36)

Контроль целостности программных модулей (файлов) СКЗИ «Dcrypt 1.0 v.2», а также программных модулей (файлов) ОС, указанных в таблице Таблица 2 для каждого исполнения СКЗИ «Dcrypt 1.0 v.2», согласно формуляру 4012-006-61649217-18 01 30 обеспечивается аппаратно-программным модулем доверенной загрузки (далее – АПМДЗ), сертифицированным по требованиям ФСБ России к АПМДЗ. Контроль целостности программных модулей (файлов) СКЗИ «Dcrypt 1.0 v.2», а также программных модулей (файлов) ОС для СКЗИ «Dcrypt 1.0 v.2» исп. 2, 3, 5, 6, 17, 18, 20, 21, 32, 33, 35 и 36 осуществляется АПМДЗ до загрузки ОС.

Для СКЗИ «Dcrypt 1.0 v.2» исп. 6, 21 и 18 дополнительно к программным модулям (файлам), приведенным в таблице Таблица 2, администратор безопасности до старта ОС должен настроить АПМДЗ на контроль целостности следующих файлов:

* файл с секретным ключом «secret.key»;
* файл со списком разрешенных файлов и их контрольными суммами «macs.txt».

Если в результате контроля целостности при загрузке ОС появляется сообщения о нарушении целостности контролируемого файла, то пользователь обязан прекратить работу и обратиться к администратору безопасности.

Администратор безопасности, проанализировав причину, приведшую к нарушению целостности, должен переустановить ПО СКЗИ «Dcrypt 1.0 v.2», либо файлы операционной среды.

Для СКЗИ «Dcrypt 1.0 v.2» исп. 3, 18 и 33 дополнительно к программным модулям (файлам), приведенным в таблице Таблица 2, администратор безопасности должен настроить АПМДЗ на контроль целостности следующих значений системного реестра MS Windows до старта ОС:

* значение реестра MS Windows:

KLM\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\ProcessingMode;

* значение реестра MS Windows:

HKLM\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\DmCryptKey;

* все значения ключа MS Windows (рекурсивно cо всеми подключами):

HKLM\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\ProtectedList;

* все значения ключа MS Windows (рекурсивно cо всеми подключами):

HKLM\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\WhiteList.

## Обеспечение разграничения прав доступа пользователей

Администратор безопасности, обязан распределить права доступа пользователей к конфигурационным параметрам, журналу событий ЗПС (в соответствии с разделом 5 «Обеспечение замкнутой программной среды» настоящего руководства) и программным модулям (файлам) СКЗИ «Dcrypt 1.0 v.2», приведенным в третьем столбце таблицы Таблица 2, при помощи средств ОС или сертифицированных ФСБ России средств защиты от НСД, при условии оценки влияния СКЗИ «Dcrypt 1.0 v.2» на данные средства защиты от НСД по техническому заданию, согласованному с 8 Центром ФСБ России.

Администратор безопасности может распределять права доступа пользователей в соответствии с принятой в организации политикой разграничения прав доступа при помощи средств ОС или сертифицированных ФСБ России средств защиты от НСД, при условии оценки влияния СКЗИ «Dcrypt 1.0 v.2» на данные средства защиты от НСД по техническому заданию, согласованному с 8 Центром ФСБ России.

## Обеспечение динамического контроля целостности программного обеспечения посредством ЗПС (для СКЗИ «Dcrypt 1.0 v.2» исп. 3, 6, 18, 21, 33 и 36)

Динамический контроль целостности программных модулей замкнутой программной среды (далее – ЗПС) осуществляется средствами самой ЗПС согласно разделу 5 «Обеспечение замкнутой программной среды»

Администратор безопасности должен сформировать ЗПС в соответствии с требованиями настоящего документа, изложенными в разделе 5 «Обеспечение замкнутой программной среды»».

### Обеспечение динамического контроля целостности программного обеспечения СКЗИ «Dcrypt 1.0 v.2» исп. 3, 18 и 33

В целях обеспечения ЗПС для СКЗИ «Dcrypt 1.0 v.2» для исполнений 3, 18 и 33 используются совместно средства доверенной загрузки и программные модули «DmCSE.sys» и «DmCSEManager.exe», «DmCSEDI.dll», «DmCSE.inf», «DmCSEService.exe».

На этапе настройки механизма ЗПС составляются два списка исполняемых файлов: «White List» и «Protected List».

«White List» может быть сформирован как автоматически (в режиме обучения), так и вручную. «Protected List» может быть сформирован исключительно вручную.

При этом для файлов из этих списков рассчитываются эталонные контрольные суммы для их последующего контроля.

На этапе применения настроек ЗПС выполняет контроль целостности (далее - КЦ) файлов, входящих в списки «White List» и «Protected List».

КЦ файлов осуществляется с момента перехода ЗПС в режим применения настроек «-enforce\_start» до выхода из этого режима «-enforce\_stop».

При выполнении команды «-enforce\_start» производится верификация контрольных сумм файлов, входящих в списки «White List» и «Protected List», а затем, до выполнения команды «-enforce\_stop», производится отслеживание изменений (модификации, переименования, удаления) этих файлов (т.е. выполняется динамический контроль целостности).

Несовпадение контрольной суммы файла при верификации или последующее изменение файла трактуется ЗПС как нарушение КЦ.

До тех пор, пока нарушений контроля целостности не выявлено, ЗПС допускает выполнение произвольного файла только в том случае, если он входит в список «White List» или в список «Protected List».

С момента обнаружения нарушения КЦ, ЗПС:

* Запрещает доступ к файловой системе всем пользователям, кроме следующих\*:
  + SID: S-1-5-21domain-500 //Name: Administrator Description: A user account for the system administrator. By default, it is the only user account that is given full control over the system;
  + SID: S-1-5-18 //Name: Local System Description: A service account that is used by the operating system;
  + SID: S-1-5-19 //Name: NT Authority Description: Local Service;
  + SID: S-1-5-20 //Name: NT Authority Description: Network Service;
  + SID: S-1-5-90-X //Windows 8; UserName: Window Manager\DWM-1;
  + SID: S-1-5-83-X //Windows 8 and Windows Server 2012; NT VIRTUAL MACHINE\XXX-XXX-XXX-XXX-XXX.
* Запрещает всем пользователям запуск файлов, входящих в список «Protected List»;
* В режиме обучения и применения настроек запрещается доступ к файлам, расположенным в сетевых папках.

