

**УТВЕРЖДЕН**  
RU.НКБГ.70021 87-ЛУ

**СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**  
**«КЛИЕНТ КРИПТОГРАФИЧЕСКОГО СЕРВЕРА ДОСТУПА DISEC-LV2»**

Руководство администратора

RU.НКБГ.70021 87

Листов 75

2026

<i>Инв. № подл.</i>	
<i>Подп. и дата</i>	
<i>Взам. инв. №</i>	
<i>Инв. № дубл.</i>	
<i>Подп. и дата</i>	

**АННОТАЦИЯ**

Настоящий документ предназначен для администратора средства криптографической защиты информации «Клиент криптографического сервера доступа DiSec-LV2» RU.НКБГ.70021 (далее по тексту – служба DiSec-LV2 или DiSec-LV2).

Документ содержит следующие сведения, достаточные для настройки и мониторинга работы DiSec-LV2:

- состав аппаратной и программной среды функционирования DiSec-LV2;
- уровень квалификации специалистов по администрированию DiSec-LV2;
- описание комплекта поставки DiSec-LV2;
- действия по установке и удалению DiSec-LV2;
- действия по настройке и мониторингу работы DiSec-LV2 с использованием графического интерфейса и интерфейса командной строки.

**СОДЕРЖАНИЕ**

1. НАЗНАЧЕНИЕ .....	5
2. УСЛОВИЯ ПРИМЕНЕНИЯ.....	7
2.1. Среда функционирования .....	7
2.1.1. Аппаратная среда функционирования.....	7
2.1.2. Программная среда функционирования.....	7
2.2. Интерфейсы управления .....	7
2.3. Квалификация администратора .....	7
3. ПОДГОТОВКА К УСТАНОВКЕ .....	9
4. ГРАФИЧЕСКОЕ ПРИЛОЖЕНИЕ DISEC-LV2 .....	11
4.1. Установка DiSec-LV2 .....	11
4.2. Удаление DISEC-LV2 .....	13
4.3. Выполнение DiSec-LV2.....	13
4.3.1. Запуск DiSec-LV2.....	13
4.3.2. Завершение работы DiSec-LV2 .....	15
4.3.3. Регистрация DiSec-LV2.....	15
4.3.4. Контроль целостности .....	18
4.3.5. Импорт сертификатов и списка отзыва сертификатов.....	20
4.3.6. Удаление сертификатов и списка отзыва сертификатов .....	23
4.3.7. Создание VPN-туннеля .....	26
4.3.8. Редактирование параметров VPN-туннеля .....	34
4.3.9. Удаление VPN-туннеля .....	35
4.3.10. Подключение VPN-туннеля (туннелей) .....	36
4.3.11. Подключение VPN-туннеля при запуске DiSec-LV2.....	37
4.3.12. Отключение VPN-туннеля .....	37
4.3.13. Настройка параметров DiSec-LV2 .....	38
4.3.14. Работа с USB-Рутокен .....	39
4.3.15. Обновление списка отзыва сертификатов.....	40
4.4. Регистрация действий администратора\пользователя и протоколирование	42
5. СЛУЖБА DISEC-LV2.....	45
5.1. Установка службы DiSec-LV2.....	45
5.2. Удаление DiSec-LV2.....	46
5.3. Выполнение DiSec-LV2.....	46
5.3.1. Утилиты .....	46
5.3.2. Запуск DiSec-LV2.....	46

5.3.3. Завершение работы DiSec-LV2 .....	46
5.3.4. Контроль целостности .....	47
5.3.5. Регистрация DiSec-LV2 .....	47
5.3.6. Импорт сертификатов и списков отзыва сертификатов .....	48
5.3.7. Удаление сертификатов и списка отзыва сертификатов .....	50
5.3.8. Создание VPN-туннеля .....	50
5.3.9. Редактирование параметров VPN-туннеля .....	52
5.3.10. Создание нового VPN-туннеля.....	52
5.3.11. Удаление VPN-туннеля .....	53
5.3.12. Подключение\отключение VPN-туннеля .....	53
5.3.13. Подключение\отключение VPN-туннеля при запуске DiSec-LV2 .....	54
5.3.14. Регистрация действий администратора\пользователя и протоколирование .....	54
6. СООБЩЕНИЯ .....	56
7. ПЕРЕЧЕНЬ ТЕРМИНОВ.....	65
8. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ .....	66
ПРИЛОЖЕНИЕ 1 ПАРАМЕТРЫ VPN-ТУННЕЛЯ .....	67
ПРИЛОЖЕНИЕ 2 УТИЛИТЫ .....	72

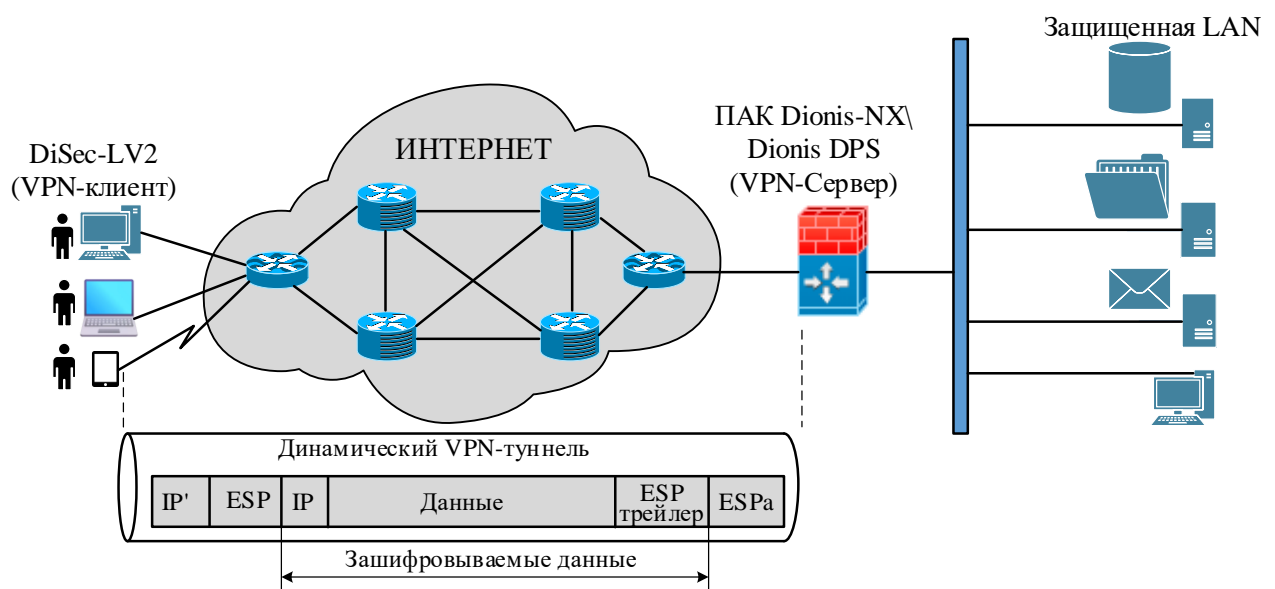
## 1. НАЗНАЧЕНИЕ

1.1. DiSec-LV2 предназначено для обеспечения безопасного доступа удаленного пользователя к ресурсам защищенной локальной сети (LAN).

1.2. Безопасный доступ основан на использовании технологии VPN (клиент-сервер). DiSec-LV2 является VPN-клиентом. В качестве VPN-сервера используются ПАК Dionis-NX и ПАК Dionis DPS производства ООО «Фактор-ТС».

Между VPN-клиентом и VPN-сервером организуется динамический VPN-туннель по запросу пользователя (VPN-клиента). Согласование параметров VPN-туннеля выполняется по протоколу ISAKMP (Internet Security Association and Key Management Protocol). ISAKMP обеспечивает обмен конфигурационной информацией между VPN-клиентом и VPN-сервером, криптографическую аутентификацию сторон, исключение вмешательства посторонних лиц в процесс установления VPN-туннеля, обмен секретными ключами.

1.3. DiSec-LV2 позволяет настроить VPN-туннели с неограниченным количеством VPN-серверов. Схема организации VPN-туннеля приведена на рисунке 1.1.



IP' - новый IP заголовок; ESP – ESP заголовок; IP - исходный IP заголовок; ESPa – данные ESP аутентификации

Рисунок 1.1

1.4. Защита передаваемой в VPN-туннеле конфиденциальной информации реализована с использованием асимметричного криптографического метода шифрования.

Асимметричный криптографический метод шифрования основан на использовании открытого и закрытого ключей. Открытый ключ используется для зашифрования данных и может передаваться по незащищенным каналам. Закрытый ключ используется для расшифрования полученной информации.

1.5. Для установления безопасного зашифрованного соединения между VPN-клиентом и VPN-сервером через Internet используется группа протоколов IPsec VPN (Internet Protocol Security).

В состав IPsec входят протоколы:

- протокол обмена ключами (IKE);
- протокол безопасной инкапсуляции полезной нагрузки (ESP);
- ассоциация безопасности (SA).

IKE применяется для защищенного обмена ключами и создания SA между VPN-клиентом и VPN-сервером.

SA представляет собой набор параметров, характеризующих защищенное соединение (алгоритм шифрования, ключ шифрования).

ESP обеспечивает шифрование передаваемых данных и проверку подлинности и целостности IP-пакетов.

1.6. ESP устанавливает режим передачи IP-пакетов: транспортный или туннельный.

1.7. В транспортном режиме заголовок ESP вставляется после исходного заголовка IP-пакета. Трейлер ESP и значение аутентификации добавляются в конец пакета. В этом режиме шифруется только полезная нагрузка IP-пакета, заголовок IP-пакета не защищен.

1.8. В туннельном режиме исходный IP-пакет инкапсулируется в новый IP-пакет. В этом режиме зашифровывается полезная нагрузка и заголовок IP-пакета.

1.9. IPsec VPN работает в туннельном режиме, обеспечивая создание VPN-туннеля.

1.10. Основные используемые порты и номера протоколов:

- протокол UDP, порт 500 (IKE управление ключами);
- протокол UDP, порт 4500 (IPSEC NAT-Traversal mode);
- протокол ESP, значение 50 (for IPSEC).

## **2. УСЛОВИЯ ПРИМЕНЕНИЯ**

### **2.1. Среда функционирования**

#### **2.1.1. Аппаратная среда функционирования**

2.1.1.1. В качестве аппаратной среды функционирования DiSec-LV2 используется вычислительное средство (персональный компьютер, ноутбук, смартфон), функционирующее под управлением операционной системы на основе Linux и оборудованное портом USB для подключения USB-флеш-накопителя или Рутокен ЭЦП 2.0 Flash/Рутокен ЭЦП 3.0 3120/Смарт-карта Рутокен ЭЦП 3.0 NFC 3100/Рутокен Lite 1010 (далее по тексту USB-Рутокен).

#### **2.1.2. Программная среда функционирования**

2.1.2.1. В качестве программной среды функционирования DiSec-LV2 используются Linux подобные операционные системы:

- Astra Linux SE 1.7 Smolensk «Рабочая станция» (ядра Linux 6.1, 5.15 и 5.10 x64);
- Astra Linux SE 1.8 Smolensk «Рабочая станция» (ядро Linux 6.1 x64);
- Альт «Рабочая станция» 9.2 (ядро Linux 5.10 x64);
- Альт «Рабочая Станция» К 10.3 (ядро Linux 6.1 x64);
- РЕД ОС 7.3 «Рабочая станция» (ядро Linux 6.1 x64);
- РЕД ОС 8 «Рабочая станция», ядро Linux 6.12 x64.

2.1.2.2. Операционная система должна соответствовать требованиям, приведенным в документе «СКЗИ «Клиент криптографического сервера доступа DiSec-LV2» Правила пользования» RU.НКБГ.70021 90.

### **2.2. Интерфейсы управления**

2.2.1. Настройка и мониторинг функционированием DiSec-LV2 выполняется с использованием графического интерфейса и (или) интерфейса командной строки.

### **2.3. Квалификация администратора**

2.3.1. Администратор должен иметь опыт администрирования операционных систем на базе ядра Linux.

2.3.2. В задачи администратора входит:

- установка, настройка, управление и мониторинг функционирования операционной системы;
- установка, настройка и управление параметрами безопасности DiSec-LV2;
- взаимодействие с администраторами VPN-серверов в части согласования параметров VPN-туннеля;
- взаимодействовать с Администратором безопасности или лицом уполномоченным по работе с ключевой информацией в части получения закрытого ключа, сертификатов головного удостоверяющего центра (ГУЦ) и\или регионального удостоверяющего центра (УЦ), клиентского сертификата открытого ключа, списка отзыва сертификатов;
- взаимодействовать со службой поддержки ООО «Фактор-ТС» в части получения лицензии на использование DiSec-LV2.

### 3. ПОДГОТОВКА К УСТАНОВКЕ

3.1. DiSec-LV2 поставляется в виде дистрибутивов:

- 1) RU.НКБГ.70021 93 01;
- 2) RU.НКБГ.70021 93 02.

3.2. В состав дистрибутива RU.НКБГ.70021 93 01 входит установочный файл с расширением deb, например, disec-lv2-cli-<номер\_версии>.deb. Установочный файл содержит службу DiSec-LV2. Управление работой службы DiSec-LV2 выполняется в консольном режиме с использованием интерфейса командной строки.

3.3. В состав дистрибутива RU.НКБГ.70021 93 02 входит установочный файл с расширением deb, например, disec-lv2-<номер\_версии>.deb. Установочный файл содержит службу DiSec-LV2 и графическое приложение службы DiSec-LV2. Управление работой службы DiSec-LV2 выполняется в графическом режиме с использованием графического приложения или в консольном режиме с использованием интерфейса командной строки.

3.4. Дистрибутивы DiSec-LV2 поставляются на USB-флеш-накопителе или компакт-диске.

3.5. Комплект поставки DiSec-LV2 приведен в документе «СКЗИ «Клиент криптографического сервера доступа DiSec-LV2» Формуляр» RU.НКБГ.70021 30.

3.6. Перед установкой DiSec-LV2 необходимо получить от Администратора безопасности или лица, уполномоченного по работе с ключевой информацией:

- файл с сертификатом ГУЦ (например, ca.cer) и сертификатами УЦ (при наличии);
- файл с закрытым ключом VPN-клиента, например, user2.p15;
- файл с сертификатом открытого ключа VPN-клиента (user2.cer);
- файл со список отзыва сертификатов (crl.crl).

#### **Примечания:**

1. Файл с закрытым ключом VPN-клиента передается на USB-флеш-накопителе или USB-Рутокен.

2. Файл с закрытым ключом должен находиться в файловой системе накопителя на уровне не выше третьего (начиная с 1) уровня вложенности.

## 4. ГРАФИЧЕСКОЕ ПРИЛОЖЕНИЕ DiSec-LV2

### 4.1. Установка DiSec-LV2

4.1.1. Установка графического приложения и службы DiSec-LV2 в среде ОС Astra Linux SE 1.7 выполняется от имени суперпользователя (root) в следующей последовательности:

1) Выполнить запуск ОС.

2) Выполнить проверку наличия, ранее установленных графического приложения и службы DiSec-LV2.

При наличии ранее установленных графического приложения и службы DiSec-LV2 - следует выполнить их удаление (см. подраздел 4.2.).

3) Выполнить запуск эмулятора терминала Terminal Fly.

4) Вставить USB-флеш-накопитель с дистрибутивом DiSec-LV2 в порт USB или компакт-диск с дистрибутивом DiSec-LV2 в оптический накопитель вычислительного средства (ВС).

**Примечание.** Дистрибутив графического приложения и службы DiSec-LV2 - RU.НКБГ.70021 93 02.

5) Подключить (монтировать) файловую систему USB-флеш-накопителя или компакт-диска с дистрибутивом DiSec-LV2 в каталог ОС, например, media.

*Пример - `sudo mount /dev/<файл устройства> /media/`*

6) Перейти в выбранный каталог ОС и выполнить установку DiSec-LV2.

*Пример - `sudo dpkg -i disec-lv2-<номер_версии>.deb`*

После завершения установки графического приложения и службы DiSec-LV2 на рабочем столе ОС в меню «Пуск» в разделе «Утилиты» появятся пункты: «DiSec-LV2» и «DiSec-LV2 Управление», например, как показано на рисунке 4.1 для ОС Astra Linux SE 1.7.

Вызов «DiSec-LV2» предназначен для пользователя (оператора) и используется для управления VPN-туннелями, просмотра конфигурации VPN-туннелей и сообщений, регистрируемых в процессе функционирования DiSec-LV2.

Вызов «DiSec-LV2 Управление» предназначен для администратора и используется для создания\удаления VPN-туннелей, редактирования

параметров VPN-туннелей, управления VPN-туннелями, установки уровня детализации сообщений, регистрируемых в процессе функционирования DiSec-LV2.

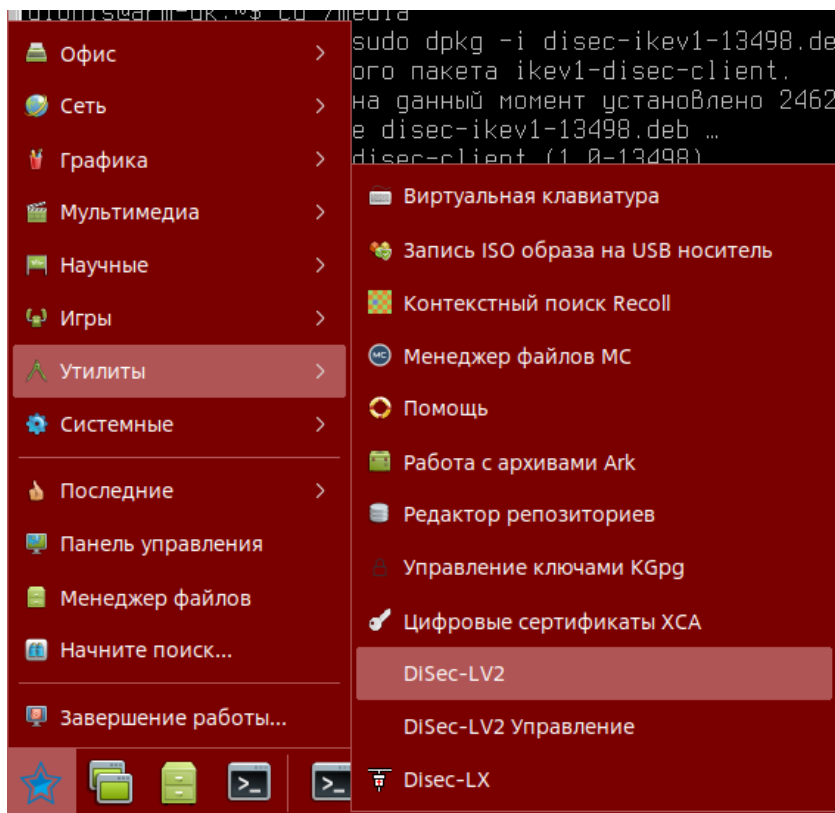


Рисунок 4.1

Процесс установки DiSec-LV2 сопровождается выводом информационных сообщений на экран монитора ВС, например, как показано на рисунке 4.2.

```
dionis@arm-gk:/media$ sudo dpkg -i disec-lv2-2667.deb
Выбор ранее не выбранного пакета disec-lv2-ui.
(Чтение базы данных ... на данный момент установлено 295711 файлов и каталогов.)
Подготовка к распаковке disec-lv2-2667.deb ...
Распаковывается disec-lv2-ui (1.0.0-2667) ...
Настраивается пакет disec-lv2-ui (1.0.0-2667) ...
Обрабатываются триггеры для xserver-xorg-core (2:21.1.7-1ubuntu4.astra.se48) ...
update exec ids due to /usr/bin changed
Обрабатываются триггеры для desktop-file-utils (0.27-2astra2+b2) ...
Обрабатываются триггеры для mime-support (3.62) ...
Обрабатываются триггеры для hicolor-icon-theme (0.17-2+b1) ...
dionis@arm-gk:/media$
```

Рисунок 4.2

7) Безопасно извлечь (отмонтировать) USB-флеш-накопитель или компакт-диск с дистрибутивом DiSec-LV2.

**Пример - `sudo umount /media/`**

8) Извлечь USB-флеш-накопитель из порта USB или компакт-диск из оптического накопителя вычислительного средства.

4.1.2. Перед установкой DiSec-LV2 в среде РЕД ОС 8 «Рабочая станция» необходимо выполнить следующие действия от имени суперпользователя (root):

1) Установить пакет `openresolv`.

**Пример - `sudo dnf install openresolv -y`**

2) Установить права на файл `/usr/sbin/resolvconf.openresolv`.

**Пример - `sudo chmod +x /usr/sbin/resolvconf.openresolv`**

## 4.2. Удаление DiSEC-LV2

4.2.1. Удаление графического приложения и службы DiSec-LV2 выполняется в консольном режиме от имени суперпользователя (root).

4.2.2. Удаление DiSec-LV2 выполняется по команде:

**`sudo dpkg --purge disec-lv2-ui.`**

## 4.3. Выполнение DiSec-LV2

### 4.3.1. Запуск DiSec-LV2

#### 4.3.1.1. Запуск DiSec-LV2 в ручном режиме

4.3.1.1.1. Запуск графического приложения DiSec-LV2 в ручном режиме выполняется в следующей последовательности:

1) Выполнить загрузку ОС.

2) На панели задач нажать кнопку  (Меню «Пуск») и в разделе «Утилиты» выбрать пункт «DiSec-LV2» или «DiSec-LV2 Управление» (см. рисунок 4.1).

Выбор пункта «DiSec-LV2» запускает DiSec-LV2 от имени пользователя (оператора).

Выбор пункта «DiSec-LV2 Управление» запускает DiSec-LV2 от имени администратора.

3) При запуске DiSec-LV2 от имени администратора в открывшемся окне «Требуется аутентификация» (см. рисунок 4.3) ввести пароль учетной записи администратора и нажать кнопку «Да».

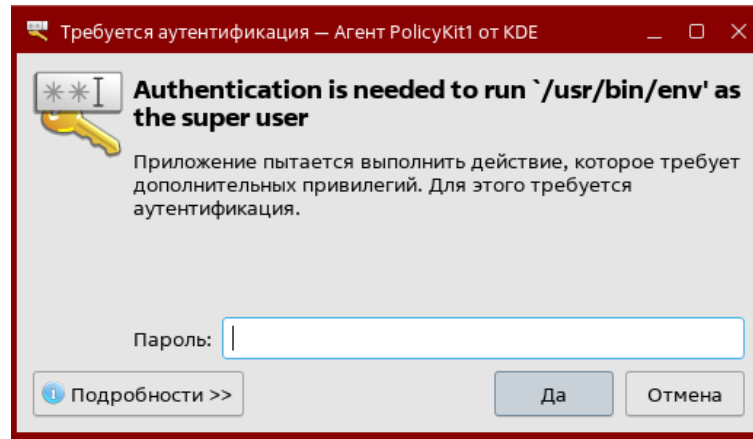


Рисунок 4.3

#### 4.3.1.2. Запуск DiSec-LV2 в автоматическом режиме

4.3.1.2.1. Запуск графического приложения DiSec-LV2 от имени пользователя (оператора) в автоматическом режиме выполняется при загрузке ОС. Настройка автоматического режима запуска DiSec-LV2 приведена в разделе 4.3.13.

#### 4.3.1.3. Главное диалоговое окно DiSec-LV2

4.3.1.3.1. После запуска DiSec-LV2 открывается главное диалоговое окно DiSec-LV2. Структура главного диалогового окна DiSec-LV2 приведена на рисунке 4.4.

