УТВЕРЖДЕНО

RU.НКБГ.70009-02 92 - ЛУ

Клиент криптографического сервера доступа «DiSec-W»

Версия 7.0

Руководство пользователя

RU.НКБГ.70009-02 92

Листов 113

СОДЕРЖАНИЕ

1 Общие сведения о программе

Настоящий документ предназначен для ознакомления с принципами функционирования Программного обеспечения «Клиент криптографического сервера доступа «DiSec» RU.НКБГ.70009-02, правилами подготовки к эксплуатации и настройке изделия.

Полное наименование изделия - «Клиент криптографического сервера доступа «DiSec»

Краткое наименование изделия - ПО DISEC или DISEC

Обозначение изделия - RU.НКБГ.70009-02.

Настоящий документ предназначен как для персонала, обслуживающего программно-технические средства, так и для конечного пользователя DISEC. Обслуживающий персонал должен иметь соответствующий уровень подготовки, необходимый для выполнения основных функций по установке и настройке программных средств в среде операционной системы WINDOWS, а также для проведения анализа и обнаружения неисправностей в программно-техническом и сетевом окружении.
В данном разделе приведена информация о назначении и области применения Программного обеспечения (ПО) DISEC, а также приведены основные понятия, используемые в данном документе.

1.1. Назначение и область применения программы

ПО DISEC предназначено для обеспечения криптографической защиты данных, передаваемых в открытых каналах связи по протоколам TCP/IP, предоставляя доступ удалённым пользователям к ресурсам сегментов глобальной вычислительной сети, защищённых сетевыми устройствами (Серверами VPN).
ПО DISEC совместно с Сервером VPN реализует набор протоколов IPsec (IP Security) для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяя осуществлять подтверждение подлинности взаимодействующих сторон (взаимную аутентификацию), проверку целостности и/или шифрование IP-пакетов, а также включает в себя протоколы для защищённого обмена ключами шифрования. Таким образом, ПО DISEC применяется для организации VPN-соединений и относится к классу программ VPN-клиент.

> ПО DISEC функционирует на устройствах, таких как персональный компьютер, сервер, ноутбук, планшет, под управлением операционных систем семейства Windows фирмы Microsoft: 64-разрядных версий операционных систем Microsoft Windows Server 2016, Microsoft Windows 10.

Далее по тексту, где не требуется детализация, будет использоваться общий термин "устройство пользователя DISEC " или Клиент DISEC.
Сетевые устройства, обеспечивающие защиту корпоративной сети и доступ к ней пользователей DISEC, представляют собой программно-аппаратные комплексы (ПАК), в которых реализованы средства построения виртуальных частных сетей (Virtual Private Network - VPN). Для краткости в данном документе для сетевого устройства будет использоваться термин «Сервер VPN».
Для защиты конфиденциальной информации при передаче ее по незащищенной IP-сети организуется виртуальный защищенный канал (или просто канал), состоящий из одного или нескольких криптотуннелей (или просто туннелей) между компьютером с установленным ПО DISEC и Сервером VPN. Виртуальный защищенный канал организуется посредством процедуры подключения в соответствии с настройками ресурса подключения.

> *Примечание*. В дальнейшем по тексту будет использоваться как термин канал, так и Подключение. Иногда также может использоваться термин туннель, когда неважно различие между терминами "канал" и "туннель".

ПО DISEC, установленное на одном компьютере, доступно для использования всеми пользователями WINDOWS, которые работают независимо друг от друга, при этом настройки ПО DISEC хранятся отдельно в персональных репозиториях.
Сводка основных функциональных возможностей ПО DISEC приведена в Приложении (см. раздел Приложение 1. Функциональные возможности DiSec версии 7.0).
На общей схеме IP-доступа к ресурсам защищенных сетей (Рис. 1) представлено взаимодействие клиентов DiSec, находящихся в открытой сети, с ресурсами защищенных сетей.
К открытой IP-сети (**Открытая сеть**) может быть подключено множество Серверов VPN, каждый из которых обеспечивает защиту внутренних сетей и расположенных в них информационных ресурсов (**Защищенная сеть 1** и **Защищенная сеть 2**).

С помощью средств Серверов VPN пользователи компьютеров с ПО DISEC имеют возможность доступа к ресурсам каждой сети **Защищенной сети 1** и **Защищенной сети 2** посредством СТАТИЧЕСКОГО либо ДИНАМИЧЕСКОГО туннеля.

Вся информация (IP-пакеты) при передаче между компьютерами с ПО DISEC и ресурсами **Защищенной сети 1** и **Защищенной сети 2** через туннель шифруется, что делает возможным обмен конфиденциальной информацией по каналам связи открытой сети.

Статические туннели могут быть организованы непосредственно на компьютере, имеющим постоянный статический либо динамический IP-адрес. Возможность работы по статическому туннелю с компьютера, имеющего динамически присваиваемый, меняющийся IP-адрес, зависит от настроек на Сервере VPN.

При работе по статическому туннелю используются симметричные ключи шифрования.

Пользователи ПО DISEC могут инициировать создание динамического туннеля, при работе по которому используются ассиметричные ключи шифрования.

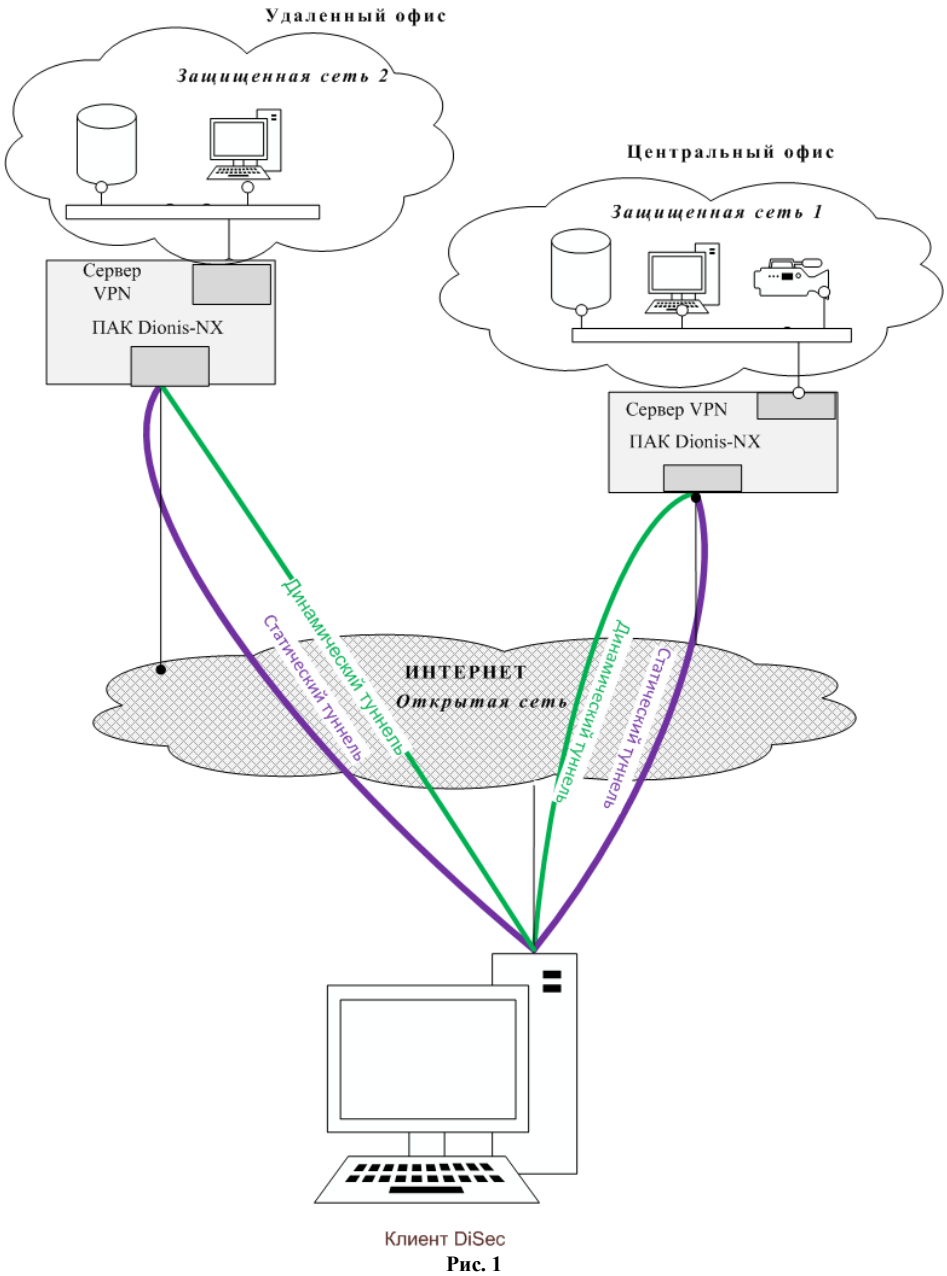


Рис. 1

1.2. Способы организации туннелей

DISEC может работать с туннелями двух типов, отличающихся по способу их организации (присутствие или отсутствие фазы переговоров с Сервером VPN по протоколу ISAKMP): **статическими** и **динамическими**, которые различаются следующими характеристиками.
Конец туннеля на стороне сервера VPN имеет постоянный IP-адрес подключения к открытой сети, известный клиенту.

Статический туннель

1. Конец туннеля клиента может иметь как постоянный, так и меняющийся IP-адрес. В последнем случае на Сервере VPN должна быть выполнена соответствующая настройка на прием любого адреса.
2. Параметры туннеля согласуются администратором Сервера VPN и пользователем DISEC с помощью обычных каналов связи (телефон, e-mail …), т.е. без использования какого-либо специального протокола.
3. На Сервере VPN статический туннель запускается как правило в момент запуска сервера и существует до его остановки, либо до снятия туннеля по инициативе администратора сервера.
4. DiSec может подключаться и отключаться от туннеля по инициативе пользователя DISEC (возможно, в режиме автоматического подключения).

Динамический туннель

1. Динамический туннель организуется только по инициативе пользователя DISEC (возможно, в режиме автоматического подключения), и для его организации каждый раз выполняется согласование параметров настройки противоположных концов туннеля посредством протокола ISAKMP (IKE).
2. Динамический туннель реализует набор протоколов IPsec с использованием российских криптоалгоритмов.

IPsec - это набор стандартов Интернет, который функционирует на сетевом уровне семиуровневой модели OSI и использует в качестве базового сетевой протокол IP. Таким образом, IPsec представляет собой «надстройку» над IP-протоколом. Ядро IPsec составляют три протокола:
Internet Security Association and Key Management Protocol (ISAKMP) — протокол, используемый для первичной настройки соединения, взаимной аутентификации конечными узлами друг друга и обмена секретными ключами. Протокол предусматривает использование различных механизмов обмена ключами, в частности таких протоколов, как **Internet Key Exchange (IKE)**.
Encapsulating Security Payload (ESP) обеспечивает конфиденциальность (шифрование) передаваемой информации, ограничение потока конфиденциального трафика. Кроме этого, он может обеспечить целостность виртуального соединения (передаваемых данных), аутентификацию источника информации и функцию по предотвращению повторной передачи пакетов.
Ключевым понятием IPSec является Ассоциация Безопасности (SA - Security Association), далее SA. SA представляет собой набор параметров, характеризующих соединение, в частности, используемые алгоритм шифрования и хэш-функция, секретные ключи.
В ПО DISEC в режиме динамического туннеля (IKE) используются оба этих протокола (IKE и ESP). При этом протокол IKE используется для защищенного обмена ключами и создания SA. В процессе установления соединения выполняется согласование двух SA (1-я фаза протокола IKE - согласование SA IKE, 2-я фаза протокола IKE - согласование SA ESP).

Каждый вид SA имеет свой набор параметров - алгоритмов шифрования, имитовставки - хеш-функций, размеров ключей шифрования и проч., и имеет уникальный идентификатор, состоящий из пары символьных последовательностей - индексов параметров безопасности (Security Parameters Index), SPI_I - индекс инициатора и SPI_R - индекс ответчика). Параметры для каждой SA хранятся в соответствующей политике (политика IKE и политика ESP).

Протокол IKE реализован на основе рекомендаций RFC 2407-2409 с использованием российских криптоалгоритмов ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012. Встраивание российских криптоалгоритмов выполнено в соответствии с рекомендациями технического комитета по стандартизации «Криптографическая защита информации» (ТК26) (www.tk26.ru).
При реализации дополнительных возможностей протокола IKE использовались следующие рекомендации:

- **RFC 3947** Negotiation of NAT-Traversal in the IKE;
- **RFC 3948** - UDP Encapsulation of IPsec ESP Packets для работы в сетях, использующих протокол NAT (RFC 3715 IPsec-Network Address Translation (NAT) Compatibility Requirements).
- **RFC3706** A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers - Метод обнаружения потери жизнеспособности канала связи с использованием передачи сообщений.
- The ISAKMP Configuration Method <draft-ietf-ipsec-isakmp-mode-cfg-05.txt> - Дополнительные способы конфигурации туннеля. В соответствии с этим документом реализована возможность более полной интеграции в защищенную сеть, включающую получение от Сервера VPN посредством протокола MODE_CONFIG "нового" мобильного IP-адреса для устройства пользователя

DISEC, а также получение новых значений адресов серверов DNS. Также реализована получения от Сервера VPN IP-адреса подсети в качестве доступного ресурса (целевой объект).

1.3. Туннелирование и инкапсуляция

Туннелированием называется процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции сетевых пакетов сетевого протокола IP в пакет специального инкапсулирующего протокола, при этом передаваемая порция данных вместе со служебными полями инкапсулируется ("упаковывается") в новый «конверт» для обеспечения конфиденциальности и целостности всей передаваемой порции.
В ПО DISEC применяется туннелирование на сетевом уровне, т.е. инкапсуляции подвергается IP-пакет, как правило, вместе с заголовком, который зашифровывается и передается по сети посредством одного из транспортных протоколов.
В качестве транспортного протокола может служить в зависимости от настроек туннеля один из IP-протоколов (или их комбинация):

- IP-in-IP (IP-протокол с номером 4) - основной протокол инкапсуляции для статического туннеля;
- UDP (IP-протокол с номером 17) - дополнительный протокол инкапсуляции;
- ESP (IP-протокол с номером 50) - протокол инкапсуляции для динамического туннеля.

При этом протокол UDP предоставляет "наружный" конверт и используется в случае, когда существует вероятность того, что на пути маршрута пакета имеются сетевые устройства, использующие NAT - подмену адресов, либо не пропускающие используемый "внутренний" протокол. В случае статического туннеля использование протокола UDP определяется настройками на стороне клиента и сервера. В случае динамического туннеля - процедура согласования (IKE) сама определяется необходимость его использования.
Концами туннеля служат с одной стороны устройство пользователя, с другой стороны - Сервер VPN.
Процедура туннелирования состоит в следующем.
Из всего потока информации, предназначенной для отправки в сеть, выделяется та, которая соответствует правилам отбора в туннель. Исходный сетевой пакет, соответствующий правилам отбора, подвергается обработке (выполняется зашифрование) и размещается в поле данных транспортного сетевого пакета (выполняется процедура инкапсуляции посредством основного протокола инкапсуляции). При этом:

- добавляется заголовок инкапсулирующего пакета;
- в заголовок инкапсулирующего пакета заносится информация, идентифицирующая туннель и другая служебная информация;
- при необходимости добавляется заголовок дополнительного протокола инкапсуляции;
- корректируется заголовок транспортного пакета IP (новая длина пакета, контрольная сумма и т.п.).
- сформированный таким образом транспортный сетевой пакет при необходимости разбивается на фрагменты (фрагментируется) и отправляется в открытую IP-сеть.

При получении сетевого пакета выполняется процедура декапсуляции, то есть процесс восстановления данных в соответствии с заданным протоколом инкапсуляции. При этом:

- выполняется расшифрование данных;
- проверка на соответствие правилам отбора в туннель ("посторонние" пакеты отбрасываются);
- трансформированный таким образом пакет проверяется на корректность (формат сетевых заголовков, отсутствие искажений - правильная контрольная сумма и т.д.);
- при отсутствии ошибок сетевой пакет отправляется "вверх" по стеку TCP\IP получателю - прикладной программе.

Процедуре декапсуляции может предшествовать процедура дефрагментирования пакетов (сборки одного пакета из нескольких принятых), также проверяется корректность заголовков пакета.

1.3.1. Режим статического туннеля

Для статического туннеля в качестве инкапсулирующего (транспортного) протокола используется протокол IP-in-IP (номер 4).

Поверх протокола IP-in-IP может быть использован протокол UDP с произвольными, но согласованными номерами портов источника и назначения.

1.3.2. Режим динамического туннеля

При туннелировании в режиме Динамического туннеля используются протоколы:

- ESP (RFC 4303 - IP Encapsulating Security Payload) - протокол шифрования и проверки подлинности IP-пакетов, передаваемых через криптотуннель;

- UDP (RFC 3948 - UDP Encapsulation of IPsec ESP Packets) - дополнительная инкапсуляция вышеперечисленных протоколов, применяемая при использовании защищенных сетей, использующих протокол NAT для маскирования адресов внутренних ресурсов.

Туннельный и транспортный режимы ESP

В режиме динамического туннеля реализованы два режима ESP-инкапсуляции: транспортный и туннельный.

В транспортном режиме шифруются (или подписываются) только данные IP-пакета, исходный заголовок сохраняется. В туннельном режиме шифруется весь исходный IP-пакет: данные, заголовок, маршрутная информация, а затем он вставляется в поле данных нового пакета, то есть происходит инкапсуляция.

> *Примечание*. Туннельный режим является более защищенным, поэтому рекомендуется использовать именно его. Транспортный режим может быть полезен только при работе с серверами, поддерживающими только этот режим, где это необходимо.

Протокол ESP реализован на основе рекомендаций RFC 4303 с использованием российских криптоалгоритмов ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012. Встраивание российских криптоалгоритмов в указанные протоколы производилось в соответствии с рекомендациями технического комитета по стандартизации «Криптографическая защита информации» (ТК26) (www.tk26.ru).

1.4. Интеграция в защищенную сеть

Для более полной интеграции в защищенную сеть может использоваться назначение новых сетевых параметров, так называемые параметры RLAN (расширенная локальная сеть), включающие новый IP-адрес устройства пользователя DISEC, новые адреса DNS серверов и т.п, устанавливаемые на сетевом интерфейсе устройства пользователя DISEC.

> *Примечание*. Сетевой интерфейс, по которому создается туннель, определяется автоматически по адресу Сервера VPN. Если адрес Сервера VPN задан доменным именем, то DISEC преобразует его в IP-адрес в соответствии с флажком типа IP-протокола, а затем определяет адрес локального сетевого интерфейса.

Для Статического туннеля новый IP-адрес (вместе с маской подсети) и адресов DNS-серверов (основного и альтернативного) назначаются в настройках Подключения.

Для Динамического туннеля для получения IP-адреса (вместе с маской подсети) и адресов DNS-серверов (основного и альтернативного) используется возможности протокола IKE - обмен сообщениями MODE_CONFIG, при этом в настройках Подключения указывается, какие из этих адресов следует запрашивать.

Работа с IP-адресом RLAN\MODE_CONFIG

Для нового IP-адреса добавляется сетевой маршрут, с адресом GW (gateway), равным адресу удаленного конца туннеля. При туннелировании во всех сетевых пакетах, подлежащих туннелированию перед их зашифрованием (перед отправкой в туннель) в заголовке IP-пакета меняется адрес назначения (destination) на "новый" адрес. При получении выполняется обратная операция - после расшифрования "новый адрес" заменяется на реальный адрес IP-интерфейса, по которому принят пакет, а сам пакет при отсутствии ошибок передается далее по TCP\IP стеку прикладным программам.

Работа с IP-адресами DNS-серверов RLAN\MODE_CONFIG

ПО DISEC отслеживает текущие адреса DNS-серверов или режим DHCP (для IPv4 и IPv6), установленные на сетевых интерфейсах.

При запуске Подключения приложением **DiSec** или службой **DiSecSRV** с заменой DNS-серверов перед началом туннелирования на соответствующем интерфейсе устанавливаются новые DNS-сервера, а после отключения эти настройки снимаются и возвращаются прежние значения. Во время работы с туннелем DNS-запросы маршрутизируются в соответствующий туннель, только если их адреса соответствуют правилам отбора.

> *Примечания*. Если подмена DNS-серверов назначена в нескольких Подключениях, которые запускаются одновременно, то эта процедура будет выполнена ТОЛЬКО для первого из них, а для последующих будет выдано предупреждение, что смена DNS не выполнена. Работу с туннелем можно продолжать без использования DNS-запросов.
>
> Не рекомендуется вручную менять адреса DNS-серверов на интерфейсах с установленными туннелями. Если такая замена необходима, следует завершить все Подключения, и после этого выполнить замену DNS серверов на интерфейсах.

1.5.Доступ к защищенным ресурсам

Цель создания туннеля - обеспечить доступ клиента DISEC к защищенным ресурсам IP-сети, при этом доступ регулируется правилами отбора в туннель, представляющими собой список ресурсов - каждый элемент которого состоит из IP-адреса отдельного устройства или подсети с указанием (опционально) протокола и диапазона портов (для протоколов прикладного уровня - UDP и TCP).
Список ресурсов задается в настройках Подключения и в данном документе называется Целевыми объектами. Ресурсы разделены символом ";". Из назначенного списка формируются правила отбора в туннель и передаются в драйвер **DiSec**, который сопоставляет каждый проходящий через него пакет с правилами и при соответствии - направляет в туннель.
Для Статического туннеля Целевые объекты формируются "вручную" перечислением ресурсов, либо при помощи дополнительного окна.
Следует учитывать, что:

- если Целевые Объекты не содержат никаких записей, это означает, что доступна вся защищенная сеть;
- правила могут быть как "разрешающие" так и "запрещающие";
- правила отбора обрабатываются последовательно сверху вниз, как только встречается правило, не пропускающее пакет в туннель, обработка списка правил прекращается;
- если задано выполнение контроля жизнеспособности туннеля (TnlPing), то DISEC автоматически формирует правило отбора для посылки сигналов в соответствии с настройками: если IP-адрес задан, то формируется правило, в котором этот адрес является адресом назначения, в противном случае, адресом назначения является адрес удаленного конца туннеля;
- если в настройках RLAN заданы адреса DNS-серверов, то формируются правила, разрешающие прохождение DNS-запросов по этим адресам;
- если в настройках задано обработка мультикастовых пакетов, то для них также автоматически создается правило отбора.

  Примечание. Автоматически сформированные правила добавляются только в случае, если они не входят в диапазон действия предыдущих правил.

Для Динамического туннеля правила отбора могут формироваться двумя способами: также, как для Статического туннеля - вручную, и посредством сообщений MODE_CONFIG IKE-протокола. В последнем случае необходимо установить флажок **Запросить IP-подсеть (MODE_CFG).**
Для Динамического туннеля также создаются дополнительные правила отбора для DNS-запросов в случае, если в процессе "переговоров" по IKE-протоколу получены адреса DNS-серверов.