*\* В частности, это означает что запрещенные пользователи не смогут зарегистрироваться в ОС. (Для получения дополнительной информации: https://support.microsoft.com/en-us/help/243330/well-known-security-identifiers-in-windows-operating-systems).*

# Обеспечение замкнутой программной среды

## Описание и настройка замкнутой программной среды в СКЗИ «Dcrypt 1.0 v.2» для вариантов исполнения 6, 21 и 36

Для обеспечения ЗПС в СКЗИ «Dcrypt 1.0 v.2» для вариантов исполнения 6, 21 и 36, сертифицированных по классам КС3, должны совместно использоваться средства доверенной загрузки и программные модули СКЗИ «Dcrypt 1.0 v.2» «dmiced» и «tss\_sys\_hook.ko».

### Описание модуля ЗПС

Модуль ЗПС создает замкнутую среду на основе 2 списков файлов:

* «белый» список: в нем указаны файлы, которые разрешены для запуска. Все остальные программы в среде функционирования будут запрещены для запуска;
* «защищенный» список: в нем указаны файлы, которые также разрешены для запуска, но в случае нарушения целостности или НСД эти файлы будут заблокированы для запуска. «Защищенный» список предназначен для внесения в него файлов СКЗИ «Dcrypt 1.0 v.2».

В «защищенном» списке для каждого внесенного файла хранится контрольная сумма, вычисленная по алгоритму ГОСТ 28147-89 в режиме имитовставки. Ключ алгоритма берется из файла, указанного через параметр «--key».

Оба списка («белый» и «защищенный») можно наполнять вручную. Например, для внесения файла «/usr/local/sbin/dmvpnd» в «белый» список необходимо выполнить следующую команду:

«dmiced --mode addp --key ~/secret.key --white ~/whitelist.txt --protected ~/protectedlist.txt /usr/local/sbin/dmvpnd --log ~/kc3.log».

Аналогично, для внесения файла «/bin/bash» в «белый» список необходимо выполнить следующую команду:

«dmiced --mode addw --key ~/secret.key --white ~/whitelist.txt --protected ~/protectedlist.txt /bin/bash --log ~/kc3.log».

Для формирования «белого» списка в автоматическом режиме модуль ЗПС имеет режим обучения. Для этого необходимо выполнить команду:

«dmiced --mode learn --key ~/secret.key --white ~/whitelist.txt --protected ~/protectedlist.txt --log ~/kc3.log».

В этом режиме модуль ЗПС отслеживает все запускаемые на исполнение файлы, автоматически вычисляя для них контрольные суммы и добавляя в «белый» список.

### Настройка модуля ЗПС

Настройкой модуля ЗПС должен заниматься привилегированный пользователь (администратор безопасности) среды функционирования. Вначале необходимо запретить чтение и модификацию файлов с ключевой информацией, списками и журналом для всех пользователей среды функционирования. Для этого привилегированный пользователь должен выполнить следующие команды:

«chmod 600 secret.key

chmod 600 whitelist.txt

chmod 600 protectedlist.txt

chmod 600 kc3.log».

Затем привилегированный пользователь переводит модуль ЗПС в режим обучения следующей командой:

«dmiced --mode learn --key secret.key --white whitelist.txt --protected protectedlist.txt --log kc3.log».

После этого необходимо произвести обычную работу в среде функционирования (авторизоваться, открыть файл, закрыть файл и т.д.) для того, чтобы модуль ЗПС смог составить «белый» список разрешенных программ.

Модуль ЗПС в режиме обучения приведен на рисунке Рисунок 9.