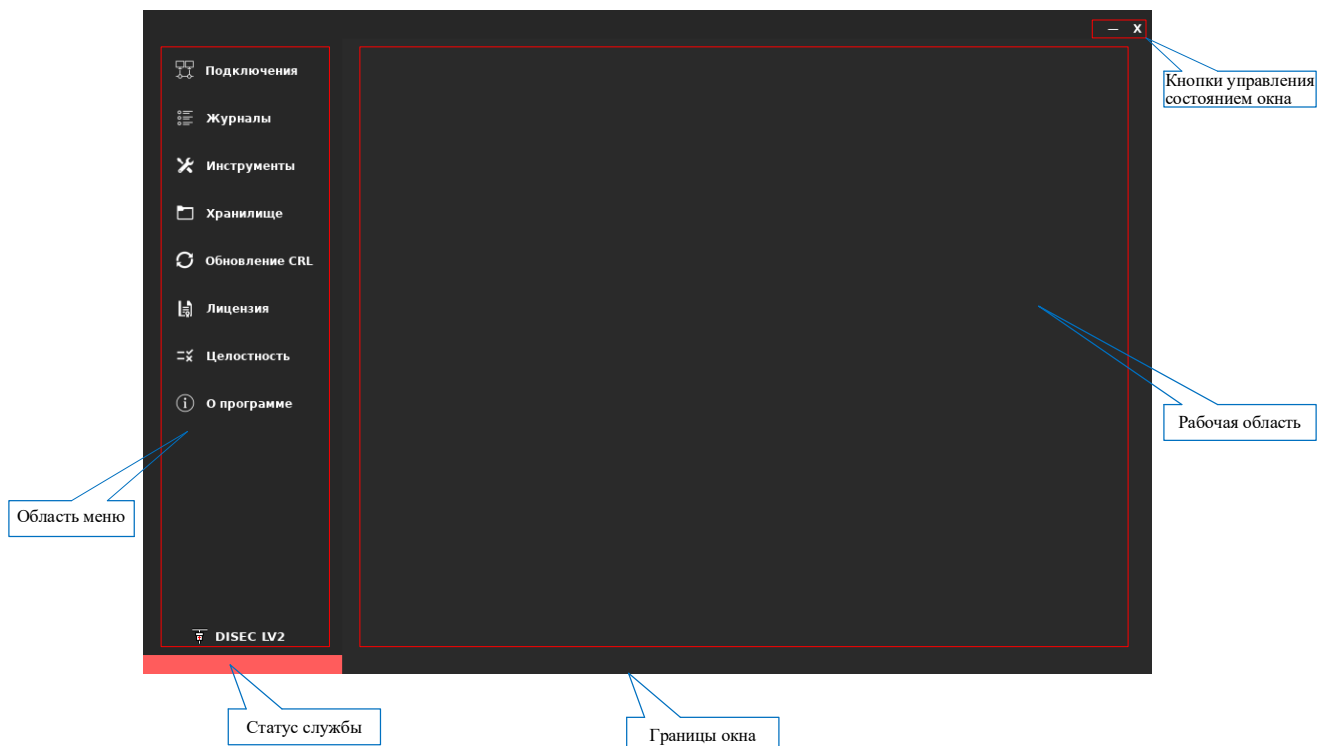


Рисунок 4.4

Область меню	Перечень разделов, которые определяют основные функции DiSec-LV2
--------------	--

Рабочая область	Действия, которые могут быть выполнены в данной области главного окна
Кнопки управления состоянием окна	Кнопки, позволяющие управлять окном: закрыть, свернуть на панель задач ОС
Статус службы	DiSec-LV2 запущен\ DiSec-LV2 не запущен
Границы окна	Рамка ограничивающая окно со всех сторон

### 4.3.2. Завершение работы DiSec-LV2

4.3.2.1. Завершение работы DiSec-LV2 выполняется в следующей последовательности:


- 1) В правом верхнем углу главного окна DiSec-LV2 нажать кнопку  (см. рисунок 4.5).



Рисунок 4.5

- 2) В открывшемся окне (например, как показано на рисунке 4.6) нажать кнопку «Да».

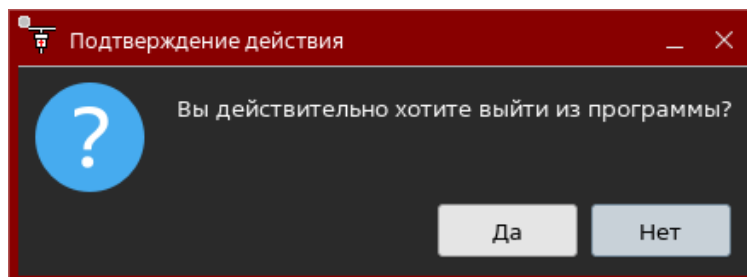


Рисунок 4.6

### 4.3.3. Регистрация DiSec-LV2

4.3.3.1 Регистрация DiSec-LV2 выполняется при первом запуске в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.).

В области меню главного окна DiSec-LV2 (см. рисунок 4.7) при первом запуске автоматически выбирается раздел «Лицензия».

В рабочей области раздела «Лицензия» нажать кнопку «Копировать» для копирования в буфер обмена ID аппаратной платформы ВС.

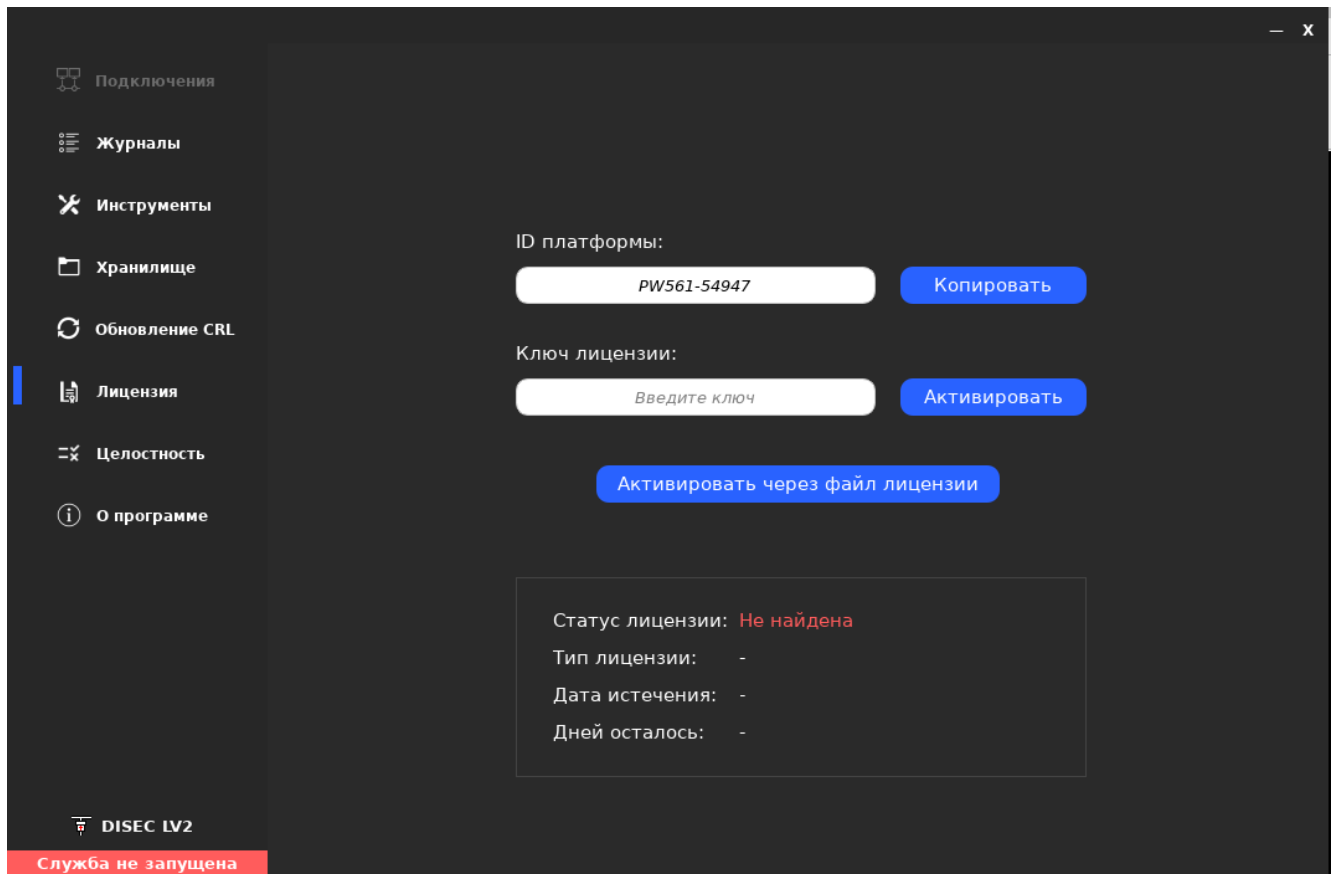


Рисунок 4.7

- 2) В открывшемся окне (например, как показано на рисунке 4.8) нажать кнопку «Да».

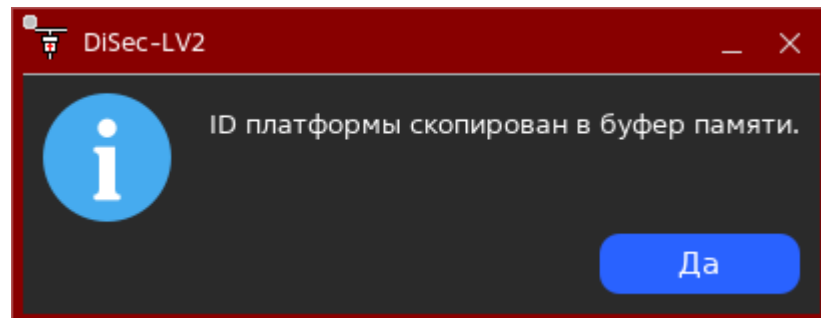


Рисунок 4.8

- 3) Сообщить ID платформы в службу поддержки DiSec-LV2 (см. раздел меню «О программе») и получить файл с ключом активации лицензии на использование DiSec-LV2 или ключ активации. Файл с ключом активации лицензии должен иметь расширение lic.
- 4) Если из службы поддержки DiSec-LV2 получен файл с ключом активации лицензии:
- выполнить запись этого файла на USB-флеш-накопитель или накопитель на жестком магнитном диске BC;

- b) в рабочей области раздела «Лицензия» нажать кнопку «Активировать через файл лицензии»;
- c) в открывшемся окне (например, как показано на рисунке 4.9) выбрать файл с лицензией и нажать кнопку «Открыть».

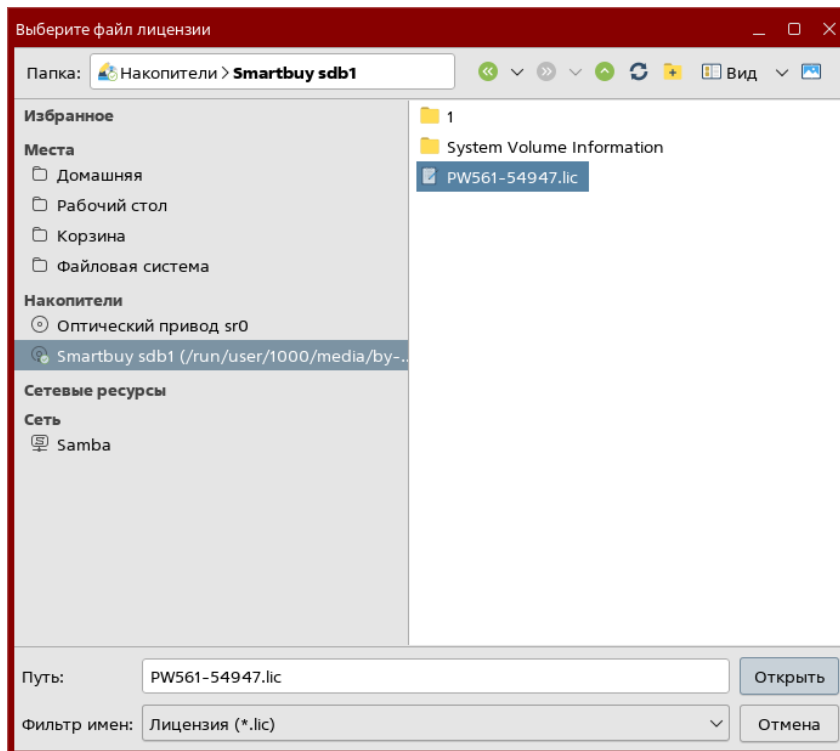


Рисунок 4.9

- d) в открывшемся окне (например, как показано на рисунке 4.10) нажать кнопку «Да».



Рисунок 4.10

- 5) Если из службы поддержки DiSec-LV2 получен ключ активации лицензии, то ввести его в поле ввода «Ключ лицензии:» (например, как показано на рисунке 4.7) и нажать кнопку «Активировать».
- 6) После активации лицензии (например, как показано на рисунке 4.11) в рабочей области раздела «Лицензия»:
- в поле «Статус лицензии:» запись «Не найдена» изменится на «Активна»;

- в поле «Тип лицензии:» появится тип примененной лицензии на использование DiSec-LV2;
- в поле «Дата истечения:» появится дата окончания действия лицензии;
- в поле «Дней осталось:» появится количество дней до окончания действия лицензии.

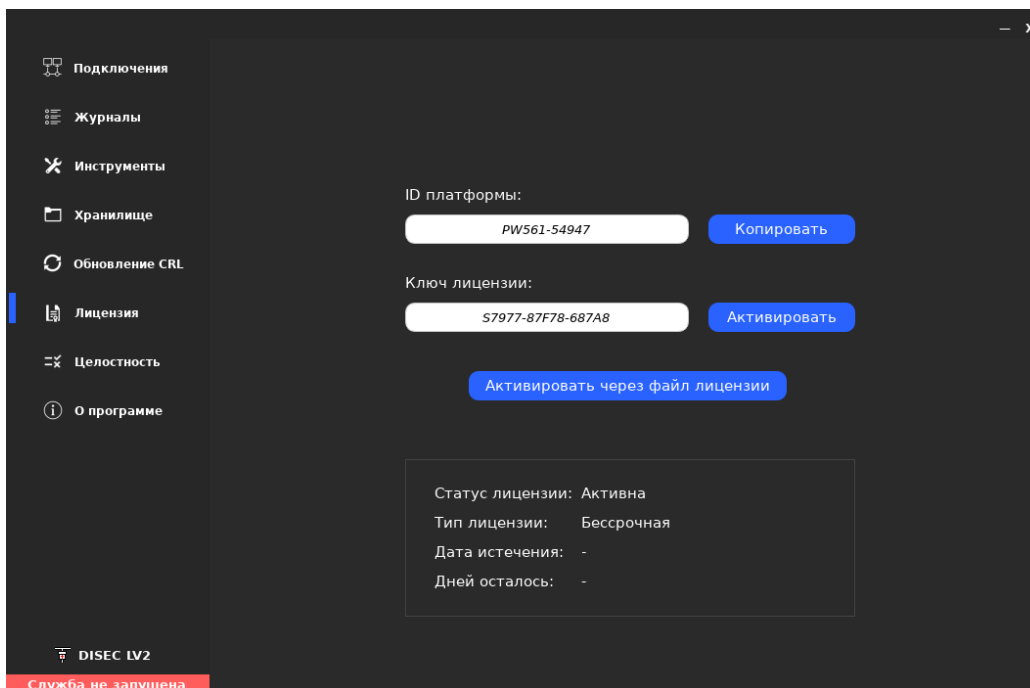


Рисунок 4.11

#### 4.3.4. Контроль целостности

4.3.4.1. Контроль целостности выполняется при запуске и в процессе эксплуатации DiSec-LV2 в соответствии с внутренним регламентом эксплуатирующей организации.

4.3.4.2. Контроль целостности в процессе эксплуатации DiSec-LV2 выполняется в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.).
- 2) В главном диалоговом окне DiSec-LV2 выбрать раздел «Целостность» (например, как показано на рисунке 4.12).

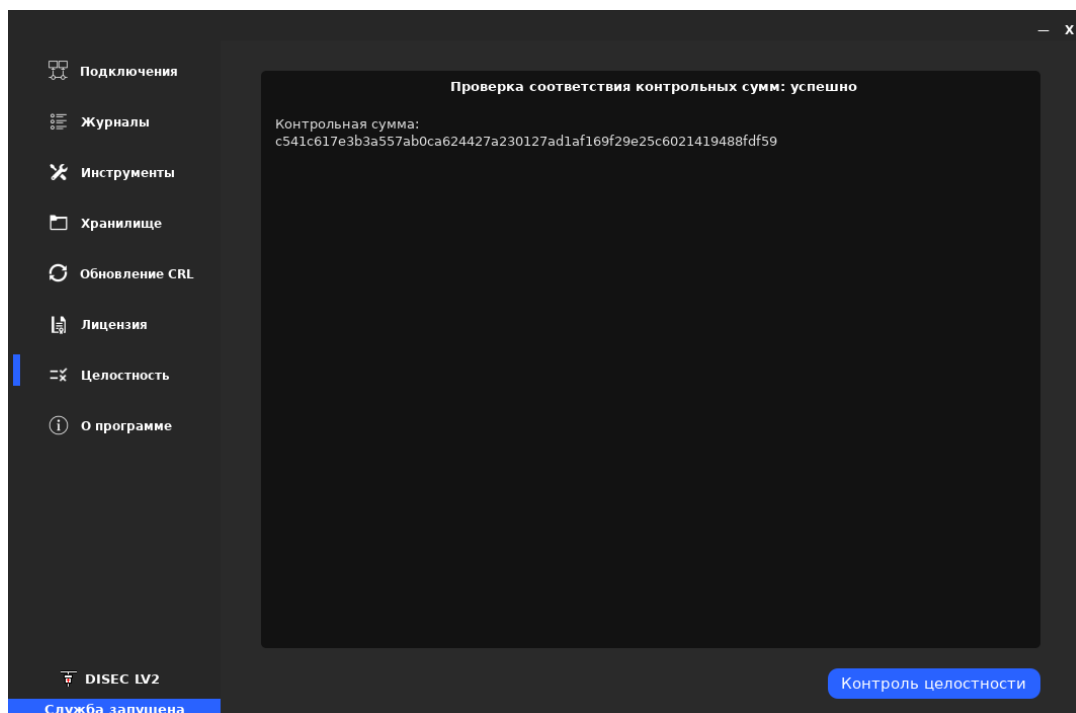


Рисунок 4.12

- 3) В рабочей области раздела «Целостность» нажать кнопку «Контроль целостности».
- 4) Сравнить значение контрольной суммы (КС) в открывшемся окне (например, как показано на рисунке 4.13) с КС в документе «СКЗИ «Клиент криптографического сервера доступа DiSec-LV2» Формуляр» RU.НКБГ.70021 30 и нажать кнопку «Да».

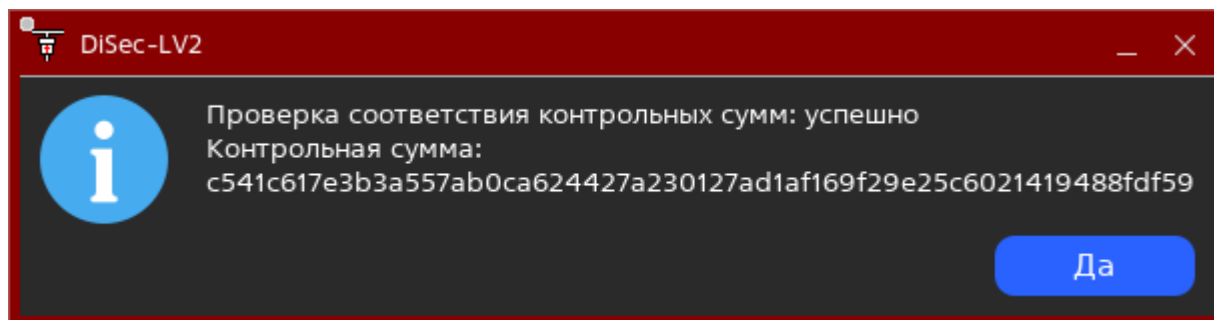


Рисунок 4.13

- 5) Если контроль целостности DiSec-LV2 завершился с отрицательным результатом, рассчитанная контрольная сумма не совпала с контрольной суммой, приведенной в формуляре, следует прекратить дальнейшее использование DiSec-LV2 и обратиться в службу техподдержки ООО «Фактор-ТС». Контактные данные службы техподдержки ООО «Фактор-ТС» приведены в разделе «О программе» области меню главного окна DiSec-LV2.

### 4.3.5. Импорт сертификатов и списка отзыва сертификатов

4.3.5.1. Импорт сертификата VPN-клиента, сертификата ГУЦ, сертификатов УЦ (при наличии) и списков отзыва сертификатов (CRL) выполняется после активации лицензии на использование DiSec-LV2.

4.3.5.2. Перед импортом сертификатов и списков отзыва сертификатов следует выполнить следующие действия:

- 1) Записать на USB-флеш-накопитель или в выбранный каталог на накопителе ВС следующие файлы:
  - файл с сертификатом (ГУЦ), например, ca.cer;
  - файлы с сертификатами УЦ (при наличии);
  - файл с сертификатом открытого ключа VPN-клиента, например, user2.cer;
  - файл со списком отзыва сертификатов, например, crl.crl.
- 2) Вставить USB-флеш-накопитель в порт USB вычислительного средства и подключить (монтировать) USB-флеш-накопитель.

**Примечание.** Действия выполняются, если файлы с сертификатами и списком отзыва сертификатов были записаны на USB-флеш-накопитель.
- 3) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.)

4.3.5.3. Импорт на выбор одного или нескольких сертификатов и списка отзыва сертификатов (CRL) выполняется в следующей последовательности:

- 1) В области меню главного окна DiSec-LV2 (см. рисунок 4.14) выбрать раздел «Хранилище».

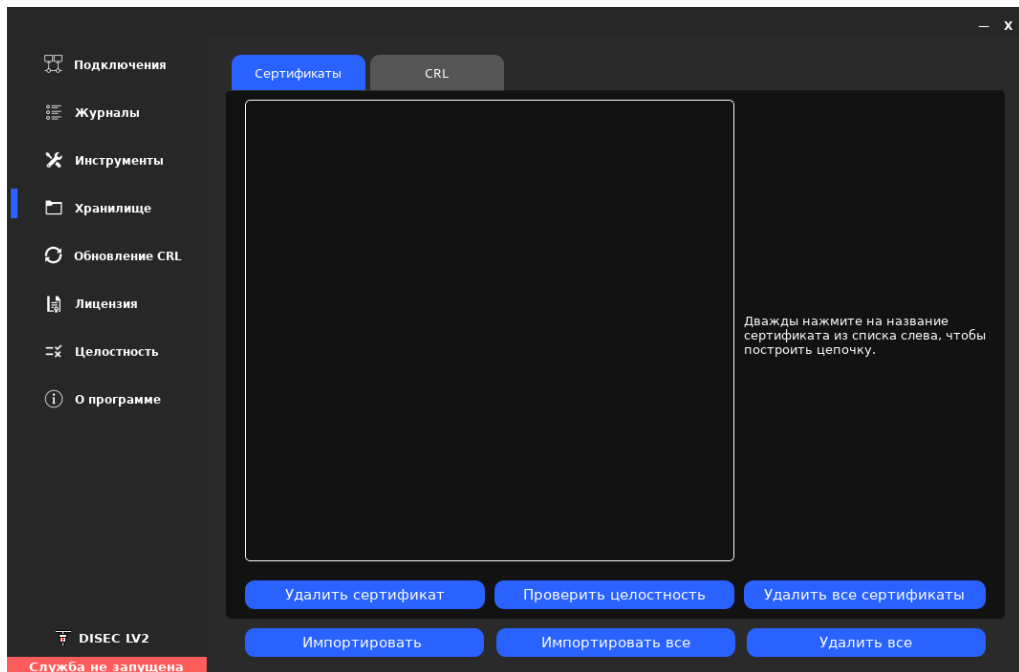


Рисунок 4.14

- 2) В рабочей области раздела «Хранилище» нажать кнопку «Импортировать» и в открывшемся окне (например, как показано на рисунке 4.15) выбрать один или несколько файлов с сертификатами и списками отзыва сертификатов (CRL) и нажать кнопку «Открыть».