2 Описание работы ПО DISEC

В данном разделе приведены сведения об основных компонентах ПО DISEC и об их взаимодействии с программно-аппаратными компонентами ОС WINDOWS; сведения об общих принципах функционирования ПО DISEC и о взаимодействии с Серверами VPN, а также об основных терминах и принципах системы криптографической защиты информации, используемых в DISEC.

2.1. Взаимодействие компонентов DiSec с компонентами WINDOWS

Клиент Криптографического сервера доступа DISEC состоит из следующих основных компонентов :

- на уровне приложений - приложение DiSec **(`DiSec.exe`)** и комплект динамически подгружаемых крипто-библиотек;
- на уровне сервиса операционной системы (службы) - служба DiSecSrv (**`Dionis Security Service`**), и вспомогательная служба DiSecAgent (**`Dionis Security NetAgent`**);
- на уровне ядра ОС - драйвер DiSec (**`DiSec.sys`**), разработанный на основе спецификации NDIS 6.30 (Network Driver Interface Specification) и встраиваемый в стек протоколов TCP\IP на сетевом уровне;
- вспомогательные утилиты инсталляции\деинсталляции драйвера, настройки, запуска, останова и настройки службы DiSecSRV.

Приложение DiSec выполняет главную задачу - организация и удаление туннеля посредством взаимодействия с Серверами VPN и настройки драйвера на выполнение функций туннелирования. Кроме того, с помощью приложения DiSec пользователь:

- выполняет настройку всех компонентов ПО DISEC;
- может получить информацию о текущем состоянии драйвера DiSec;
- может выполнить различные диагностические функции;
- может останавливать и запускать службу DiSecSrv.

Помимо этого приложение DiSec выполняет периодические задачи, такие как проверку целостности ПО, проверку валидности сертификатов, загрузку актуальных Списков Отзыва Сертификатов (CRL).

Служба DiSecSrv обеспечивает автоматическое подключение к Серверу VPN во время загрузки WINDOWS до входа в систему пользователя WINDOWS, что может использоваться при работе в доменной структуре WINDOWS для обеспечения авторизации на доменном контроллере WINDOWS, размещенном в защищенной сети, и в других ситуациях.

Служба DiSecAgent выполняет вспомогательные функции по изменению настроек интерфейсов по "заданию" приложения и службы при установке туннелей, такие как добавление и удаление маршрутов, изменение адресов серверов DNS. В режиме динамического туннеля обеспечивает доступ к глобальным объектам (сокетам), выполняя прием и диспетчеризацию полученных от сокетов сообщений, Служба запускается автоматически при загрузке ОС Windows.

Драйвер DiSec, подключенный к ядру операционной системы, контролирует IP-потоки между компонентами ядра WINDOWS, реализующими протоколы TCP\IP, и драйверами адаптеров локальных сетей, адаптерами мобильной связи и т. п.

Драйвер DiSec выполняет туннелирование и извлечение из туннеля (инкапсуляцию и декапсуляцию) сетевых пакетов, при этом выполняет зашифрование и расшифрование информации, используя в своей работе ключевой материал, сформированный приложением или службой на основе индивидуальной ключевой информации пользователя DISEC. При необходимости драйвер выполняет фрагментирование и дефрагментирование зашифрованных пакетов.

При обнаружении ошибок в процедурах фрагментирования или дефрагментирования, инкапсуляции или декапсуляции, зашифрования или расшифрования, а также при обнаружении некоторых видов сетевых атак (например, Replay-атаки) драйвер отбрасывает забракованный пакет и может выполнить запись в системный журнал WINDOWS (Event Log).

Драйвер DiSec запускается автоматически при старте операционной системы и до загрузки в него параметров динамического туннеля работает в «прозрачном» режиме, т.е. пропускает все IP-пакеты без изменений.

2.2. Взаимодействие ПО DISEC с Сервером VPN

Взаимодействие ПО DISEC и Сервера VPN включает в себя два этапа .

1-й этап - организация туннеля.

2-й этап - передача зашифрованной информации между пользователем DISEC и Сервером VPN по организованному туннелю.

Схема взаимодействия для ДИНАМИЧЕСКОГО туннеля:

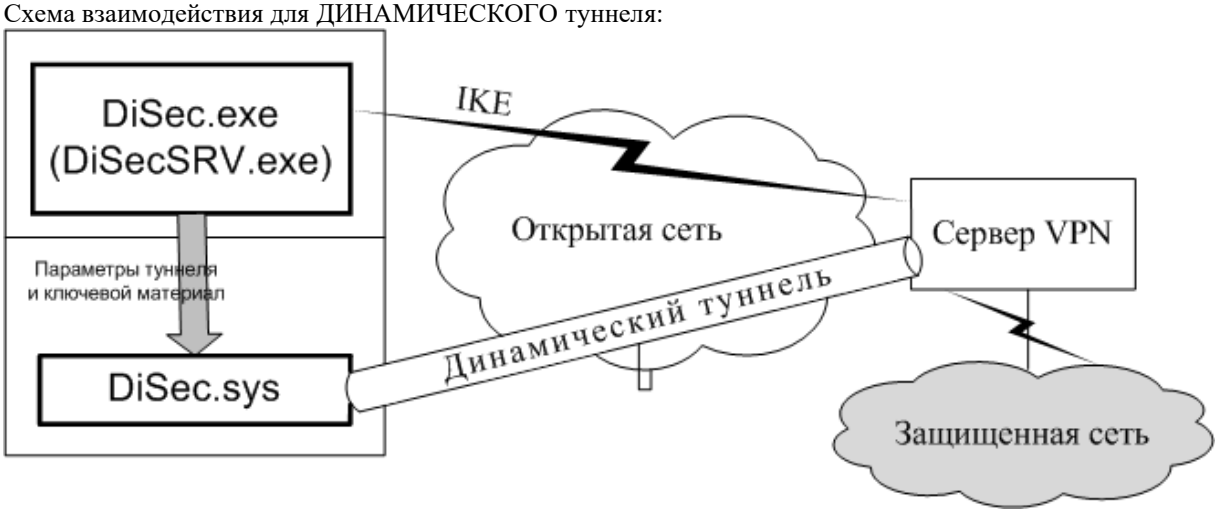


Рис. 2

Схема взаимодействия для СТАТИЧЕСКОГО туннеля:

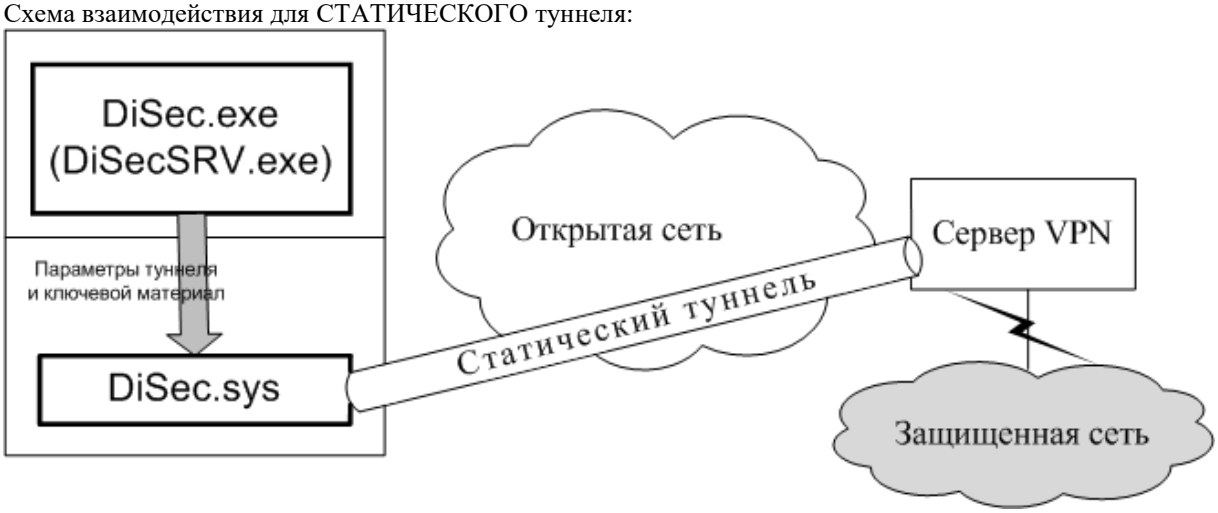


Рис. 3

Выполнение 1-го этапа осуществляется следующим образом для статических туннелей и для динамических туннелей.

2.2.1. Организация динамического туннеля

Для организации динамического туннеля на 1-м этапе выполняется передача запроса на подключение от пользователя DISEC к Серверу VPN, криптографическая аутентификация и авторизация пользователя и согласование параметров динамического туннеля (защищенного соединения) по протоколу ISAKMP (IKE).
Во время 1-го этапа выполняется следующая последовательность действий.

1) Пользователь DISEC устанавливает связь с IP-сетью стандартными для WINDOWS средствами.
2) Пользователь DISEC посылает запрос на подключение к Серверу VPN.

   Для динамического туннеля посылается запрос в соответствии с протоколом IKE версии 1.
3) Выполняется взаимная аутентификация.

   Выполняется обмен сообщениями для аутентификации и авторизации пользователя DISEC и установления SA IKE (Security Association IKE) - ассоциации безопасности, в рамках которой будет проводиться дальнейшее согласование туннеля с использованием зашифрованных сообщений.
4) Согласование параметров динамического туннеля и формирование ключевого материала.

Выполняется установление SA ESP (Security Association ESP) - ассоциации безопасности, в рамках которой вырабатывается ключевой материал на основе ключевой информации обеих сторон (пользователя DISEC и сервера VPN), передаваемый в драйвер для шифрования и расшифрования сетевых пакетов в туннеле.

5) В процессе согласования SA ESP определяются правила отбора (целевые объекты) для устанавливаемого туннеля.

6) Согласованные параметры работы туннеля, а также сформированный ключевой материал (крипто-материала) для зашифрования и расшифрования данных, загружаются в драйвер DiSec.

   На Сервер VPN посылается сообщение о готовности туннеля. На Сервере VPN активизируется динамический туннель. С этого момента IP-поток между компьютером с DISEC и Сервером VPN становится закрытым (зашифрованным).

   Примечание - Данные, для которых туннелирование не выполняется, могут либо передаваться без изменения, либо отбрасываться в зависимости от настроек DISEC.

7) Выполняется с заданной в настройках периодичностью обновление ключевого материала (рекиинг) по инициативе DISEC. Таким образом, выполняется обновление SA IKE и SA ESP с выработкой новых криптоключей защиты обмена сообщениями протокола IKE и нового крипто-материала для выполнения функций шифрования в туннеле.

2.2.2. Организация статического туннеля

Для статического туннеля согласования параметров не выполняется, DISEC загружает с ключевого носителя ключевую информацию, на базе которой формирует ключевой материал для зашифррования и расшифрвания данных туннеля, передает параметры туннеля и ключевой материал в драйвер и переходит в состояние готовности передачи и приема зашифрованного трафика.

При настройке параметров статического туннеля имеется возможность выбора протокола инкапсуляции («чистый» IP-in-IP или поверх него дополнительно – протокол UDP). Данные параметры должны соответствовать настройкам статического туннеля на сервере.

Также при настройке статического туннеля на стороне DISEC могут быть сформированы правила отбора в туннель.

2.2.3. Функционирование туннеля

После организации туннеля с Сервером VPN все приложения компьютера пользователя DISEC получают возможность работы с ресурсами сети, защищенными данным Сервером, в соответствии с установленными правилами отбора в туннель.

Пока туннель открыт, каждый IP-пакет анализируется на соответствие правилам отбора и подвергается соответствующей обработке (зашифровывается, если подпадает под разрешающие правила, и передается без изменения или отбрасывается в противном случае). Посредством правил отбора ограничивается состав ресурсов, обмен данными с которыми будет защищен криптографическими средствами. Параметры туннеля и правила доступа (правила отбора в туннель) можно просмотреть средствами приложения **DiSec**.

Во время работы туннеля его «жизнеспособность» может контролироваться или Сервером VPN, или DISEC, или тем и другим. Имеется возможность настройки параметров проверки жизнеспособности туннеля. Для статического туннеля имеется возможность установить значения интервала посылок, таймаутов ожидания ответа, порогового значений количества ошибок. Для динамического туннеля - установить интервала посылок, таймаутов ожидания ответа, порогового значений количества ошибок, назначить действие, которое выполняется при достижении порогового значения.

Одновременно с защищенными ресурсами пользователь DISEC может работать с открытыми ресурсами при соответствующей настройке (Режим блокировки открытых данных).

По окончании работы с защищенными ресурсами пользователь DISEC выполняет закрытие туннеля и отсоединение от Сервера VPN (Команда Отключиться).

Закрыть туннель может:

- сам пользователь DISEC по завершении работы с защищенными ресурсами;
- Сервер VPN при обнаружении разрыва соединения с клиентом,

- а также DISEC в результате контроля жизнеспособности туннеля или обнаружения ошибок драйвером.

В случае закрытия статического туннеля никакая информация или команда не передается взаимодействующей стороне, поэтому отсутствие туннеля может быть обнаружено только по отсутствию ответов на сообщения проверки жизнеспособности туннеля.
Имеется возможность восстановления туннеля после его разрыва при обнаружении нежизнеспособности туннеля, а также переход на следующее подключение в организованном заранее списке подключений.
После закрытия туннеля драйвер **DiSec** продолжает работать в «прозрачном» режиме.

2.3. Организация туннелей с несколькими Серверами VPN

Открытая сеть может содержать большое число Серверов VPN, каждый из которых защищает свою закрытую сеть.
Пользователь DISEC может настроить практически неограниченное число подключений.
Пользователь может запустить несколько (до 10) подключений одновременно, как статических, так и динамических.
Пользователь может также выполнить несколько защищенных соединений последовательно, то есть организовать **цикл**, в котором переход к следующему подключению будет выполняться автоматически после непредвиденного прекращения работы предыдущего. Выполнение всего цикла прекращается по команде пользователя, либо после выполнения заданного числа повторов.
В настройках можно задать количество попыток установления каждого подключения (это количество действует для каждого подключения в цикле).
При запуске подключения DISEC контролирует правила отбора в туннель и при их "пересечении", т.е. при возникновении ситуации, когда невозможно решить, в какой туннель следует направлять сетевые пакеты, новое подключение не выполняется.

2.4. Система криптозащиты в DISEC

ПО DISEC предназначено для обеспечения криптографической защиты данных, передаваемых в открытых каналах связи.
Средства криптографической защиты информации (СКЗИ) входят в состав драйвера, приложения и службы DiSecSRV.
В качестве основного элемента системы криптозащиты используется программный шифратор производства ООО «ФАКТОР-ТС», использующий алгоритмы шифрования ГОСТ 28147-89.
В процессе выполнения подключения к Серверу VPN (в процессе организации туннеля) приложение DiSec (или служба DiSecSrv) считывает с ключевого носителя ключевую информацию и выполняет инициализацию шифратора.

> *Примечание*. Выполняется программная проверка энтропии программного шифратора при каждой его инициализации, а также при выдаче случайной последовательности.

Режим организации СТАТИЧЕСКОГО туннеля использует симметричную ключевую систему - способ шифрования, в котором для шифрования и расшифрования применяется один и тот же криптографический ключ. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Распределение ключей шифрования производится заранее доверенным способом.
Режим организации ДИНАМИЧЕСКОГО туннеля использует несимметричную ключевую систему (пару открытый и закрытый ключ) на основе инфраструктуры открытых ключей PKI (Public Key Infrastructure). Для аутентификации пересылаемых открытых ключей используются сертификаты открытого ключа, соответствующие рекомендациям X.509. При этом открытый ключ передаётся по открытому каналу и используется для шифрования сообщений. Для расшифровки сообщений используется закрытый ключ.
Сертификат открытого ключа - это электронный документ, содержащий открытый ключ, информацию о владельце ключа, области применения ключа, подписанный выдавшим его Удостоверяющим центром (УЦ), и подтверждающий принадлежность открытого ключа владельцу. Формат сертификата открытого ключа X.509 v3 описан в **RFC 5280** (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile).
В процессе согласования SA IKE Сервер VPN и DISEC могут пересылать друг другу сертификаты (1-я фаза протокола IKE), либо должны иметь у себя оба сертификата, а также все данные для построения ЦЕПОЧКИ ДОВЕРИЯ - иерархии сертификатов, в которой каждый сертификат подписан закрытыми ключами тех сертификатов, которые находятся выше в цепочке сертификатов. Последний "самоподписанный"сертификат в цепочке называется **корневым** (Root certificate).
В процессе согласования SA IKE строится **Цепочка Доверия** для проверки локального сертификата и сертификата оппонента, при этом проверяется валидность каждого сертификата в цепочке. При проверке

используются специальные объекты, называемые "Список отозванных сертификатов" (COC или CRL - certificate revocation list).
CRL представляет собой список отозванных сертификатов с указанием времени. Он подписывается Удостоверяющим Центром и свободно распространяется через общедоступный репозиторий. В списке CRL каждый отозванный сертификат опознается по своему серийному номеру. Когда возникает необходимость в использовании сертификата, то проверяется не только подпись сертификата и срок его действия, но и просматривает последний из доступных списков CRL, проверяя, не отозван ли этот сертификат.
ПО DISEC предоставляет возможность автоматически актуализировать COC(CRL), выполняя обращение к серверам хранения для загрузки обновленного COC(CRL), а также выполнять оперативную проверку актуальности сертификата по протоколу OCSP (Online Certificate Status Protocol).

2.4.1. Ключевые носители

Пользователь DISEC должен иметь в своем распоряжении ключевой носитель с персональной ключевой информацией, на базе которой формируется ключевой материал для шифрования данных в туннеле.
В качестве ключевых носителей могут быть использованы любые носители, которые ОС WINDOWS может определить как съемные (дискета НГМД, съемный USB-носитель и.т.).
На ключевых носителях должна быть сформирована ключевая информация средствами генерации ключей.
В качестве ключевых носителей также могут использоваться устройства типа ТОКЕН, ключевая информация на которые записывается в формате PKCS11:

- **ruToken** производства компании Актив (тип «ruToken» и «ruToken S»);
- **ruToken** и **JaCarta** компании Aladdin.
- **eSMART** группы компаний ISBC.

ПО DISEC не выполняет установку ПО токенов, обеспечивающего функционирование этих устройств в ОС WINDOWS. Пользователю необходимо загрузить соответствующее ПО с сайта производителя и установить его до использования в ПО DISEC.
Список типов токенов и названия соответствующих библиотек производителя ПО помещено в файл **PKCS.ini**, входящий в состав ПО DISEC и расположенный в директории установки. При возникновении необходимости работы с другими типами токенов, следует дополнить файл **PKCS.ini** соответствующей информацией после установки нового ПО и протестировать возможность работы с ними.
Ключевые носители могут быть защищены паролем. Пароль сообщается пользователю при получении ключевых носителей от службы распределения ключей.
Хранение и использование ключевых носителей должно соответствовать ПРАВИЛАМ.

> *Примечание.* Ключевой носитель содержит секретную информацию. Пользователь ДОЛЖЕН обеспечить его надежное хранение. КАТЕГОРИЧЕСКИ запрещается модифицировать содержимое ключевого носителя. В то же время, на носителе не должна быть установлена защита от записи.

2.4.2. Состав ключевой информации

При работе с симметричной ключевой системой на ключевом носителе содержится сетевой набор ключей определенной серии. На ключевом носителе может быть несколько сетевых наборов, размещенных в разных директориях. В настройках подключения необходимо указать:

- директорию,
- номер серии ключей,
- номер ключа пользователя DISEC,
- номер ключа Сервера VPN (оппонента).

При работе с ключевой системой PKI пользователь DISEC должен получить на ключевом носителе свой закрытый ключ вместе с сертификатом открытого ключа (локальный сертификат).

Закрытый ключ (и необходимая для его использования информация) помещается на съемном ключевом носителе в так называемом «контейнере», расположенном в любой директории (для носителей типа USB-флеш и НГМД).

DISEC поддерживает формат «контейнера закрытого ключа» **PKCS#15 (РУС)** – расширение формата PKCS#15, разработанного в рамках работ, проводимых техническим комитетом по стандартизации

«Криптографическая защита информации» (ТК26), с целью обеспечения совместимости ключевых носителей разных разработчиков.

На ключевой носитель может быть помещен сертификат ключа пользователя.

Кроме того, при работе с ключевой системой PKI пользователь DISEC должен иметь:

- сертификаты открытых ключей всех Серверов VPN (оппонентов), с которыми предполагается устанавливать туннель,
- сертификаты всех соответствующих Удостоверяющих Центров (УЦ) - издателей как локального сертификата, так и сертификата оппонента,
- актуальные списки отозванных сертификатов CRL(СОС) для каждого УЦ.

Перечисленная выше информация может быть размещена на этом же ключевом носителе, в том числе, и на носителях типа ТОКЕН в формате PKCS11, либо на любом другом носителе, в том числе, и на несъемном. Исключение составляют сертификаты Корневых доверенных УЦ, которые должны размещаться на съемном ключевом носителе пользователя DISEC. Сертификаты и CRL Удостоверяющих Центров, составляющих "цепочку" подписавших сертификат пользователя или оппонента могут размещаться как в отдельных файлах (объекта - в случае токенов), так и в одном контейнере - файле с расширением "p7b", созданных средствами генерации ключей.

Ключевой носитель должен быть доступен для записи, поскольку в процессе настройки криптосистемы на него записывается необходимая для дальнейшей работы информация (см. раздел Настройка криптосистемы).

2.4.2.1. ТРЕБОВАНИЯ К КЛЮЧЕВОЙ ИНФОРМАЦИИ В ФОРМАТЕ PKCS11

PKCS #11 — один из стандартов семейства Public-Key Cryptography Standards (PKCS). Он определяет платформо-независимый программный интерфейс доступа к криптографическим устройствам (смарткартам, токенам).

ПО DISEC использует токены, указанные в разделе Ключевые носители и использует ключевую информацию в формате PKCS11, отвечающую следующим требованиям:

- Контейнер не защищен паролем, имеет приватную зону защищённую пин-кодом,
- закрытые ключи записаны в формате PKCS15 (один ключ в одном объекте P15), P15 всегда пишутся в приватную область,
- сертификаты пользователей, записанные в формате DER. Пишутся в публичную область.
- сертификаты промежуточных УЦ, записанные в формате DER. Пишутся в публичную область.
- корневые сертификаты УЦ, записанные в формате DER. Могут писаться как в приватную, так и в публичную области.
- CRL, записанные в формате DER. Пишутся в публичную область.
- nam-файлы. Пишутся в публичную область, имеют имя, совпадающее с именем объекта P15 (закрытого ключа) за исключением расширения. Расширение имени nam-файла должно быть - ".nam". Содержание объекта не имеет значения.