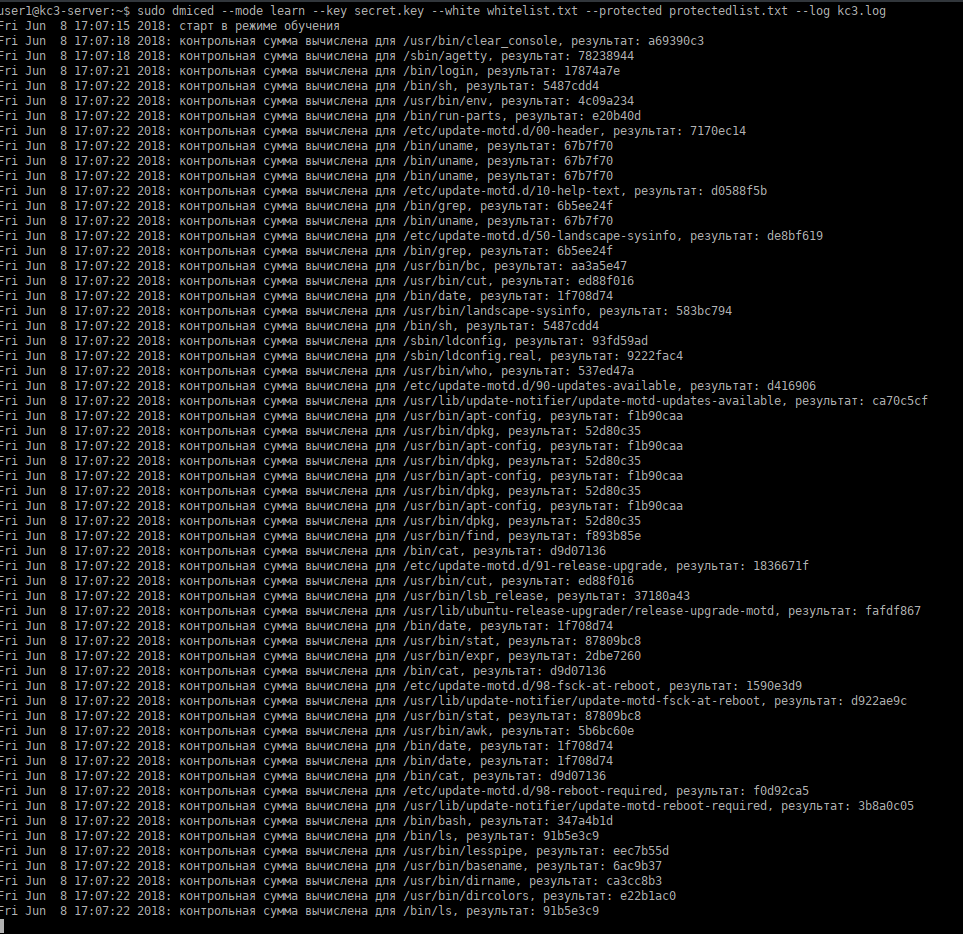


Рисунок 9 – Модуль ЗПС в режиме обучения

Файл с «белым» списком будет иметь следующее содержимое:

«

/bin/bash mac:347A4B1D

/bin/cat mac:D9D07136

/bin/date mac:1F708D74

/bin/grep mac:6B5EE24F

/bin/login mac:17874A7E

/bin/ls mac:91B5E3C9

/bin/mount mac:E15E611B

/bin/run-parts mac:0E20B40D

/bin/sh mac:5487CDD4

/bin/uname mac:067B7F70

/etc/update-motd.d/00-header mac:7170EC14

/etc/update-motd.d/10-help-text mac:D0588F5B

/etc/update-motd.d/50-landscape-sysinfo mac:DE8BF619

/etc/update-motd.d/90-updates-available mac:0D416906

/etc/update-motd.d/91-release-upgrade mac:1836671F

/etc/update-motd.d/98-fsck-at-reboot mac:1590E3D9

/etc/update-motd.d/98-reboot-required mac:F0D92CA5

/sbin/agetty mac:78238944

/sbin/dumpe2fs mac:8CE96601

/sbin/ldconfig mac:93FD59AD

/sbin/ldconfig.real mac:9222FAC4

/usr/bin/apt-config mac:F1B90CAA

/usr/bin/awk mac:5B6BC60E

/usr/bin/basename mac:06AC9B37

/usr/bin/bc mac:AA3A5E47

/usr/bin/clear\_console mac:A69390C3

/usr/bin/cut mac:ED88F016

/usr/bin/dircolors mac:E22B1AC0

/usr/bin/dirname mac:CA3CC8B3

/usr/bin/dpkg mac:52D80C35

/usr/bin/env mac:4C09A234

/usr/bin/expr mac:2DBE7260

/usr/bin/find mac:F893B85E

/usr/bin/landscape-sysinfo mac:583BC794

/usr/bin/lesspipe mac:EEC7B55D

/usr/bin/lsb\_release mac:37180A43

/usr/bin/stat mac:87809BC8

/usr/bin/who mac:537ED47A

/usr/lib/ubuntu-release-upgrader/check-new-release mac:1E78EF33

/usr/lib/ubuntu-release-upgrader/release-upgrade-motd mac:FAFDF867

/usr/lib/update-notifier/update-motd-fsck-at-reboot mac:D922AE9C

/usr/lib/update-notifier/update-motd-reboot-required mac:3B8A0C05

/usr/lib/update-notifier/update-motd-updates-available mac:CA70C5CF

»

После формирования «белого» списка привилегированный пользователь должен сформировать «защищенный» список из файлов СКЗИ «Dcrypt 1.0 v.2». Для этого используется следующая команда:

«dmiced --mode addp --key secret.key --white whitelist.txt --protected protectedlist.txt --log kc3.log /usr/local/sbin/dmvpnd».

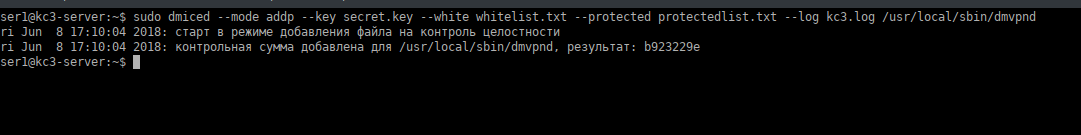
Процесс отработки приведенной команды представлен на рисунке Рисунок 10.

Рисунок 10 – Процесс формирования «защищенного» списка

Таким образом, после добавления всех модулей СКЗИ «Dcrypt 1.0 v.2», «защищенный» список будет выглядеть примерно следующим образом:

«

/usr/local/lib/libasiotap.so.1 mac:D908F19C

/usr/local/lib/libdmbase.so.1 mac:FBCA6EFF

/usr/local/lib/libdmcrypt.so.1 mac:4B0EFA8B

/usr/local/lib/libdmtcl.so.1 mac:3FA2BAEF

/usr/local/lib/libdmvpn.so.1 mac:F95C40D2

/usr/local/lib/libpugixml.so.1 mac:85302558

/usr/local/sbin/dmvpnd mac:B923229E

»

### Запуск модуля ЗПС

Для запуска модуля ЗПС в режиме применения сформированных правил привилегированный пользователь (администратор безопасности) должен выполнить следующую команду:

«dmiced --mode enforce --key secret.key --white whitelist.txt --protected protectedlist.txt --log kc3.log».

Модуль ЗПС вычислит контрольные суммы для всех файлов в списках и сравнит их с зафиксированными. Если все контрольные суммы совпадают, тогда модуль ЗПС разрешает исполнение файлов из «защищенного» списка (см. рисунок Рисунок 11).