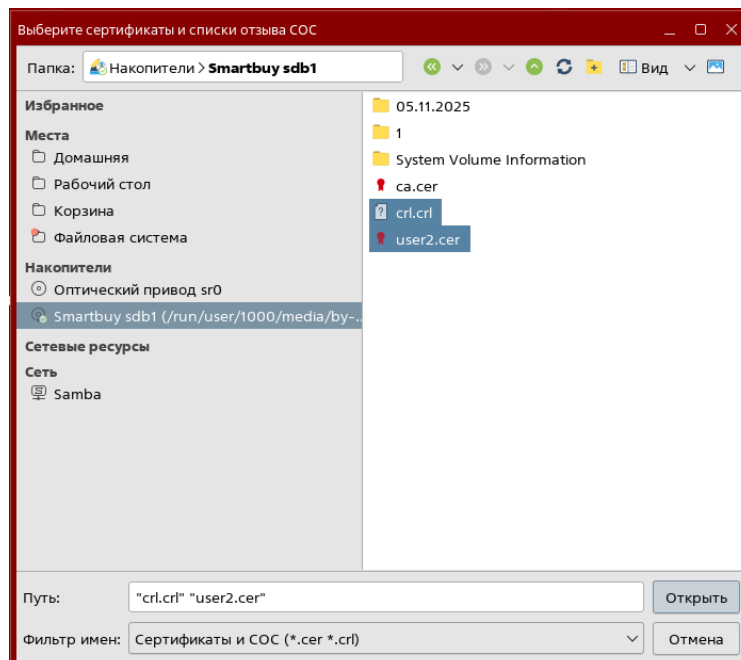


Рисунок 4.15

- 3) В открывшемся окне (например, как показано на рисунках 4.16) нажать кнопку «Да».

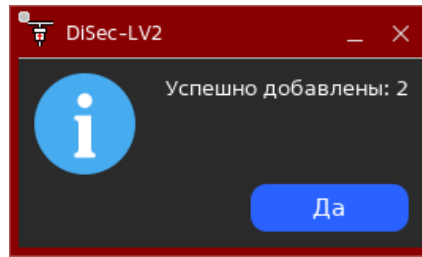


Рисунок 4.16

4.3.5.4. Импорт всех сертификатов и списка отзыва сертификатов выполняется в следующей последовательности:

- 1) В области меню главного окна DiSec-LV2 (см. рисунок 4.14) выбрать раздел «Хранилище».
- 2) В рабочей области раздела «Хранилище» нажать кнопку «Импортировать все» и в открывшемся окне (например, как показано на рисунке 4.17) выбрать накопитель или каталог на накопителе с файлами сертификатов и списками отзыва сертификатов и нажать кнопку «Открыть».

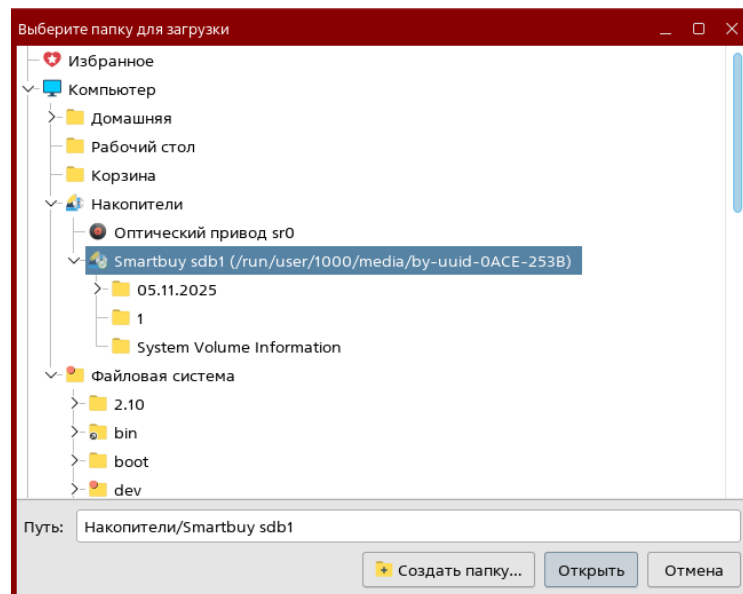


Рисунок 4.17

- 3) В открывшемся окне (например, как показано на рисунке 4.18) нажать кнопку «Да».

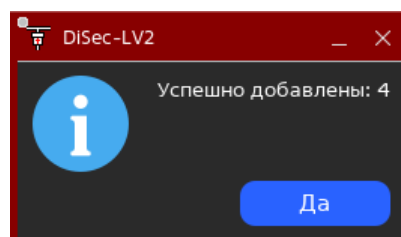


Рисунок 4.18

#### 4.3.6. Удаление сертификатов и списка отзыва сертификатов

4.3.6.1. Удаление сертификата (сертификатов) выполняется в следующей последовательности:

- 1) В рабочей области раздела «Хранилище» выбрать вкладку «Сертификаты» (например, как показано на рисунке 4.19).

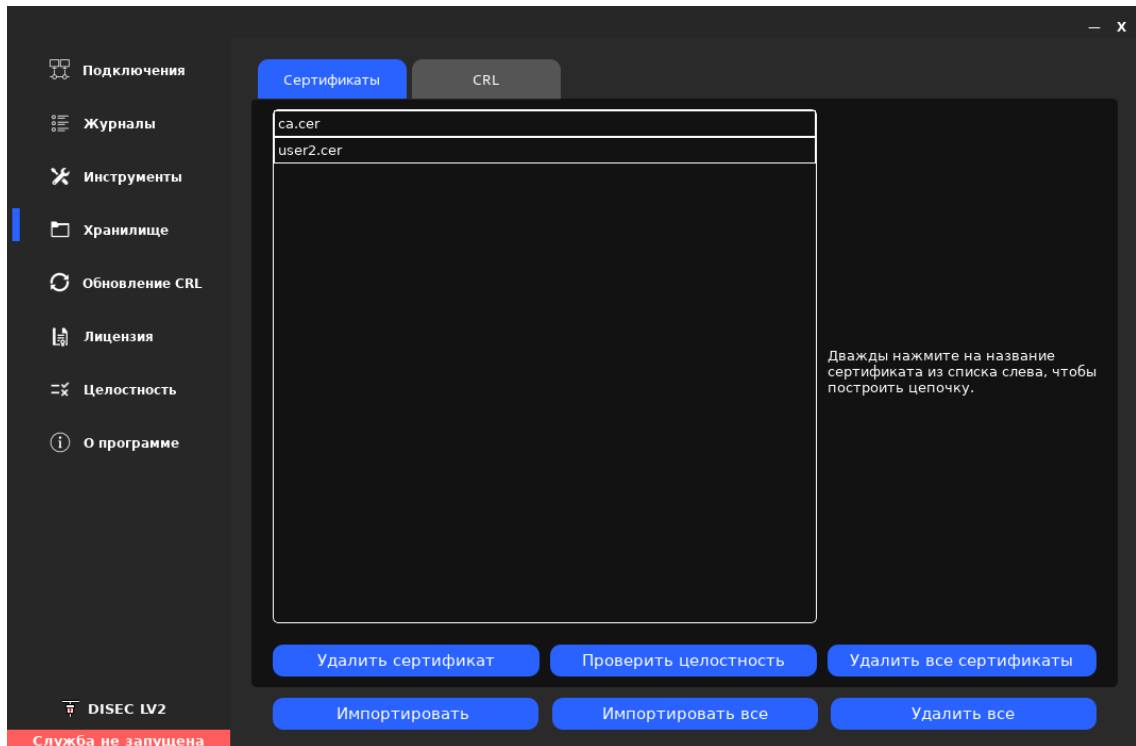


Рисунок 4.19

- 2) В списке сертификатов выбрать требуемый сертификат и нажать кнопку «Удалить сертификат».
- 3) В открывшемся окне (например, как показано на рисунке 4.20) нажать кнопку «Да».

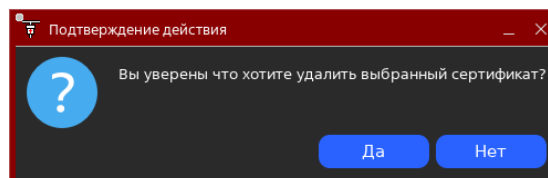


Рисунок 4.20

4.3.6.2. Удаление всех сертификатов выполняется в следующей последовательности:

- 1) В рабочей области раздела «Хранилище» выбрать вкладку «Сертификаты» (например, как показано на рисунке 4.19).
- 2) Нажать кнопку «Удалить все сертификаты».

- 3) В открывшемся окне (например, как показано на рисунке 4.21) нажать кнопку «Да».

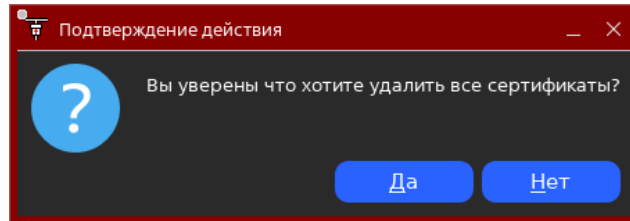


Рисунок 4.21

4.3.6.3. Удаление списка отзыва сертификатов выполняется в следующей последовательности:

- 1) В рабочей области раздела «Хранилище» выбрать вкладку «CRL» (например, как показано на рисунке 4.22).

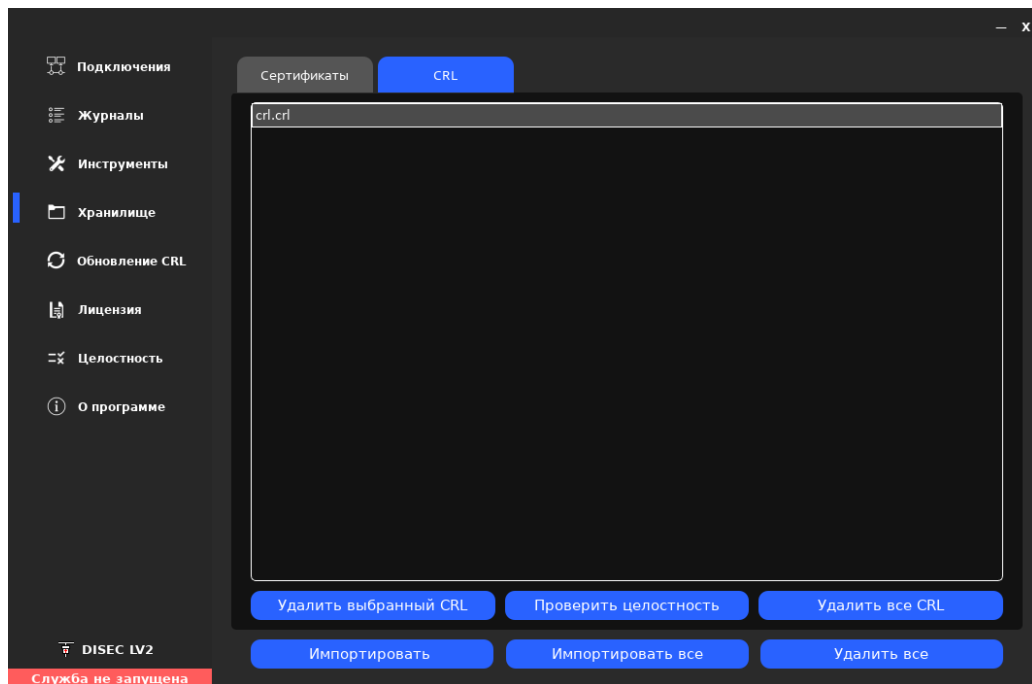


Рисунок 4.22

- 2) В списках отзыва сертификатов выбрать требуемый список и нажать кнопку «Удалить выбранный CRL».
- 3) В открывшемся окне (например, как показано на рисунке 4.23) нажать кнопку «Да».

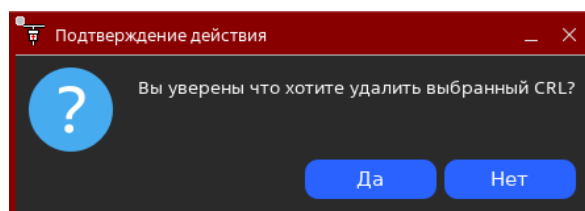


Рисунок 4.23

4.3.6.4. Удаление всех списков отзыва сертификатов выполняется в следующей последовательности:

- 1) В рабочей области раздела «Хранилище» выбрать вкладку «CRL» (например, как показано на рисунке 4.22).
- 2) Нажать кнопку «Удалить все CRL».
- 3) В открывшемся окне (например, как показано на рисунке 4.24) нажать кнопку «Да».

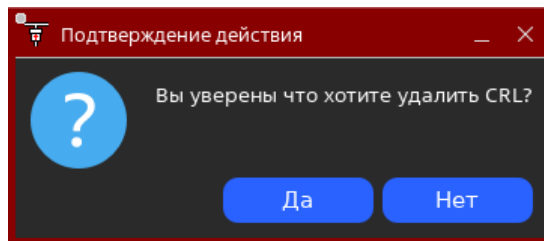


Рисунок 4.24

4.3.6.5. Удаление всех сертификатов и списков отзыва сертификатов выполняется в следующей последовательности:

- 1) В рабочей области раздела «Хранилище» нажать кнопку «Удалить все» (см. рисунок 4.22).
- 2) В открывшемся окне (например, как показано на рисунке 4.25) нажать кнопку «Да».

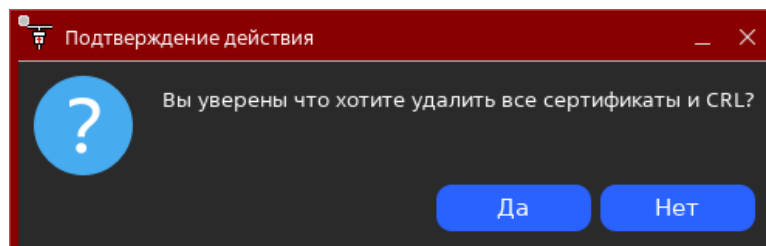


Рисунок 4.25

4.3.6.6. Просмотр цепочки доверия сертификатов выполняется в следующей последовательности:

- 1) В рабочей области раздела «Хранилище» выбрать вкладку «Сертификаты».
- 2) В списке сертификатов дважды нажать на требуемый сертификат. В правой части рабочей области раздела «Хранилище» появится цепочка доверия выбранного сертификата (например, как показано на рисунке 4.26).

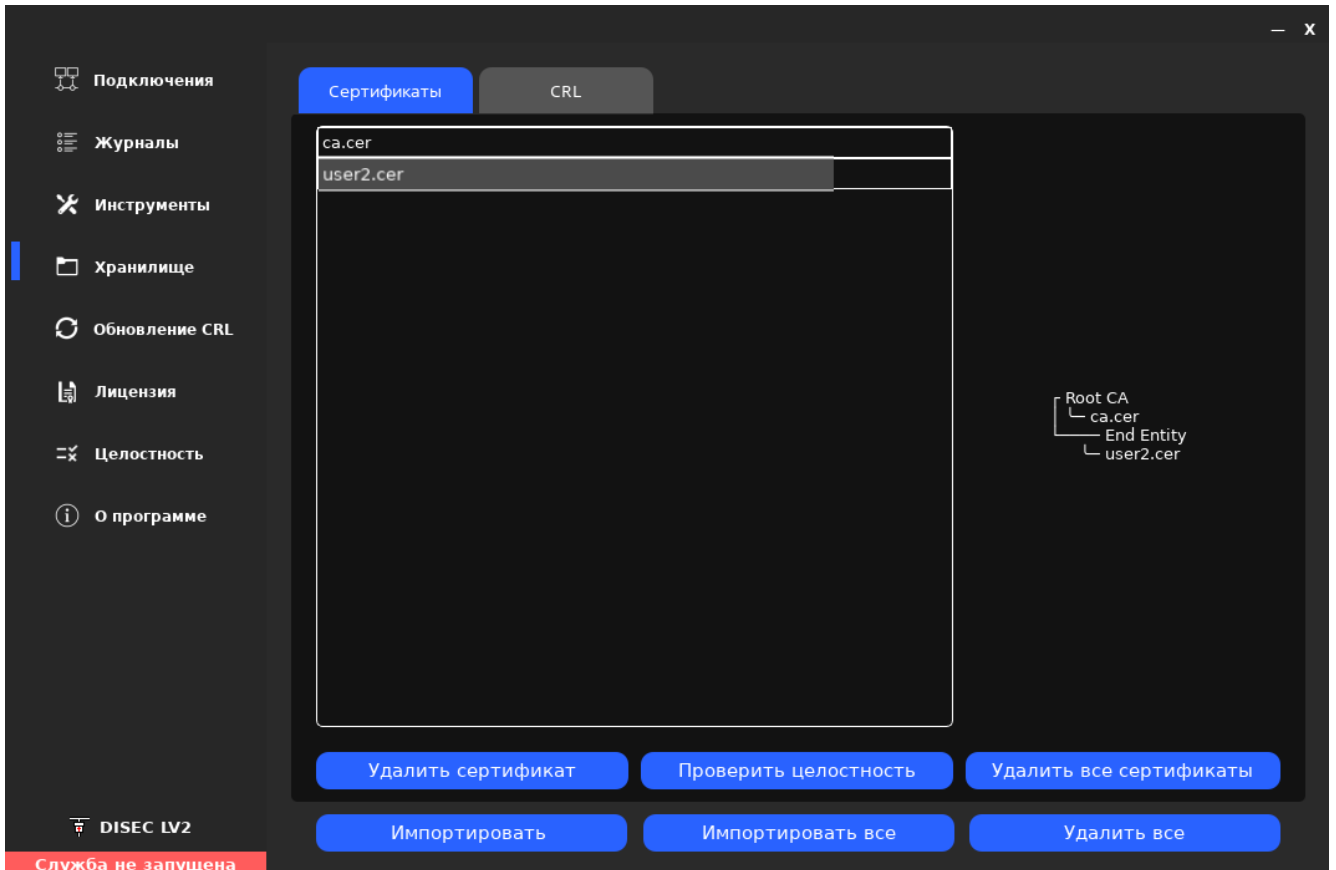


Рисунок 4.26

### 4.3.7. Создание VPN-туннеля


4.3.7.1. Перед созданием VPN-туннеля следует согласовать его параметры с администратором VPN-сервера.

4.3.7.2. В DiSec-LV2 VPN-туннель может быть создан одним из следующих способов:

- загрузкой файла конфигурации (disec.xml);
- путем ввода параметров VPN-туннеля;
- копированием параметров действующего VPN-туннеля.

4.3.7.3. Создание VPN-туннеля путем загрузки файла конфигурации выполняется в следующей последовательности:

- 1) Подготовить файл конфигурации (disec.xml) в любом XML-редакторе. Файл конфигурации состоит из одной или нескольких секций, каждая из которых содержит параметры отдельного VPN-туннеля. Пример файла конфигурации и описание параметров VPN-туннеля приведены в приложении 1.
- 2) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.).

- 3) В области меню главного окна DiSec-LV2 (см. рисунок 4.14) выбрать раздел «Подключения».
- 4) В рабочей области раздела «Подключения» (см. рисунок 4.27) нажать кнопку  «Загрузить конфигурацию».

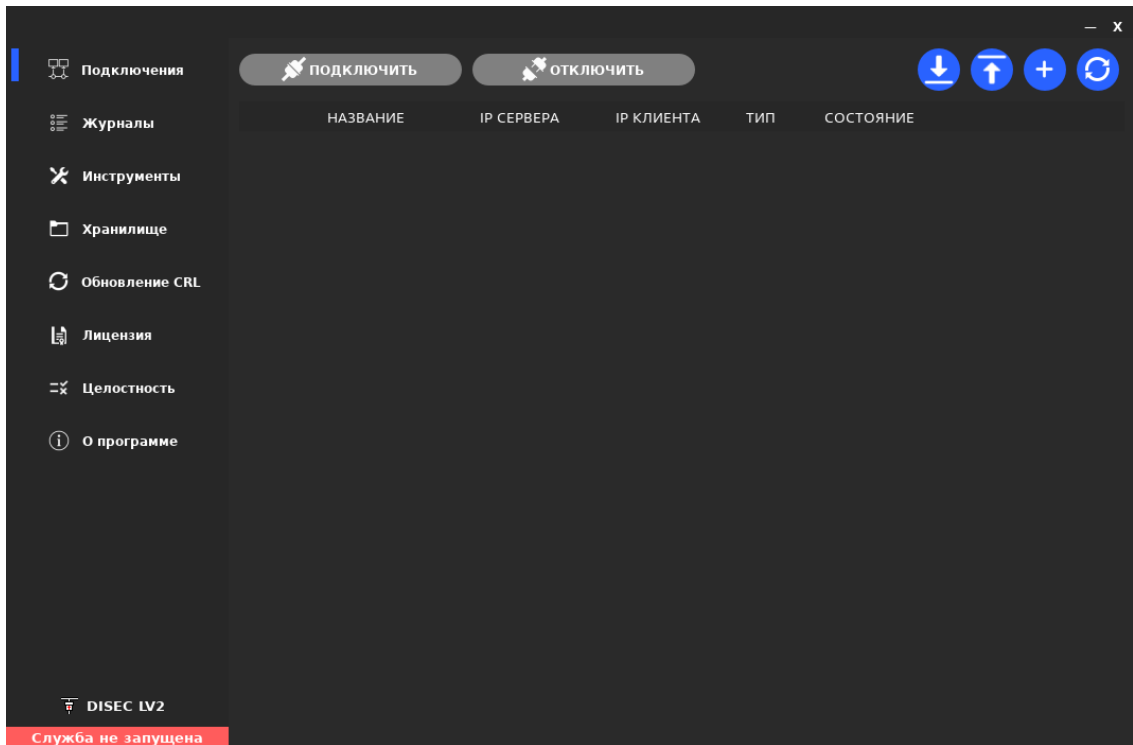


Рисунок 4.27

- 5) В открывшемся окне (например, как показано на рисунке 4.28) ввести путь к файлу конфигурации (disec.xml) и нажать кнопку «Открыть».

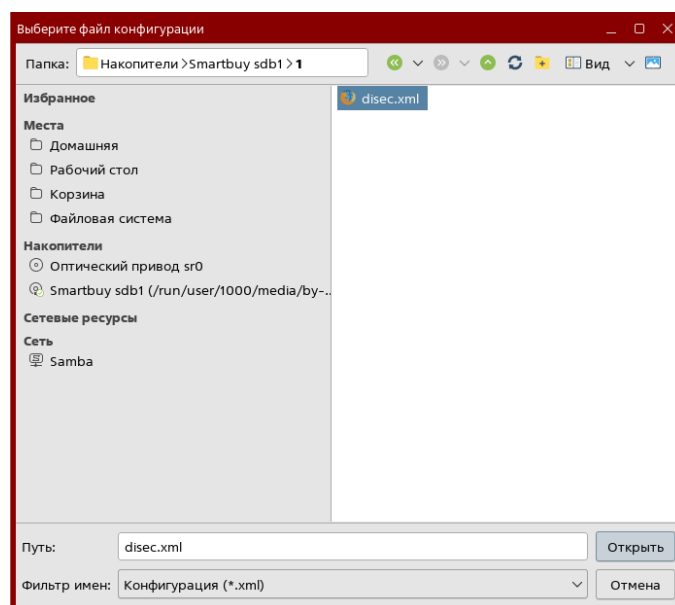


Рисунок 4.28

После нажатия кнопки «Открыть» в таблице соединений рабочей области раздела «Подключения» появится запись о созданном VPN-туннеле и статус службы DiSec-LV2 изменится на «Служба запущена» (например, как показано на рисунке 4.29).