2.4.3. Средства генерации ключей для DISEC

Ключевые носители, необходимые для работы DISEC, готовятся в Центре управления ключевой системой, имеющем в своем составе средства генерации ключевой информации и изготовления ключевых носителей. Доставляются ключевые носители пользователю DISEC по надежному каналу связи.

Для генерации симметричных ключей и формирования ключевых носителей могут использоваться изделия производства ООО «ФАКТОР-ТС» - «Автоматизированное рабочее место генерации ключей АРМ ГК/КВ2» (НКБГ. 467369.865).
Для генерации несимметричных ключей и формирования ключевых носителей могут использоваться изделия производства ООО «ФАКТОР-ТС» - «Модуль генерации ключей» (НКБГ.501430.774) (создает контейнер в формате **PKCS#15(РУС))** совместно с программно-аппаратными средствами Удостоверяющего центра, поддерживающими формат сертификатов, соответствующий рекомендациям X.509.
В качестве средств генерации ключевой информации и формирования ключевых носителей могут использоваться другие изделия, сертифицированные установленным порядком и поддерживающие необходимые форматы.
В любом случае в ПО DISEC должны использоваться ключи, вырабатываемые криптографическим средством, сертифицированным ФСБ России по классу, не ниже класса криптографической защиты данного ПО.

2.4.4. Хранение и верификация сертификатов

При организации динамических туннелей IKE используются ассиметричные ключи шифрования в соответствии с инфраструктурой открытых ключей (PKI).
Для взаимной аутентификации используется ЭЦП, основанная на сертификатах открытых ключей взаимодействующих сторон. Во время формирования ЭЦП пользователя клиента, а также во время проверки ЭЦП оппонента строится цепочка доверия сертификатов.
Цепочка доверия состоит из проверенных (валидных) сертификатов издателей. Проверка в обязательном порядке включает проверку сертификата на отсутствие отзыва в результате утери доверия, т.е. на отсутствие в списках отзыва (CRL). Цепочка доверия завершается корневым (самоподписанным) сертификатом.
Списки отзыва формируются на удостоверяющих Центрах и размещаются или в центрах распространения. На момент настройки ресурса подключения, а также на момент выполнения процедуры подключения, Клиент DISEC должен иметь в своем распоряжении валидные сертификаты из обеих цепочек доверия - для своего (локального) сертификата и для сертификата оппонента и соответствующие им валидные CRL.

Примечание. При отсутствии валидных сертификатов пользователя DISEC или оппонента, либо при невозможности построения цепочек доверия подключение не будет установлено.

Списки отзыва обычно выпускаются с небольшим сроком действия. Поэтому они должны регулярно актуализироваться либо вручную (предоставляться администратором безопасности или лицом с аналогичными функциями), либо встроенными в ПО DISEC средствами.
Все сертификаты и списки CRL хранятся для каждого ресурса подключения отдельно от других ресурсов в двух видах хранилищ - локальном хранилище и хранилище корневых сертификатов. В локальном хранилище хранятся все перечисленные объекты, кроме корневых сертификатов, которые, соответственно, хранятся в хранилище корневых сертификатов. Хранилище корневых сертификатов может быть защищено имитовставкой. (рекомендуется), которая проверяется перед использованием объектов, хранящихся в нем (перед редактированием ресурса подключения или перед установкой подключения).

Примечание. При обнаружении несоответствия имитовставки подключение не будет установлено.

2.4.4.1. ОБНОВЛЕНИЕ СПИСКОВ CRL

Для каждого ресурса подключения может быт настроена процедура автоматического обновления списков CRL, а также обеспечивается возможность оповещения о скором окончании срока действия CRL.
Оповещение о скором окончании срока действия CRL выполняется в рамках периодической или инициированной пользователем DISEC процедуры проверки сертификатов Подключений.
Процедура автоматического обновления списков CRL входит в состав настройки параметров безопасности (Настройка PKI) ресурса подключения.

2.4.4.2. ПРОВЕРКА ПО ПРОТОКОЛУ OCSP

Для каждого ресурса подключения может быт настроена процедура проверки по протоколу **OCSP (Online Certificate Status Protocol**), которая выполняется в рамках периодической или инициированной пользователем DISEC процедуры проверки сертификатов Подключений.
Установка опций проверки по протоколу **OCSP** сертификатов, используемых в данном Подключении, выполняется при настройке крипто-параметров имеется возможность .

Протокол **OCSP** представляет собой Интернет протокол для проверки статуса X.509-сертификата (RFC 6960), используется как альтернатива или совместно с проверкой по CRL-спискам.

Протокол OCSP работает следующим образом: DISEC посылает запрос серверу, адрес (URI) которого указан в настройках В ответ он получает один из следующих вариантов OCSP-ответа:

- ***good*** - X.509-сертификат не отозван и не заблокирован.
- ***revoked*** - X.509-сертификат отозван.
- ***unknown*** - не удалось установить статус X.509-сертификата, так как серверу не известен издатель.

Эти OCSP-ответы позволяют пользователям узнать статус X.509-сертификата и определить возможность использования данного сертификата.

> *Примечание*. При проверке перед установкой подключения в случае получения отрицательного результата проверки по протоколу OCSP одного из сертификатов, участвующих в процедуре, в том числе, при отсутствии доступа к серверу OCSP, подключение не будет установлено. При проверке после установки подключения - подключение будет разорвано.

3 Условия применения ПО DISEC

ПО DISEC обеспечивает выполнение решаемых им задач при выполнении требований данного документа.

Ниже приведены требования:

- к оборудованию компьютера пользователя DISEC (раздел Требования к оборудованию),
- к операционной среде - настройке программных компонентов ОС WINDOWS (раздел Требования к программному окружению) и программных средств, работающих под ее управлением.к программно-аппаратным средствам подключения к сети Интернет (раздел Сетевое окружение и подключение к сети Интернет),
- к настройкам Сервера VPN (раздел Настройки на Сервере VPN),
- к ключевой информации (раздел Требования к ключевой информации).

3.1. Требования к оборудованию

ПО DISEC устанавливается на компьютер, функционирующий под управлением 64-разрядных версий операционных систем Microsoft:

- Microsoft Windows Server 2016,
- Microsoft Windows 10.

DISEC функционирует на сетевых интерфейсах типа Ethernet, интерфейсе беспроводной связи Wi-Fi, а также через модем "обычной" телефонной линии и широкополосные адаптеры мобильной связи GSM (модем Mobile Broadband), USB-модемы операторов мобильных телефонных сетей.
Компьютер должен быть оснащен устройством для считывания ключевых носителей (USB-порт).

3.2. Требования к программному окружению

Настройки ОС WINDOWS должны быть произведены в соответствии с ПРАВИЛАМИ безопасности, регулируемыми соответствующими службами организации, использующей данное ПО.
Требуется выполнять регулярное обновление ОС WINDOWS, а также программного обеспечения (драйверов) сетевых плат Ethernet, адаптеров и модемов.
Для работы с ключевыми носителями типа ТОКЕН должно быть установлено программное обеспечение (драйверы) разработчика токенов.

3.3. Сетевое окружение и подключение к сети Интернет

Компьютер пользователя DISEC может располагаться внутри локальных сетей любого типа, поддерживающих IP-протокол версии 4 (IPv4) и 6 (IPv6), и иметь подключение к открытой IP-сети любым доступным способом посредством выделенного, коммутируемого, беспроводного и т.п. соединения, а также VPN-соединения.
Локальная сеть, в которой размещается компьютер пользователя ПО DISEC, может быть как однородной, так и сегментированной, или же состоять из единственного компьютера.
Коммуникационное оборудование и средства межсетевого экранирования должны пропускать для СТАТИЧЕСКОГО туннеля:

- UDP-пакеты с портами, установленными в настройках подключения (портом источника и портом назначения для исходящего),
- туннелированные пакеты (протокол IP in IP - номер 4) в случае отсутствия UDP-инкапсуляции.

Для ДИНАМИЧЕСКОГО туннеля:

- UDP-пакеты с портом 500 и 4500 (портом источника а и портом назначения для исходящего),
- туннелированные пакеты (протокол ESP - номер 50).

3.4. Требования к ключевой информации и средствам аутентификации

При использовании симметричной ключевой системы для аутентификации взаимодействующих сторон используется ключевая информация на ключевых носителях. Для них должны выполняться следующие требования:

- ключи взаимодействующих сторон должны быть сформированы одним средством генерации ключей;

- ключевая информация на DISEC и на Сервере VPN (оппонента) должна иметь одну и ту же серию.

При использовании асимметричной ключевой системы (PKI) должны выполняться следующие требования:

1. Для ключевой информации и средств аутентификации пользователя DISEC:
   - ключевая информация (закрытый ключ в формате PKCS15) должна соответствовать сертификату пользователя;
   - сертификат пользователя должен быть выпущен Удостоверяющим Центром в формате x.509 и быть актуальным (действующим) на момент использования.
   - Поле «Key Usage» сертификата пользователя должно содержать свойства **Digital Signature** и **Non-Repudiation**.
   - Поле «Enhanced Key Usage» сертификата должно содержать OID 1.3.6.1.5.5.8.2.2 (IKE-посредник IP-безопасности);
   - сертификат должен быть подписан Доверенным УЦ, который должен либо быть "самоподписанным" (корневым), либо в свою очередь подписан следующим Доверенным УЦ. Вся цепочка УЦ должна заканчиваться подписью доверенного корневого УЦ и иметься в распоряжении пользователя во время настройки ресурсов подключения.
   - для каждого УЦ в распоряжении пользователя или лица, отвечающего за настройку ресурсов подключения,должен присутствовать актуальный CRL - список отзыва сертификата.
2. Для средств аутентификации оппонента:
   - в распоряжении пользователя или лица, отвечающего за настройку ресурсов подключения, должен находиться сертификат оппонента и все сертификаты и CRL из цепочки подписавших его УЦ. При настройках может использоваться только сертификат УЦ (без указания конкретного сертификата пользователя). В этом случае в процессе выполнения переговоров IKE может быть использован любой сертификат, изданный указанным УЦ, кроме самого сертификата УЦ.

Формат ключевых носителей должен соответствовать требованиям, приведенным в Ключевые носители.

3.5. Настройка туннелей на Сервере VPN

Для того чтобы пользователь DISEC мог организовать туннель, на Сервере VPN должны быть выполнены необходимые настройки. Эти настройки зависят от топологии сети, от требований, предъявляемых к криптографическим и технологическим параметрам туннелей, и т.п.

Ниже (раздел Настройки на Сервере VPN для организации статического туннеля) приведена типовая настройка Сервера VPN для организации СТАТИЧЕСКОГО туннеля.

В разделе Настройки на Сервере VPN для организации динамического туннеля приведена настройка Сервера VPN для организации ДИНАМИЧЕСКОГО туннеля на примере настройки криптомаршрутизатора «ПАК Dionis-NX».

3.5.1. Настройки на Сервере VPN для организации статического туннеля

Для обеспечения возможности организации ***статического*** туннеля на Сервере VPN должны быть выполнены следующие настройки.

1. При использование UDP-инкапсуляции должно быть разрешено прохождение входящих пакетов протокола UDP с портом назначения и исходящих пакетов с портом источника; значение портов совпадает со значением соответствующих портов UDP-инкапсуляции.
2. В случае если UDP-инкапсуляция не используется должно быть разрешено прохождение сетевых пакетов с транспортным протоколом "IP in IP" - номер протокола 4.
3. Должен быть организован статический туннель для IP-адреса компьютера пользователя DISEC.
4. Статический туннель должен быть настроен на загруженные ключи шифрования.
5. Пользователю DISEC должен быть передан идентификатор статического туннеля и номер ключа удаленного конца туннеля.
6. Пользователю DISEC также должны быть известны список доступных ресурсов (для настройки правил отбора в туннель) и опции инкапсуляции трафика (протокол - IP-in-IP или UDP вместе с номерами портов UDP-инкапсуляции).

3.5.2. Настройки на Сервере VPN для организации динамического туннеля

Для обеспечения возможности организации динамического туннеля IPSEC необходимо на Сервере VPN выполнить настройку криптосистемы, системы Crypto IKE, в рамках которой настроить одно или несколько IPSEC-соединений (connection).

ПО DISEC предъявляет следующие требования к настройкам IPSEC-соединений на Сервере VPN:

- Назначить согласованные параметры крипто алгоритмов для фазы 1 (SAIKE) и фазы 2 (SAESP), либо позволить ПО DISEC выбирать эти параметры (режим "no strict");
- Отключить инициирование пересогласования (рекиинг) как SAIKE (Фаза 1 IKE), так и SAESP (Фаза 2 IKE);
- Согласовать параметры времени жизни обеих SA таким образом, чтобы сами значения времени жизни в ПО DISEC были меньше, чем значения на Сервере VPN.

Состав и формат команд на Сервере VPN для выполнения этих настроек приведен в документации «ПАК Dionis-NX».

3.6. Подготовка и порядок работы с DISEC

ПО DISEC защищено от несанкционированного использования. Для его использования необходимо иметь Регистрационный ключ. Регистрационный ключ позволяет запускать ПО DISEC на одном компьютере либо в течение ограниченного периода времени (ознакомительный период), либо неограниченно по времени. При этом допускается обновление версии ПО без перерегистрации.
При переходе на другой компьютер следует выполнить "Разрегистрацию" на данном компьютере и заново выполнить регистрацию на новом.
Перед началом выполнения процедуры настройки Ресурсов подключений пользователю DISEC следует выполнить подготовительные действия, получить ВСЮ необходимую для этого информацию о настройках Сервера VPN и получить персональную ключевую информацию на съемном носителе.

3.6.1. Подготовка к работе в режиме статического туннеля

Для организации туннеля пользователь DISEC должен иметь информацию, необходимую для подключения к Серверу VPN:

- Сетевой IP-адрес (IPv4 или IPv6) или доменное имя Сервера VPN в сети Интернет. IP-адрес должен соответствовать адресу, по которому он доступен компьютеру пользователя DISEC;
- Получить из Центра управления ключевой системой или от ответственного лица организации персональный ключевой носитель и необходимую информацию о нем (номер и серия ключа, и, возможно, пароль или ПИН-код).

Для настройки туннеля пользователь DISEC должен знать:

- **идентификатор** (номер) статического туннеля;
- **криптономер** ключа сервера VPN из той же серии, что и ключ пользователя;
- **метод инкапсуляции** трафика (применение UDP-инкапсуляции и ее параметры - порты);
- **IP-адреса** доступных защищенных ресурсов, а возможно разрешенный протокол и диапазон портов прикладного протокола типа TCP или UDP (правила отбора).

3.6.2. Подготовка к работе в режиме динамического туннеля

Для организации туннелей надо предварительно выполнить следующее.

1) Получить из Центра управления ключевой системой или от ответственного лица организации свой **закрытый ключ**, свой **сертификат**, всю цепочку сертификатов доверенных УЦ, вплоть до корневого, и действующий список отозванных сертификатов этих УЦ. Все полученные сертификаты и списки должны быть помещены в соответствующие хранилища DISEC (см. Работа с хранилищами).

2) Получить от администратора Сервера VPN следующие данные:

- IP-адрес в формате IPv4 (формат IPv6 не поддерживается протоколом IKE v1) или доменное имя Сервера VPN, с которым будет устанавливаться туннель;
- IP-адреса доступных защищенных ресурсов. В случае настройки IPSEC-соединения на сервере, обеспечивающей выдачу IP-адреса клиента, DNS-серверов и IP-адреса подсети (режим MODE_CONFIG), эта информация не требуется.

3) Получить от службы безопасности организации или от ответственного лица:

- сертификаты всех Серверов VPN, с которыми предполагается устанавливать туннель;
- сертификаты всех УЦ и списки отозванных сертификатов, необходимые для корректного построения цепочек доверия для сертификатов Серверов VPN.

Примечание. Сертификаты доверенных УЦ присылаются на DISEC по доверенному каналу связи, остальные - произвольным способом.

Для организации туннелей требуется, чтобы значения перечисленных ниже крипто-параметров на DISEC соответствовали значениям соответствующих параметров на Сервере VPN:

- узел замены (алгоритм ГОСТ 28147-89), используемый для шифрования протокола IKE (необязательно в случае использования политики "**no strict**");
- параметры алгоритма ГОСТ Р 3410-2001, используемые для выработки сессионного ключа фазы 1 протокола IKE (необязательно в случае использования политики "**no strict**");
- параметры алгоритма ГОСТ Р 3410-2001, используемые для выработки общего секрета фазы 2 протокола IKE в режиме PFS (необязательно в случае использования политики "**no strict**");
- узел замены (алгоритм ГОСТ 28147-89), используемый для шифрования данных в протоколе ESP (необязательно в случае использования политики "**no strict**");
- преобразование ESP - туннельное или транспортное;
- режим ***Perfect Forward Secrecy*** (PFS);
- для устойчивости соединения необходимо, чтобы значения времен жизни 1-й и 2-й фазы протокола IKE соответствовали требованиям.

3.6.3. Порядок работы с DISEC

Для работы с DISEC необходимо выполнить следующие действия.

1. Инсталлировать ПО DISEC.
2. После выполнения перезагрузки WINDOWS запустить приложение **DiSec** .
3. При необходимости запросить, а затем ввести ввести Ключ регистрации (соответствующий номеру лицензии на данное ПО).
4. Сообщить ПО DISEC все необходимые данные, для чего выполнить команду **Настройка** из Главного меню приложения и заполнить список **Подключения (ресурсы подключения)** .
5. Штатными средствами WINDOWS (или средствами, предоставленными провайдером услуг доступа в сеть Интернет) выполнить подключение к IP-сети.
6. Подсоединить ключевой носитель.
7. Дать команду **Подключиться** из Главного меню приложения и, выбрав необходимый ресурс (ресурсы) из списка, отправить ему запрос для подключения к Серверу VPN.
8. После успешного тестирования подключения возможно назначение его (или всего списка) для автоматического запуска при запуске ОС WINDOWS .

4 Инсталляция и деинсталляция DISEC

В результате инсталляции ПО DISEC на компьютере будут установлены все основные и служебные программы, а также документация.
В результате деинсталляции - удалены все основные и служебные программы, а также документация. Настройки пользователя (ресурсы подключений и другие) остаются.
При переходе с одной версии на другую состав и место хранения настроек может меняться, поэтому рекомендуется каким-либо способом сохранить основные параметры (например, при помощи экспорта в файл), а после инсталляции новой версии - выполнить настройки заново, используя сохраненные в качестве справочного материала.

Примечание. При переходе на новую версию строго не рекомендуется использовать процедуру импорта.

4.1. Комплект поставки DISEC

Изделие ПО DISEC поставляется в виде дистрибутивного пакета на одном носителе (компакт-диске). В комплект поставки входят следующие компоненты:

- **DiSecSetup.exe** - программа установки DISEC, обеспечивающая установку всех компонент ПО;
- данный документ (Руководство пользователя).

Дистрибутивный пакет сопровождается обязательным документом на бумажном носителе «Клиент Криптографического сервера доступа «DiSec». Формуляр. НКБГ.501430.734ФО».

4.2. Процедура инсталляции ПО DISEC

Для инсталляции ПО DISEC пользователь должен обладать правами администратора ОС WINDOWS.
Если на компьютере пользователя уже установлено ПО DISEC, то перед установкой новой версии рекомендуется предыдущую версию деинсталлировать.
Инсталляция выполняется запуском программы **DiSecSetup.exe** с дистрибутивного носителя.
Перед началом инсталляции будет выполнена проверка наличия установленного, необходимого для функционирования ПО DISEC системного программного обеспечения.Net Framework фирмы Microsoft, и при его отсутствии откроется окно текущего Интернет браузера на странице загрузки данного системного ПО.
На дистрибутивном носителе имеется предлагаемая для установки версия .Net Framework фирмы Microsoft, которой можно воспользоваться, например, при отсутствии по какой-либо причине доступа в Интернет или к сайту Microsoft.
Начинается установка с предупреждающего сообщения о необходимости деинсталлировать предыдущую версию DISEC и возможной несовместимости DISEC с другими программами.

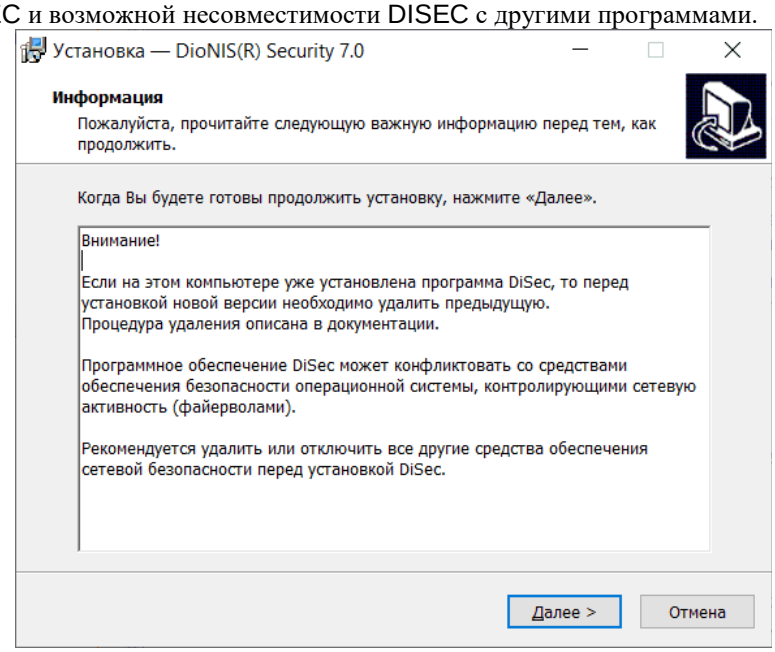


Рис. 4

Далее программа установки выведет на экран окно с полученной от пользователя информацией для инсталляции и после нажатия кнопки **Установить** выполнит разархивирование и копирование файлов с дистрибутивного носителя в стандартную папку:
<системный_диск>:**Program Files\Factor-TS\DioNIS Security**.
Будет выдано сообщение системной службы безопасности, запрашивающее разрешение на установку драйвера DiSec.

Рис. 5

Рекомендуется установить флажок **Always trust software from "OOO Factor-TS"**. По завершении установки драйвера выдается окно с сообщением:

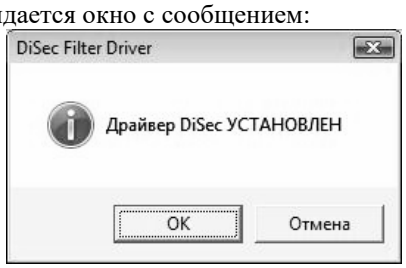


Рис. 6

Перед окончанием инсталляции будет выдано сообщение о взаимодействии со средствами защиты от несанкционированной установки программных компонентов.