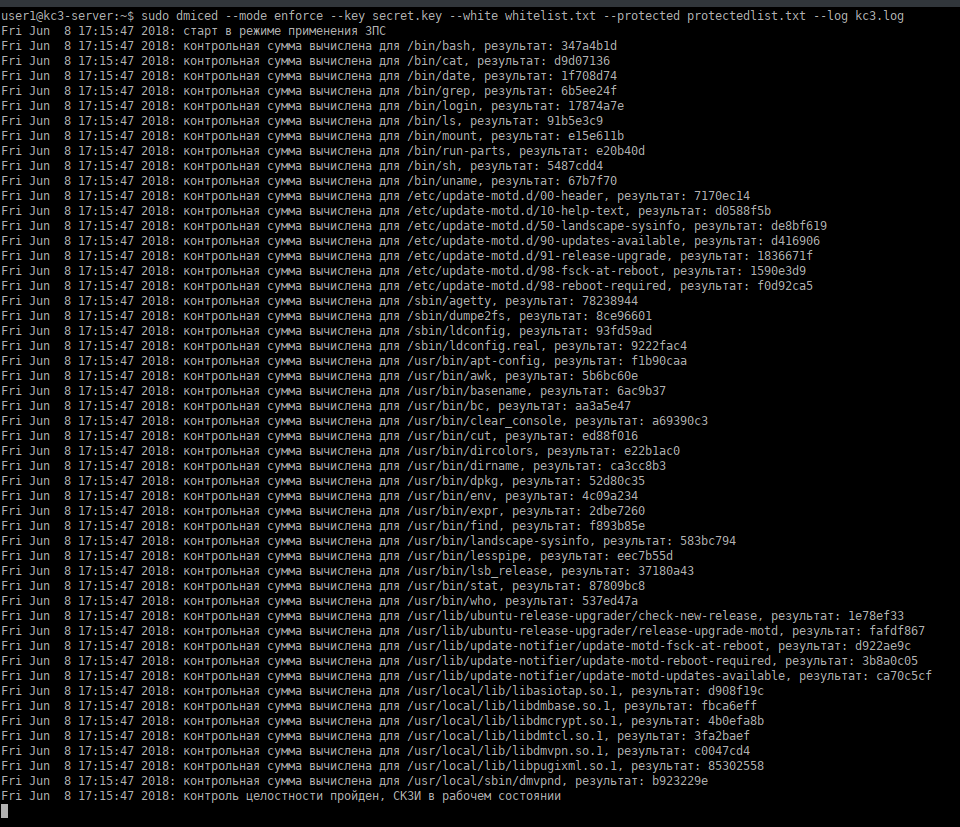
Если контрольные суммы для какого-нибудь файла не совпали, тогда все файлы из «защищенного» списка будут заблокированы для запуска пользователями (см. рисунок Рисунок 12).

Рисунок 11 – Контроль целостности пройден

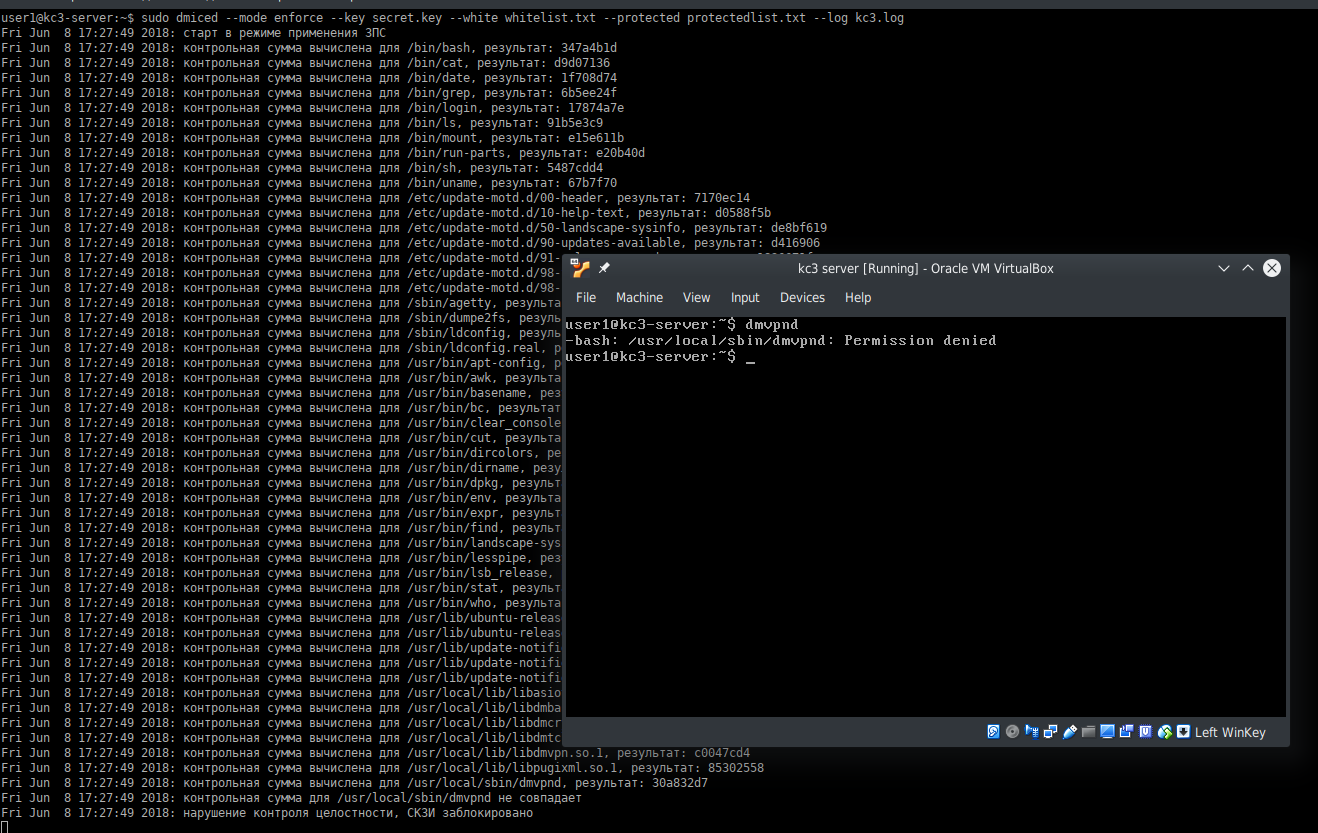


Рисунок 12 – Контроль целостности не пройден

Модуль ЗПС осуществляет также и динамический контроль целостности, отслеживая изменения файлов из списков и проверяя их контрольные суммы во время работы уполномоченных пользователей в среде функционирования. Если контрольные суммы какого-либо из файлов не совпадают с зафиксированной, тогда модуль ЗПС блокирует файлы из «защищенного» списка (см. рисунок Рисунок 13).