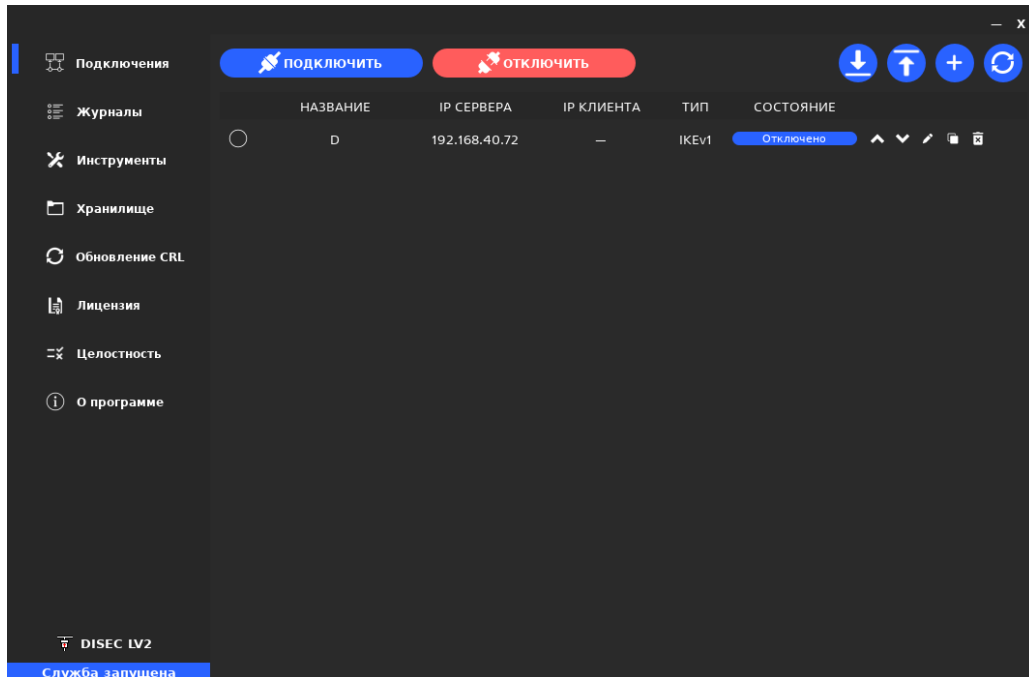


Рисунок 4.29

В создании VPN-туннеля будет отказано при наличии синтаксических ошибок в файле конфигурации. В этом случае в открывшемся окне (см. рисунок 4.30) следует нажать кнопку «Да», устранить ошибки в файле конфигурации и повторить действия по его загрузке.

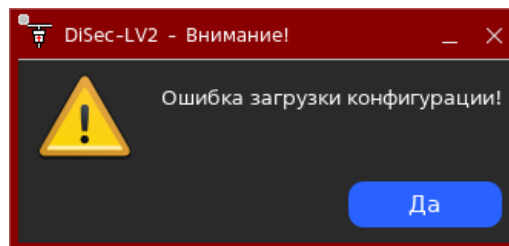



Рисунок 4.30

4.3.7.4. Создание VPN-туннеля вручную (путем ввода параметров) выполняется в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.).
- 2) В рабочей области раздела «Подключения» (см. рисунок 4.27) нажать кнопку  «Создать».

- 3) В области параметров раздела «Подключения» (см. рисунок 4.31) установить параметры VPN-туннеля. Описание параметров VPN-туннеля приведено в таблице 1.

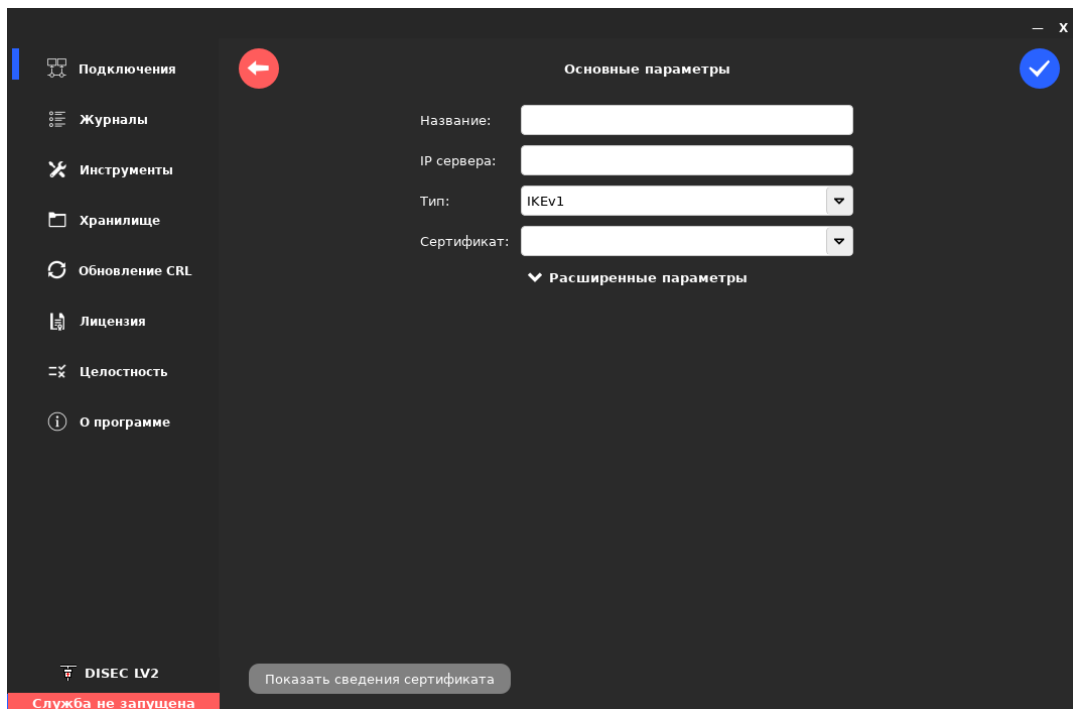


Рисунок 4.31



Таблица 1- Описание параметров VPN-туннеля

Параметр	Описание
<b>Основные параметры</b>	
Название	Название соединения. Параметр: ike_conn.
IP сервера	IP-адрес или fqdn (доменное имя) VPN-сервера. Параметр: remote_ip.
Тип	Версия протокола обмена ключами (IKE). Значения: – IKEv1; – IKE v2. На данный момент поддерживается только IKEv1. В настоящее время поле не обрабатывается. Параметр: version.
Сертификат	Имя файла с сертификатом открытого ключа VPN-клиента. Расширение файла – cer. Параметр: cert.
<b>Расширенные параметры</b>	
IP клиента	Строка содержащая IP-адрес VPN-клиента, либо значение «Автоматически». Параметр: local_ip.
<b>DPD</b>	

Параметр	Описание
действие	<p>Действие, которое необходимо выполнить, если VPN-сервер не отвечает через промежуток времени, указанный в поле «интервал» (dpd_interval).            Параметр: dpd_action.            Значения:</p> <ul style="list-style-type: none"> <li>- initiate;</li> <li>- close;</li> <li>- route;</li> <li>- restart.</li> </ul>
интервал	<p>Промежуток времени, через который надо выполнить действие, указанное в параметре «DPD действие». Параметр: dpd_interval.</p>
ожидание	<p>Промежуток времени, по истечении которого считается, что VPN-сервер не работает. Параметр: dpd_timeout.</p>
Число попыток	<p>Число попыток службы IKE по обмену ключевой информацией до разрыва соединения. Параметр: keying_tries.</p>
<b>ИКЕ фаза 1</b>	
время жизни соединения	<p>Максимальное значение времени жизни IKE фаза 1.            Параметр: ph1_life_time.</p>
transforms	<p>Набор криптопараметров для IKE фаза 1. Параметр: ph1_transforms.            Значение: &lt;алгоритм шифрования&gt;-&lt;функция хеширования&gt;-&lt;алгоритм согласования ключей&gt;, где            Алгоритм шифрования:</p> <ul style="list-style-type: none"> <li>- gost89a - алгоритм ГОСТ 28147-89, режим GOST-CFB-IMIT, узел замены CryptoPro Set A;</li> <li>- gost89b - алгоритм ГОСТ 28147-89, режим GOST-CFB-IMIT, узел замены CryptoPro Set B;</li> <li>- gost89c - алгоритм ГОСТ 28147-89, режим GOST-CFB-IMIT, узел замены CryptoPro Set C;</li> <li>- gost89d - алгоритм ГОСТ 28147-89, режим GOST-CFB-IMIT, узел замены CryptoPro Set D;</li> <li>- gost89z - алгоритм ГОСТ 28147-89, режим GOST-CFB-IMIT, узел замены CryptoPro Set Z;</li> <li>- magmacfb - ГОСТ 34.13-2018 в режиме CFB.</li> </ul> <p>Функция хеширования:</p> <ul style="list-style-type: none"> <li>- gost3411_94 - ГОСТ Р 34.11-94;</li> <li>- gost3411_12_512 - ГОСТ Р 34.11-12 с размером хэша 512 бит.</li> </ul> <p>Алгоритм согласования ключей:</p> <ul style="list-style-type: none"> <li>- gostvko01a - ВКО ГОСТ Р 34.10-2001 с размером ключа 256 бит и набором параметров id-GostR3410-2001-CryptoPro-A-ParamSet;</li> <li>- gostvko01b - ВКО ГОСТ Р 34.10-2001 с размером ключа 256 бит и набором параметров id-GostR3410-2001-CryptoPro-B-ParamSet;</li> <li>- gostvko12_256a - ВКО ГОСТ Р 34.10-2012 с размером ключа 256 бит с набором параметров id-GostR3410-2001-CryptoPro-A-ParamSet;</li> <li>- gostvko12_256b - ВКО ГОСТ Р 34.10-2012 с размером ключа 256 бит с набором параметров id-GostR3410-2001-CryptoPro-B-ParamSet;</li> <li>- gostvko12_512a - ВКО ГОСТ Р 34.10-2012 с размером ключа 512 бит набором параметров id-tc26-gost-3410-12-512-paramSetA;</li> <li>- gostvko12_512b - ВКО ГОСТ Р 34.10-2012 с размером ключа 512 бит набором параметров id-tc26-gost-3410-12-512-paramSetB.</li> </ul>

Параметр	Описание
<b>IKEv1 фаза 2</b>	
время жизни соединения	Максимальное значение времени жизни IKE фаза 2. По истечению времени происходит переподключение. Параметр: ph2_life_time.
transforms	<p>Набор криптопараметров для IKE фаза2. Параметр: ph2_transforms. Значение: &lt;алгоритм шифрования ESP&gt;-&lt;алгоритм согласования ключей&gt;, где</p> <p>Алгоритм шифрования ESP:</p> <ul style="list-style-type: none"> <li>- gost4m_imit_a - алгоритм ГОСТ 28147-89, режим GOST-4M-IMIT, узел замены CryptoPro Set A;</li> <li>- gost4m_imit_b - алгоритм ГОСТ 28147-89, режим GOST-4M-IMIT, узел замены CryptoPro Set B;</li> <li>- gost4m_imit_c - алгоритм ГОСТ 28147-89, режим GOST-4M-IMIT, узел замены CryptoPro Set C;</li> <li>- gost4m_imit_d - алгоритм ГОСТ 28147-89, режим GOST-4M-IMIT, узел замены CryptoPro Set D;</li> <li>- gost4m_imit_z - алгоритм ГОСТ 28147-89, режим GOST-4M-IMIT, узел замены CryptoPro Set Z;</li> <li>- gost1k_imit_a - алгоритм ГОСТ 28147-89, режим GOST-1K-IMIT, узел замены CryptoPro Set A;</li> <li>- gost1k_imit_b - алгоритм ГОСТ 28147-89, режим GOST-1K-IMIT, узел замены CryptoPro Set B;</li> <li>- gost1k_imit_c - алгоритм ГОСТ 28147-89, режим GOST-1K-IMIT, узел замены CryptoPro Set C;</li> <li>- gost1k_imit_d - алгоритм ГОСТ 28147-89, режим GOST-1K-IMIT, узел замены CryptoPro Set D;</li> <li>- gost1k_imit_z - алгоритм ГОСТ 28147-89, режим GOST-1K-IMIT, узел замены CryptoPro Set Z;</li> <li>- gost_magma_4m – Р 1323565.1.026-2019, алгоритм Магма в режиме MGM.</li> </ul> <p>Алгоритм согласования ключей – см. IKEv1 фаза 1&gt; transforms.</p>
<b>Параметры отправки пакетов</b>	
ph_margin_fuzz	Максимальное время, в течении которого IP-пакет может быть повторен. Параметр: ph_margin_fuzz.
ph_margin_time	Допустимый диапазон случайных изменений времени отправки IP-пакетов. Параметр: ph_margin_time.
Метрика маршрута одного соединения	Числовое значение, которое определяет предпочтительный маршрут для передачи данных. Параметр: route_metric.
<b>Флажки</b>	
Сверять DN	Способ аутентификации сервера. Если установлен переключатель «Вручную» - DN (Distinguished Name) сервера указывается в поле ввода. Если установлен переключатель «Из сертификата» - DN формируется из сертификата открытого ключа VPN-клиента. Сертификат открытого ключа VPN-клиента выбирается из раскрывающегося списка. Параметры: check_dn и remote_id.
Защита от компрометации	Параметр для включения функционала «perfect forward secrecy» для защиты от компрометации всех сессионных ключей при компрометации одного. Параметр: pfs_mode_force.

Параметр	Описание
Строгая политика CRL	Уровень строгости проверки отзыва пользовательских сертификатов. Параметр: strictcrlpolicy. Если установлен флажок – в разделе «Обновление CRL» может быть выполнена проверка наличия сертификата в списке отзыва сертификатов (crl). Путь к списку отзыва сертификатов указан в таблице «Основные параметры» столбец «URI». Если флажок не установлен - проверка не выполняется.
UDP инкапсуляция ESP	Включение UDP инкапсуляции ESP пакета. Параметр: udp_encap.
Фрагментирование IKE	Включение функции фрагментации пакетов. Параметр: fragmentation.
Автозапуск	Автоматическое подключение ранее установленных соединений после перезапуска DiSec-LV2. Параметр: start_action.

- 4) После завершения ввода параметров VPN-туннеля (например, как показано на рисунке 4.32) нажать кнопку  «Сохранить» или кнопку  для отмены (при необходимости) установленных параметров VPN-туннеля.

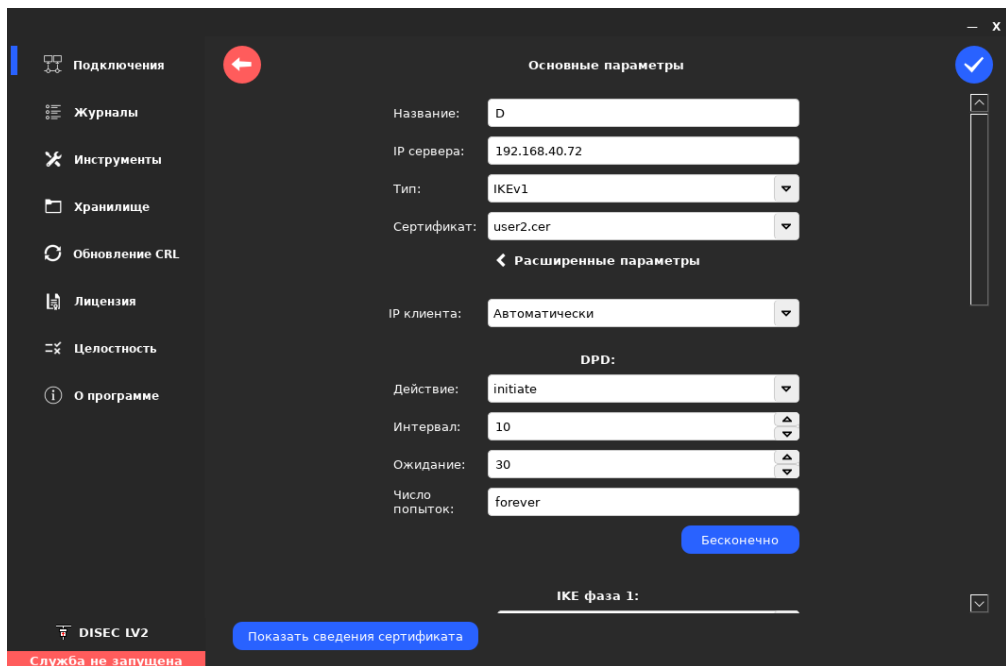



Рисунок 4.32

После нажатия кнопки  в таблице соединений рабочей области раздела «Подключения» появится запись о созданном VPN-туннеле (например, как показано на рисунке 4.33).

Статус службы DiSec-LV2 изменится на «Служба запущена», если была выполнена конфигурация первого VPN-туннеля.

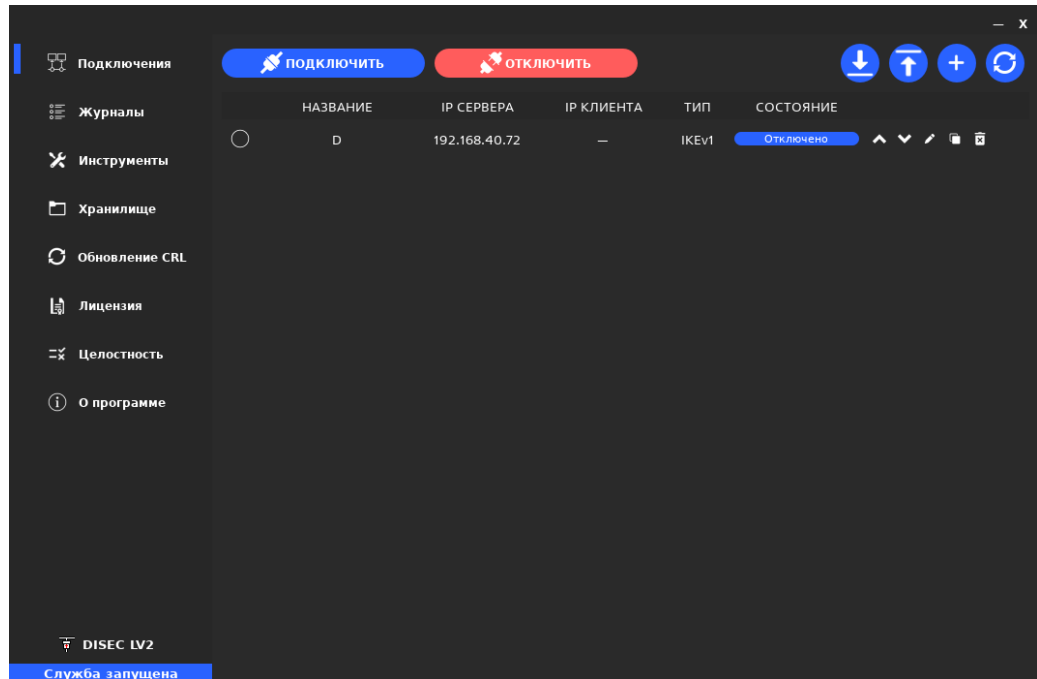



Рисунок 4.33

4.3.7.5. Создание VPN-туннеля путем копирования параметров действующего VPN-туннеля выполняется в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.).
- 2) В рабочей области раздела «Подключения» (например, как показано на рисунке 4.34) в таблице соединений нажать кнопку  справа от выбранного VPN-туннеля.

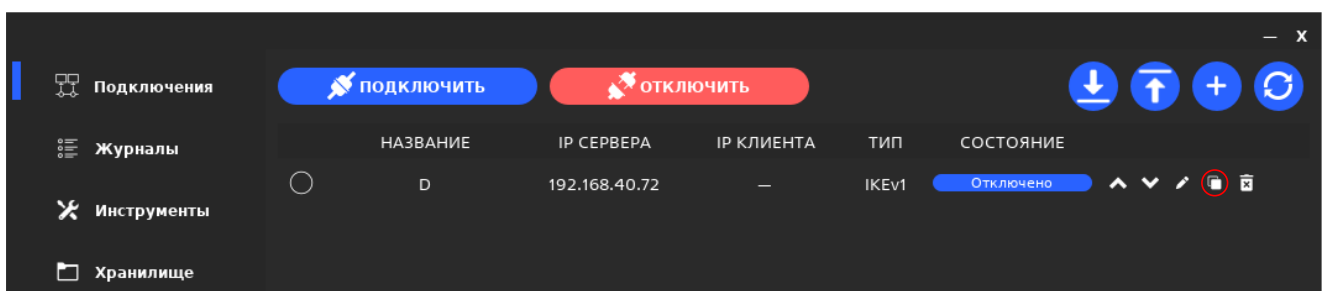





Рисунок 4.34

- 3) В области параметров раздела «Подключения» (см. рисунок 4.32) внести изменения в параметры VPN-туннеля (название VPN-туннеля, IP-адрес VPN-сервера и другие параметры при необходимости). Описание параметров VPN-туннеля приведено в таблице 1.

4) Нажать кнопку  «Сохранить» (например, как показано на рисунке 4.32) для сохранения параметров VPN-туннеля или нажать кнопку  «Отменить» для отмены сохранения параметров VPN-туннеля.

4.3.7.6. Для сохранения параметров созданных VPN-туннелей в файле конфигурации в рабочей области раздела «Подключения» (см. рисунок 4.33) нажать кнопку  и в открывшемся окне (например, как показано на рисунке 4.35) ввести путь сохранения файла конфигурации (disec.xml) и нажать кнопку «Открыть».

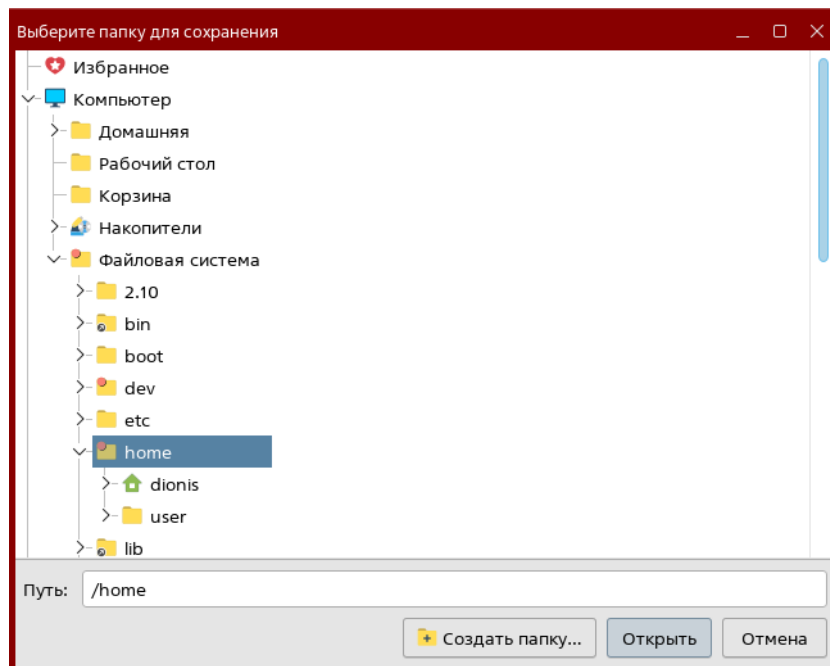



Рисунок 4.35

#### 4.3.8. Редактирование параметров VPN-туннеля

4.3.8.1. Редактирование параметров VPN-туннеля выполняется в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.).
- 2) В рабочей области раздела «Подключения» (например, как показано на рисунке 4.36) в таблице соединений нажать кнопку  справа от требуемого соединения.