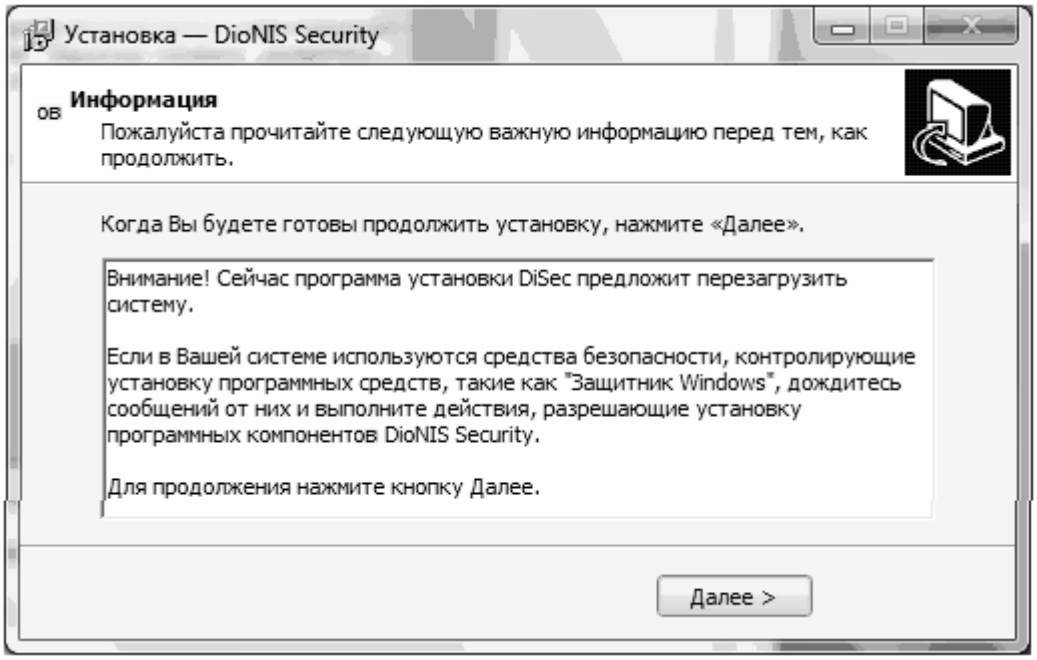


Рис. 7

По окончании инсталляции будет предложено перезагрузить компьютер.

> *Примечание*. Перезагрузку выполнить **необходимо**, поскольку в процессе перезагрузки выполняются действия по регистрации (формировании записей в системном реестре) сетевых адаптеров драйвером DiSec.

После перезагрузки необходимо войти в систему и выполнить настройку DISEC. После перезагрузки компьютера на рабочих столах всех пользователей ОС WINDOWS появится ярлык вызова приложения DiSec.
В стартовых системных меню всех пользователей компьютера появится программная папка **FACTOR Applications\DioNIS Security**, в которой помещены:

- ярлык для запуска приложения DiSec,

- ярлык программы деинсталляции DISEC,
- ярлык служебной программы проверки контрольных сумм **Контрольные суммы,**
- ярлык программы Лицензирование, позволяющий отправить запрос на получении лицензии, необходимой для запуска DISEC.
- ярлык вспомогательной программы "Состояние системы" для сбора и отправки информации о компьютере пользователя в Службу поддержки для диагностирования ошибочной ситуации..

В этой же папке находятся:

- ярлыки программ для работы со службой DiSecSrv (настройка, запуск и останов службы);
- ярлыки программ для работы со службой DiSecAgent (запуск и останов службы);
- ярлыки программ для работы с драйвером DiSec (инсталляция, настройка и деинсталляция);
- **Документация**.

  Примечание. Если в процессе инсталляции основного ПО процедура установки драйвера DiSec завершилась неудачей, например, было получено сообщение о необходимости перезагрузки (**NEED REBOOT**), то после перезагрузки необходимо выполнить установку драйвера вручную по команде из программной папки **DioNIS Security**.

При последующих включениях или перезагрузке компьютера драйвер DiSec будет автоматически запускаться каждый раз при старте операционной системы и функционировать в «прозрачном» режиме до загрузки в драйвер DiSec параметров туннеля, т.е. драйвер будет пропускать все пакеты по всем сетевым интерфейсам, имеющимся в системе, не выполняя никаких преобразований.

4.3. Проверка контрольных сумм

Для проверки служит программа **Контрольные суммы** и список файлов программного обеспечения, подлежащих проверке. При инсталляции DISEC программа **Контрольные суммы** помещена в той же папке, что и сама система (**<**системный диск**>\Program Files\Factor-TS\DioNIS Security**).

Список файлов программного обеспечения, подлежащих обязательной проверке, вместе с эталонными значениями контрольных сумм приведен в документах «СКЗИ «Клиент криптографического сервера доступа «DiSec» Правила пользования».

Перед первым запуском DISEC для проверки целостности полученного программного обеспечения: пользователь должен запустить программу **Контрольные суммы**:

Пуск ⇨ Программы ⇨ FACTOR Applications ⇨ Контрольные суммы.

Программа **Контрольные суммы** вычислит контрольные суммы для файлов, приведенных в списке, сравнит их с эталонными значениями и выведет на экран вместе со значениями контрольных сумм.

При первом включении DISEC пользователь должен визуально убедиться в идентичности значений контрольных сумм, выведенных на экран, и контрольных сумм, содержащихся в Правилах пользования.

При совпадении сумм программа выдаст сообщение, что контрольные суммы проверены успешно.

При несовпадении программа укажет файл, для которого имеет место ошибка контрольной суммы. В этом случае необходимо удалить установленное программное обеспечение.

В дальнейшем контроль целостности ПО будет проводиться с периодичностью, заданной в настройках программы. Периодичность проверки зависит от условий эксплуатации и определяется политикой безопасности эксплуатирующей организации. Периодический контроль выполняется автоматически, если приложение DiSec запущено. Если приложение DiSec не запущено, то проверка выполнится при его запуске.

4.4. Деинсталляция DISEC

Для выполнения удаления (деинсталляции) DISEC необходимо обладать повышенными правами администратора WINDOWS.

При необходимости перед удалением ПО DISEC можно сохранить **Журналы событий**, которые находятся в поддиректории **Logs** программной директории **DiSec** («**<системный диск>:\Program Files\Factor-TS\Dionis Security\Logs**»).

Для того чтобы полностью удалить DISEC с компьютера, рекомендуется выполнить следующие действия:

- запустить приложение DiSec (если оно не запущено);
- отключить все активные подключения, если они были установлены;
- запустить программу **Драйвер DiSec-настройка**, снять флажок "**Разрешить запись протокола**";

- из **Главного меню** приложения DiSec выполнить команду **Выход** (выйти из приложения).

Удаление DISEC выполняется командой **Деинсталляция DiSec** из папки **FACTOR Applications** стартового системного меню.

В процессе деинсталляции DISEC выполняются следующие процедуры:

- останов и деинсталляция службы DiSecSrv;
- останов и деинсталляция службы DiSecAgent;
- удаление драйвера DiSec,
- удаление приложения DiSec и всех ее компонентов, а также служебных программ.

Если одно из рекомендованных ранее для полного удаления DISEC действий не было выполнено, то некоторые файлы могут быть не удалены, поэтому будет предложено выполнить перезагрузку системы для продолжения процедуры.

После перезагрузки будут удалены не удаленные ранее файлы и директории.

При необходимости следует удалить вручную ветки реестра, созданные при инсталляции ПО DISEC (для этого требуются повышенные права администратора Windows):

- "***HKCU/Software/Factor-TS***" - настройки пользователей, работавших с ПО DISEC;
- "***HKLM/Software/Factor-TS***" - настройки службы.

5 Режимы работы ПО DISEC

В данном разделе описаны различные режимы работы ПО DISEC, а именно:

- доступ различных категорий пользователей ОС WINDOWS к выполнению различных задач в рамках настройки, использования и обслуживания DISEC;
- возможность использования ПО различными пользователями ОС WINDOWS компьютера независимо друг от друга в режиме работы с приложением DiSec;
- работа в режиме службы WINDOWS.

5.1. Пользователи ПО DISEC

ПО DISEC позволяет выполнять большинство задач различным категориям пользователей ОС WINDOWS с различными правами доступа к программным ресурсам и функциям системы.
Для выполнения основной задачи - работы по организации туннеля и обмена информацией с защищенными сетевыми ресурсами - не требуется особых прав доступа, однако для выполнения некоторых «вспомогательных» задач необходимо обладать административными правами в операционной системе WINDOWS. Под административными правами понимается вхождение пользователя в системную группу Администраторы (**`Administrators`**), необходимо обладать «повышенными» (**`elevated`**) административными правами, далее по тексту такого пользователя будем называть ***привилегированным***.
К работам, которые должны выполняться ***привилегированным*** пользователем относятся:

- инсталляция и деинсталляция всего ПО или его части (службы, драйвера),
- настройка режимов работы **драйвера**, включая настройку режимов протоколирования сети,
- настройка службы DiSecSrv**,** а также ее запуск и останов.
- импорт конфигурации DISEC из файла конфигурации.

При инициировании соответствующих операций будет выдан запрос на авторизацию выполнения этих действий в системе.
После инсталляции DISEC любой пользователь данного компьютера, в том числе не ***привилегированный***, может его использовать. В процессе настройки DISEC для каждого пользователя создаются индивидуальные параметры работы DISEC. Индивидуальные параметры работы создаются посредством команд приложения DiSec, хранятся в разделе системного реестра WINDOWS для каждого пользователя и недоступны для изменения неавторизованным пользователем.
Проверка контрольных сумм не требует наличия у пользователя ***привилегированных*** прав.
Запуск службы DiSecSrv выполняется либо от имени одного «выделенного» пользователя, имеющего соответствующие права (право входа в систему в качестве службы), либо, как правило, от имени системной учетной записи LOCAL SYSTEM. Рекомендуется использовать второй способ.

5.2. Работа с приложением DISEC

Приложение DiSec позволяет настраивать ресурсы подключения для текущего пользователя и для службы DiSecSRV, выполнять запуск этих подключений, а также выполнять настройку работы программы и драйвера для получения дополнительной диагностической информации, необходимой для решения проблем.

5.2.1. Получение Ключа Регистрации

После установки ПО DISEC и перезагрузки компьютера (как это требуется в процедуре инсталляции) на рабочем столе каждого пользователя WINDOWS появляется ярлык программы для запуска приложения DiSec.
ПО DISEC защищено от несанкционированного копирования, т.е. для каждой ее инсталляции на отдельном устройстве необходимо получить ключ регистрации от фирмы-разработчика или дистрибьютера.
При первом запуске приложения DiSec с помощью ярлыка программы или посредством команды стартового системного меню: **`Пуск ⇨ Программы ⇨ DioNIS Security ⇨ DiSec`** на экран будет выдано окно, содержащий номер сформированной для данного устройства лицензии.

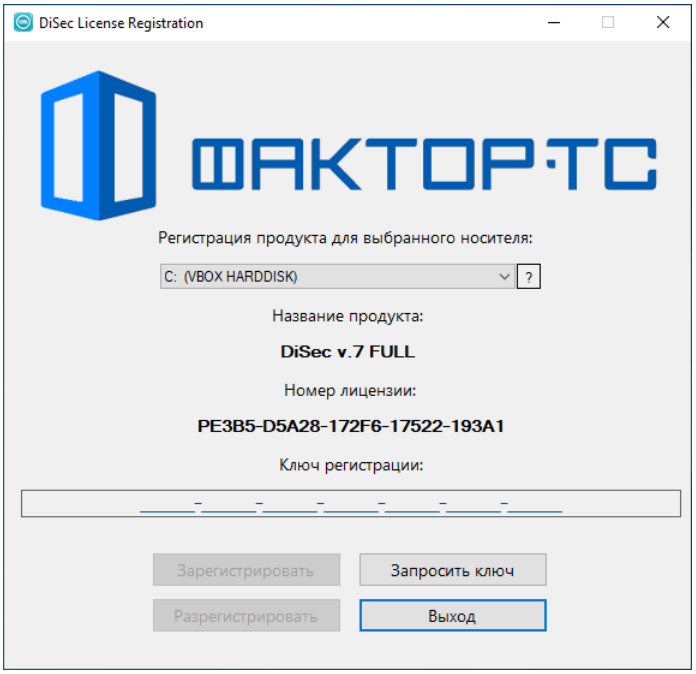


Рис. 8

Необходимо нажать кнопку Запросить ключ. При этом на экран будет выдана следующая форма.

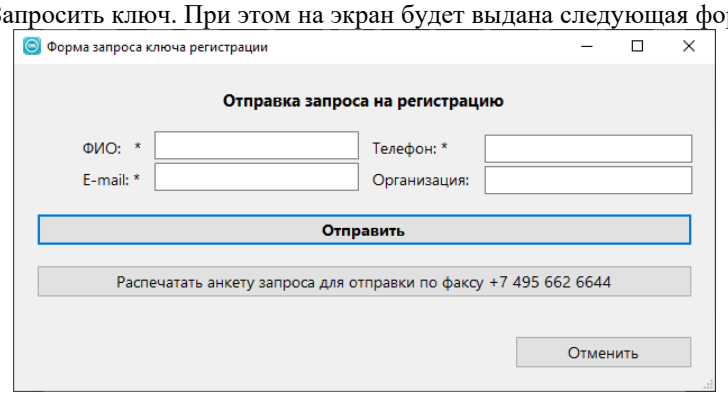


Рис. 9

Следует заполнить все поля и выполнить отправку запроса одним из предлагаемых способов.
Получив от фирмы-разработчика ответ с регистрационным ключом, следует снова запустить приложение DiSec, ввести ключ в соответствующее поле и нажать ставшую активной кнопку **Зарегистрировать**.

5.2.2. Запуск приложения и индикация состояния

После успешной регистрации ПО DISEC при последующих запусках приложение успешно запустится, и на панели задач рабочего стола пользователя в области уведомлений (SYSTEM TRAY) появится значок программы , который служит признаком того, что приложение активно.
Значок отображает состояние компонентов DISEC: зеленый цвет значка ( ) означает наличие туннеля, белый - его отсутствие. Значок означает, что работают несколько туннелей одновременно.
Наличие фона (оранжевого цвета) показывает, что инициатором установки туннеля была служба DiSecSrv, означает, что работают несколько туннелей одновременно, один из которых запускается службой.
Отсутствие значка означает, что приложение не запущено, и его необходимо запустить.

> *Примечание*. Обычно значки в системной области уведомлений скрываются системой после непродолжительного периода времени после их появления. Рекомендуется перевести значок DiSec в режим показа значка и уведомлений.

При постоянном использовании DISEC рекомендуется установить режим автоматического запуска приложения при старте операционной системы, в противном случае флажок автоматического запуска следует снять.
При постоянной работе с какими-либо ресурсами (подключениями) рекомендуется выполнить настройку автоматического установления соединения при запуске приложения. В этом случае после входа в систему пользователь сразу сможет работать с соответствующими защищенными ресурсами.
В процессе работы приложения DiSec и выполнения ее команд ведется журнал событий, таких как:

- запуск и останов приложения, при этом фиксируется имя текущего пользователя.
- основные события работы службы,
- сообщения, выдаваемые в процессе установления и отключения соединения с Сервером VPN,
- сообщения о результатах изменения параметров сетевых интерфейсов, выполняемых при установке и снятии туннелей,
- сообщения об системных событиях, получаемых от ОС.

Журнал событий можно просмотреть при помощи соответствующей команды **Главного меню** приложения DiSec.
В целях безопасности при переключении пользователя ОС WINDOWS без перезагрузки компьютера посредством системной команды смены пользователя (**`Fast User Switching - FUS`**) или выхода и последующего входа в систему (**`Logoff/Logon`**) выполняется отключение установленных Подключений для предотвращения их несанкционированного использования, а также выход из Приложения DiSec, для обеспечения возможности работы вошедшего в системы пользователя.

> *Примечание*. Приложение DiSec не является многопользовательской программой, и в каждый момент возможна работа только одного пользователя.

При переходе компьютера в «спящий» режим туннель не отключается, более того, при наличии активного туннеля заблокирован переход компьютера в этот режим, и, как следствие, заблокировано отключение от интернета для мобильных устройств (планшетов). Дисплей может выключаться при соответствующей настройке энергосбережения.

5.2.3. Команды приложения DiSec

Работа с приложением DiSec выполняется посредством команд **Главного меню** приложения. Для вывода на экран **Главного меню** приложения необходимо кликнуть правой кнопкой «мыши» на значке запущенной программы  , расположенном на панели задач рабочего стола в области уведомлений (SYSTEM TRAY).

Команды **Главного меню** приложения служат для выполнения следующих действий:

- настройка всех компонентов DISEC;
- подключение (и отключение) к одной или нескольким защищенным сетям в соответствии с этими настройками;
- анализ состояния сетевых компонентов и подключений;
- анализ диагностической информации как текущей (команда **`Диагностика`**), так и долговременной, хранящейся в журналах и протоколе сети;
- получение справочной информации, касающейся всех этих действий;
- получение информации о текущей версии программы.

По команде **`Подключиться`** выполняется процедура подключения к одному или нескольким выбранным из списка ресурсов. Команда **`Подключиться`** также активизируется при двойном щелчке мышью на значке в системной области. Действия, выполняемые при этом, зависят от типа туннеля и режима его организации.
По команде **`Отключиться`** выполняется разъединение с выбранным из списка активных подключений. Команда доступна только при наличии активных подключений (Организация туннелей с несколькими Серверами VPN). Если одновременно установлены несколько подключений, то при наведении курсора мыши на команду **`Отключиться`** выдается список, из которого можно выбрать одно или ВСЕ подключения. Действия, выполняемые при активизации команды, зависят от типа подключения и режима его организации.

`Команда Состояние` позволяет просмотреть текущее состояние параметров работы драйвера DiSec, в том числе, информацию об установленных туннелях и статистические данные по сетевым интерфейсам, а также информацию об активных подключениях приложения DiSec.
`Команда Настройка` обеспечивает выполнение следующих функций:

- установка основных параметров всех составляющих системы - драйвера DiSec, приложения DiSec и службы DiSecSrv;
- настройка реквизитов подключения к защищенным сетям для приложения и службы;
- задание параметров ведения журналов работы ПО DISEC;
- задание параметров ведения протокола сети;
- настройка выполнения периодических заданий;
- выполнение разовых работ (вкладка **Обслуживание**).

Выполнение команды **Настройка** может быть защищено паролем. Он задается (опционально) при первом выполнении команды, в дальнейшем при вызове команды, если пароль был задан, выполняется запрос на ввод пароля. При неуспешном вводе пароля окно не открывается.

Команда Журналы позволяет просмотреть на экране журнал работы приложения DiSec, журнал работы службы DiSecSrv и журнал вспомогательной службы DiSecAgent.

Команда Диагностика служит для просмотра накопленных во время сеанса работы DISEC диагностических сообщений, которые выдает приложение DiSec при подключении к Серверу VPN.

Примечание. Отображается объем информации размером не более одного мегабайта.

При просмотре диагностической информации предоставляется возможность прокрутки текста в обоих направлениях, поиск фрагмента текста в обоих направлениях, а также возможность сохранения информации в файле для последующего анализа после возникновения ошибочных ситуаций.

Команда Протокол сети позволяет просмотреть на экране файл, содержащий протокол работы сети - заданную при настройке информацию о проходящих через драйвер DiSec сетевых пакетах.

Команда Справка позволяет получить полную справочную информацию по работе с DISEC.

Команда О программе позволяет получить информацию о составе и версиях компонентов ПО DISEC.

Команда Выход позволяет завершить работу с приложением DiSec. Данная команда используется при удалении ПО DiSec с компьютера, а также при работе в режиме ручного запуска приложения. Команда недоступна при открытом **окне Настройка**.

Примечание. Если туннель был организован посредством службы DiSecSrv, то он продолжает функционировать. Протоколирование сети продолжается, если оно задано в настройках.

5.3. Работа в режиме службы WINDOWS

Клиент криптографического доступа DISEC может работать в режиме службы WINDOWS. Данный режим позволяет организовывать одно или несколько подключений автоматически при старте WINDOWS, в результате можно выполнить авторизацию пользователя WINDOWS на контроллерах домена WINDOWS, размещенных во внутренней защищенной сети и не имеющих доступа из открытой IP-сети (сеть Интернет).

Для работы в режиме службы необходимо выполнить настройку службы DiSecSrv, вызвав соответствующую команду стартового меню или выполнив ее вызов с **вкладки Обслуживание** окна **Настройка**.

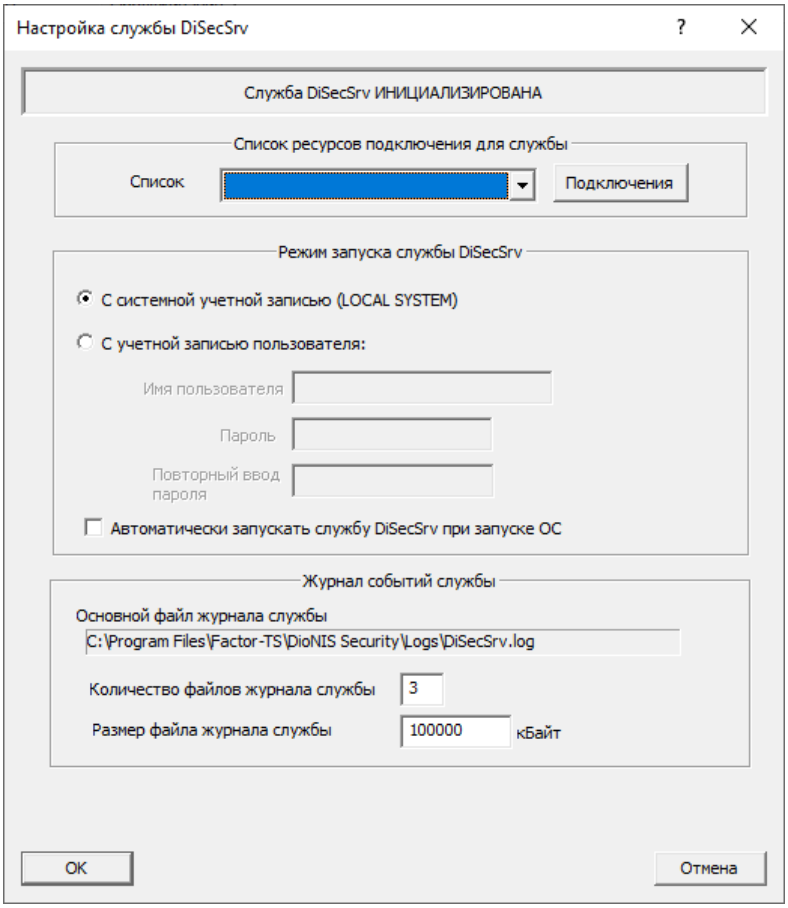


Рис. 10

Служба DiSecSrv может выполняться либо от имени системы (LOCAL SYSTEM), либо от имени специально организованного пользователя. В последнем случае администратор WINDOWS должен выполнить следующие действия:

- создать учетную запись, назначить ей пароль (рекомендуется снять ограничения на время действия пароля);
- назначить административные права (включить в группу Администраторы);
- разрешить вход в качестве службы.