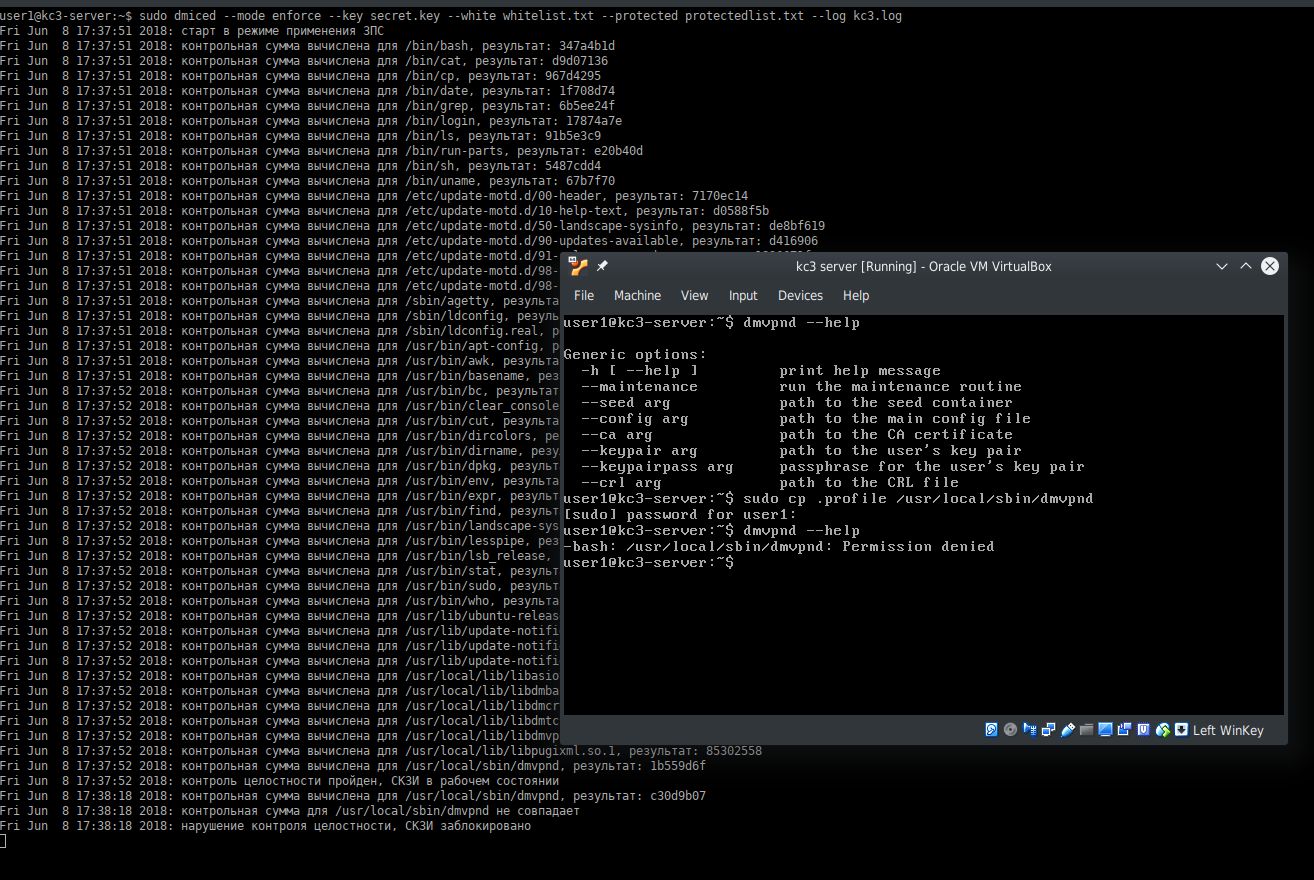


Рисунок 13 – Процедура блокирования файлов

Кроме того, модуль СКЗИ «Dcrypt 1.0 v.2» отслеживает и блокирует попытки пользователя запустить на исполнение файлы, которые не входят в «белый» список (защита от НСД) (см. рисунок Рисунок 14).