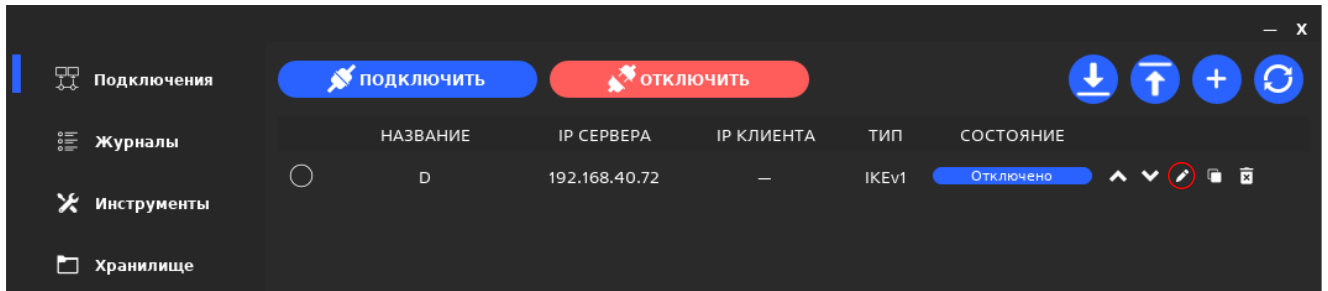





Рисунок 4.36

3) В области параметров раздела «Подключения» (см. рисунок 4.32) выполнить редактирование параметров выбранного VPN-туннеля. Описание параметров VPN-туннеля приведено в таблице 1.

4) Нажать кнопку  «Сохранить» для сохранения параметров VPN-туннеля или кнопку  «Отменить» для выхода без сохранения изменений параметров VPN-туннеля.

#### 4.3.9. Удаление VPN-туннеля

4.3.9.1. Удаление VPN-туннеля выполняется в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.).
- 2) В рабочей области раздела «Подключения» (например, как показано на рисунке 4.37) в таблице соединений нажать кнопку  справа от выбранного соединения.

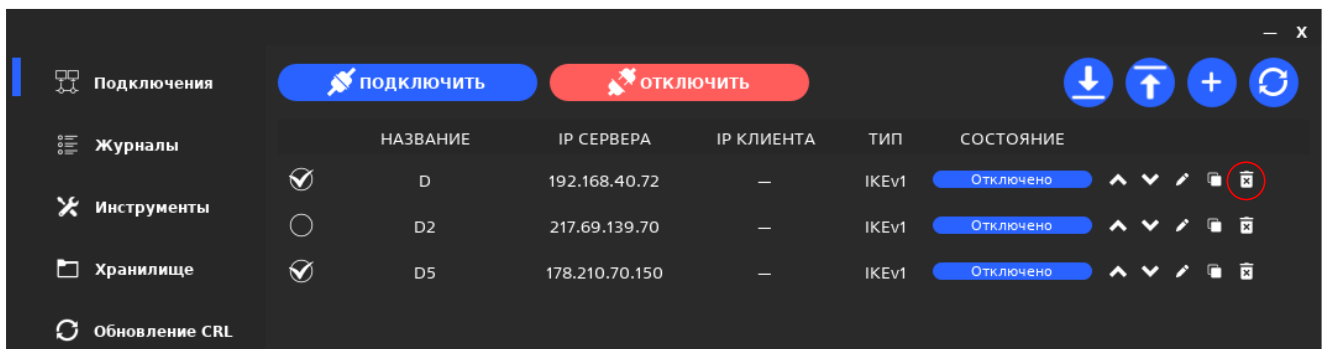


Рисунок 4.37

3) В открывшемся окне (например, как показано на рисунке 4.38) нажать кнопку «Да».

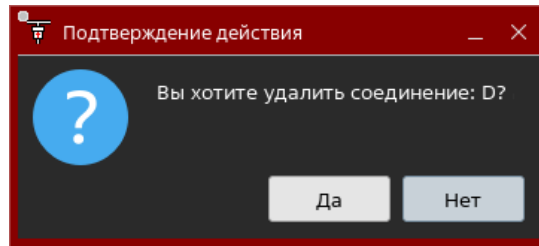


Рисунок 4.38

#### 4.3.10. Подключение VPN-туннеля (туннелей)

4.3.10.1. Подключение VPN-туннеля выполняется в следующей последовательности:

1) Установить USB-флеш-накопитель или USB-Рутокен с закрытым ключом VPN-клиента (например, user2.p15) в порт USB вычислительного средства.

**Примечание.** Файл с закрытым ключом должен находиться в файловой системе накопителя на уровне не выше третьего (начиная с 1) уровня вложенности.

2) Подключить (монтировать) USB-флеш-накопитель.

**Примечание.** Монтировать USB-Рутокен не требуется.

3) Выполнить запуск DiSec-LV2 от имени администратора или пользователя (см. подраздел 4.3.1.).

4) В рабочей области раздела «Подключения» (например, как показано на рисунке 4.39) в таблице соединений выполнить одно из следующих действий:

- нажать кнопку «Отключено» в графе «СОСТОЯНИЕ» таблицы соединений подключаемого VPN-туннеля;
- в таблице соединений установить флажки  слева от подключаемых VPN-туннелей и нажать кнопку «Подключить» над таблицей соединений.

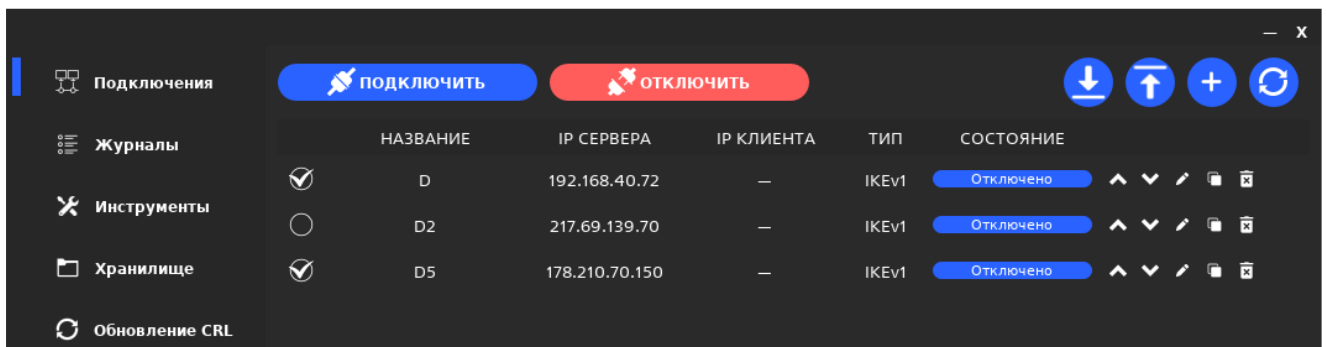


Рисунок 4.39

Если в результате выполненных действий будут подключены VPN-туннели, то их состояние в таблице соединений изменится на «Подключено» (например, как показано на рисунке 4.40).

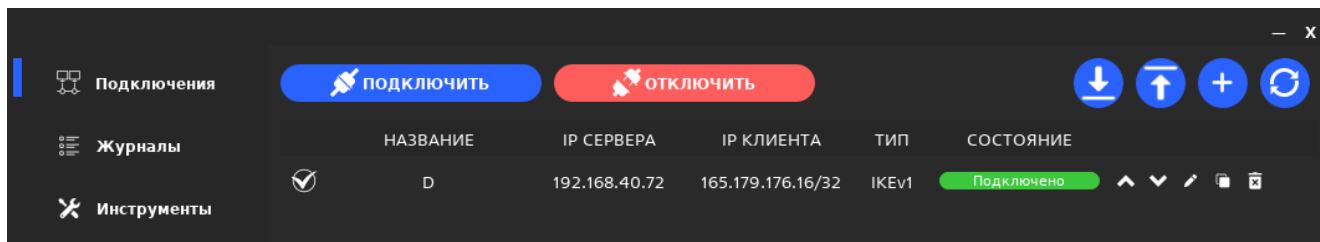


Рисунок 4.40

Если статус подключаемого VPN-туннеля не изменится на «Подключено», то следует провести анализ информации в Журнале службы (раздел меню «Журналы»), проверить параметры VPN-туннеля и при необходимости связаться с администратором VPN-сервера. После устранения причины, по которой подключение не было выполнено, повторить попытку установления соединения.

#### 4.3.11. Подключение VPN-туннеля при запуске DiSec-LV2

4.3.11.1. Автоматическое подключение ранее установленного VPN-туннеля при перезапуске DiSec LV2 выполняется в следующей последовательности:

- 1) Установить флажок «Автозапуск» в области расширенных параметров VPN-туннеля (см. раздел 4.3.7).
- 2) Выполнить подключение VPN-туннеля (см. раздел 4.3.10).
- 3) Завершить работу DiSec LV2 (см. раздел 4.3.2).
- 4) Выполнить запуск DiSec LV2 (см. раздел 4.3.1). После запуска DiSec LV2 ранее установленные VPN-туннели будут подключены автоматически.

#### 4.3.12. Отключение VPN-туннеля

4.3.12.1. В рабочей области раздела «Подключения» (например, как показано на рисунке 4.40) в таблице соединений выполнить одно из следующих действий:

- в таблице соединений в строке отключаемого VPN-туннеля в графе «СОСТОЯНИЕ» нажать кнопку «Подключено»;
- в таблице соединений установить флажки  слева от отключаемых VPN-туннелей и нажать кнопку «Отключить» над таблицей соединений.

После выполнения указанных действий состояние VPN-туннеля в таблице соединений изменится на «Отключено» (например, как показано на рисунке 4.41).

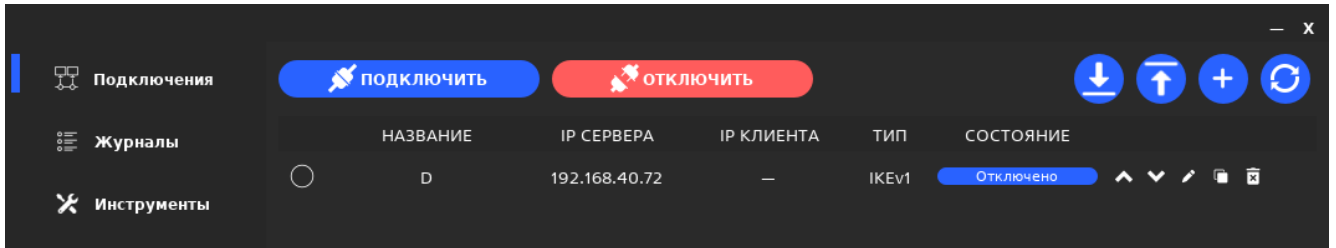


Рисунок 4.41

### 4.3.13. Настройка параметров DiSec-LV2

4.3.13.1. Настройка параметров DiSec-LV2 выполняется в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.).
- 2) В области меню главного окна DiSec-LV2 (см. рисунок 4.14) выбрать раздел «Инструменты».
- 3) В рабочей области раздела «Инструменты» (см. рисунок 4.42) выбрать вкладку «Настройки».

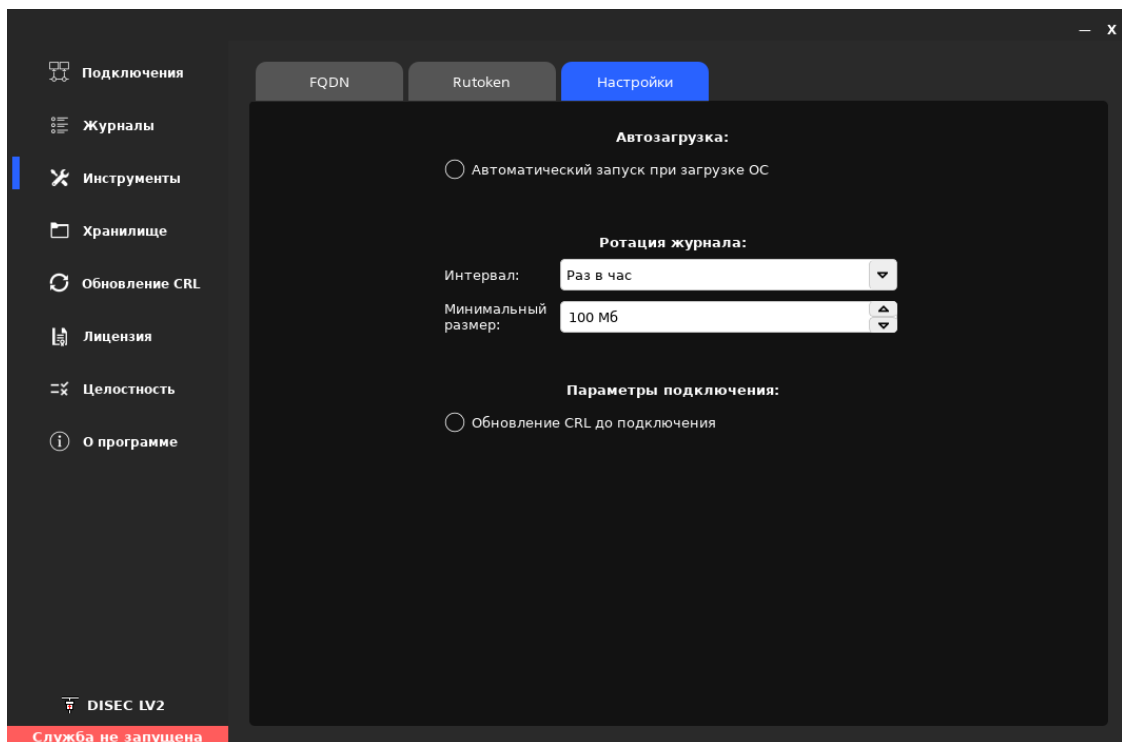



Рисунок 4.42

- 4) Установить (при необходимости) флажок «Автоматический запуск при загрузке ОС. В этом случае запуск DiSec-LV2 будет выполняться автоматически при загрузке ОС от имени пользователя (оператора).
- 5) Выбрать (при необходимости) в раскрывающемся списке «Интервал:» промежуток времени, через который выполняется ротация журнала службы DiSec-LV2. По умолчанию установлено значение «1 час».
- 6) Установить (при необходимости) в счетчике «Минимальный размер:» объем журнала службы DiSec-LV2. По умолчанию установлено значение «10 Мб».
- 7) Установить (при необходимости) флажок «Обновление CRL до подключения». В этом случае выполняется обновление списка отзыва сертификатов (crl) до установления соединения.
- 8) Для сохранения установленных параметров нажать кнопку  и в открывшемся окне (см. рисунок 4.43) нажать кнопку «ОК».

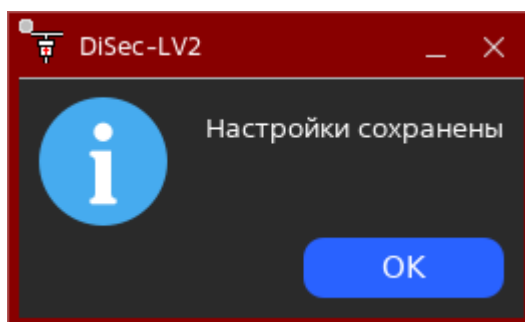


Рисунок 4.43

#### 4.3.14. Работа с USB-Рутокен

4.3.14.1. Просмотр характеристик, используемых USB-Рутокен и списка файлов, записанных на USB-Рутокен, выполняется в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.).
- 2) В области меню главного окна DiSec-LV2 (см. рисунок 4.14) выбрать раздел «Инструменты».
- 3) В рабочей области раздела «Инструменты» (см. рисунок 4.44) выбрать вкладку «Rutoken».

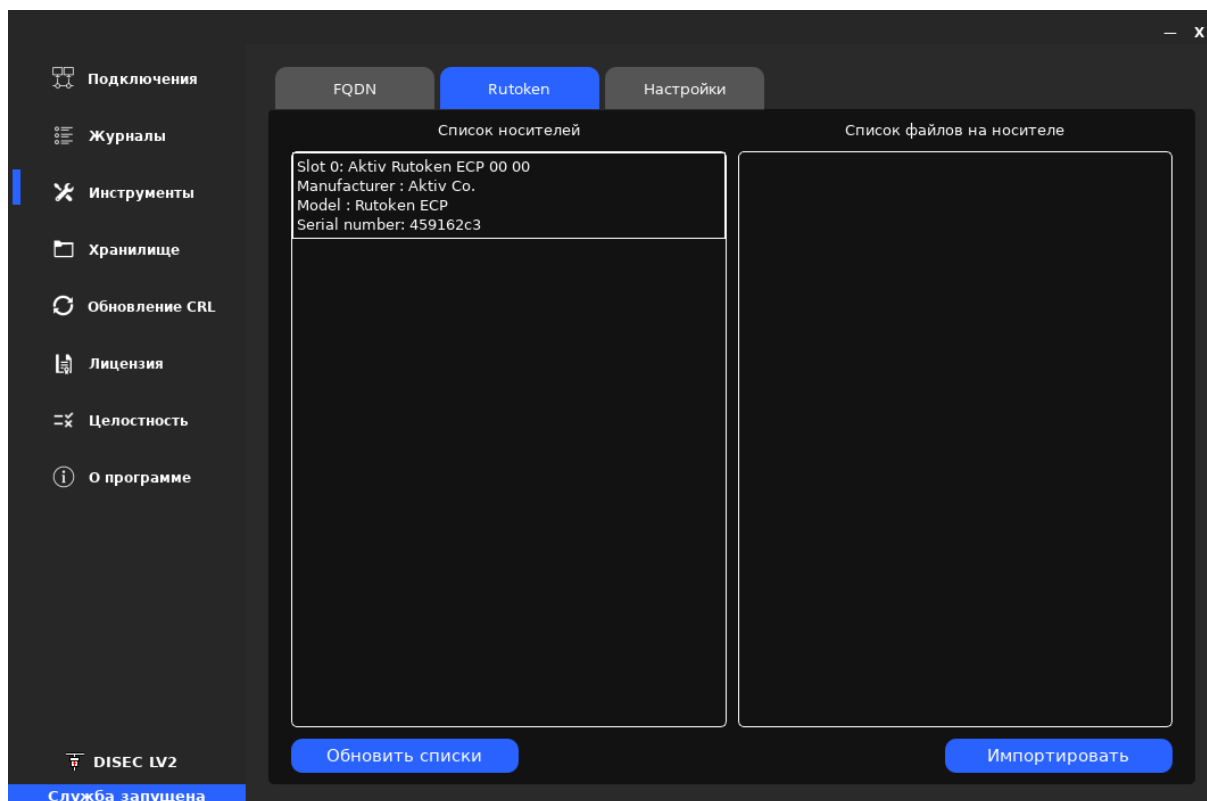


Рисунок 4.44


- 4) Нажать кнопку «Обновить списки». В области «Список носителей» отобразятся характеристики все используемых USB-Рутокен. При выборе требуемого USB-Рутокен из списка носителей в области «Список файлов на носителе» отобразятся файлы, записанные на данном USB-Рутокен.



4.3.14.2. Запись файлов на USB-Рутокен выполняется в следующей последовательности:

- 1) Выбрать требуемый USB-Рутокен в области «Список носителей».
- 2) Нажать кнопку «Импортировать».

#### 4.3.15. Обновление списка отзыва сертификатов

4.3.15.1. Обновление списка отзыва сертификатов выполняется в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.).
- 2) В области меню главного окна DiSec-LV2 (см. рисунок 4.14) выбрать раздел «Подключения».
- 3) В рабочей области раздела «Подключения» выбрать требуемое подключение и нажать кнопку .

- 4) В виджете «Основные параметры» установить флажок «Строгая политика CRL» и нажать кнопку  «Сохранить».
- 5) В области меню главного окна DiSec-LV2 (см. рисунок 4.14) выбрать раздел «Обновление CRL».
- 6) В рабочей области раздела «Обновление CRL» (например, как показано на рисунке 4.44а) нажать кнопку  .

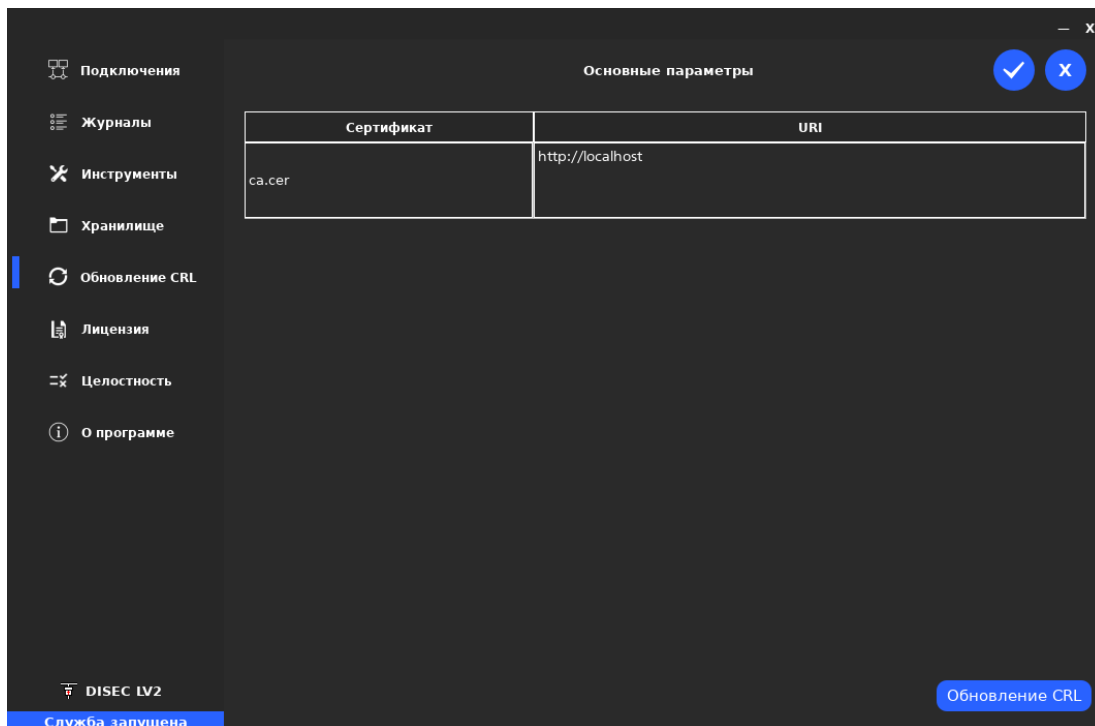




Рисунок 44а

После нажатия кнопки «Обновление CRL» будет выполнено обновление действующих списков отзыва сертификатов на списки отзыва сертификатов, находящихся на ресурсе, указанном в графе «URI» таблицы «Основные параметры».

**Примечание.** Информация в таблицу «Основные параметры» записывается автоматически из секции `crl_uris` файла конфигурации.

- 7) Нажать кнопку  «Сохранить» для сохранения выполненного обновления списков отзыва сертификатов или кнопку  «Отменить» для отмены обновления.