Для разрешения пользователю входа в качестве службы необходимо выполнить следующую последовательность действий:

меню Пуск ⇨ Панель управления ⇨ Администрирование ⇨ Локальная политика безопасности ⇨ Локальные политики ⇨ Назначение прав пользователя ⇨ Вход в качестве службы.

В открывшемся окне нажать кнопку **Добавить** пользователя или группу и ввести имя пользователя (можно воспользоваться предоставляемыми возможностями по выбору пользователя из списка).

> *Примечание.* Для различных версий ОС WINDOWS названия команд и последовательность действий может несколько отличаться от приведенных выше.

После полной настройки службы и рекомендуется проверить ее работу при помощи команды запуска службы DiSecSRV, а после проверки ее запуска следует включить автоматический запуск службы при загрузке ОС и перезагрузить компьютер.

После перезагрузки ОС служба автоматически начнет работу в соответствии с произведенными настройками.

В случае успешного подключения и создания туннеля обеспечивается доступ к защищенной сети. После входа пользователя в WINDOWS значок программы DiSec в области уведомлений рабочего стола (SYSTEM TRAY) становится зеленым на оранжевом фоне

При невозможности выполнить подключение служба остается в «рабочем» состоянии и через определенные интервалы делает попытки поиска ключевого носителя и подключения к заданному ресурсу. В этом случае после входа пользователя в систему значок программы DiSec имеет белый цвет на оранже-

вом фоне. Рекомендуется отключить службу и изучить журнал службы с целью определения причины неудачного подключения.

5.3.1. Запуск службы в ручном режиме

Запустить службу может только пользователь с правами администратора WINDOWS, воспользовавшись либо командой **Запуск службы DiSecSrv** из программной папки **DioNIS Security** стартового системного меню, либо кнопкой **Запустить службу DiSecSRV** на вкладке **Обслуживание** окна **Настройка**.

5.3.2. Останов службы DiSecSrv

Остановить работу службы может только пользователь с правами администратора, воспользовавшись либо командой **Останов службы DiSecSrv** из программной папки **DioNIS Security** стартового системного меню, либо кнопкой **Запустить службу DiSecSRV** на вкладке **Обслуживание** окна **Настройка**.
Для диагностирования проблем с запуском службы следует просмотреть журнал событий **DiSecSrv.log** при помощи соответствующий команды **Главного меню** приложения ПО DISEC.

5.4. Запуск приложения DiSec из командной строки

Приложение DiSec может быть запущено из командной строки ОС WINDOWS или из batch-файла с параметрами командной строки.
Из командной строки приложение запускается с целью выполнения отдельных конкретных задач.
В настоящее время реализована одна задача - импорт конфигурации ПО DISEC их файла. При этом следует учитывать, что данная задача будет выполнена только при запуске с привилегированными полномочиями.
Формат команды:

disec.exe /IM <Имя файла конфигурации>

Пример запуска приведен на рис.

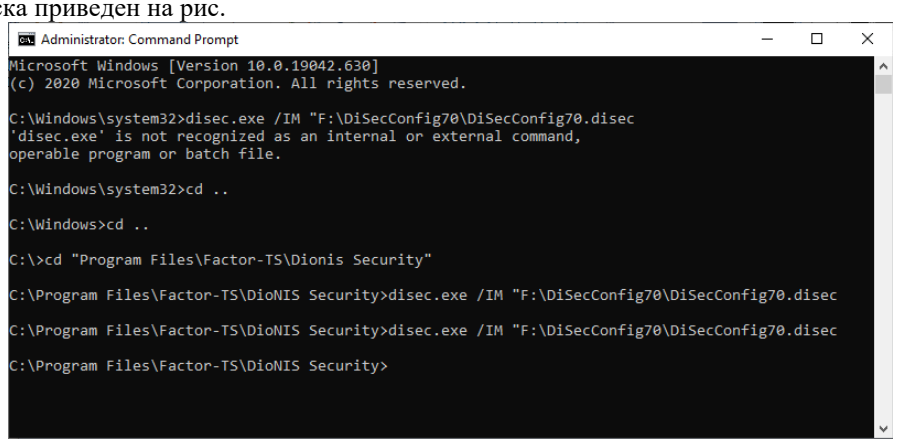


Рис. 11

Результат в случае, когда

командное окно запущено с правами администратора:

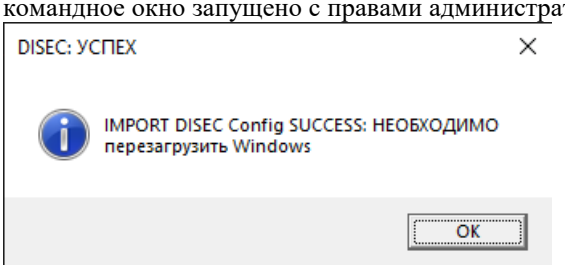


Рис. 12

командное окно запущено без прав администратора:

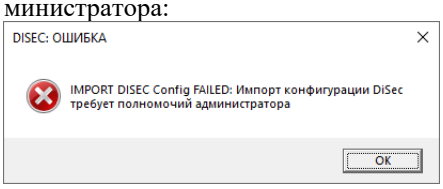


Рис. 13

6 Команда Настройка

Команда **Настройка Главного меню** приложения позволяет установить параметры работы для всех компонентов DISEC - драйвера, службы и приложения, а также выполнить задачи по обслуживанию DISEC.

Команда позволяет:

- задать список ресурсов подключений и указать необходимые для подключения реквизиты;
- задать режим запуска приложения и параметры ведения журнала событий;
- задать периодичность проверки целостности ПО;
- задать режимы работы драйвера (доступно только ***привилегированному*** пользователю), в частности, задать режим протоколирования сетевой активности, режимы блокировки или беспрепятственного пропускания определенного типа сетевых пакетов;
- задать настройки и выполнить запуск службы DiSecSrv (доступно только ***привилегированному*** пользователю).

По команде **Настройка** открывается окно, содержащее различные параметры.
Чтобы сохранить выполненные изменения настроек, надо выйти из окна, нажав кнопку **ОК**.

Для сохранения промежуточных изменений следует нажать кнопку **Принять**.

Нажатие кнопки **Отмена** закрывает окно с отменой выполненных, но не сохраненных по кнопке **Принять** изменений настроек.

Кнопка **Справка** вызывает на экран окно, содержащее справочную информацию по элементам управления.

6.1. Вкладка Параметры

После активизации команды **Настройка** на экран будет выведено окно **Настройка ПО DISEC**, открытое на вкладке **Параметры**.

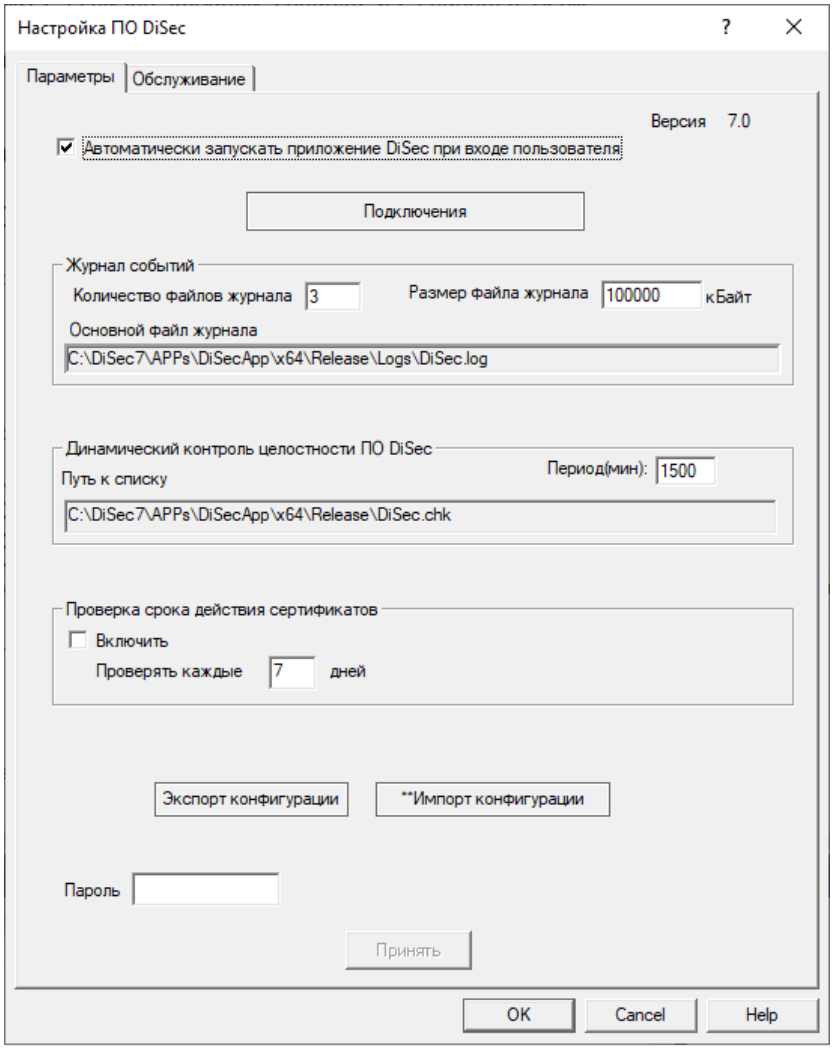


Рис. 14

Вкладка позволяет выполнить следующие настройки:

- задать режим запуска приложения DiSec,
- задать параметры ведения журнала событий,
- задать периодичность выполнения проверки целостности всех компонент ПО DISEC (проверка котрольных сумм),
- задать пароль на выполнение настроек ПО DISEC,
- настроить параметры проверки сертификатов ключей, используемых в режиме ДИНАМИЧЕСКОГО туннеля,
- выполнить экспорт конфигурации всего ПО DISEC в файл и импорт конфигурации всего ПО DISEC из ранее сформированного файла.

6.1.1. Режим запуска приложения DISEC

Флажок **`Авто-запуск приложения DiSec при входе пользователя`** обеспечивает автоматический запуск приложения DiSec после успешной авторизации пользователя в ОС WINDOWS после ее загрузки. При этом после загрузки ОС в области уведомлений SYSTEM TRAY рабочего стола пользователя появляется значок программы .

При снятом флажке автоматический запуск приложения не выполняется, и для ее запуска пользователю необходимо выполнить стандартные действия посредством ярлыка программы, находящегося на рабочем столе пользователя, или посредством команды (программы) **`DiSec`** стартового системного меню WINDOWS из папки FACTOR Applications.

> *Примечание*. При автоматическом запуске службы DiSecSRV при старте ОС WINDOWS, устанавливается автоматический запуск приложения. После отмены автоматического запуска службы DiSecSRV автоматический запуск приложения сохраняется. Для его отмены пользователю следует снять флажок вручную.

После установки флажка **Авто-запуск приложения DiSec при входе пользователя** для корректной работы других пользователей ОС WINDOWS настоятельно рекомендуется изменить настройки конфиденциальности учетной записи текущего пользователя.
Для этого следует выполнить следующие действия:

- вызвать окно Параметры из стартового меню Windows (Settings);
- открыть группу параметров Учетные записи (Accounts);

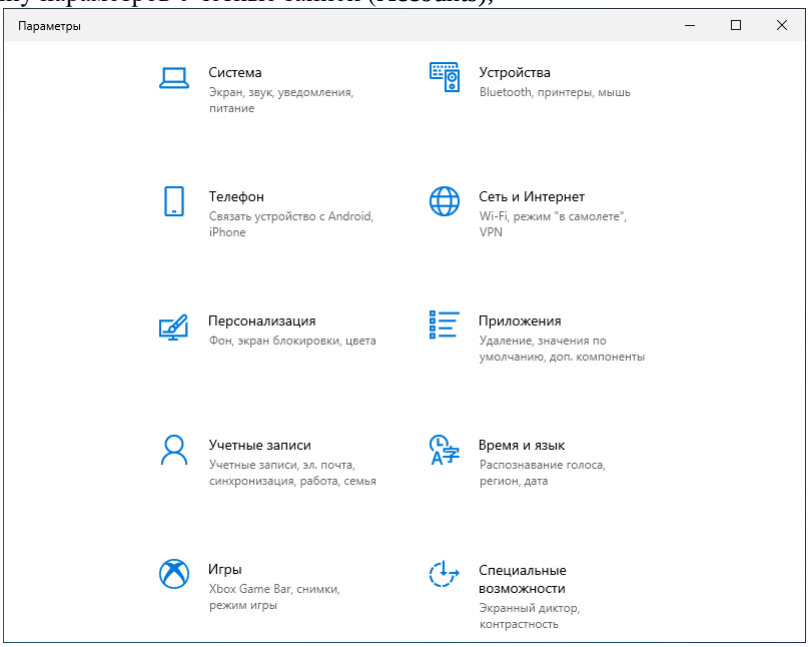


Рис. 15

- выбрать позицию **Варианты входа** (Sign-in options):

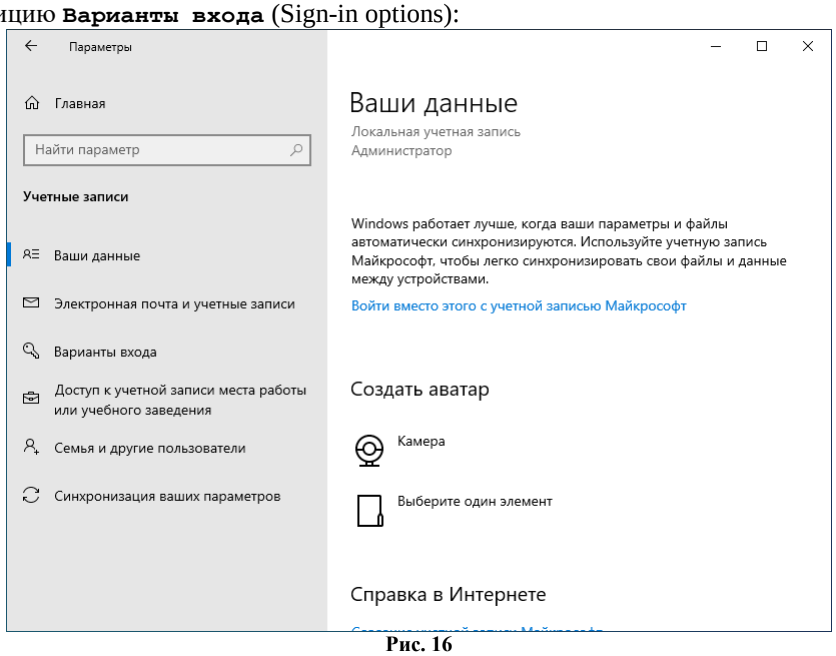


Рис. 16

- перейти к позиции **Конфиденциальность** и отключить параметр "**Использовать мои данные для входа для автоматического завершения настройки устройства после перезапуска или обновления**".

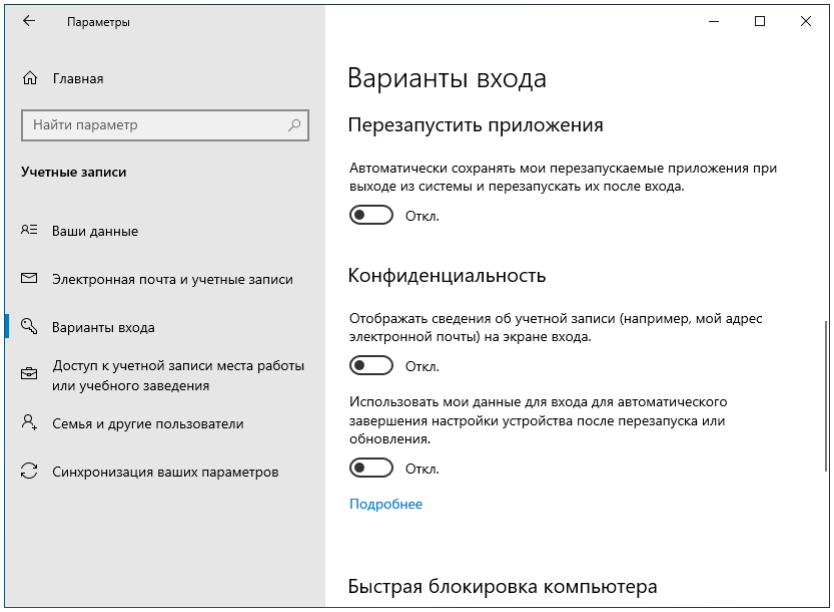


Рис. 17

При невыполнении указанной настройки после входа в систему пользователя Windows автоматически может запустить приложение **DiSec** от имени другого пользователя, а текущий получит сообщение (при попытке запуска приложения как автоматическом, так и вручную) сообщение о том, что Приложение **DiSec** уже запущено.

6.1.2. Настройка параметров Журнала

Журнал событий служит для записи сообщений, выдаваемых в процессе работы ПО DISEC. Журнал должен обязательно храниться на диске компьютера и, как правило, достаточно длительное время.

Группа параметров **Журнал событий** позволяет задать параметры ведения журнала, обеспечивающие оптимальные значения с точки зрения экономии дисковой памяти и срока хранения записанных в журналы данных.

Параметр **Количество файлов журнала** - задает количество файлов, в которые будет записываться информация. Если параметр имеет значение *0* или *1*, то журнал занимает один файл неограниченного размера (значение следующего параметра не играет роли).

Параметр **Размер файла журнала** - определяет размер каждого из файлов журнала, если файлов два и больше.

Информация всегда записывается в первый (основной) файл. Когда основной файл превысит установленный размер, он закрывается и переименовывается. Запись информации начнется снова в основной файл.

Параметр **Основной файл журнала** - имя первого (единственного) файла журнала приложения; имя задается программой, и изменить его нельзя: основной файл журнала приложения DiSec - **DiSec.log**, для службы DiSecSrv - **DiSecSrv.log**, для службы DiSecAgent - **DiSecAgent.log**.

Все файлы журнала размещаются в поддиректории **Logs** программной директории ПО DISEC.

Имена второго и последующих файлов образуются из имени основного добавлением двух цифр: **DiSec01.log**, **DiSec02.log** и т.д. Для службы DiSecSrv имена журналов имеют вид **DiSecSrv01.log**, **DiSecSrv02.log** и т.д. Аналогично для службы DiSecAgent - имя основного журнал с именем **DiSecAgent.log**.

Параметры журнала могут различаться для приложения и службы. Для службы DiSecSrv параметры журнала задаются в программе ее настройки.

6.1.3. Динамический контроль целостности

В группе параметров **Динамический контроль целостности ПО DISEC** отображаются параметры контроля.

Изменен может быть только один - **Период (мин.)**. Однако рекомендуется оставить установленное значение. При этом с заданной периодичностью будет выполняться подсчет и сверка контрольных сумм программных компонентов DISEC. При несовпадении будет выдано сообщение об ошибке, и программа закроется с отключением всех активных туннелей.

Периодичность выдерживается только во время работы программы.

6.1.4. Параметры проверки сертификатов

В секции под заголовком **Проверка сертификатов подключений** отображаются параметры контроля.
Флажок **Включить** - включает или отключает проверку.
Числовое поле **Проверять каждые** позволяет задать количество дней, определяющих периодичность проверки
Проверка выполняется автоматически после запуска приложения **DiSec** с заданной периодичностью в случае установки флажка **Включить**. При выходе из программы периодичность не соблюдается, и очередная проверка будут выполнена после запуска приложения.
При этом выбираются все имеющиеся в списке данного пользователя Подключения и для тех, которые используют PKI-ключи, выполняется проверка валидности соответствующих сертификатов, как локальных, так и сертификатов оппонента.
При проверке сертификатов выполняется обновление Списков отозванных сертификатов (CRL) и проверка по протоколу OCSP в соответствии с настройками данного Подключения.
При наличии настройки интервала для оповещения о скором окончании действия сертификатов в процессе проверки будет выводится соответствующее сообщение в окно Диагностика и в журнал.

6.1.5. Экспорт конфигурации

При нажатии кнопки **Экспорт** открывается окно выбора папки для записи списка выбранных ресурсов

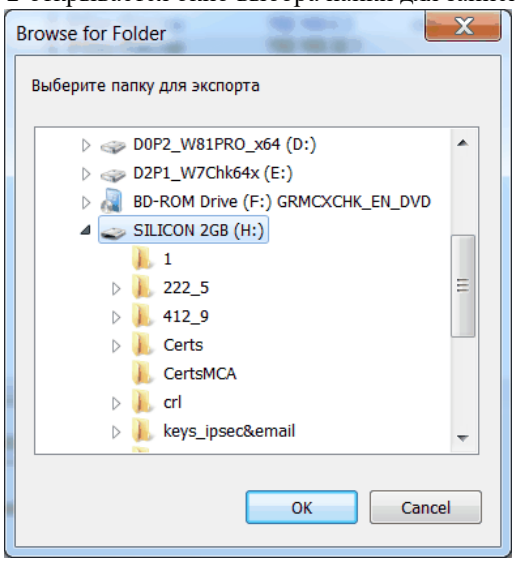


Рис. 18

После выбора директории и файла на любом носителе и нажатия кнопки **OK** выводится сообщение.

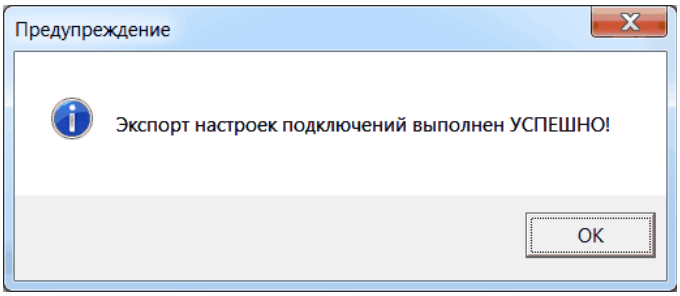


Рис. 19

Файл конфигурации имеет имя **DiSecConfig70.disec** и содержит записи ветвей реестра, относящиеся к ПО DISEC.

Полученный файл конфигурации можно использовать для импорта на другом устройстве или для другого пользователя того же устройства.

6.1.6. Импорт конфигурации

Выполнение процедуры импорта конфигурации необходимо наличие привилегированных полномочий. Поэтому необходимо выполнить следующую последовательность действий:

- выйти из приложения DiSec;
- запустить ее с административными правами, нажав правой кнопкой на ярлыке, выбрать "Run as Administrator";
- ответить утвердительно на запрос системы о запуске и ввести авторизационную информацию (логин и пароль администратора);
- выполнить команду **Настройка**;
- нажать кнопку **Импорт**.