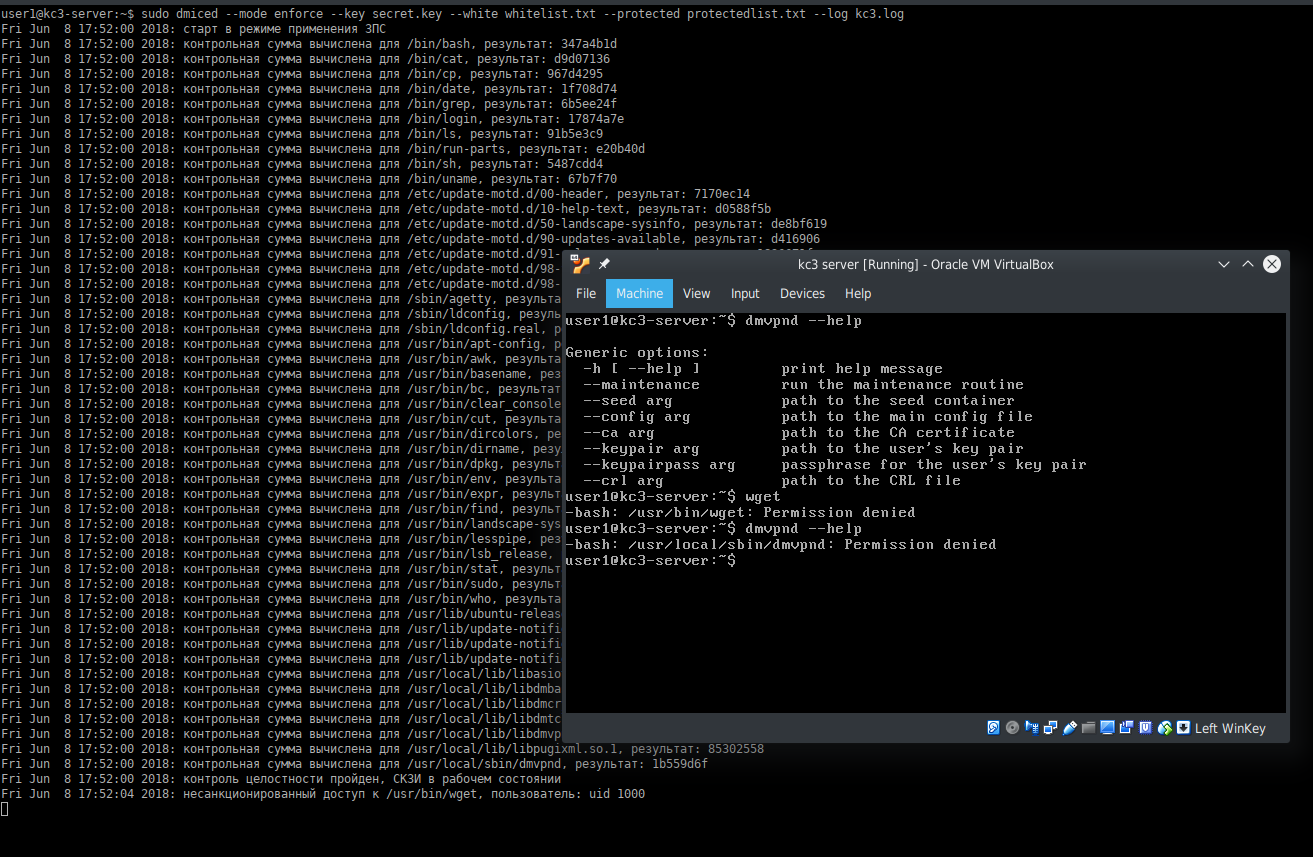


Рисунок 14 – Демонстрация защиты от НСД

Все действия привилегированного пользователя по настройке и запуску модуля ЗПС, а также события во время работы модуля, заносятся в журнал событий, который указан в параметре «--log». Файл журнала должен быть защищен от модификации со стороны пользователя, как это изложено в пункте 5.1.2 «Настройка модуля ЗПС».

## Описание и настройка замкнутой программной среды в СКЗИ «Dcrypt 1.0 v.2» для вариантов исполнения 3, 18 и 33

Для обеспечения ЗПС в СКЗИ «Dcrypt 1.0 v.2» для вариантов исполнения 3, 18 и 33, сертифицированных по классам КС3, должны использоваться совместно:

* средства доверенной загрузки;
* программные модули «DmCSE.sys» и «DmCSEManager.exe», «DmCSEDI.dll», «DmCSE.inf», «DmCSEService.exe».

### Назначение ЗПС

Механизм ЗПС обеспечивает:

* контроль доступа пользователей к файловой системе компьютера;
* контроль запуска процессов.

На этапе настройки механизма ЗПС составляются два списка исполняемых файлов: «White List» и «Protected List».

«White List» может быть сформирован как автоматически (в режиме обучения), так и вручную. «Protected List» может быть сформирован исключительно вручную.

При этом для файлов из этих списков рассчитываются эталонные контрольные суммы для их последующего контроля.

### Установка ЗПС

Обязательно должна быть включена учетная запись «Администратор|Administrator», создаваемая по умолчанию при установке операционной системы (в противном случае при нарушении контрольной целостности никто не сможет зайти в систему). Администратор безопасности должен произвести установку ЗПС согласно следующему порядку действий:

1. Определиться с битностью ЗПС (и распространяемого пакета Visual C++ для Visual Studio 2015. Их битность должна совпадать с битностью ОС.
2. Установить распространяемый пакет Visual C++ для Visual Studio 2015 соответствующей битности.
3. Создать 4 каталога: (Например: «C:\DmCse\», «C:\DmCSEManager\», «C:\DmCSEService\» и «C:\DmCSEService\Log\»).
4. Скопировать в каталог «C:\DmCse\» файлы «DmCse.sys» и «DmCse.inf», входящих в состав ЗПС.
5. Скопировать в каталог «C:\DmCSEManager\» файл «DmCSEManager.exe» входящий в состав ЗПС.
6. Скопировать в каталог «C:\DmCSEService\» файлы «DmCSEService.exe» и «DmCSEDI.dll», входящих в состав ЗПС.
7. Создать криптографический ключ и сохранить его в файле «C:\DmCSEManager\Key.bin» (Размер файла = 32 байта).
8. Запустить командную строку «cmd» с повышением привилегий.
9. Перейти в каталог «C:\DmCse\».
10. Для регистрации драйвера «DmCse.sys» выполнить команду: «RUNDLL32.EXE SETUPAPI.DLL,InstallHinfSection DefaultInstall 132 C:\DmCse\DmCse.inf».
11. Перейти в каталог «C:\DmCSEManager\».
12. Для установки криптографического ключа выполнить команду: «DmCSEManager.exe -set\_key "C:\DmCSEManager\Key.bin». Где «key.bin» - файл с криптографическим ключом (размер файла = 32 байта). После произведенной установки криптографического ключа файл с ключевой информацией «key.bin» необходимо удалить.
13. Перейти в каталог «C:\DmCSEService\».
14. Для регистрации сервиса «DmCSEService» выполнить команду: «DmCSEService /Service».
15. Ограничить доступ к конфигурационным параметрам ЗПС. Для этого запустить regedit.exe.
16. Найти ключ:

«HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters»

1. Произвести нажатие правой клавишей мыши, в меню опций выбрать: «Разрешения"|"Permissions...».
2. В появившемся диалоге нажать «дополнительно» | «Advanced».