#### **4.4. Регистрация действий администратора\пользователя и протоколирование**

4.4.1. В процессе работы DiSec-LV2 в Журнале приложения, регистрируется в хронологическом порядке следующая информация:

- запуск\останов приложения;
- статус лицензии на использование DiSec-LV2 при активации и запуске приложения;
- результаты проверки соответствия контрольных сумм при запуске и в процессе работы приложения;
- статус службы при запуске;
- статус приложения при запуске;
- информация о соединении: удачные\неудачные попытки установления соединения, причины неудачных попыток установления соединения;
- информация о добавлении сертификатов.

Журнал приложения, сохраняется в файле `disec-lv2-ui.log` в каталоге `/var/log/disec-lv2`.

Объем файла `disec-lv2-ui.log` составляет 20 Мб.

При заполнении файла Журнала приложения, выполняется его архивация, открывается новый файл `disec-lv2-ui.log`, в который продолжает записываться в хронологическом порядке информация о работе приложения.

4.4.2. В процессе работы DiSec-LV2 в Журнале службы (`disec-lv2`), регистрируется в хронологическом порядке следующая информация:

- сообщения о событиях, происходящих в службе `disec-lv2`;
- сообщения, касающиеся IKE-протокола;
- сообщения, касающиеся ESP-протокола;
- сообщения, касающиеся конфигурации службы;
- сообщения, касающиеся сетевых интерфейсов;
- сообщения, касающиеся библиотечных вызовов;
- сообщения, касающиеся утилит службы.

Журнал службы, сохраняется в файле `disec-lv2.log` в каталоге `/var/log/disec-lv2`.

Объем файла `disec-lv2.log` составляет 20 Мб.

При заполнении файла Журнала службы, выполняется его архивация, открывается новый файл `disec-lv2.log`, в который продолжает записываться в хронологическом порядке информация о работе службы `disec-lv2`.

4.4.3. Настройка уровня детализации сообщений в Журнале приложения и Журнале службы (далее по тексту – журналы) выполняется в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 от имени администратора (см. подраздел 4.3.1.).
- 2) В области меню главного окна DiSec-LV2 выбрать раздел «Журналы» (например, как показано на рисунке 4.45).

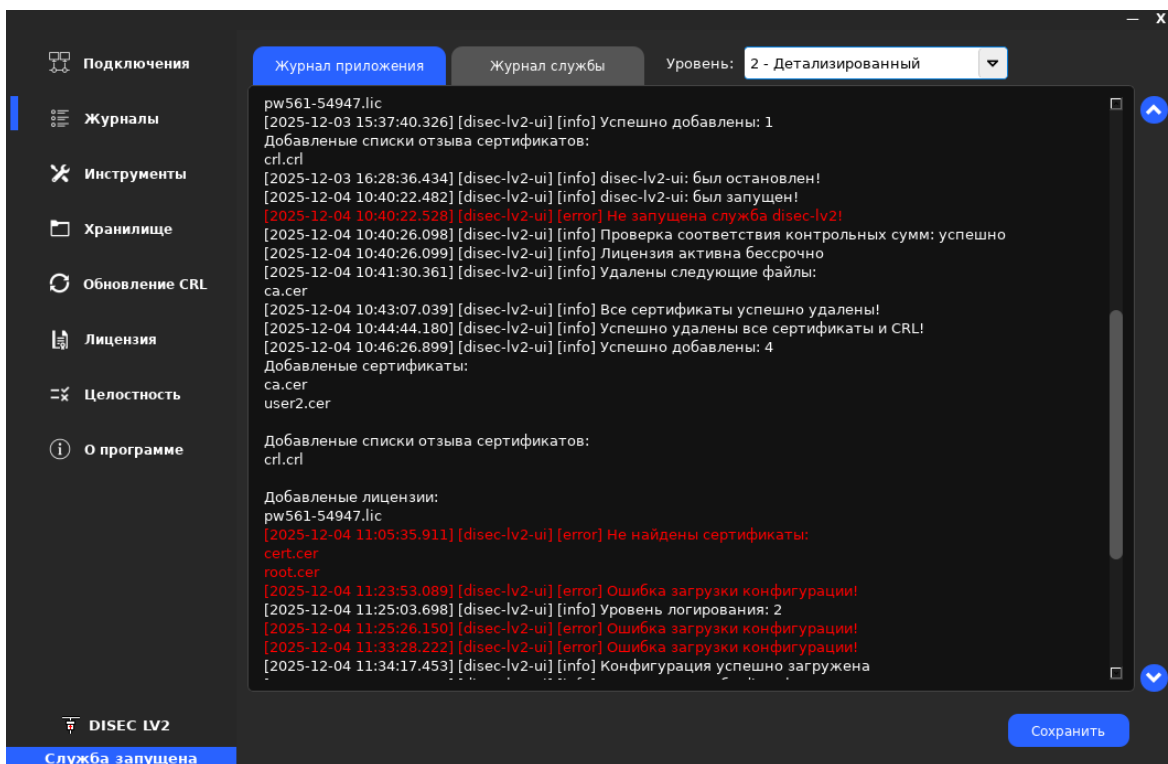


Рисунок 4.45

- 3) В выпадающем меню «Уровень:» выбрать уровень детализации информации, регистрируемой в журналах:
  - 0 – Минимальный;
  - 1 - Стандартный;
  - 2 - Детализированный;

– 3 - Сырые данные.

4.4.4. Просмотр журналов и поиск в них требуемой информации выполняется в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 от имени администратора или пользователя (см. подраздел 4.3.1.).
- 2) В области меню главного окна DiSec-LV2 (см. рисунок 4.45) выбрать раздел «Журналы».
- 3) Выбрать вкладку «Журнал приложения» или «Журнал службы».
- 4) Для просмотра выбранного журнала используется полоса прокрутки справа от его содержимого (см. рисунок 4.45).
- 5) Для сохранения выбранного журнала в файле следует нажать кнопку «Сохранить» и в открывшемся окне (например, как показано на рисунке 4.46) ввести путь для сохранения файла и нажать кнопку «Сохранить».

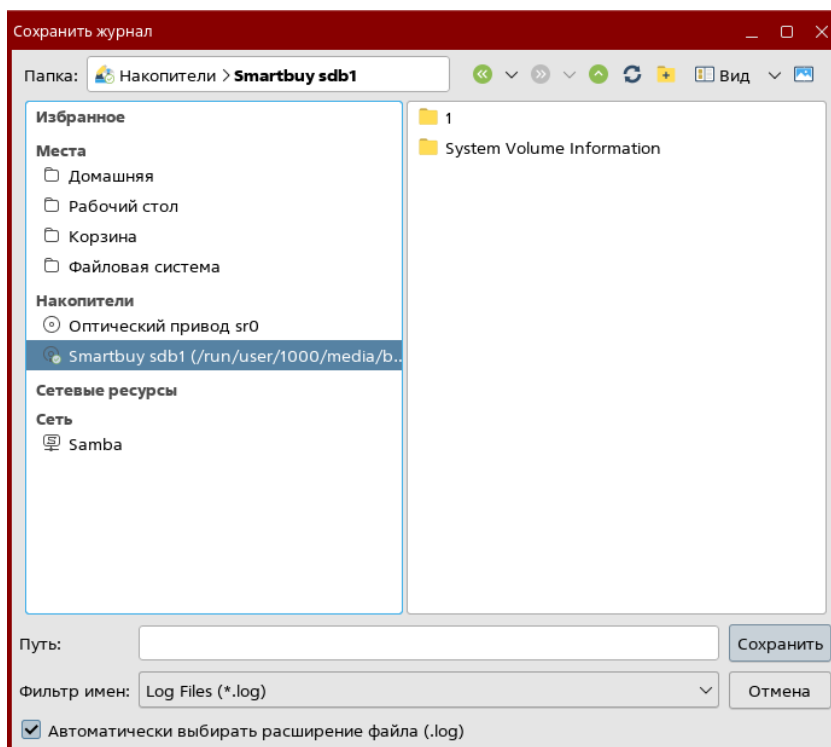


Рисунок 4.46

## 5. СЛУЖБА DISEC-LV2

### 5.1. Установка службы DiSec-LV2

5.1.1. Установка службы DiSec-LV2 в среде ОС Astra Linux SE 1.7 выполняется от имени суперпользователя (root) в следующей последовательности:

- 1) Выполнить запуск ОС.
- 2) Выполнить проверку наличия, ранее установленной службы DiSec-LV2.

При наличии ранее установленной службы DiSec-LV2 – следует выполнить её удаление (см. подраздел 5.2.).

- 3) Выполнить запуск эмулятора терминала Terminal Fly.
- 4) Вставить USB-флеш-накопитель с дистрибутивом DiSec-LV2 в порт USB или компакт-диск с дистрибутивом DiSec-LV2 в оптический накопитель вычислительного средства (ВС).

**Примечание.** Дистрибутив RU.НКБГ.70021 93 01.

- 5) Подключить (монтировать) USB-флеш-накопитель или компакт-диск с дистрибутивом DiSec-LV2.
- 6) Выполнить установку DiSec-LV2.

*Пример - sudo dpkg -i disec-lv2-cli-<номер\_версии>.deb*

Процесс установки DiSec-LV2 сопровождается выводом информационных сообщений на экран монитора ВС, например, как показано на рисунке 5.1.

```
dionis@arm-gk:/media$ sudo dpkg -i disec-lv2-cli-2667.deb
Выбор ранее не выбранного пакета disec-lv2-client.
(Чтение базы данных ... на данный момент установлено 295711 файлов и каталогов.)
Подготовка к распаковке disec-lv2-cli-2667.deb ...
Распаковывается disec-lv2-client (1.3.14-2667) ...
Настраивается пакет disec-lv2-client (1.3.14-2667) ...
Обрабатываются триггеры для xserver-xorg-core (2:21.1.7-1ubuntu4,astra.se48) ...
update exec ids due to /usr/bin changed
dionis@arm-gk:/media$
```

Рисунок 5.1

- 7) Отмонтировать USB-флеш-накопитель или компакт-диск с дистрибутивом DiSec-LV2.
- 8) Извлечь USB-флеш-накопитель из USB-порта или компакт-диск из оптического накопителя вычислительного средства.

5.1.2. Перед установкой DiSec-LV2 в среде РЕД ОС 8 «Рабочая станция» необходимо выполнить следующие действия от имени суперпользователя (root):

1) Установить пакет `openresolv`.

**Пример** - `sudo dnf install openresolv -y`

2) Установить права на файл `/usr/sbin/resolvconf.openresolv`.

**Пример** - `sudo chmod +x /usr/sbin/resolvconf.openresolv`

## 5.2. Удаление DiSec-LV2

5.2.1. Удаление DiSec-LV2 выполняется командой:

`sudo dpkg --purge disec-lv2-client`

## 5.3. Выполнение DiSec-LV2

### 5.3.1. Утилиты

5.3.1.1. Для управления работой DiSec-LV2 (создание и удаление VPN-туннелей, редактирование параметров VPN-туннелей, подключение и отключение VPN-туннелей) применяются следующие утилиты:

- `disec_ID`;
- `disec_config`;
- `disec_starter`;
- `disec_status`.

Параметры утилит приведены в приложении 2.

### 5.3.2. Запуск DiSec-LV2

5.3.2.1. Запуск DiSec-LV2 выполняется от имени суперпользователя (`root`) в следующей последовательности:

- 1) Выполнить запуск ОС.
- 2) Выполнить запуск эмулятора терминала Terminal Fly.
- 3) Выполнить запуск DiSec-LV2 по команде: `sudo disec_config --disec --start`.

#### **Пример**

```
dionis@arm-gk:~$ sudo disec_config --disec --start
disec_config 14:59:38 Info: Starting disec-lv2
disec_config 14:59:41 Info: disec-lv2 is ready to use
```

### 5.3.3. Завершение работы DiSec-LV2

5.3.3.1. Завершение работы DiSec-LV2 выполняется от имени суперпользователя (`root`) по команде: `sudo disec_config --disec --stop`.

**Пример**

```
dionis@arm-gk:~$ sudo disec_config --disec --stop
disec_config 11:08:57 Stopping disec-lv2 ... OK
disec_config 11:08:58 disec-lv2 stopped
```

**5.3.4. Контроль целостности**

5.3.4.1. Контроль целостности выполняется при запуске DiSec-LV2 и периодически в соответствии с внутренним регламентом эксплуатирующей организации.

5.3.4.2. Контроль целостности DiSec-LV2 выполняется в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 (см. подраздел 5.3.2.).
- 2) Выполнить команду проверки целостности DiSec-LV2:

*disec\_status --check-integrity* или *\$ disec\_status -i*.

**Пример**

```
dionis@arm-gk:/media$ disec_status -i
disec_status 13:40:24 Checking disec integrity ... OK
```

- 3) Выполнить команду расчета контрольной суммы DiSec-LV2:

*disec\_status --calculate-hashsum* или *\$ disec\_status -u*.

**Пример**

```
dionis@arm-gk:~$ disec_status -u
disec_status 14:53:30 Calculating hash ... OK
disec-lv2-1.0.0-2843 a799776d55f62f453f3e6e4322b9333a08fef64ddd390aac2cae78f2aa49c300
```

- 4) Выполнить сравнение контрольной суммы со значением в документе «СКЗИ «Клиент криптографического сервера доступа DiSec-LV2» Формуляр» RU.НКБГ.70021 30.

**5.3.5. Регистрация DiSec-LV2**

5.3.5.1. Регистрация DiSec LV2 выполняется при первом запуске от имени суперпользователя (root) в следующей последовательности:

- 1) Выполнить запуск DiSec-LV2 (см. подраздел 5.3.2.).
- 2) Определить ID аппаратной платформы ВС по команде:

*disec\_id --get-id* или *sudo disec\_id -g*

**Пример**

```
dionis@arm-gk:~$ disec_id --get-id
disec_id 14:55:47 Идентификатор платформы: PW561-54947
```

- 3) Сообщить идентификатор платформы в службу техподдержки ООО «Фактор-ТС» и получить файл с расширением lic, содержащий лицензию на использование DiSec-LV2.
- 4) Записать файл с лицензией на USB-флеш-накопитель.
- 5) Вставить USB-флеш-накопитель в порт USB BC.
- 6) Подключить (монтировать) USB-флеш-накопитель.
- 7) Активировать лицензию по команде от имени суперпользователя (root):

*sudo disec\_config --import <имя файла>.lic*

### Пример

```
dionis@arm-gk:/media$ sudo disec_config --import PW561-54947.lic
disec_config 15:10:01 Info: File PW561-54947.lic is ready to use in disec-lv2... OK
dionis@arm-gk:/media$ █
```

**Примечание.** Активация лицензии на использование DiSec-LV2 может быть выполнена совместно с установкой сертификата ГУЦ, сертификатов УЦ (при наличии) и списков отзыва сертификатов (см. п. 5.3.6.4.).

- 8) Выполнить проверку статуса лицензии по команде:

*disec\_id --license-status* или *sudo disec\_id -l*.

### Пример

```
dionis@arm-gk:~$ disec_id -l
disec_id 15:06:53 Checking current license ... OK
disec_id 15:06:53 License type ... unlimited
```

## 5.3.6. Импорт сертификатов и списков отзыва сертификатов

5.3.6.1. Импорт сертификата ГУЦ, сертификатов УЦ и списков отзыва сертификатов (CRL) выполняется по командам от имени суперпользователя (root).

5.3.6.2. Импорт сертификата ГУЦ (например, ca.cer), сертификатов УЦ (при наличии), сертификата открытого ключа VPN-клиента (например, user2.cer) и списка отзыва сертификатов (например, crl.crl), записанных на USB-флеш-накопителе выполняется по команде:

*sudo disec\_config --import <имя файла>*

### Пример

```
dionis@arm-gk:/media$ sudo disec_config --import ca.cer
disec_config 15:12:06 Info: Certificate ca.cer is valid
disec_config 15:12:06 Info: File ca.cer is ready to use in disec-lv2 ... OK
```

5.3.6.3. Импорт сертификата ГУЦ (например, ca.cer), сертификатов УЦ (при наличии), сертификата открытого ключа VPN-клиента (например, user2.cer) и списка отзыва сертификатов (например, crl.crl), записанных на USB-Рутокен выполняется по команде:

***sudo disec\_config --rtk --import --s <номер слота> <имя файла>.***

***Пример***

```
dionis@arm-gk:~$ sudo disec_config --rtk --import --s 0 ca.cer
disec_config 11:49:45 Info: File ca.cer is ready to use in disec-lv2 ... OK
dionis@arm-gk:~$ sudo disec_config --rtk --import --s 0 user2.cer
disec_config 11:50:36 Info: File user2.cer is ready to use in disec-lv2 ... OK
dionis@arm-gk:~$ sudo disec_config --rtk --import --s 0 crl.crl
disec_config 11:50:57 Info: File crl.crl is ready to use in disec-lv2 ... OK
```

5.3.6.4. Импорт всех сертификатов и списков отзыва сертификатов, записанных на USB-флеш-накопителе, выполняется по команде:

***sudo disec\_config --import-all /<путь>.***

***Пример***

```
dionis@arm-gk:~$ sudo disec_config --import-all /media
disec_config 14:57:51 Info: Certificate user2.cer is valid
disec_config 14:57:51 Info: File user2.cer is ready to use in disec-lv2 ... OK
disec_config 14:57:51 Info: Certificate ca.cer is valid
disec_config 14:57:51 Info: File ca.cer is ready to use in disec-lv2 ... OK
disec_config 14:57:51 Info: File crl.crl is ready to use in disec-lv2 ... OK
disec_config 14:57:51 Info: Valid license: S7977-87F78-687A8 ... OK
disec_config 14:57:51 Info: File pw561-54947.lic is ready to use in disec-lv2... OK
```

**Примечание.** По этой команде, кроме применения сертификатов и списка отзыва сертификатов, выполняется активация лицензии на использование DiSec-LV2.

5.3.6.5. Просмотр сведений об установленных сертификатах выполняется по команде: ***sudo disec\_config --list --certs.***

5.3.6.6. Просмотр сведений о списках отзыва сертификатов выполняется по команде: ***sudo disec\_config --list --crls.***

5.3.6.7. Просмотр сведений об установленных сертификатах и списках отзыва сертификатов может быть выполнен по команде: ***sudo disec\_config --list --all.***

**Пример**

```
dionis@arm-gk:/media$ sudo disec_config --list --certs
disec_config 11:42:39 Listing certificates:
disec_config 11:42:39 - ca.cer
disec_config 11:42:39 - user2.cer
dionis@arm-gk:/media$ sudo disec_config --list --crls
disec_config 11:43:22 Listing crls:
disec_config 11:43:22 - crl.crl
dionis@arm-gk:/media$ sudo disec_config --list --all
disec_config 11:43:52 Listing certificates:
disec_config 11:43:52 - ca.cer
disec_config 11:43:52 - user2.cer
disec_config 11:43:52 Listing crls:
disec_config 11:43:52 - crl.crl
```

**5.3.7. Удаление сертификатов и списка отзыва сертификатов**

5.3.7.1. Удаление сертификатов и списков отзыва сертификатов выполняется по команде от имени суперпользователя (root):

```
sudo disec_config --delete <имя файла>
```

**Пример**

```
dionis@arm-gk:~$ sudo disec_config --delete user2.cer
disec_config 13:30:20 Info: Deleting user2.cer: ... OK
disec_config 13:30:20 Info: Deleting user2.hash: ... OK
```

5.3.7.2. Удаление всех списков отзыва сертификатов выполняется по команде:

```
sudo disec_config --delete --crls
```

5.3.7.3. Удаление всех сертификатов выполняется по команде:

```
sudo disec_config --delete --certs
```

5.3.7.4. Удаление всех сертификатов и списков отзыва сертификатов выполняется по команде:

```
sudo disec_config --delete --all
```

**Пример**

```
dionis@arm-gk:~$ sudo disec_config --delete --all
disec_config 13:26:49 Info: All certs are successfully deleted
disec_config 13:26:49 Info: All crls are successfully deleted
```

**5.3.8. Создание VPN-туннеля**

5.3.8.1. Создание VPN-туннеля (туннелей) выполняется в следующей последовательности:

- 1) Создать шаблон файла конфигурации (disec\_example.xml) по команде от имени суперпользователя root:

*sudo disec\_config --create-example /<путь>.*

- 2) Выполнить редактирование шаблона файла конфигурации (disec\_example.xml) в любом редакторе XML. Файл конфигурации состоит из одной или нескольких секций, каждая из которых содержит параметры отдельного VPN-туннеля. Пример файла конфигурации и описание параметров VPN-туннеля приведены в приложении 1.

- 3) Сохранить файл disec\_example.xml под именем disec.xml.

- 4) Выполнить конвертирование файла конфигурации во внутренний формат DiSec-LV2 по команде от имени суперпользователя root:

*sudo disec\_config --prepare /<путь>.*

### Пример

```
dionis@arm-gk:/media$ sudo disec_config --prepare /media/1/disec.xml
disec_config 15:22:52 Info: Stopping disec-lv2 ... OK
disec_config 15:22:53 Info: disec-lv2 stopped
disec_config 15:22:53 Info: Certificate user2.cer is valid
disec_config 15:22:53 Info: File user2.cer is ready to use in disec-lv2 ... OK
disec_config 15:22:53 Info: Adding connection "D" ... OK
disec_config 15:22:53 Info: Certificate ca.cer is valid
disec_config 15:22:53 Info: File ca.cer is ready to use in disec-lv2 ... OK
disec_config 15:22:53 Info: Analysing XML for PKI policy
disec_config 15:22:53 Info: Chain is built and valid for user2.cer
disec_config 15:22:53 Info: Added CRL policy with name ca ... OK
disec_config 15:22:53 Info: PKI policy is correct
disec_config 15:22:53 Info: File swanctl.conf is ready to use in disec-lv2 ... OK
disec_config 15:22:54 Info: Starting disec-lv2 ... OK
disec_config 15:22:56 Info: disec-lv2 is ready to use
dionis@arm-gk:/media$
```

При наличии синтаксических ошибок в файле конфигурации в создании VPN-туннеля будет отказано (например, как показано на рисунке 5.2). В этом случае следует устранить ошибки в файле конфигурации и повторить действия по его конвертированию.

```
dionis@arm-gk:~$ sudo disec_config --prepare /media/disec.xml
disec_config 15:13:08 Info: Certificate user2.cer is valid
disec_config 15:13:08 Info: File user2.cer is ready to use in disec-lv2 ... OK
disec_config 15:13:08 Error: In 1st connection section:
disec_config 15:13:08 Error: Field "start_action" is missing
disec_config 15:13:09 Error: Invalid XML config format
disec_config 15:13:09 Info: Parsing XML config status: ... FAIL
```

Рисунок 5.2

- 5) Выполнить проверку установленной конфигурации VPN-туннеля по команде: **disec\_status --configuration -c <название VPN-туннеля>**, или всех VPN-туннелей по команде: **disec\_status --configuration -c all**.