По кнопке **Импорт конфигурации** выводится окно выбора носителя и директории для входного файла с конфигурацией ПО DISEC:

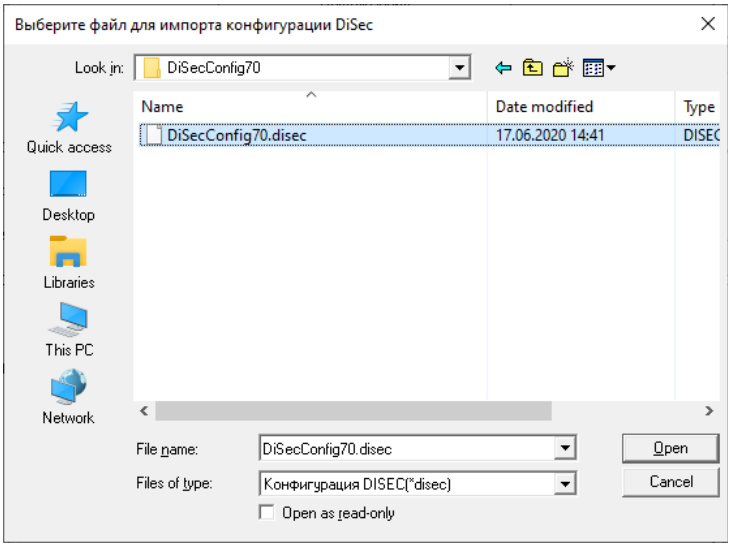


Рис. 20

Следует перейти к файлу с именем DiSecConfig70.disec, содержащему экспортированную ранее конфигурацию и нажать кнопку Open (Открыть).
После завершения импорта при отсутствии ошибок будет выдано сообщение о результатах импорта.

6.1.7. Защита настроек паролем

При необходимости ограничения доступа к процедуре настроек ПО DISEC со стороны неавторизованных лиц ответственное лицо организации (или сам пользователь ПО DISEC) может ввести пароль, который будет проверяться при попытке выполнить команду **Настройка**.
При попытке открытия окна **Настройка** в случае установленного пароля появится окно **Ввод пароля**.

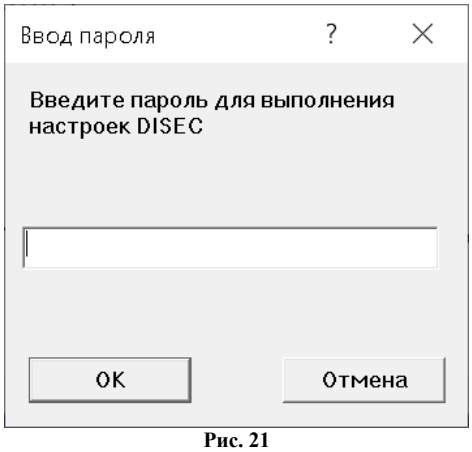


Рис. 21

При несовпадении пароля с заданным окно **Настройка** не открывается. Первоначально пароль не задан (пустой).

6.2. Окно Подключения

Окно **Подключения** открывается по нажатию кнопки **Подключения** на вкладке **Параметры** окна **Настройка** (либо в окне **Настройка службы DiSecSRV**). Оно содержит список имеющихся ресурсов подключения и кнопки для его реорганизации.

Имеется возможность сформировать список ресурсов и задать параметры для автоматического подключения.

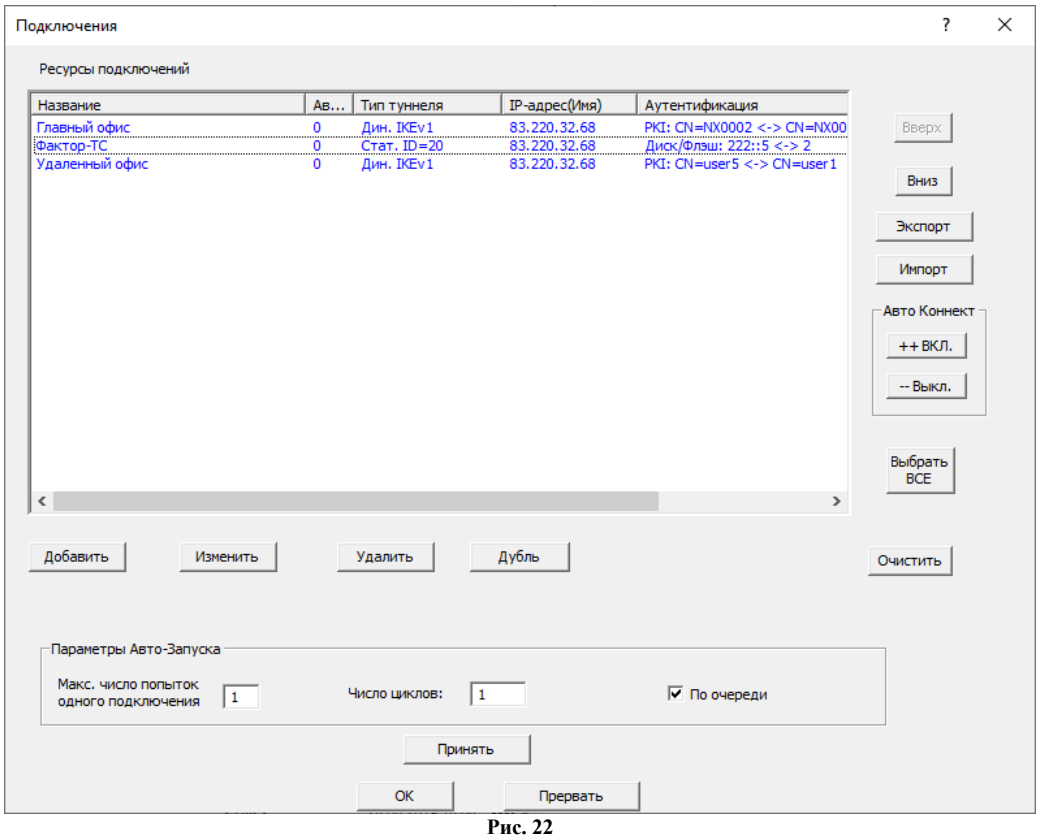


Рис. 22

При настройке подключений для службы DiSecSRV окно имеет следующий вид.

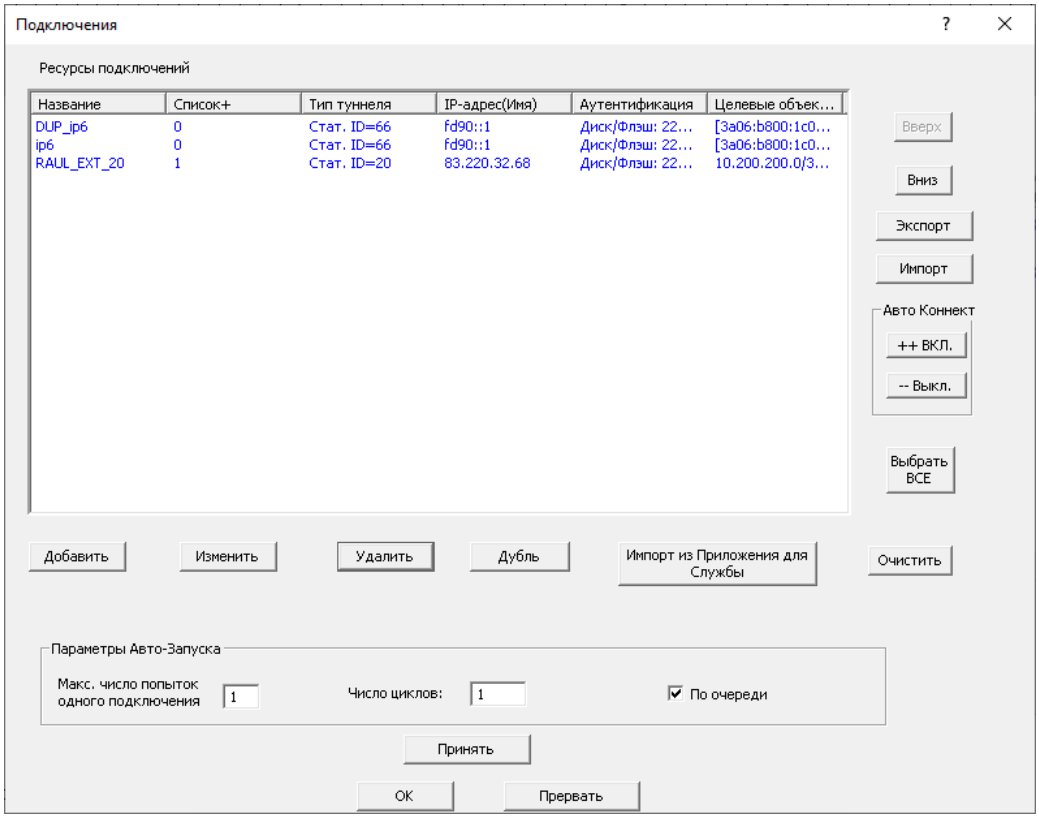


Рис. 23

Под заголовком **Ресурсы подключений** выводится список ресурсов подключений и их реквизиты в виде таблицы. Каждый ресурс занимает одну строку. В столбцах таблицы – реквизиты ресурсов; при наведении указателя мыши на заголовок столбца выводится его полное название в виде всплывающей подсказки. Реквизиты рассмотрены ниже.

Кнопки под списком **Ресурсы подключений** позволяют внести изменения в список ресурсов подключений.

- **Кнопка Добавить**
- **Кнопка Изменить**
- **Кнопка Удалить**
- **Кнопка Дубль**
- **Кнопка Очистить**
- **Импорт от пользователя**

Справа от таблицы помещены кнопки для реорганизации списка подключений:

- перемещение элемента списка **вверх** или **вниз** соответствующими кнопками;
- **Экспорт** и **Импорт** реквизитов подключения в\из директории на диске. Процедура экспорта и импорта настроек подключений может использоваться для упрощения процедуры настройки при переходе пользователя на новое устройство, при использовании данных ресурсов в качестве "шаблона" настроек, когда после их импортирования на другое устройство или для другого пользователя того же компьютера проводится их дополнительная настройка под конкретного пользователя;
- включение (и выключение) ресурса в список автоматического подключения при запуске приложения **DiSec** (**Авто-коннект**);
- кнопка **Выбрать ВСЕ** позволяет выполнить групповую операцию (экспорт, назначение или сброс авто-подключения) для всех ресурсов. Следует отметить, что для выбора нескольких ресурсов в таблице можно использовать стандартные методы: щелчок мышью при нажатой клавише *Shift* или *Ctrl*.

6.2.1. Кнопка Добавить

Кнопка **Добавить** позволяет внести в список новый ресурс; после ее нажатия открывается окно выбора базовых параметров Подключения, а затем окно Реквизиты подключения, и пользователю предоставляется возможность ввести все необходимые данные; ресурс будет добавлен в конец списка;

6.2.2. Кнопка Изменить

Кнопка **Изменить** чтобы изменить реквизиты конкретного ресурса, надо перевести курсор на соответствующую строку таблицы и нажать кнопку **Изменить** или кликнуть двойным щелчком мыши; при ее нажатии открывается окно **Реквизиты подключения** с установленными ранее значениями реквизитов, и пользователю предоставляется возможность изменить данные.

6.2.3. Кнопка Удалить

Нажатие кнопки **Удалить** после утвердительного ответа на дополнительный запрос удаляет выделенный курсором ресурс или ресурсы.

6.2.4. Кнопка Дубль

Сдублировать отдельное подключение можно кнопкой **Дубль**. При этом новому ресурсу присваивается новое имя, которое можно изменить отредактировав реквизиты (кнопка **Изменить**).

6.2.5. Кнопка Очистить

Удалить ВСЕ ресурсы подключений из списка кнопкой **Очистить**.

6.2.6. Кнопка Экспорт

При нажатии кнопки **Экспорт** открывается окно выбора папки для записи списка выбранных ресурсов

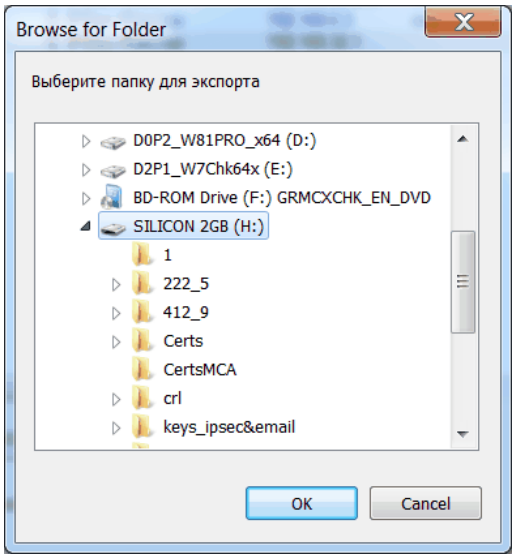


Рис. 24

После выбора директории на любом носителе и нажатия кнопки OK выводится сообщение.

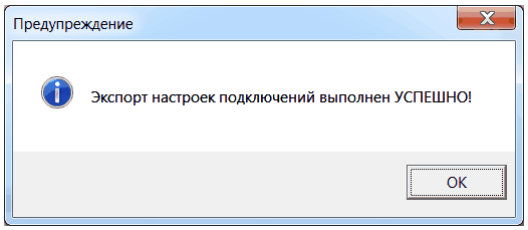


Рис. 25

А в выбранной директории (папке) появляется директория `DisecConns70`, в которой сформированы файлы с именами подключений с расширением **".conn"**.

Для этого списка можно выполнить процедуру импорта на другом устройстве или для другого пользователя того же устройства.

6.2.7. Кнопка Импорт

При нажатии кнопки **Импорт** открывается окно для выбора одного или нескольких файлов импортируемых ресурсов:

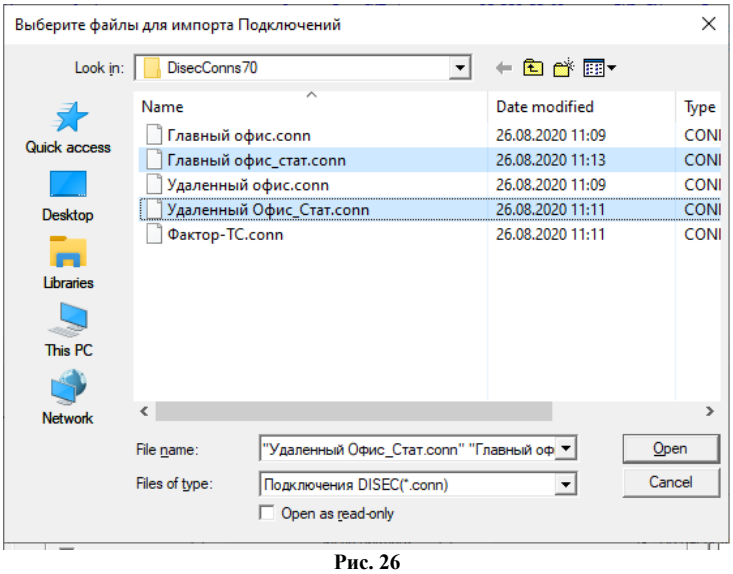


Рис. 26

Если в списке присутствует несколько файлов, то можно стандартными средствами WINDOWS, например используя клавиши *SHIFT* и *CTRL*, а также *CTRL+A* выбрать несколько или все файлы и нажать кнопку **Open**. Последовательно для каждого файла будет выдан запрос о необходимости его импорта.

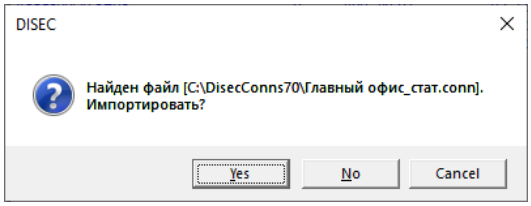


Рис. 27

При положительном ответе при наличии подключения с данным именем будет выдано сообщение:

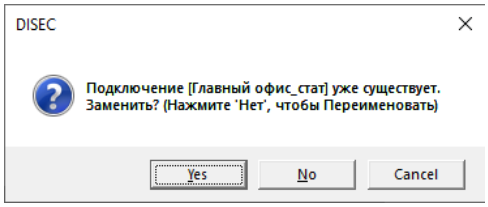


Рис. 28

При нажатии "*No*" ("Нет") будет выполнен импорт настроек из выбранного файла, новое подключение будет переименовано (добавится префикс "IMP_").:

По нажатию "*Yes*" ("Да") будет изменено существующее подключение.

После окончания будет предложено проверить настройки безопасности.

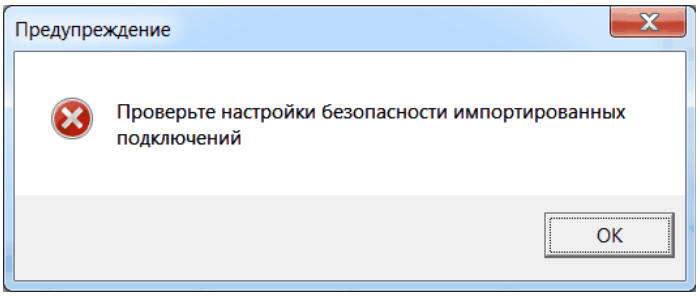


Рис. 29

6.2.8. Импорт от пользователя

Кнопке **Импорт от пользователя** активна при настройке службы DiSecSRV. При ее нажатии на экран выводится список подключений текущего пользователя DISEC.

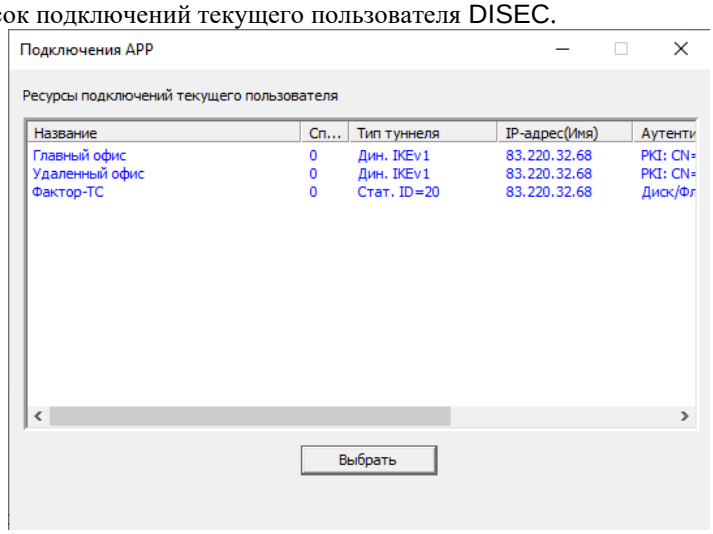


Рис. 30

Необходимо выделить один или несколько ресурсов и нажать кнопку **Выбрать** или выполнить двойной щелчок мышью.
В списке подключений службы появится выбранный ресурс.

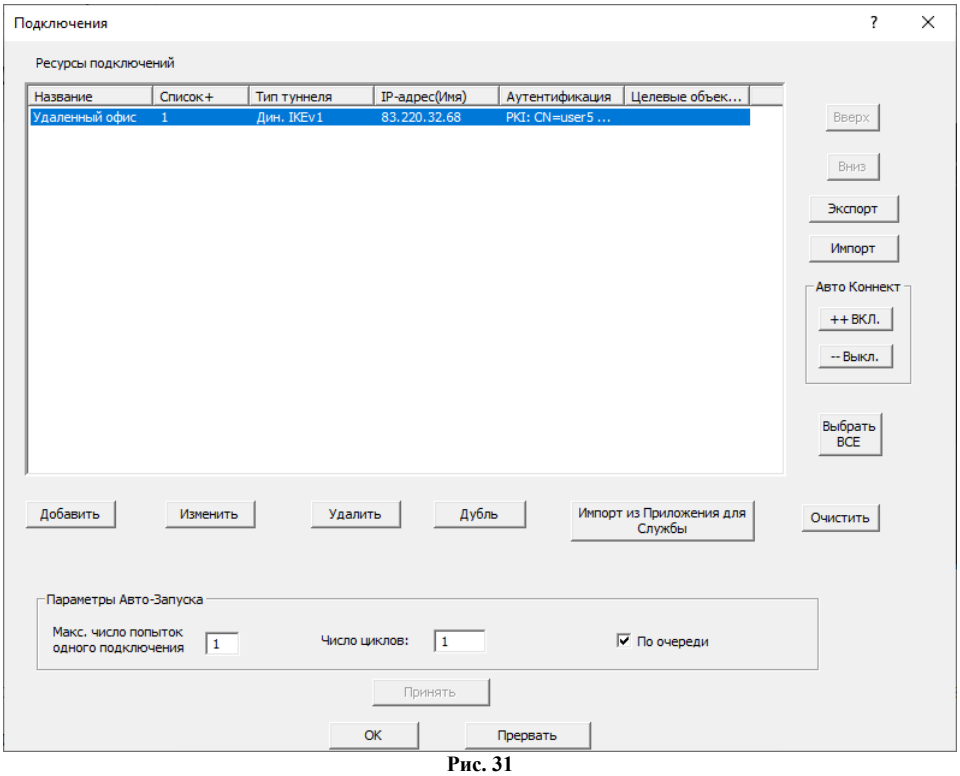


Рис. 31

6.2.9. Авто-коннект

Выполняет формирование списка авто-подключения, т.е. для каждого ресурса (или для выделенных ресурсов) выполняет включение в список авто-подключения при запуске приложения посредством кнопки **++Вкл**. и исключает из списка посредством кнопки **--Выкл.**

Последовательность запуска определяется последовательностью отображения в списке подключений. Остальные параметры авто-подключения настраиваются здесь.

6.2.10. Параметры Авто-запуска

Параметры Авто-запуска

Группа параметров **Параметры Авто-запуска** отображает настройку авто-подключения и будут использованы, если хотя бы одного ресурса задано свойство ***Авто-коннект***, равное 1.

Макс. число попыток одного подключения

Параметр **Макс. число попыток подключения** задает число попыток для КАЖДОГО ресурса в списке авто-подключения. В список включаются все ресурсы с установленным (равным 1) значением ***Авто-коннект.*** Стандартное значение - 2.

Число циклов

Параметр **Число циклов** задает число повторов выполнения всего списка авто-подключения. Принудительно выполнение списка может быть выполнено пользователем командой Отключиться. Стандартное значение - 0 (бесконечный цикл).

По очереди

Параметр определяет, будут ли выбранные для автоматического запуска подключения выполняться одновременно или после неудачного завершения предыдущего в списке.

6.2.11. Базовые параметры подключения

При создании нового ресурса подключения в первую очередь следует определиться с типом подключения. От выбранного значения зависят все остальные настройки.

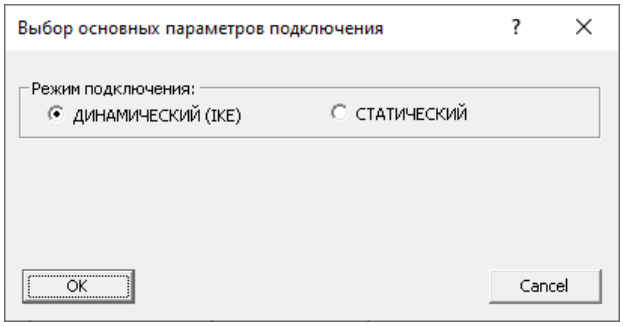


Рис. 32

Впоследствии данный параметр ресурса подключения изменить невозможно.