В появившемся диалоге убрать галочку «Добавить разрешения, наследуемые от родительских объектов» |Include inheritable permissions from this object's parent».

1. В появившемся диалоге нажать «Добавить» | «Add». Нажать кнопку «OK».
2. В списке «Элементы разрешений» | «Group or user names» удалить все записи кроме «SYSTEM» и «Administrators». Нажать кнопку «OK».
3. Ограничить доступ к логам ЗПС. Для этого:
4. В проводнике Windows кликнуть правой кнопкой мыши на каталог C:\DmCSEService\Log\, выбрать «Свойства».
5. В появившемся диалоге выбрать вкладку «Безопасность».
6. В появившемся диалоге нажать «дополнительно» | «Advanced».
7. В появившемся диалоге убрать галочку «Добавить разрешения, наследуемые от родительских объектов» | «Include inheritable permissions from this object's parent».
8. В появившемся диалоге нажать «Добавить» | «Add». Нажать кнопку «OK».
9. Удалить из списка «Группы и пользователи» удалить все записи кроме «Система» и «Администраторы». Нажать кнопку «OK» во всех диалоговых окнах.
10. Запустить интерпретатор командной строки «cmd» с повышением привилегий и выполнить команду: «sc config DmCSEService start= auto && net start DmCSEService».

### Удаление ЗПС

Если подтверждено, что установка ЗПС была выполнена в соответствии с пунктом 5.2.2 «Установка ЗПС», для удаления ЗПС необходимо:

1. Запустить интерпретатор командной строки «cmd» с повышением привилегий.
2. Перейти в каталог «C:\DmCSEManager».
3. Выполнить команду: «DmCSEManager.exe -enforce\_stop».
4. Перейти в каталог «C:\DmCSEService\».
5. Выполнить команду: «DmCSEService /UnregServer».
6. Перейти в каталог «C:\DmCse\».
7. Выполнить команду: «RUNDLL32.EXE SETUPAPI.DLL,InstallHinfSection DefaultUninstall 132 C:\DmCse\DmCse.inf».

### Конфигурационные параметры

ЗПС хранит все свои конфигурационные параметры в следующем разделе реестра:

«KEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters».

ЗПС имеет следующие конфигурационные параметры:

1. Значение: «HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\ProcessingMode». Тип (REG\_DWORD). Допустимые значения:
2. 0: Режим по умолчанию (DEFAULT) - Драйвер ничего не делает (Прозрачно пропускает все запросы).
3. 1: Режим обучения (LEARNING) - Драйвер собирает информацию о запускаемых процессах.
4. 2: Режим применения настроек (ENFORCING) - Драйвер контролирует запуск процессов в соответствии с пунктом 5.2.1 «Назначение ЗПС»).
5. Значение: «HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\DmCryptKey». Тип (REG\_BINARY). Содержит криптографический ключ (32 байта).
6. Ключ: «HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\ProtectedList» с подключами.
7. Содержит список «Protected List».
8. Подключи данного ключа соответствуют серийным номерам томов файловой системы.
9. Каждый из подключей содержит значения, соответствующие файлам, расположенным на данном томе.
10. Ключ: «HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\WhiteList» с подключами.
11. Содержит список «White List». Данные сгруппированы по томам, на которых расположены файлы.
12. Подключи данного ключа соответствуют серийным номерам томов файловой системы.
13. Каждый из подключей содержит значения, соответствующие файлам, расположенным на данном томе.

### Безопасность конфигурационных параметров

Получить доступ к конфигурационным параметрам ЗПС можно:

1. Непосредственно обращаясь из приложения к реестру. Это контролируется следующим образом: для ключа «HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters» и всех его подключей устанавливается разрешение, запрещающие доступ к ним кроме пользователя «SYSTEM» и группы «локальные администраторы» (локальными администраторами в данном контексте принято считать администраторов безопасности).
2. Опосредованно, подключившись к сервису и отдавая ему команды. Это контролируется следующим образом: При создании программного компонента «пайпа» на стороне сервера ему назначаются атрибуты безопасности, запрещающие доступ к нему всем кроме группы «локальные администраторы».
3. Опосредованно, подключившись к драйверу и отдавая ему команды. Это контролируется следующим образом: необходимо подключиться к драйверу «DmCse.sys» для того чтобы отправить ему команду. Осуществить данное действие, может только уполномоченный пользователь «SYSTEM» или член группы «локальные администраторы».

Доступ к настройкам и управлению ЗПС имеют только пользователь «SYSTEM» и члены группы «локальные администраторы».

### Подготовка к использованию

***Важно: утилита «dmcsemanager.exe» должна выполняться в контексте безопасности локального администратора с повышенными привилегиями.***

Подготовка к использованию осуществляется следующим образом:

1. Для начала обучения выполнить команду: «DmCSEManager.exe -learn\_start».
2. Компьютер будет автоматически перезагружен через 10 секунд. После перезагрузки ЗПС фиксирует все автоматически запуcкающиеся процессы при старте ОС.
3. Для автоматического добавления программ в «White List» их необходимо запустить.
4. Для завершения обучения выполнить команду: «DmCSEManager.exe -learn\_stop».
5. При этом старое содержимое «White List» будет удалено и на его место будет записан новый «White List» из памяти драйвера.
6. Если необходимо, вручную добавить или удалить файлы в «White List» (файлы, которые не были учтены в «White List» при обучении), то следует выполнять следующие команды:
7. Добавление файла «c:\1.exe» в «White List»: Необходимо выполнить команду: «DmCSEManager.exe -add\_wl "c:\1.exe"».
8. Удаление файла «c:\1.exe» из «White List»: Необходимо выполнить команду: «DmCSEManager.exe -del\_wl "c:\1.exe"».
9. Вручную добавить или удалить файлы в «Protected List» посредством следующих команд:
10. Добавление файла «c:\1.exe» в «Protected List». Необходимо выполнить команду: «DmCSEManager.exe -add\_pl "c:\1.exe"».
11. Удаление файла «c:\1.exe» из «Protected List». Необходимо выполнить команду: «DmCSEManager.exe -del\_pl "c:\1.exe"».