### Пример

```
dionis@arm-gk:~$ disec_status --configuration -c D
disec_status 15:28:47 Checking service status      ... OK
disec_status 15:28:47 Get configuration           ... OK
-----
Parameter      Value
-----
connection     D
version        IKEv1
reauthentication 3400
remote         192.168.40.72
id:
  CN            user2
  serialNumber
  ST
  L
  street
  O
  OU
  C             RU
child SA:
  mode          TUNNEL
  rekeying      1000
-----
```

## 5.3.9. Редактирование параметров VPN-туннеля

5.3.9.1. Редактирование параметров VPN-туннеля (туннелей) выполняется в следующей последовательности:

- 1) Выполнить редактирование параметров VPN-туннеля (туннелей) в файле конфигурации (disec.xml).
- 2) Выполнить конвертирование файла конфигурации во внутренний формат DiSec-LV2 по команде от имени суперпользователя root:

***sudo disec\_config --prepare /<путь>***.

## 5.3.10. Создание нового VPN-туннеля

5.3.10.1. Создание нового VPN-туннеля выполняется в следующей последовательности:

- 1) В действующий файл конфигурации (disec.xml) включить секцию с параметрами нового VPN-туннеля.
- 2) Выполнить конвертирование файла конфигурации во внутренний формат DiSec-LV2 по команде от имени суперпользователя root:

***sudo disec\_config --prepare /<путь>***.

### 5.3.11. Удаление VPN-туннеля

5.3.11.1. Удаление VPN-туннеля (туннелей) выполняется в следующей последовательности:

- 1) В действующем файле конфигурации (disec.xml) удалить секцию (секции) с параметрами требуемого (требуемых) VPN-туннеля (туннелей).
- 2) Выполнить конвертирование файла конфигурации во внутренний формат DiSec-LV2 по команде от имени суперпользователя root:

```
sudo disec_config --prepare /<путь>.
```

### 5.3.12. Подключение\отключение VPN-туннеля

5.3.12.1. Подключение VPN-туннеля выполняется в следующей последовательности:

- 1) Вставить USB-флеш-накопитель или USB-Рутокен с закрытым ключом VPN-клиента (например, user2.p15) в порт USB вычислительного средства.

**Примечание.** Файл с закрытым ключом должен находиться в файловой системе накопителя на уровне не выше третьего (начиная с 1) уровня вложенности.

- 2) Подключить (монтировать) файловую систему USB-флеш-накопителя в каталог ОС, например, media.

**Примечание.** Монтировать USB-Рутокен не требуется.

- 3) Выполнить запуск эмулятора терминала Terminal Fly.
- 4) Подключить VPN-туннель по команде:

```
disec_starter -c <название vpn-туннеля> --enable.
```

**Пример**

```
dionis@arm-gk:~$ disec_starter -c D --enable
disec 15:31:35 Check service status      ... OK
disec 15:31:35 Check license             ... OK
disec 15:31:35 Load connection D        ... OK
disec 15:31:35 Is connection already enabled ... NO
disec 15:31:35 Check connection cacert  ... OK
disec 15:31:35 Check connection cert    ... OK
disec 15:31:35 Check connection cacert  ... OK
disec 15:31:35 Check connection cert    ... OK
disec 15:31:35 Establishing connection  ... OK
disec 15:31:37 Connection D              ... online
dionis@arm-gk:~$
```

5.3.12.2. Отключение VPN-туннеля выполняется по команде:

***disec\_starter -c <название vpn-туннеля> --disable.***

***Пример***

```
dionis@arm-gk:~$ disec_starter -c D --disable
disec 15:33:10 Check service status           ... OK
disec 15:33:10 Disable connection D         ... OK
dionis@arm-gk:~$
```

### 5.3.13. Подключение\отключение VPN-туннеля при запуске DiSec-LV2

5.3.13.1. Автоматическое подключение ранее установленного соединения при запуске DiSec-LV2 выполняется в следующей последовательности:

- 1) Подключить VPN-туннеля (туннели) (см. раздел 5.3.12).
- 2) Выполнить команду:

***sudo disec\_config --autostart --enable***

***Пример***

```
dionis@arm-gk:~$ sudo disec_config --autostart --enable
disec_config 10:53:19 Info: Enabling disec-lv2-autostart           ... OK
disec_config 10:53:21 Info: disec-lv2-autostart enabled
```

- 3) Завершить работу DiSec-LV2 (см. раздел 5.3.3).
- 4) Выполнить запуск DiSec-LV2 (см. раздел 5.3.2). После запуска DiSec-LV2 ранее подключенные VPN-туннели установятся автоматически.

5.3.13.2. Отключение автоматического подключения ранее установленных соединений при запуске DiSec-LV2 выполняется по команде:

***sudo disec\_config --autostart --disable***

***Пример***

```
dionis@arm-gk:~$ sudo disec_config --autostart --disable
disec_config 11:10:22 Info: Disabling disec-lv2-autostart           ... OK
disec_config 11:10:24 Info: disec-lv2-autostart disabled
```

### 5.3.14. Регистрация действий администратора\пользователя и протоколирование

5.3.14.1. В процессе работы DiSec-LV2 в Журнале службы (disec-lv2), регистрируется в хронологическом порядке следующая информация:

- сообщения о событиях, происходящих в службе disec-lv2;
- сообщения, касающиеся IKE-протокола;

- сообщения, касающиеся ESP-протокола;
- сообщения, касающиеся конфигурации службы;
- сообщения, касающиеся сетевых интерфейсов;
- сообщения, касающиеся библиотечных вызовов;
- сообщения, касающиеся утилит службы.

Журнал службы, сохраняется в файле `disec-lv2.log` в каталоге `/var/log/disec-lv2`.

Объем файла `disec-lv2.log` составляет 20 Мб.

При заполнении файла Журнала службы, выполняется его архивация, открывается новый файл `disec-lv2.log`, в который продолжает записываться в хронологическом порядке информация о работе службы.

5.3.14.2. Установка уровня детализации сообщений выполняется по команде от имени суперпользователя (root): ***sudo disec\_config --log-level <0-4>***.

#### *Пример*

```
dionis@arm-gk:~$ sudo disec_config --log-level 2
disec_config 11:12:39 Logging level set to 2
```

5.3.14.3. Просмотр текущего уровня детализации сообщений выполняется по команде от имени суперпользователя (root):

***sudo disec\_config --log-level --get*** или ***disec\_status --show-logging-level***.

#### *Пример*

```
dionis@arm-gk:~$ sudo disec_config --log-level --get
disec_config 11:14:05 Current logging level is 2
dionis@arm-gk:~$ disec_status --show_log_level
disec_status 11:15:28 Log level value ... 2
```

5.3.14.4. Для поиска в журнале требуемой информации используется любой текстовый редактор.

## 6. СООБЩЕНИЯ

6.1. В процессе функционирования DiSec-LV2 администратору выдаются:

- информационные сообщения;
- предупреждения;
- сообщения об ошибках.

6.2. Администратору следует принять к сведению информационные сообщения.

6.3. Администратору рекомендуется провести анализ предупреждений и сообщений об ошибках и устранить причины их появления. Перечень предупреждений и сообщений об ошибках и рекомендуемые действия по их устранению приведены в таблице 2.

Таблица 2

Сообщение	Описание	Действия по устранению
Утилита DISEC_CONFIG		
Warning: libtpkcs11ecp.so not found. No RuToken operations will be available!	Предупреждение: файл libtpkcs11ecp.so не найден. Операции с USB-Рутокен будут недоступны.	Необходимо установить пакет драйверов USB-Рутокен с сайта <a href="https://www.rutoken.ru">https://www.rutoken.ru</a> .
Warning: Unsupported file: %s	Неподдерживаемый файл	Проверить, правильно ли указано имя файла.
Warning: Argument is directory. Use --import-all instead!	Аргументом является каталог, а не файл. Используйте атрибут «--import-all» вместо него.	В команде после «--import-all» следует указать каталог, в котором находятся требуемые файлы.
Warning: Invalid format of licence file: %s"	Неверный формат файла лицензии.	Обратиться в службу поддержки DiSec-LV2 для замены файла лицензии.
Warning: Invalid format of crl file: %s	Неверный формат файла списка отзывает сертификатов.	Получить у Администратора безопасности или лица, уполномоченного по работе с ключевой информацией, файл списка отзыва сертификатов.
Warning: Invalid format of X509 file: %s	Неверный формат файла сертификата.	Получить у Администратора безопасности или лица, уполномоченного по работе с ключевой информацией, файл с сертификатом открытого ключа VPN-клиента.
Warning: Certificate %s is not yet valid	Сертификат пока не действителен.	Обратиться к Администратору безопасности или лицу, уполномоченному по работе с ключевой информацией.

Сообщение	Описание	Действия по устранению
Warning: Certificate %s has expired	Срок действия сертификата истек.	Обратиться к Администратору безопасности или лицу, уполномоченному по работе с ключевой информацией.
Warning: Certificate chain depth exceeded maximum limit!	Глубина цепочки сертификатов превысила максимально допустимый предел.	Файл с сертификатом должен находиться в файловой системе накопителя на уровне не выше третьего (начиная с 1) уровня вложенности.
Warning: Root certificate %s already exists under the name %s	Корневой сертификат уже существует в хранилище под этим именем.	-
Warning: Could not resolve IP for FQDN: %s. Maybe try later	Не удалось разрешить IP-адрес для полного доменного имени: %s. Возможно, стоит попробовать позже.	Проверить правильно ли указан IP-адрес. Повторить попытку.
Warning: Further XML parsing is impossible	Дальнейшая обработка файла конфигурации невозможна.	Проверить файл конфигурации, устранить ошибки, повторить попытку.
Warning: Invalid protocol in URL %s	Недопустимый протокол в поле URL	Устранить ошибку в названии протокола.
Warning: No more than 3 URIs allowed! Only first 3 will be saved	Допускается не более трех URI. Будут сохранены только первые 3 URI.	-
Warning: Line %s	Ошибка в указанной строке.	Устранить ошибку и повторить попытку.
Warning: Skipping unused authority %s	Пропуск неиспользуемых полномочий указанных в секции authority файла конфигурации.	-
Warning: In field <url_uri> should be only one URI, got: %s	В поле <url_uri> должен быть только один URI.	В поле <url_uri> удалить лишние URI и повторить попытку.
Warning: Invalid pincode!	Неверный пин-код устройства рутокен.	-
Warning: Maximum allowed attempts reached. Exiting application.	Достигнуто максимально допустимое количество попыток ввода пин-кода. Приложение закрыто.	-
Warning: No pincode entered for RuToken!	Для RuToken не введен пин-код.	Ввести пин-код.
Warning: Specify name of XML config. Example: -prepare <my_conf.xml>	Укажите имя XML-файла конфигурации.	В команде – prepare указать файл конфигурации.
Warning: Too many options	Указано слишком много опций	Сократить количество опций и повторить попытку.
Warning: At least one filename required	Требуется как минимум одно имя файла	Указать имя файла и повторить попытку.
Warning: Invalid license: %s	Лицензия недействительна	Обратиться в службу поддержки DiSec-LV2 для замены файла лицензии.
Error: Failed to open: <filename>	Не удалось открыть файл.	Обратиться в службу поддержки DiSec-LV2.

Сообщение	Описание	Действия по устранению
Error: Failed to read from: <filename>	Ошибка чтения из файла <filename>.	Возможно файл поврежден. Попробовать использовать другую копию файла. Обратиться в службу поддержки DiSec-LV2.
Error: Failed to write in: <filename>	Ошибка записи в файл <filename>.	Возможно указано недопустимое имя файла. Изменить имя файла и повторить попытку. Обратиться в службу поддержки DiSec-LV2.
Error: Failed to find: <filename>	Не найден файл <filename>.	Возможно указан неверный путь к файлу. Скорректировать путь и повторить попытку. Обратиться в службу поддержки DiSec-LV2.
Error: Failed to copy: <filename>	Ошибка копирования файла <filename>.	1) Возможно указан неверный путь к файлу. Скорректировать путь и повторить попытку. 2) Возможно нет свободного места на накопителе. Освободить место и повторить попытку. 3) Возможно недостаточно прав на выполнение операции копирования. Обратиться в службу поддержки DiSec-LV2.
Error: File <filename> is empty! Unable to get data	Файл <filename> пуст. Невозможно извлечь данные.	1) Заменить копию файла и повторить попытку. 2) Возможно указан не тот файл. Проверить введенное имя файла. Повторить попытку.
Error: Unable to open directory: %s	Невозможно открыть директорию (каталог).	Возможно ошибка в имени директории. Исправить ошибку и повторить попытку.
Error: Nothing found in %s	В директории %s ничего не найдено.	Возможно ошибка в имени директории. Исправить ошибку и повторить попытку.
Error: Cannot find issuer certificate for %s	Не удалось найти сертификат издателя для сертификата %s	Обратиться к Администратору безопасности или лицу, уполномоченному по работе с ключевой информацией.

Сообщение	Описание	Действия по устранению
Error: Invalid certificate: %s	Поврежден сертификат %s	Использовать копию сертификата (при наличии) или обратиться к Администратору безопасности или лицу, уполномоченному по работе с ключевой информацией.
Error: Cannot extract DN from certificate: %s	Не удалось извлечь DN (Distinguished Name) из сертификата: %s.	Обратиться к Администратору безопасности или лицу, уполномоченному по работе с ключевой информацией
Error: Malformed PKI policy in XML	Некорректная политика PKI в файле конфигурации.	Устранить ошибки в файле конфигурации и повторить попытку.
Error: Unable to find hash file! File %s is untrusted!	Не удалось найти файл с эталонной контрольной суммой. Файл %s не является доверенным.	Обратиться в службу поддержки DiSec-LV2.
Error: Hashes do not match! File %s is untrusted!	Контрольная сумма файла не совпадает с эталонной. Файл %s не заслуживает доверия.	Обратиться в службу поддержки DiSec-LV2.
Error: Empty ip field	Не задано значение в поле IP-адреса в файле конфигурации.	Указать IP-адрес в файле конфигурации.
Error: Invalid IP address: %s	Неверный IP-адрес в файле конфигурации.	Исправить IP-адрес в файле конфигурации.
Error: Invalid subnet value: %s	Недопустимое значение подсети в файле конфигурации.	Исправить значение подсети в файле конфигурации.
Error: Mask must have value in range 1 - 32	Значение маски подсети должно находиться в диапазоне от 1 до 32 в файле конфигурации.	Исправить значение маски подсети в файле конфигурации.
Error: Empty transforms field	Пустое поле transforms в файле конфигурации.	Указать криптопараметры для протокола IKE в файле конфигурации.
Error: Invalid format of transforms string	Неверный формат значения в поле transforms файла конфигурации.	Исправить значение в поле transforms файла конфигурации.
Error: Invalid encryption algorithm name: %s	Недопустимое имя алгоритма шифрования: %s.	Исправить имя алгоритма шифрования в файле конфигурации.
Error: Invalid integrity algorithm name: %s	Недопустимое имя алгоритма обеспечения целостности: %s.	Исправить имя алгоритма целостности в файле конфигурации.
Error: Invalid key exchange algorithm name: %s	Недопустимое имя алгоритма обмена ключами: %s.	Исправить имя алгоритма обмена ключами в файле конфигурации.
Error: Could not parse file: %s	Невозможно обработать файл конфигурации: %s	Проверить имя и содержимое файла конфигурации. Устранить ошибки в файле конфигурации.

Сообщение	Описание	Действия по устранению
Error: <dpd_action> field should contain only close, route, restart or initiate	Поле <dpd_action> в файле конфигурации должно содержать только значения: close, route, restart, initiate.	Установить в поле <dpd_action> одно из следующих значений: close, route, restart, initiate.
Error: <dpd_interval> value should be number	Поле <dpd_interval> файла конфигурации должно содержать только числовое значение.	Установить в поле <dpd_interval> числовое значение.
Error: <dpd_timeout> value should be number	Поле <dpd_timeout> должно содержать только числовое значение.	Установить в поле <dpd_timeout> числовое значение.
Error: <keying_tries> value should be forever or number	Поле <keying_tries> должно содержать только «forever» или номер.	Установить в поле <keying_tries> значение «forever» или номер.
Error: <pfs_mode_force> field should contain only yes or no	Поле <pfs_mode_force> должно содержать только значения «yes» или «no».	Установить в поле <pfs_mode_force> значение «yes» или «no».
Error: <fragmentation> field should contain only yes or no	Поле <fragmentation> должно содержать только значения «yes» или «no».	Установить в поле <fragmentation> значение «yes» или «no».
Error: <strictcrpolicy> field should contain only yes or no	Поле <strictcrpolicy> должно содержать только значения «yes» или «no».	Установить в поле <strictcrpolicy> значение «yes» или «no».
Error: <ph_margin_fuzz> value should be number	В поле <ph_margin_fuzz> должно быть число.	Установить в поле <ph_margin_fuzz> числовое значение.
Error: <ph_margin_time> value should be number	В поле <ph_margin_time> должно быть число.	Установить в поле <ph_margin_time> числовое значение.
Error: <ph1_life_time> value should be number	В поле <ph1_life_time> должно быть число.	Установить в поле <ph1_life_time> числовое значение.
Error: <ph2_life_time> value should be number	В поле <ph2_life_time> должно быть число.	Установить в поле <ph2_life_time> числовое значение.
Error: <udp_encap> field should contain only force or no	Поле <udp_encap> должно содержать только значения «force» или «no».	Установить в поле <udp_encap> значение «force» или «no».
Error: <route_metric> value should be number from 0 to 10000	Поле <route_metric> должно содержать числовые значения от 0 до 10000.	Установить в поле <route_metric> числовое значение в диапазоне от 0 до 10000.
Error: Invalid XML config format	Неверный формат файла конфигурации.	Устранить ошибки в файле конфигурации.
Error: Too many <authorities> sections. Must be only one!	Слишком много секций <authorities> в файле конфигурации. Должна быть только одна секция.	Удалить лишние секции <authorities> в файле конфигурации.
Error: <check_dn> field should contain only yes or no	Поле <check_dn> должно содержать только значения «yes» или «no».	Установить в поле <check_dn> значение «yes» или «no».
Error: <start_action> field should contain only yes or no	Поле <start_action> должно содержать только значения «yes» или «no».	Установить в поле <start_action> значение «yes» или «no».
Error: A connection with name \"%s\" already exists	Соединение \"%s\" уже существует.	-
Error: Authority with name \"%s\" already exists	Секция «authority» уже существует.	-

Сообщение	Описание	Действия по устранению
Error: Value in field %s is too long!	Значение в поле %s слишком длинное.	Скорректировать значение в поле %s.
Error: Line %s	Ошибка в строке %s.	Устранить указанную ошибку.
Error: Certificate %s in <root_cert> section is not root!	Указанный в поле <root_cert> сертификат не является корневым.	Заменить сертификат в поле <root_cert> на корневой.
Error: Certificate %s in <cert> section is root!	Указанный в поле <cert> сертификат является корневым.	Указать в поле <cert> сертификат открытого ключа VPN-клиента.
Error: No valid URLs found in the <crl_uris> section	В секции <crl_uris> не найдено ни одного действительного URL (Uniform Resource Locator).	Указать в секции <crl_uris> один или более URL.
Error: Certificate %s from <root_cert> is not root for %s	Сертификат %s в поле <root_cert> не является корневым для %s.	Указать в поле <root_cert> корневой сертификат.
Error: No valid ike conn names found in <conn_names>	В секции <conn_names> не найдено ни одного допустимого имени соединения.	Указать в секции <conn_names> имя соединения.
Error: Connection %s with certificate %s could not be validated	Не удалось проверить соединение %s с сертификатом %s.	-
Error: Root certificate %s is already used	Корневой сертификат %s используется.	-
Error: In %s connection section:	Ошибка в секции <connection>.	Проверить параметры в секции <connection> файла конфигурации и устранить ошибки.
Error: In %s authority section:	Ошибка в секции <authority>.	Проверить параметры в секции <authority> файла конфигурации и устранить ошибки.
Error: Field \"%s\" is missing	Поле \"%s\" отсутствует в файле конфигурации.	Включить в состав файла конфигурации поле \"%s\".
Error: No connection with name %s in XML	Отсутствует соединение с именем %s в файле конфигурации.	Проверить файл конфигурации.
Error: Section \"%s\" is missing	Секция \"%s\" отсутствует в файле конфигурации.	Включить в состав файла конфигурации секцию \"%s\".
Error: Too many connections. Maximum 10 connections allowed	Слишком много соединений. Максимально допустимое количество соединений – 10.	Сократить количество соединений до 10.
Error: Field <remote_id> must contain either a valid DN or a certificate name	Поле <remote_id> должно содержать либо допустимое DN, либо имя файла сертификата.	Указать в поле <remote_id> DN или имя файла сертификата.
Error: Connection %s and %s have the same certificate and remote ip	Соединения %s и %s имеют одинаковый сертификат и удаленный IP-адрес.	Изменить сертификат и IP-адрес одного из соединений.
Error: Quantity of <conn_name> sections should correspond to quantity of connections	Количество секций <conn_name> должно соответствовать количеству соединений.	Привести в соответствие количества соединений с количеством секций в файле конфигурации.
Error: invalid value!	Недопустимое значение.	Исправить значение.
Error: Internal error in RuToken lib	Внутренняя ошибка библиотеке RuToken.	Выполнить перезапуск DiSec-LV2
Error: Failed to open session with RuToken	Не удалось открыть сессию с RuToken.	Выполнить перезапуск DiSec-LV2

Сообщение	Описание	Действия по устранению
Error: Failed to find %s on RuToken	Не найден файл %s на RuToken.	-
Error: Invalid slot number	Указан неверный номер слота	Указать корректный номер слота и повторить попытку.
Error: No RuToken found in slot %s	В слоте %s не найден RuToken	Установить RuToken в слот %s.
Error: ICV mismatch, Rutoken password is corrupted	Имитовставка не совпала с эталонной, пароль Rutoken поврежден.	Заменить Rutoken.
Error: Unable to encrypt password	Не удалось зашифровать пароль	Выполнить перезапуск DiSec-LV2.
Error: Unable to decrypt password	Не удалось расшифровать пароль.	Выполнить перезапуск DiSec-LV2.
Error: Only root may run disec_config	Утилитой disec_config может пользоваться только суперпользователь (root).	Запустить disec_config от имени суперпользователя (root).
Error: disec-lv2 start failed, %s	Не удалось запустить службу disec-lv2	Повторить попытку. Выполнить перезапуск DiSec-LV2.
Error: disec-lv2 stop failed	Не удалось остановить службу disec-lv2.	Повторить попытку. Завершить работу DiSec-LV2.
Error: Level value should be from 1 to 3	Уровень детализации сообщений в Журнале службы должен быть установлен в диапазоне от 1 до 3.	Установить уровень детализации сообщений в диапазоне от 1 до 3.
Error: The minimum size value must be greater than 0	Минимальное значение уровня детализации сообщений должно быть больше 0.	Установить уровень детализации сообщений в диапазоне от 1 до 3.
Error: The interval can only take these values: --hourly, --daily, --weekly, --monthly, --yearly	Интервал ротации Журнала службы может принимать только следующие значения: hourly, daily, weekly, monthly, yearly.	Установить одно из следующих значений: hourly, daily, weekly, monthly, yearly.
Error: Failed to delete %s from disec-lv2 dir	Не удалось удалить файл %s из каталога disec-lv2.	Повторить попытку от имени суперпользователя (root).
Error: disec-lv2-autostart enabling failed	Не удалось включить disec-lv2-autostart.	
Error: disec-lv2-autostart disabling failed	Отключения disec-lv2-autostart завершилось неудачей.	
<b>Утилита DISEC_ID</b>		
disec_id: слишком мало аргументов при вызове!	Утилите было передано недостаточное количество аргументов.	Указать требуемые аргументы при запуске утилиты.
disec_id: License activation failed for %s	Активация лицензии не удалась.	1. Проверить правильно ли был введен ключ лицензии. 2. Проверить правильно ли было указано имя файла с лицензией.
disec_id: Could not write license file for %s!	Не удалось записать файл лицензии.	
<b>Утилита DISEC_STATUS</b>		
disec_status: слишком мало аргументов при вызове!	Утилите было передано недостаточное количество аргументов.	Указать требуемые аргументы при запуске утилиты.