7 Реквизиты подключения

Окно **Реквизиты подключения**. содержит несколько вкладок, на которых сгруппированы все необходимые для работы настройки Подключения.
Содержание вкладок **Параметры** и **Безопасность** зависит от выбранного режима организации туннеля ДИНАМИЧЕСКОГО или СТАТИЧЕСКОГО.
Открывается окно на вкладке **Общие**.

7.1. Вкладка Общие

На вкладке **Общие** назначаются основные параметры.

Для СТАТИЧЕСКОГО туннеля вкладка имеет следующий вид:

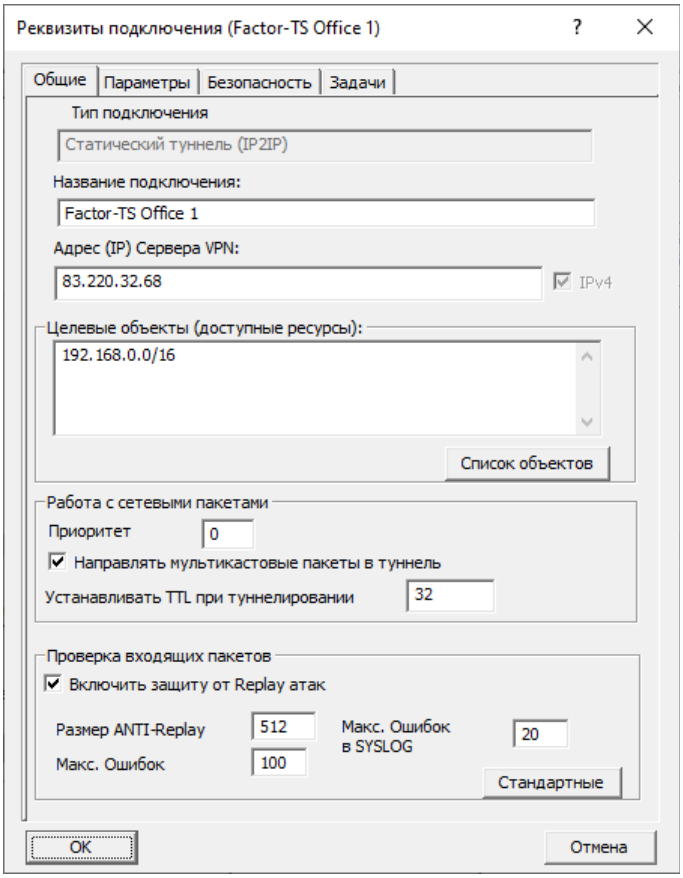


Рис. 33

Для ДИНАМИЧЕСКОГО туннеля вид будет следующий:

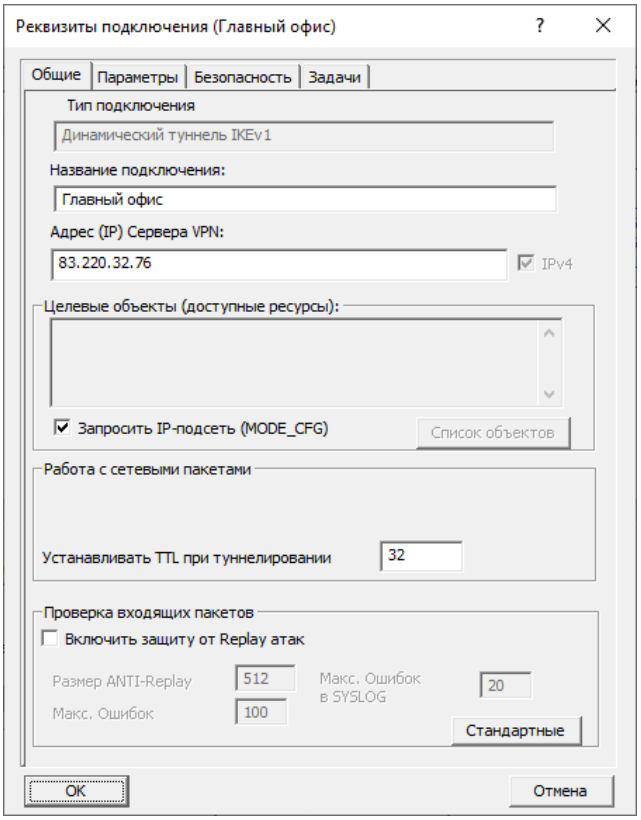


Рис. 34

Тип подключения

Данное поле имеет значение - ***Динамический туннель IKEv1*** или С***татический туннель(IP2IP)***, которое задается при первоначальном создании ресурса и не может быть изменено при последующем редактировании.

Название подключения

Значением поля **Название подключения** является произвольная последовательность букв и цифр, идентифицирующая данный ресурс подключения; рекомендуется присваивать понятные названия, которые позволят легко отличить данный объект от других при выборе ресурса из списка во время выполнения команды **Подключиться** (раздел Команда Подключиться).

Адрес (IP) Сервера VPN

В поле **Адрес (IP) Сервера VPN** следует ввести IP-адрес Сервера VPN или его доменное имя. В последнем случае активизируется флажок IPv4 для выбора соответствующего сетевого протокола.

IPv4

Флажок **IPv4** активен, только если задано доменное имя Сервера VPN. Его можно снять, если желательно выполнять подключение по протоколу IPv6. При задании числового значения IP-адреса, флажок IPv4 - не активен и автоматически установлен в соответствующее адресу значение.

Далее следуют несколько групп параметров:

Группа параметров **Целевые объекты (доступные ресурсы)** позволяет задать список доступных по туннелю объектов вручную на стороне клиента (список должен быть согласован с настройками на Сервере VPN). Для динамического туннеля в соответствии с настройками на Сервере VPN имеется возможность задать режим получения списка по запросу в процессе переговоров по протоколу IKE (сообщения MODE_CONFIG).

Группа параметров **Работа с сетевыми пакетами** позволяет задать некоторые параметры туннельных пакетов, передаваемых в туннель.

Группа параметров **Проверка входящих пакетов** позволяет задать параметры защиты от некоторых видов сетевых атак, в частности Replay-атак.

7.1.1. Целевые объекты (доступные ресурсы)

Список целевых объектов соответствует правилам отбора сетевых пакетов в туннель, при этом реализована проверка только по характеристикам получателя без учета характеристик отправителя.

Список целевых объектов состоит из отдельных объектов, разделенных символом «;» (точка с запятой).

Каждый целевой объект может состоять из трех элементов, элементы отделяются друг от друга символом «:» (двоеточие):

- IP-адрес конкретного ресурса или IP-адрес сети с указанием маски (маска отделяется от IP-адреса символом слэш «**/**» или обратный слэш «****»);
- прикладной протокол стека TCP\IP, который должен быть указан в числовом виде, либо иметь символьное значение "0".
- диапазон значений портов для протокола TCP или UDP.

Пример списка из двух объектов: ***10.1.1.0/24;10.1.2.10\32:6:80*** .

В 1-ом случае правилом определяется доступ к подсети с начальным адресом 10.1.1.0, размером 256 адресов и доступом по любому протоколу. Во 2-м случае определяется доступ к конкретному адресу 10.1.2.10 по протоколу TCP (номер протокола - 6) и порту 80.

Некоторые элементы целевого объекта могут отсутствовать. В этом случае обработка выполняется следующим образом:

1. Если поле под заголовком **Целевые объекты (доступные ресурсы)** оставить не заполненным, то клиент DISEC получит доступ только к самому Серверу VPN. Значение параметра должно быть согласовано с соответствующей настройкой на Сервере VPN.
2. Если не указана маска, то подразумевается, что указан IP-адрес конкретного ресурса, и маске присваивается значение «*32*».
3. Если не указан протокол или порт, то им присваивается значение «*0*» и "0-0" соответственно, означающее, что туннель действует для ВСЕХ протоколов и портов.

Примечание. При настройке подключения для работы с несколькими целевыми объектами, на стороне Сервера VPN необходимо создать несколько соединений (connection), отличающихся значениями параметра **local subnet** (см раздел 14, п. 15, с. 112). На стороне DISEC одно подключение может содержать весь список объектов.

Запросить IP-подсеть(MODE_CFG)

Флажок **Запросить IP-подсеть(MODE_CFG)** позволяет установить режим получения списка доступных ресурсов в виде подсети от Сервера VPN по запросу в протоколе IKE.

Кнопка **Список объектов** предоставляет возможность более удобного и надежного способа задания списка целевых объектов.

7.1.1.1. СПИСОК ОБЪЕКТОВ

Кнопка **Список объектов** предоставляет более удобный способ задания и контроля правильности отдельных целевых объектов в списке. После ее нажатия открывается окно **Настройка списка целевых объектов**, которое позволяет создать, изменить, удалить отдельный объект, а также изменить последовательность элементов списка.

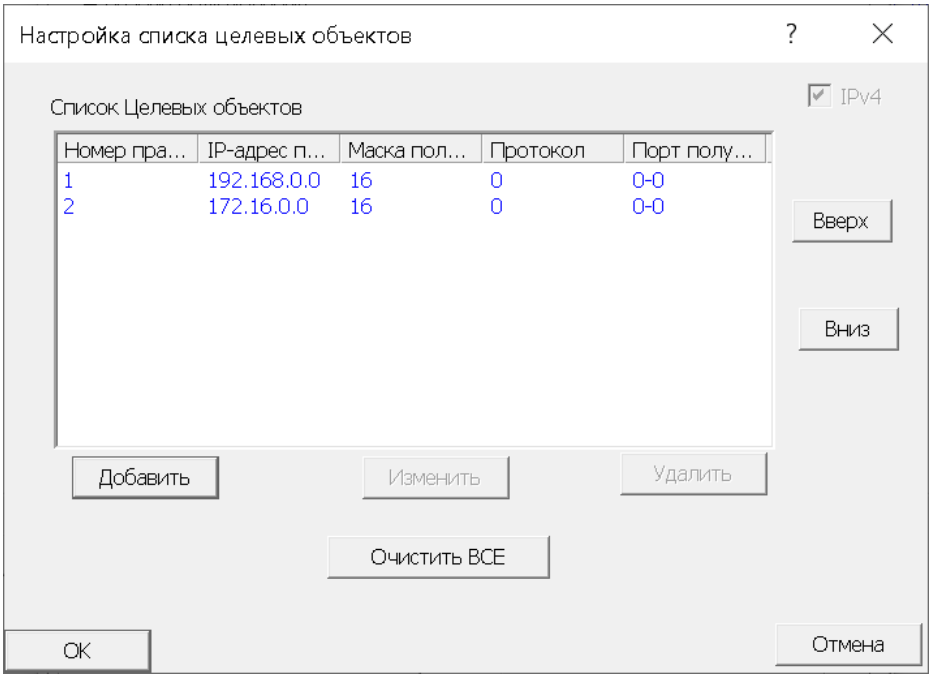


Рис. 35

При нажатии кнопки **Добавить** (или **Изменить**) открывается **Целевой объект**, которое позволяет задать (отредактировать) все параметры целевого объекта, к которому необходимо получить доступ через туннель.

Окно Целевой объект

В данном окне имеется возможность задать отдельные компоненты целевого объекта, для которых будет автоматически сформирован целевой объект. с соблюдением необходимых синтаксических правил.

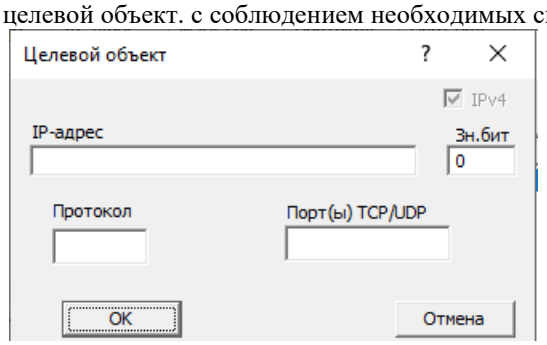


Рис. 36

При формировании правила выполняется проверка введенных данных и в случае ошибки выводится соответствующее сообщение, например:

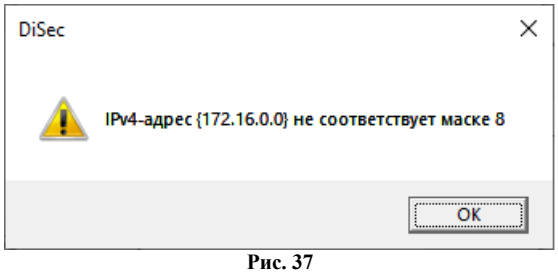


Рис. 37

7.1.2. Работа с сетевыми пакетами

Группа параметров **Работа с сетевыми пакетами** позволяет выполнять дополнительную обработку сетевых пакетов перед отправкой их в туннель.

Приоритет

Для **статических** туннелей данный параметр позволяет организовывать несколько подключений с "пересекающимися" правилами отбора . Подключения с пересекающимися правилами отбора запускаются одновременно, если для них установлен разный приоритет. При этом активным является туннель с большим приоритетом. Туннель с меньшим приоритетом, как бы находится в резерве. В случае отключения подключения с большим приоритетом выполняется переход на туннель с меньшим значением приоритета. Параметр может принимать значения от нуля (стандартное) до *10*.

Направлять мультикастовые пакеты в туннель

Для **статических** туннелей данный параметр позволяет выполнять туннелирование мультикастовых пакетов, а также действия, обеспечивающие их надежную доставку к целевому объекту. Данную опцию следует устанавливать, например, если предполагается передача видео-контента по туннелю. Следует учитывать, что данная функция будет действовать только для одного подключения, для всех остальных - будет игнорироваться.

Устанавливать TTL при туннелировании

Данный параметр позволяет менять значение TTL (***Time-To-Live***) в заголовках инкапсулирующих (туннельных) IP-пакетах. Стандартное значение - 32. Не рекомендуется менять данное значение.
Значение, равное "0" - означает, что значение TTL не будет меняться и останется равным значению в исходном пакете.

7.1.3. Проверка входящих пакетов

Группа параметров **Проверка входящих пакетов** позволяет выполнять контроль последовательных номеров входящих пакетов и регистрировать значительное нарушение этой последовательности, что позволяет осуществлять защиту от определенного рода сетевых атак.

Включить защиту от Replay атак

Флажок **Включить защиту от Replay атак** позволяет включить или отключить данную защиту, которая по специальному алгоритму проверяет номера принятых сетевых пакетов. Номера принятых пакетов должны последовательно увеличиваться, при этом допускаются некоторые отклонения.
Некоторые виды сетевых атак приводят к нарушению этих правил, и включенная защита позволяет своевременно их обнаружить. С другой стороны, данная защита отнимает значительные ресурсы и производительность.

Размер ANTI-Replay окна

Параметр **Размер ANTI-Replay окна** определяет диапазон допустимых отклонений порядковых номеров входящих сетевых пакетов, т.е. порядковые номера:

- не должны повторяться в пределах этого окна, в противном случае пакет отбрасывается и счетчик ошибок увеличивается,
- номер принятого пакета не должен выходить за "левую" рамку окна, т.е. не быть слишком "старым". После получения "правильного" пакета окно сдвигается в соответствии с его номером.

Макс. Ошибок

Параметр **Макс.Ошибок** определяет пороговое значение количества полученных подряд ошибок. По достижению заданного количества ошибок туннель будет закрыт, и в системный журнал Windows (EventLog) будет занесено соответствующее сообщение.

Макс. Ошибок в SYSLOG

Параметр **Макс. Ошибок в SYSLOG** ограничивает количество записей в системный журнал во избежание слишком большого количества записей.

По кнопке **Стандартные** устанавливаются значения параметров защиты: размер окна равным *512*, максимальное количество ошибок, равным *100*, и максимальное число записей сообщения об ошибках в системный журнал, равным *20*.

7.2. Вкладка Параметры для статического туннеля

Для статического туннеля вкладка **Параметры** имеет вид:

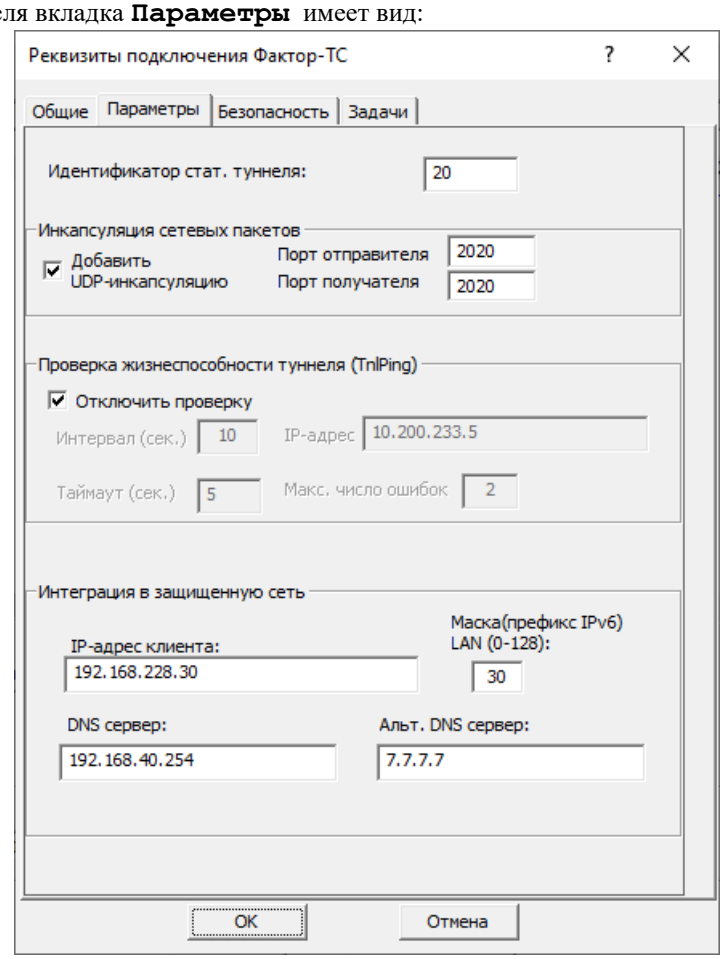


Рис. 38

Идентификатор стат. туннеля

Для статического туннеля необходимо указать его идентификатор - **ID туннеля**, который должен быть заранее получен от администратора Сервера VPN.

Группа параметров **Инкапсуляция сетевых пакетов** состоит из следующих элементов: флажка, включающего или отключающего UDP-инкапсуляцию и дополнительных параметров (значение портов UDP-протокола).

Группа параметров **Проверка жизнеспособности туннеля(TnlPing)** позволяет задать соответствующие параметры.

Группа параметров **Интеграция в защищенную сеть** позволяет задать виртуальные IP-адреса, принадлежащие "внутренней" локальной сети.

7.2.1. Инкапсуляция сетевых пакетов

Группа параметров **Инкапсуляция сетевых пакетов** состоит из следующих элементов: флажка, включающего или отключающего UDP-инкапсуляцию и дополнительных параметров (значение портов UDP-протокола).

Добавить UDP-инкапсуляцию

Флажок **Добавить UDP-инкапсуляцию** меняет способ туннелирования (инкапсуляции) сетевых пакетов: дополнительно к протоколу IP-in-IP драйвер будет использовать протокол UDP с назначенными портами. Установка флажка активирует элементы управления **Порт отправителя** и **Порт получателя** и присваивает им стандартные значения ***1025***. Значения этих полей можно изменить, при этом они должны соответствовать настройкам статического туннеля на Сервере VPN.

7.2.2. Проверка жизнеспособности туннеля (TnlPing)

Группа параметров **Проверка жизнеспособности туннеля (TnlPing)** позволяет настроить параметры проверки.

Флажок **Отключить проверку жизнеспособности туннеля** позволяет выполнить указанное отключение (***не рекомендуется***). В этом случае тестовые сообщения проверки жизнеспособности туннеля (Ping-пакеты) не будут посылаться на Сервер VPN. Данная настройка рекомендуется, если по туннелю проходит достаточно большой трафик, и лишняя нагрузка не нужна.

Интервал(сек.)

В данном поле можно задать промежуток времени между получением ответа на очередную посылку и посылкой следующего Ping-пакета. Стандартное значение - 30 секунд.

IP-адрес

В данном поле можно указать альтернативный адрес для Ping-посылок, при отсутствии значения, Ping-посылки отправляются по адресу конца туннеля (Сервера VPN).

Таймаут(сек.)

В данном поле можно задать промежуток времени, в течение которого выполняется ожидание ответа, после чего фиксируется ошибка. Стандартное значение - 5 секунд.

Макс. число ошибок

В данном поле можно задать пороговое значение для количества полученных ПОДРЯД ошибок. При получении ошибки до достижения этого порогового значения увеличивается значение счетчика ошибок, и через заданный интервал времени выполняется очередная посылка. Если будет получен ответ, то счетчик сбрасывается. При достижении порогового значения числа ошибок выполняется закрытие туннеля (отключение). Стандартное значение - 3.

7.2.3. Интеграция в защищенную сеть (RLAN)

Группа параметров **Интеграция в защищенную сеть** позволяет функционировать клиенту DISEC, как если бы его компьютер принадлежал к защищенной локальной сети.

Параметр **IP-адрес клиента** позволяет использовать заданный адрес при обмене сетевыми пакетами в туннеле. Данный адрес присваивается "внутреннему" зашифрованному пакету.

При указании данного адреса следует учитывать версию IP протокола (IPv4 или IPv6), используемую для данного подключения - версия должна совпадать с версией адреса Подключения, указанного в поле **Адрес (IP) Сервера VPN**.

Маска (префикс IPv6) LAN

Данный параметр задает диапазон доступных по туннелю IP-адресов, соответствующий внутренней локальной сети

DNS-сервер, Альт. DNS-сервер

IP-адреса серверов DNS, которые будет установлены на сетевом интерфейсе, соответствующем организованному туннелю, и на которые будут направляться DNS-запросы. Поле **Альт. DNS-сервер** может оставаться не заполненным.
Правила отбора для адресов серверов DNS будут добавлены автоматически.

7.3. Вкладка Параметры для динамического режима

Для режима динамического туннеля на вкладке **Параметры** размещены элементы управления, позволяющие назначать и модифицировать политики согласования криптоалгоритмов и ключевого материала между взаимодействующими сторонами (DISEC и Сервер VPN).