*\*При ручном добавлении исполняемых файлов (расширение .exe) администратор безопасности должен убедиться в том, что все файлы, которые необходимы для функционирования данного программного модуля (расширение .dll и прочие) также были внесены в «White List» и «Protected List».*

1. Для начала применения настроек выполнить команду: «DmCSEManager.exe -enforce\_start».
2. Проверить, что выполняются требования, описанные в пункте 5.2.1 «Назначение ЗПС» (для проведения проверки можно перезагрузить или выключить/включить компьютер. После загрузки операционной системы, ЗПС будет работать в режиме применения настроек.
3. Для выхода из режима применение выполнить команду: «DmCSEManager.exe -enforce\_stop».
4. В любой промежуточный момент можно получить информацию о текущем состоянии ЗПС. Для этого необходимо выполнить команду: «DmCSEManager.exe –info». Если информация не умещается на экране, то можно сделать вывод в файл, выполнив команду: «DmCSEManager.exe -info >имя\_файла».
5. Для получения справочной информации по параметрам утилиты «DmCseManager.exe», достаточно запустить ее без параметров или ошибиться в них.

### Возможные проблемы, связанные с использованием ЗПС

***Проблема:***

Компьютер не загружается или при загрузке переходит в режим восстановления ОС.

***Решение:***

Решение состоит из следующего порядка действий:

1. Загрузить ОС с другого носителя (liveCD, флеш накопитель, iso-образ ОС (например, kubuntu), и т.д.).
2. Переименовать файл «c:\Windows\system32\drivers\DmCse.sys» в «c:\Windows\system32\drivers\DmCse.sys\_».
3. Перезагрузить средство вычислительной техники.
4. Загрузить ОС обычным образом.
5. Изменить значение реестра «HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\ProcessingMode» на 0.
6. Переименовать файл «c:\Windows\system32\drivers\DmCse.sys\_» в «c:\Windows\system32\drivers\DmCse.sys».
7. ЗПС переведена в режим «DEFAULT». Теперь ЗПС можно продолжать настраивать.

# Регистрация событий

СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5, 6, 16, 17, 18, 19, 20 и 21 обеспечивает регистрацию следующих событий:

1. Факты ввода, смены и стирания ключевой информации (в том числе технологических ключей).
2. Факты использования ключей дольше заданного срока, повторного ввода ключей.
3. Факты несанкционированного доступа к СВТ с установленным СКЗИ «Dcrypt 1.0 v.2».
4. Результаты контроля целостности ПО СКЗИ «Dcrypt 1.0 v.2».
5. Факты проведения регламентных работ.
6. Попытки неудачного ввода ключевой информации.

Регистрация событий в СКЗИ «Dcrypt 1.0 v.2» исп. 31, 32, 33, 34, 35 и 36 возложена на разработчика СКЗИ. СКЗИ «Dcrypt 1.0 v.2» исп. 31, 32, 33, 34, 35 и 36 обеспечивает регистрацию следующих событий:

1. Факты ввода, смены и стирания ключевой информации (в том числе технологических ключей).
2. Факты использования ключей дольше заданного срока, повторного ввода ключей.
3. Факты проведения регламентных работ.
4. Попытки неудачного ввода ключевой информации.

В электронном журнале событий регистрируется информация о действиях, связанных с выполнением администратором безопасности СЗКИ «Dcrypt 1.0 v.2» целевых и прочих функций.

При инсталляции СЗКИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 16, 17, 18, 31, 32 и 33 место хранения журналов событий определяется каталогом инсталляции изделия, например: «С:\Program file\Diamond Security\DmCryptUtil\Log\dcryptsvc.log», где dcryptsvc.log – журнал событий. Администратору безопасности для просмотра журнала событий необходимо открыть указанный текстовый файл.

При инсталляции СЗКИ «Dcrypt 1.0 v.2» исп. 4, 5, 6, 19, 20, 21, 34, 35 и 36 место хранения журналов событий определяется каталогом инсталляции изделия, например: «/var/lib/dcryptsvc.log», где dcryptsvc.log – журнал событий. Администратору безопасности для просмотра журнала событий необходимо открыть указанный текстовый файл.

Регистрация событий, связанных с контролем целостности ОС, обеспечивается АПМДЗ, сертифицированным по требованиям ФСБ России к АПМДЗ.

Дополнительно СКЗИ «Dcrypt 1.0 v.2» исп. 6, 21, 36 и СКЗИ «Dcrypt 1.0 v.2» исп. 3, 18, 33 регистрируют все действия привилегированного пользователя по настройке, запуску модуля ЗПС, а также события во время работы модуля ЗПС.

Для СКЗИ «Dcrypt 1.0 v.2» исп. 6, 21, 36 данные события заносятся в журнал событий, который указан в параметре «--log» (см. пункт 5.1.1 «Описание модуля ЗПС»). Файл журнала должен быть защищен от модификации со стороны пользователя, как это изложено в пункте 5.1.2 «Настройка модуля ЗПС».

Для СКЗИ «Dcrypt 1.0 v.2» исп. 3, 18, 33 внесение записей в журналы событий ведется в файлы каталога «C:\DmCSEService\Log\». Файлы имеют имена формата «DD.MM.YYYY.log». Доступ к журналам событий определяется разрешениями, установленными на каталог «C:\DmCSEService\Log\» при развертывании ЗПС согласно пункту 5.2.2 «Установка ЗПС». (Доступ запрещен всем, кроме пользователя SYSTEM и группы «локальные администраторы»).

1. Администратор безопасности в зависимости от конкретной сборки дистрибутива ОС Linux обязан определить системные модули ОС (ядро ОС Linux и начальный загрузочный образ), которые необходимо поставить на контроль целостности. [↑](#footnote-ref-1)