Сообщение	Описание	Действия по устранению
disec_status: необходимо указать имя соединения!	Не было указано имя соединения.	При запуске утилиты указать имя соединения.
disec_status: необходимо указать опцию, для которой выбран режим вывода: -g, -o, -a, -n (см. disec_config --help)	Некорректно используются опции утилиты.	При запуске утилиты корректно указать опцию.
<b>Утилита DISEC_STARTER</b>		
disec_starter: слишком мало аргументов при вызове!	Утилите было передано недостаточное количество аргументов.	Указать требуемые аргументы при запуске утилиты.
Отсутствует конфигурация параметров службы! Воспользуйтесь утилитой disec_config с опцией --prepare для подготовки конфигурации!	Не найден основной файл конфигурации.	Подготовить файл конфигурации.
Произошла внутренняя ошибка!	Внутренняя ошибка утилиты.	-
Слишком много ключей на носителе! Носитель не может содержать больше %d ключей	На носителе найдено количество ключей больше допустимого значения.	Удалить лишние ключи на носителе.
Не найден закрытый ключ!	Для соединения не найден закрытый ключ соответствующий открытому из сертификата.	Установить закрытый ключ.
Сертификат был отозван!	Используемый для соединения сертификат был отозван УЦ.	-
Не найден действительный CRL для проверки отзыва сертификата!	Не найден список отзыва сертификатов.	
Невозможно найти контрольную сумму! Возможно, повреждено внутреннее хранилище	Невозможно найти контрольную сумму для объекта хранилища.	
Разрешение адреса провалено! Невозможно разрешить адрес	Не удалось разрешить указанный в конфигурационном файле адрес.	
Провалена проверка соответствия DN, полученного от удаленной стороны!	Удаленная сторона прислала DN не совпадающий с эталонным.	
Провалена валидация сертификата локальной стороны!\n	Не удалось валидировать локальный сертификат.	
Возможно, повреждено внутреннее хранилище.\n		
Убедитесь, что в хранилище присутствуют:\n		
\t - Действительный локальный сертификат\n		
\t - Действительные сертификаты промежуточных УЦ (при наличии)\n		
\t - Действительный сертификат корневого УЦ		
Провалена валидация сертификата удаленной стороны!\n	не удалось валидировать удаленный сертификат	

Сообщение	Описание	Действия по устранению
Возможно, повреждено внутреннее хранилище.\n		
Убедитесь, что в хранилище присутствуют:\n		
\t - Действительный сертификат корневого УЦ удаленной стороны		
Соединение запущено, однако сервер не отвечает в данный момент...\n	Удаленная сторона недоступна.	

**7. ПЕРЕЧЕНЬ ТЕРМИНОВ**

Администратор	- Специалист выполняющий работы по установке, настройке DiSec-LV2 и обслуживанию программно-технических средств, в среде которых функционирует DiSec-LV2
Аппаратная платформа	- Аппаратные средства, выполняющие взаимосвязанные функции в составе ВС и обеспечивающие поддержку ОС и DiSec-LV2
Асимметричный криптографический метод шифрования	- Метод шифрования, основанный на использовании открытого и закрытого ключей
Вычислительное средство	- Персональный компьютер, ноутбук, планшет функционирующий под управлением ОС
Дистрибутив	- Форма распространения программных изделий
Закрытый ключ	- Изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование (шифр), применяемый для расшифрования информации
Открытый ключ	- Изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование (шифр), применяемый для зашифрования информации
Пользователь	- Лицо, использующее ВС с предустановленным DiSec-LV2 для безопасного удаленного доступа к ресурсам LAN
Путь	- Расположение файла в файловой системе
Суперпользователь	- Специальный акаунт, владелец которого имеет право на выполнение всех без исключения операций в среде
VPN	- Технология, используемая для создания защищенного соединения между VPN-клиентом и VPN- сервером
VPN-клиент	- СКЗИ «Клиент криптографического сервера доступа DiSec-LV2»
VPN-сервер	- Изделия разработки ООО «Фактор-ТС»: ПАК Dionis-NX и ПАК Dionis DPS

**8. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ**

АП	-	Аппаратная платформа
ВС	-	Вычислительное средство
КС	-	Контрольная сумма
ОС	-	Операционная система
ПАК	-	Программно-аппаратный комплекс
СКЗИ	-	Средство криптографической защиты информации
СОС	-	Список отзыва сертификатов
ГУЦ	-	Головной удостоверяющий центр
УЦ	-	Удостоверяющий центр
CLI	-	Интерфейс командной строки
IKE	-	Протокол обмена ключами, входящий в набор протоколов IPSec
Internet	-	Всемирная система объединённых компьютерных сетей разной тематики, позволяющая хранить и передавать информацию
LAN	-	Локальная сеть
USB	-	Универсальная последовательная шина
VPN	-	Виртуальная частная сеть

**ФАЙЛ КОНФИГУРАЦИИ**  
**(disec.xml)****Пример файла конфигурации**

```
<?xml version="1.0" encoding="UTF-8"?>
<disec_config>
  <connection>
    <version>1</version>
    <ike_conn>moscow</ike_conn>
    <cert>cert.cer</cert>
    <check_dn>yes</check_dn>
    <remote_id>DN or cert</remote_id>
    <remote_ip>0.0.0.0</remote_ip>
    <optional>
      <dpd_action>initiate</dpd_action>
      <dpd_interval>10</dpd_interval>
      <dpd_timeout>30</dpd_timeout>
      <keying_tries>forever</keying_tries>
      <route_metric>100</route_metric>
      <local_ip>%any</local_ip>
      <pfs_mode_force>yes</pfs_mode_force>
      <fragmentation>yes</fragmentation>
      <strictcrlpolicy>no</strictcrlpolicy>
      <ph_margin_fuzz>5</ph_margin_fuzz>
      <ph_margin_time>200</ph_margin_time>
      <ph1_life_time>3600</ph1_life_time>
      <ph1_transforms>gost89b-gost3411_12_512-gostvko01b</ph1_transforms>
      <ph2_life_time>1200</ph2_life_time>
      <ph2_transforms>gost_4m_imit_b-gostvko01b</ph2_transforms>
      <udp_encap>no</udp_encap>
      <start_action>no</start_action>
    </optional>
  </connection>
  <authorities>
    <authority>
      <name>name</name>
      <root_cert>root.cer</root_cert>
      <conn_names>
        <conn_name>moscow</conn_name>
      </conn_names>
      <crl_uris>
        <crl_uri>http://localhost</crl_uri>
      </crl_uris>
    </authority>
  </authorities>
</disec_config>
```

**Примечания:**

1. В примере приведены параметры для настройки одного VPN-туннеля. Для настройки более одного соединения следует включить в файл конфигурации секции connections для каждого VPN-туннеля.
2. Количество секций в файле конфигурации не должно превышать 10.

## Параметры файла конфигурации

Параметр	Описание
<b>Секция Connection</b>	
version	Версия протокола IKE. На данный момент поддерживается только IKEv1. В настоящее время поле не обрабатывается.
ike_conn	Название соединения. Для одного файла конфигурации не может быть двух соединений с одинаковыми именами. Формат данных: строка содержащая имя соединения без пробелов.
cert	Имя файла с сертификатом открытого ключа VPN-клиента. Расширение файла - cer. Формат данных: строка без пробелов, содержащая имя файла.
check_dn	Способ аутентификации сервера. При значении «yes» выполняется сверка DN (Distinguished Name) сертификата VPN-сервера с DN VPN-клиента в поле <remote_id> (либо из сертификата, указанного в этом поле). При значении «no», VPN-клиент доверяет любому сертификату от VPN-сервера. Формат данных: строка, содержащая значение «yes» или «no».
remote_id	DN (Distinguished Name) VPN-клиента. Принимается либо строка с DN, либо имя установленного в хранилище сертификата, используемого для формирования DN. Параметр используется, если в параметре <check_dn> установлено значение «no». Формат данных: строка, содержащая DN либо имя сертификата. Максимальная длина DN 1024 символов.
remote_ip	IP-адрес или fqdn (доменное имя) VPN-сервера. Формат данных: строка, содержащая ip адрес или fqdn без пробелов.
<b>Подсекция Optional</b>	
dpd_action	(dpd - dead peer detection) Параметр определяет действие, которое следует выполнить спустя время, указанное в параметре dpd_interval, если VPN-сервер не отвечает (считается мертвым). Формат данных: строка, которая может содержать только один из четырех параметров: close, route, initiate или restart.
dpd_interval	Интервал времени между проверками доступности VPN-сервера. Формат данных: строка, содержащая одно положительное целое значение (с учетом 0) без пробелов.
dpd-timeout	Промежуток времени после первой неудачной попытки dpd, по истечении которого считается, что VPN-сервер не работает. Формат данных: строка, содержащая одно положительное целое значение (с учетом 0) без пробелов.
keying_tries	Количество попыток выполнения rekeying до отказа от соединения. Формат данных - строка, содержащее одно положительное целое значение (с учетом 0) без пробелов, либо строка «forever».
route_metric	Метрика маршрута одного соединения. Формат данных: строка, содержащая одно положительное целое значение без пробелов (с учетом 0) в интервале от 0 до 10000.
local_ip	IP-адрес VPN-клиента. Формат данных: строка, содержащая либо «%any», либо ip- адрес без пробелов.
pfs_mode_force	Включение функции perfect forward secrecy для защиты от компрометации всех сессионных ключей при компрометации одного. Формат данных: строка, содержащая значение «yes» или «no».

Параметр	Описание
fragmentation	Включение функции фрагментации пакетов (стандартный пакет MTU = 1500). Формат данных: строка, содержащая значение «yes» или «no».
strictcrlpolicy	Если установлено значение «yes» - выполняется проверка наличия сертификата в списке отзыва сертификатов (crl). Путь к списку отзыва сертификатов указан в параметре <crl_uri>. Если установлено значение «no» - проверка не выполняется. Формат данных: строка, содержащая значение «yes» или «no».
ph_margin_fuzz	Максимальное время, в течение которого IP-пакет может быть повторен. Формат данных: строка, содержащая одно положительное целое значение (с учетом 0) без пробелов.
ph_margin_time	Допустимый диапазон случайных изменений времени отправки IP-пакетов. Формат данных: строка, содержащая одно положительное целое значение (с учетом 0) без пробелов.
ph1_life_time	Максимальное значение времени «жизни» IKE фазы соединения. По истечению указанного времени происходит переподключение. Формат данных: строка, содержащая одно положительное целое значение (с учетом 0) без пробелов.
ph1_transforms	<p>Набор криптопараметров для IKE фаза 1.  Значение: &lt;алгоритм шифрования&gt;-&lt;функция хеширования&gt;-&lt;алгоритм согласования ключей&gt;, где</p> <p>Алгоритм шифрования:</p> <ul style="list-style-type: none"> <li>- gost89a - алгоритм ГОСТ 28147-89, режим GOST-CFB-IMIT, узел замены CryptoPro Set A;</li> <li>- gost89b - алгоритм ГОСТ 28147-89, режим GOST-CFB-IMIT, узел замены CryptoPro Set B;</li> <li>- gost89c - алгоритм ГОСТ 28147-89, режим GOST-CFB-IMIT, узел замены CryptoPro Set C;</li> <li>- gost89d - алгоритм ГОСТ 28147-89, режим GOST-CFB-IMIT, узел замены CryptoPro Set D;</li> <li>- gost89z - алгоритм ГОСТ 28147-89, режим GOST-CFB-IMIT, узел замены CryptoPro Set Z;</li> <li>- magmacfb - ГОСТ 34.13-2018 в режиме CFB.</li> </ul> <p>Функция хеширования:</p> <ul style="list-style-type: none"> <li>- gost3411_94 - ГОСТ Р 34.11-94;</li> <li>- gost3411_12_512 - ГОСТ Р 34.11-12 с размером хэша 512 бит.</li> </ul> <p>Алгоритм согласования ключей:</p> <ul style="list-style-type: none"> <li>- gostvko01a - ВКО ГОСТ Р 34.10-2001 с размером ключа 256 бит и набором параметров id-GostR3410-2001-CryptoPro-A-ParamSet;</li> <li>- gostvko01b - ВКО ГОСТ Р 34.10-2001 с размером ключа 256 бит и набором параметров id-GostR3410-2001-CryptoPro-B-ParamSet;</li> <li>- gostvko12_256a - ВКО ГОСТ Р 34.10-2012 с размером ключа 256 бит с набором параметров id-GostR3410-2001-CryptoPro-A-ParamSet;</li> <li>- gostvko12_256b - ВКО ГОСТ Р 34.10-2012 с размером ключа 256 бит с набором параметров id-GostR3410-2001-CryptoPro-B-ParamSet;</li> <li>- gostvko12_512a - ВКО ГОСТ Р 34.10-2012 с размером ключа 512 бит набором параметров id-tc26-gost-3410-12-512-paramSetA;</li> <li>- gostvko12_512b - ВКО ГОСТ Р 34.10-2012 с размером ключа 512 бит набором параметров id-tc26-gost-3410-12-512-paramSetB.</li> </ul>

Параметр	Описание
ph2_life_time	Максимальное значение времени «жизни» ESP фазы соединения. По истечению времени происходит переподключение. Формат данных: строка, содержащая одно положительное целое значение (с учетом 0) без пробелов.
ph2_transforms	<p>Набор криптопараметров для фазы ESP. Параметр: ph2_transforms. Значение: &lt;алгоритм шифрования ESP&gt;-&lt;алгоритм согласования ключей&gt;, где</p> <p>Алгоритм шифрования ESP:</p> <ul style="list-style-type: none"> <li>- gost4m_imit_a - алгоритм ГОСТ 28147-89, режим GOST-4M-IMIT, узел замены CryptoPro Set A;</li> <li>- gost4m_imit_b - алгоритм ГОСТ 28147-89, режим GOST-4M-IMIT, узел замены CryptoPro Set B;</li> <li>- gost4m_imit_c - алгоритм ГОСТ 28147-89, режим GOST-4M-IMIT, узел замены CryptoPro Set C;</li> <li>- gost4m_imit_d - алгоритм ГОСТ 28147-89, режим GOST-4M-IMIT, узел замены CryptoPro Set D;</li> <li>- gost4m_imit_z - алгоритм ГОСТ 28147-89, режим GOST-4M-IMIT, узел замены CryptoPro Set Z;</li> <li>- gost_magma_4m – Р 1323565.1.026-2019, алгоритм Магма в режиме MGM.</li> </ul> <p>Алгоритм согласования ключей – см. IKEv1 фаза 1&gt; transforms.</p>
udp_encap	Включение UDP инкапсуляции ESP пакета Формат данных: строка, содержащая значение «force» или «no» без пробелов.
start_action	Автоматическое подключение ранее установленных соединений после перезапуска DiSec LV2
<b>Секция Authorities</b>	
name	Идентификатор PKI (инфраструктура открытых ключей) политики. Формат данных: строка содержащая одно имя.
root_cert	Имя сертификата, по которому строится цепочка валидации до пользовательских сертификатов, указанных в соединениях с именами из <conn_name>. Формат данных: строка без пробелов, содержащая одно имя файла.
<b>Секция Conn_names</b>	
conn_names	Имя соединения, для которого используется данная PKI политика. Формат данных: строка содержащая имя соединения без пробелов.
<b>Секция Crl_uris</b>	
crl_uri	URI (унифицированный (единообразный) идентификатор ресурса) на котором, при установленном значении «yes» в поле ввода параметра <strictcrlpolicy>, осуществляется обновление локального файла списка отзыва сертификатов (http://localhost). Формат данных: строка, содержащая один URI с протоколом ldap, http или ftp. Длина строки ограничена 512 символами.

**Примечания:**

1. В секции Connection приведены обязательные для заполнения параметры соединения.

2. В подсекции `Optional` приведены значения параметров по умолчанию, не обязательные для изменения.
3. Секция `Authorities` содержит настройки для PKI политик соединений. Каждая из секций `connection` может использовать как свою подсекцию `authority`, так и общую, если корневой сертификат у них одинаковый.
4. В секции `Conn_names` для каждого `<ike_conn>` использующего данную PKI политику создается отдельное поле `<conn_name>`.
5. В секции `Crl_uris` для одной PKI политики поддерживается не более трех URI для обновления `crl`.
6. Для каждого поля максимальная длина входных данных составляет 100 символов, если в его описании не приведено другое значение.
7. В файле конфигурации не должны повторяться: названия соединений, то есть значение полей `<ike_conn>`, названия PKI политик, то есть значения секций `<name>`, и не может быть двух соединений с одинаковыми сертификатами (проверяется отпечаток ключа) и с одинаковыми `<remote_ip>` (результаты резолвинга FQDN в `Ip` не проверяются).
8. Количество соединений в файле конфигурации не более 10.

**УТИЛИТЫ****Утилита disec\_config**

Утилита disec\_config применяется для администрирования СКЗИ «Клиент криптографического сервера доступа DiSec-LV2» в консольном режиме с использованием интерфейса командной строки.

**disec\_config [параметр ...] <аргумент>**

<b>Базовые команды управления службой</b>	
--disec --start	Запуск службы disec-lv2
--disec --stop	Останов службы disec-lv2
--disec --status	Информация о состоянии службы disec-lv2
[--find <event>]	Поиск указанного события в журнале службы disec-lv2
[--n <number >=0>]	Показать указанное количество строк информации о состоянии службы disec-lv2 или показать указанное количество строк после найденного события в журнале
<b>Управление автоматическим запуском</b>	
--autostart --enable	Включить автоматический запуск установленных VPN-туннелей при перезапуске DiSec-LV2
--autostart --disable	Отключить автоматический запуск установленных VPN-туннелей при перезапуске DiSec-LV2
<b>Управление конфигурацией</b>	
--prepare <path_to_xml>	Конвертировать конфигурацию из формата XML во внутренний формат службы disec-lv2
[--log-level <0-3>]	Указать необходимый уровень журналирования (опционально)
--check-xml <path_to_xml>	Проверить корректность указанного файла XML-конфигурации
[--check-creds]	Проверить указанные в XML-конфигурации сертификаты на действительность
--create-example [path]	Создать пример файла XML-конфигурации службы disec-lv2
<b>Файловые операции</b>	
--import <filename.cer   filename.crl   filename.lic>...	Импортировать файл(ы), указанные по абсолютному пути, во внутреннее хранилище службы disec-lv2
--import-all <dirpath>	Импортировать все .cer, .crl, .lic файлы из указанной директории во внутреннее хранилище службы disec-lv2
--validate <filename.cer   filename.crl>...	Проверить действительность импортированных файлов во внутреннем хранилище службы disec-lv2
--delete <filename.cer   filename.crl>...	Удалить файл(ы) из внутреннего хранилища службы disec-lv2
--delete --crls	Удалить все X.509 списки отзыва сертификатов из внутреннего хранилища службы
--delete --certs	Удалить все X.509 сертификаты из внутреннего хранилища службы disec-lv2
--delete --all	Удалить все объекты из внутреннего хранилища службы disec-lv2
<b>Операции с Рутокеном</b>	
--rtk --devices	Показать список всех доступных устройств Рутокен
--rtk --list-files [--s <num>]	Показать список всех файлов на устройстве Рутокен [в указанном слоте]

## RU.НКБГ.70021 87

--rtk --import --s <num> <filename.cer   filename.crl   filename.xml   filename.lic>	Импортировать файл(ы) с устройства Рутокен в указанном слоте
<b>Опции вывода информации</b>	
--list --crypto-algs	Вывести список всех криптографических алгоритмов для фазы 1 и фазы 2 протокола IKE
--list --certs	Вывести список всех импортированных X.509 сертификатов
--list --crls	Вывести список всех импортированных X.509 списков отзыва сертификатов
--list --all	Вывести список всех импортированных объектов
--list --chain <file.cer   file.xml   conn>	Вывести цепочку(у) доверия для каждого .cer, для всех соединений в XML или для конкретного (конкретных) соединений из XML
<b>Операции с FQDN</b>	
--fqdn --update <path_to_xml>	Обновить ip адреса для FQDN указанных в XML
--fqdn --show	Вывести все пары ip - fqdn, используемые в disec-lv2
--fqdn --clear	Удалить все пары ip - fqdn, используемые в disec-lv2
<b>Журналирование</b>	
--log-level <0-3> [--restart-disec]	Установить уровень журналирования, при этом: - 0 - журналирование самых основных событий; - 1 - стандартный журнал с выводом ошибок, хороший уровень для администрирования; - 2 - более детализированный отладочный режим; - 3 - включает СЫРЫЕ дампы данных в шестнадцатеричном формате.
--log-level --get	Показать текущий уровень журналирования
--log-size <min_size>	Установить минимальный размер для обновления журнала в МБ
--log-interval --hourly	Обновлять журнал каждый час
--log-interval --daily	Обновлять журнал каждый день
--log-interval --monthly	Обновлять журнал каждый месяц
--log-interval --yearly	Обновлять журнал каждый год
<b>Помощь и справка</b>	
-h, --help	Вывести текущую справку
-v, --version	Вывести версию утилиты

**Утилита disec-starter**

Утилита для запуска/останова соединений:

**disec\_starter [-u <имя\_соединения | all>] [-c <имя\_соединения | all> <-e | -d>]**

-h, --help	Вывести текущую справку
-v, --version	Вывести версию утилиты
-u, --update-crl=name	Обновить CRL для соединения 'name', или 'all' для обновленияD всех возможных соединений
-c, --connection=name	Указать имя соединения для запуска/останова, или 'all' для запуска/останова всех возможных соединений
-e, --enable	Запустить указанное соединение
-d, --disable	Остановить указанное соединение

**Утилита disec\_id**

Утилита активации лицензии

**disec\_id <параметр>**

-h, --help	Вывести текущую справку
-v, --version	Вывести версию утилиты
-g, --get-id	Получить идентификатор платформы
-l, --license-status	Получить статус лицензии
-a, --activate <КЛЮЧ ЛИЦЕНЗИИ>	Активировать лицензию указанным ключом (требует прав суперпользователя)
-c, --check-key <КЛЮЧ ЛИЦЕНЗИИ>	Проверить указанный ключ на действительность
-f, --check-file <ФАЙЛ КЛЮЧА>	Проверить указанный файл ключа на действительность

**Утилита disec\_status****disec\_status [параметр]... [-c <имя\_соединения | all>]**

<b>Базовые команды</b>	
-h, --help	Вывести текущую справку
-v, --version	Вывести версию утилиты
-c, --connection	Указать имя соединения, или 'all' для выбора всех возможных соединений
-g, --get-status	Получить сводку для указанного соединения
[-m, --monitor]	Выводить список в monitor-режиме
[-w, --watch]	Выводить список в watch-режиме
-o, --configuration	Показать конфигурацию для указанного соединения
[-m, --monitor]	Выводить список в monitor-режиме
[-w, --watch]	Выводить список в watch-режиме
-a, --active	Показать активные IKE SA для указанного соединения
[-m, --monitor]	Выводить список в monitor-режиме
[-w, --watch]	Выводить список в watch-режиме
-n, --nx-active	Показать активные IKE SA в стиле Dionis-NX для указанного соединения
[-m, --monitor]	Выводить список в monitor-режиме
[-w, --watch]	Выводить список в watch-режиме
<b>Контроль целостности</b>	
-u, --calculate-hashsum	Рассчитать контрольную сумму приложения
-i, --check-integrity	Проверить целостность приложения
<b>Опции для работы с PKI</b>	
-l, --certificates	Вывести список всех X.509 сертификатов
-r, --ca-certificates	Вывести список всех X.509 сертификатов УЦ
-x, --crls	Вывести список всех X.509 списков отзыва сертификатов
<b>Журналирование</b>	
-s, --show-logging-level	Показать текущий уровень журналирования