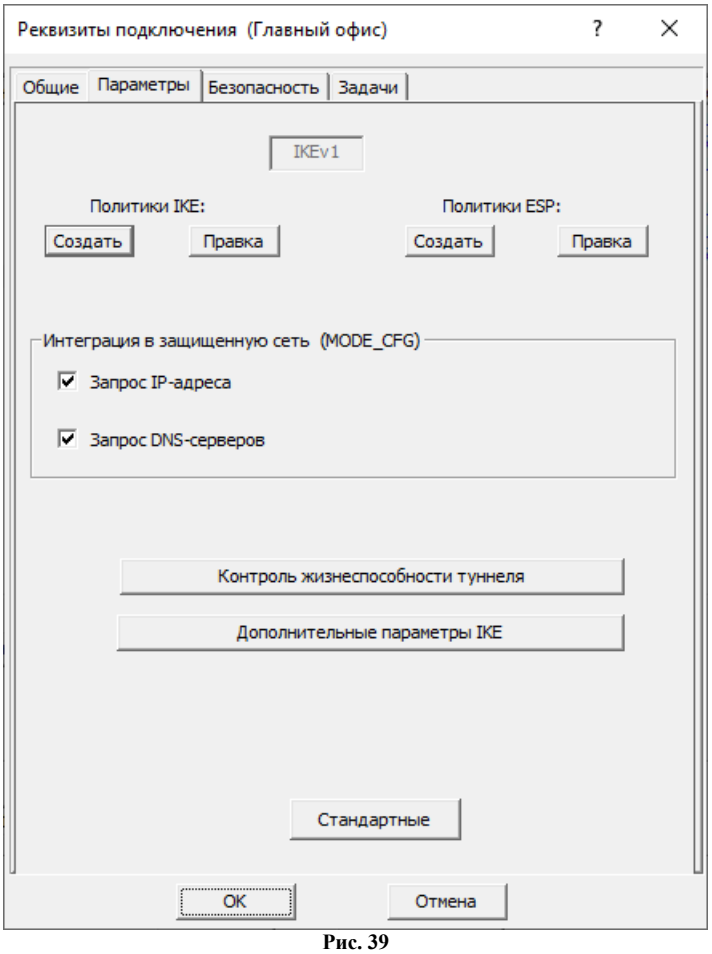


Рис. 39

Политики IKE

Элемент управления **Политики IKE** позволяет создать или модифицировать политику IKE для данного туннеля. Политика IKE содержит параметры, используемые на 1-ой фазе протокола IKE (создание SA IKE).

Политики ESP

Элемент управления **Политики ESP** позволяет создать или модифицировать политику ESP для данного туннеля. Политика ESP содержит параметры, используемые на 2-ой фазе протокола IKE (создание SA ESP), и параметры протокола ESP.

Нажатие одной из кнопок **Создать** или **Правка** для **Политики IKE** или **Политики ESP** приводит к выводу на экран соответствующего окна, и пользователь получает возможность изменять существующую или стандартную политику (создаваемую по клавише **Создать**).

Группа параметров **Интеграция в защищенную сеть (MODE CONFIG)**

Контроль жизнеспособности туннеля

По нажатию кнопки **Контроль жизнеспособности туннеля** открывается соответствующее окно.

Дополнительные параметры IKE

По нажатию кнопки **Дополнительные параметры IKE** открывается соответствующее окно.

Кнопка **Стандартные** устанавливает соответствующие значения параметров IKE протокола.

7.3.1. Настройка политики IKE

Политика IKE определяет состав, количество и содержание сообщений 1-й фазы протокола IKE, а также задает правила формирования ключей шифрования и алгоритмы шифрования сообщений протокола IKE 1-й и 2-й фазы .

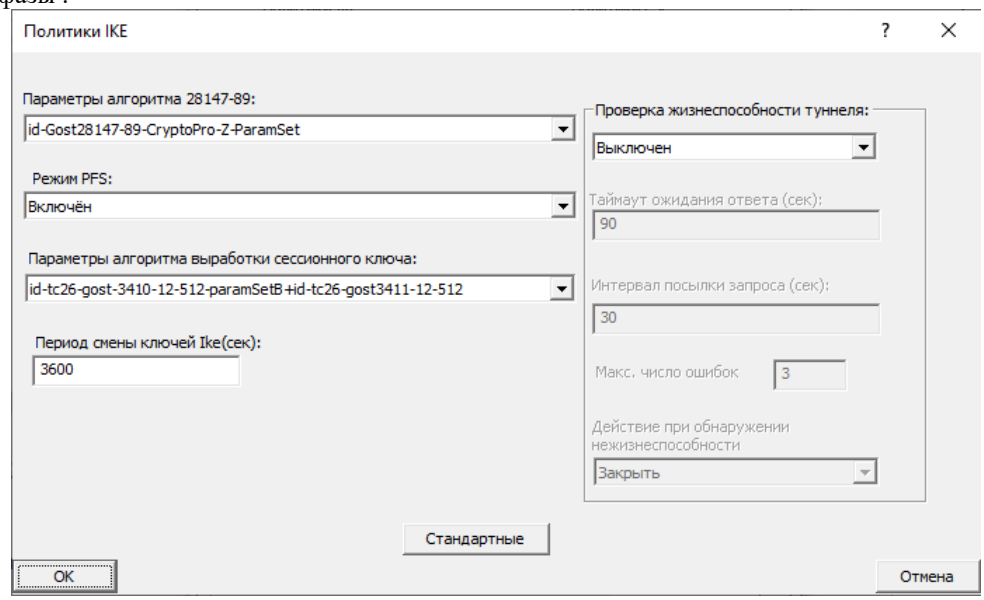


Рис. 40

Параметры алгоритма 28147-89

Данное поле определяет параметры шифрования передаваемых сообщений в соответствии с ГОСТ 28147-89. В поле должен быть задан узел замены. Значение по умолчанию - *MAGMA_Z_CFB_IMIT*. Если потребуется другое значение, его можно выбрать из выпадающего списка:

id-Gost28147-89-CryptoPro-A-ParamSet
id-Gost28147-89-CryptoPro-B-ParamSet
id-Gost28147-89-CryptoPro-C-ParamSet
id-Gost28147-89-CryptoPro-D-ParamSet
id-Gost28147-89-CryptoPro-Z-ParamSet
MAGMA_Z_CFB_IMIT

Значение параметра должно соответствовать значению на Сервере VPN.

Примечание. Символ «*A*» ... «*Z*» в значении параметров (здесь и далее) определяет используемый для шифрования **Узел Замены**.

Режим PFS

Выбор режима влияет на параметры, передаваемых в 1-ой фазе протокола IKE. При включенном режиме формируется дополнительный общий секрет для выработки ключевого материала во 2-й фазе протокола IKE.

Возможные значения *Включен* (стандартное значение), *Выключен*.

Значение параметра должно быть согласовано со значением на Сервере VPN.

Примечание. Для того чтобы между Сервером VPN («Dionis-NX») и DISEC мог быть организован туннель, должно быть следующее соотношение параметров:

если на Сервере установлен режим *OFF* или *PROPOSE*, то на DISEC значение режима - *Выключен*;

если на Сервере установлен режим *FORCE*, то на DISEC значение режима - *Включен*.

Параметры алгоритма выработки сессионного ключа

Поле определяет алгоритм выработки общего секрета 1-ой фазы протокола IKE. Стандартное значение - *id-tc26-gost-3410-12-512-ParamSetB+id-tc26-gost-3411*. Если потребуется другое значение, его можно выбрать из выпадающего списка:

id-GostR3410-2001-CryptoPro-XchA-ParamSet+id-tc26-gost3411-12-256

id-GostR3410-2001-CryptoPro-XchB-ParamSet+id-tc26-gost3411-12-256
id-tc26-gost-3410-12-512-paramSetA+id-tc26-gost3411-12-512
id-tc26-gost-3410-12-512-paramSetB+id-tc26-gost3411-12-512

Значение параметра должно соответствовать значению на Сервере VPN.

Период смены ключей Ike(сек)

Значение параметра определяет *время жизни* установленной фазы 1. По окончании указанного периода (немного заранее) будет выполнена инициализация выполнения фазы 1 протокола IKE для выработки нового ключевого материала для создания SA ESP и инициализирована выполнение фазы 2 протокола IKE для выработки нового ключевого материала туннеля.
Стандартное значение для времени жизни 1-ой фазы - *10800 сек*.

Кнопка **Стандартные** устанавливает соответствующие значения (значения по умолчанию) параметров протокола IKE.

7.3.2. Настройка политики ESP

Политика ESP определяет правила формирования ключей шифрования и алгоритмы шифрования сетевых пакетов, передаваемых по туннелю при использовании протокола ESP .

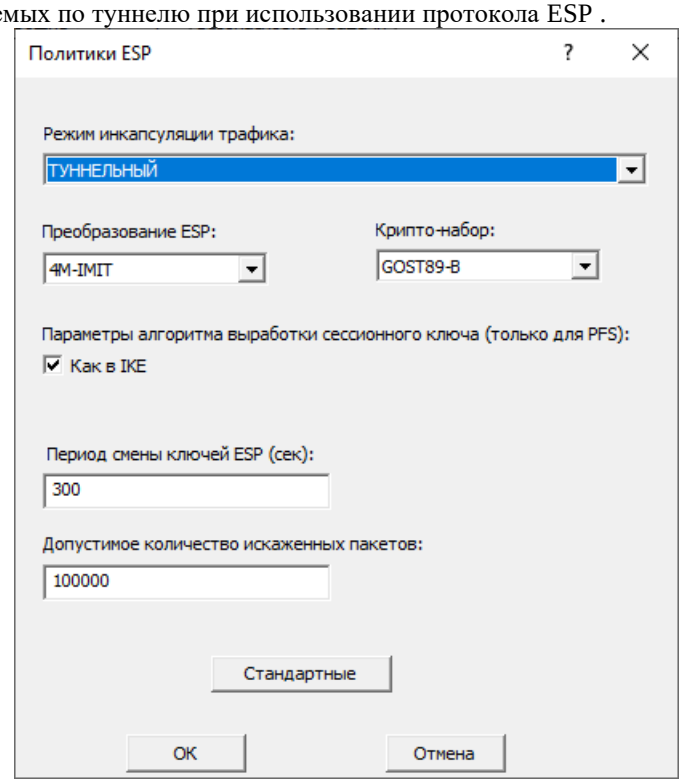


Рис. 41

Не рекомендуется менять установленные стандартные значения.

Режим инкапсуляции трафика

Параметр определяет вариант настройки протокола ESP, возможные значения:

- *ТУННЕЛЬНЫЙ* - стандартное значение;
- *ТРАНСПОРТНЫЙ*.

Значение параметра должно совпадать с соответствующим значением на Сервере VPN .

Преобразование ESP

Поле определяет два параметра, значения которых должны совпадать с соответствующими значениями на Сервере VPN:

- тип преобразования ESP, которое может принимать следующие значения: *4M_IMIT*, *1K_IMIT* (стандартное значение - *4M_IMIT*) .

- Крипто-набор (узел замены для алгоритма ГОСТ 28147-89) предоставляет выбрать одно из значений: *GOST89-A, GOST89-B, GOST89-C, GOST89-D* или *GOST89-Z.* Стандартное значение - *GOST89-Z.*

Параметры алгоритма выработки сессионного ключа (только для PFS)

Параметр определяет алгоритм выработки общего секрета 2-ой фазы протокола IKE. Выработанный на основе общего секрета 1-й и 2-й фазы ключевой материал передается в драйвер DiSec, где на его основе формируются ключи шифрования пакетов протокола ESP.

Значение по умолчанию «*как в IKE*», т.е. устанавливается то значение, которое было установлено для алгоритма выработки сессионного ключа 1-ой фазы протокола IKE (см. выше раздел Настройка политики IKE). Если потребуется другое значение, его можно выбрать из выпадающего списка. Значение параметра должно совпадать с соответствующим значением на Сервере VPN.

Период смены ключей Esp(сек):

Значение параметра определяет ***время жизни*** установленной фазы 2. По окончании указанного периода инициируется выполнение фазы 2 протокола IKE для выработки новых ключей шифрования. Стандартное значение времени жизни 2-ой фазы - *3600 сек*. Значение параметра должно быть значительно больше, чем соответствующее значение на Сервере VPN.

Допустимое количество искаженных пакетов

Если число искаженных пакетов превысит заданное параметром значение, туннель будет закрыт (наличие искажений фиксируется при проверке имитовставки пакета). Стандартное значение параметра - *100000.*
При этом в системном журнале **EventLog** будет зафиксирована ошибка.
Для просмотра сообщений об ошибках, выданных драйвером DiSec, можно воспользоваться системными средствами WINDOWS либо воспользоваться командой Протокол сети Главного меню DiSec (см. Команда Протокол сети).

Кнопка **Стандартные** устанавливает соответствующие значения (значения по умолчанию) параметров политики ESP.

7.3.3. Интеграция в защищенную сеть (MODE_CFG)

Группа параметров **Интеграция в защищенную сеть** позволяет функционировать клиенту DISEC, как если бы его компьютер принадлежал к защищенной локальной сети.

Запрос IP-адреса

По умолчанию флажок установлен, что означает наличие режима **MODECONFIG** в DISEC. При включенном режиме **MODECONFIG** DISEC посылает запрос на Сервер VPN и получает от него IP-адрес из диапазона адресов защищаемой сети.

Запрос DNS-серверов

При установке данного флажка в режиме **MODECONFIG** в процессе согласования параметров по протоколу IKE посылается запрос на получение адресов внутренних DNS-серверов. Полученные IP-адреса серверов DNS, будут установлены на сетевом интерфейсе, соответствующем организованному туннелю, и на них будут направляться DNS-запросы.

7.3.4. Контроль жизнеспособности туннеля

Группа параметров предназначена для выполнения проверки жизнеспособности туннеля посредством периодической посылки запросов - сообщений протокола IKE специального формата - и контроля поступления ответных сообщений на запрос.

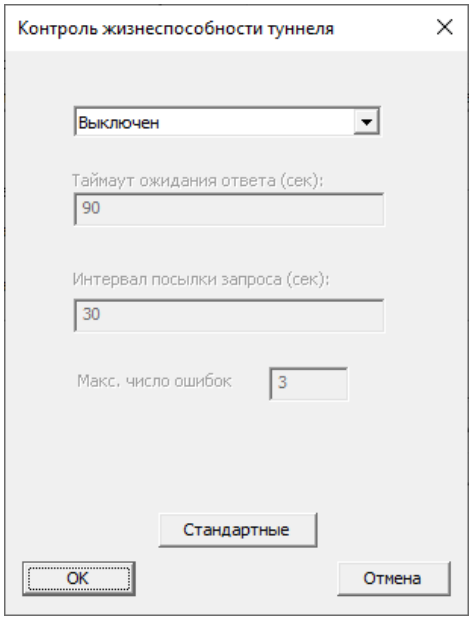


Рис. 42

Возможные варианты контроля:

- *Выключен* - не посылаются ни запросы, ни ответы на запросы Сервера VPN;
- *Пассивный* - DISEC отвечает на запросы Сервера VPN (стандартное значение);
- *Активный* - DISEC посылает запросы на Сервер VPN и контролирует ответы (анализируется порядковый номер ответа).

Три следующих параметра активны только при значении предыдущего параметра *Активный*.

Интервал посылки запроса (сек)

В поле под этим заголовком надо задать целое число - интервал посылки запросов в секундах. Стандартное значение - *60*.

Таймаут ожидания ответа (сек):

В поле под этим заголовком надо задать целое число - время в секундах, по истечении которого туннель будет закрыт или инициирован заново в отсутствие ответа на запрос о жизнеспособности туннеля. *Стандартное значение -10.*

Мак число ошибок

Данный параметр определяет пороговое значение для полученных подряд ошибок. Если до достижения данного значения получен правильный ответ, то счетчик сбрасывается, и подсчет ошибок начинается сначала. Только после достижения указанного в параметре значения предпринимаются заданные действия по обновлению или закрытию подключения. *Стандартное значение – 3.*

Кнопка **Стандартные** устанавливает соответствующие значения параметров контроля жизнеспособности туннеля.

При обнаружении нежизнеспособности DISEC отключить данное подключение.

7.3.5. Дополнительные параметры IKE

Группа параметров **Дополнительные параметры IKE** позволяют манипулировать различными временнЫми интервалами для протокола IKE. При помощи этих параметров можно подобрать необходимые задержки при низкой пропускной способности канала связи и\или производительности устройства пользователя DISEC. Рекомендуется использовать приведенные стандартные значения, которые установятся также и при нажатии кнопки **Стандартные**.

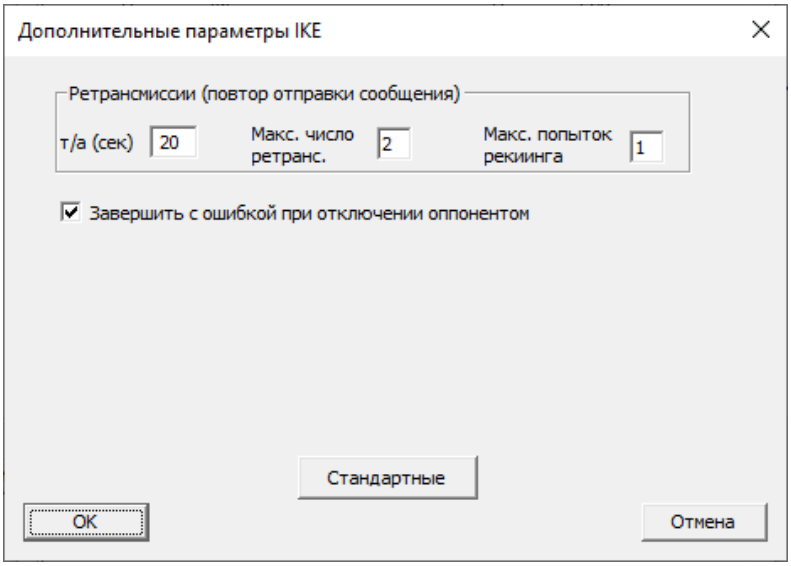


Рис. 43

Ретрансмиссии (повтор отправки сообщения)

Подгруппа параметров **Ретрансмиссии** предназначения для указания интервала времени ожидания ответа и интервала между повторными посылками любых сообщений протокола IKE при согласовании SA IKE (фаза 1), SA ESP (фаза 2) и сообщений "промежуточной" фазы MODE_CFG.

т\а(сек.)

Параметр **т\а(сек.)** позволяет установить значение начального "стартового" интервала ожидания ответа на сообщения протокола IKE. При окончании ожидания при отсутствии ответа интервал ожидания увеличивается в два раза и сообщение посылается в очередной раз. Повтор продолжается пока не будет достигнуто предельное (макс. значение). Стандартное значение - 20 сек.

Макс. число ретранс.

Параметр **Макс. число ретранс.** позволяет установить максимальное число повторных отправлений сообщений IKE. При достижении заданного максимального числа заново начинается процесс согласования SA IKE. Стандартное значение - 2.

Макс. попыток рекиинга

Параметр **Макс. попыток рекиинга** позволяет установить максимальное число повторных согласования SA IKE. При достижении заданного максимального числа согласование заканчивается и выполняется отключение. Стандартное значение - 1.

Завершить с ошибкой при отключении оппонентом

Данная опция позволяет продолжить попытки установления подключения, если они заданы, например в окне **Подключиться**.

Кнопка **Стандартные** устанавливает соответствующие значения дополнительных параметров IKE протокола.

7.4. Вкладка Безопасность для динамического туннеля

Для ДИНАМИЧЕСКОГО туннеля вкладка **Безопасность** имеет вид:

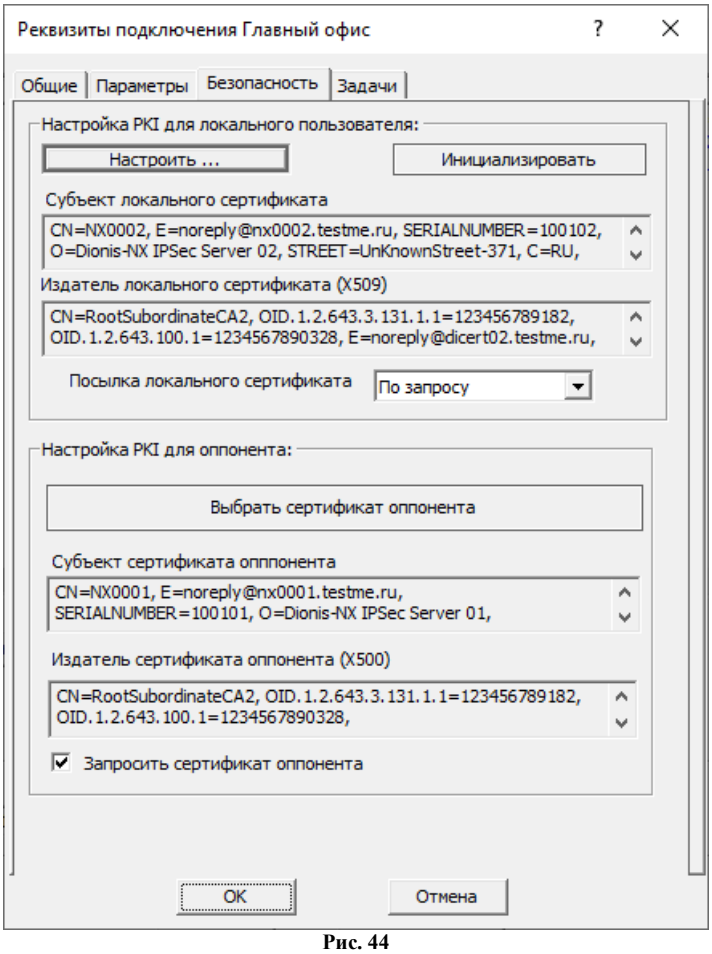


Рис. 44

Данная вкладка предоставляет возможность настроить компоненты аутентификации взаимодействующих объектов в системе PKI.

К компонентам аутентификации относятся с одной стороны информация о закрытом и открытом ключах пользователя DISEC и соответствующих сертификатах, а с другой стороны - информация об открытом ключе оппонента и соответствующих сертификатах ключа.

Настройка PKI для локального пользователя выполняется при нажатии кнопки **Настроить**. В процессе этой процедуры выполняется выбор, проверка и размещение во внутренних структурах всех необходимых ключевых объектов (ключевой контейнер, сертификат, сертификаты издателей и списки отозванных сертификатов). Также настраивается необходимость пересылки локального сертификата Серверу VPN во время процедуры взаимной аутентификации протокола IKE.

Настройка PKI для оппонента состоит в выборе сертификата оппонента и установки опции запроса сертификата с Сервера VPN в процессе подключения.

В качестве сертификата оппонента может быть выбран сертификат УЦ. В этом случае в процессе подключения будет принят к рассмотрению любой действующий присланный сертификат, выпущенный данным УЦ. В обоих случаях данный сертификат должен быть помещен в хранилище сертификатов данного Подключения.

7.4.1. Настройка PKI для пользователя

Настройка PKI пользователя позволяет выполнить следующие действия:

1. выбор ключевого носителя и ввод в систему закрытого ключа пользователя;
2. выбор личного сертификата пользователя, соответствующего ключу пользователя, и назначение этого сертификата текущим;
3. создание двух типов хранилищ сертификатов и списков отзыва (общего хранилища и хранилища корневых сертификатов);

4. занесение личного сертификата пользователя в хранилище сертификатов;
5. ввод с файловых носителей и занесение в соответствующие хранилища всех необходимых для построения цепочки доверия сертификатов УЦ и списков отозванных сертификатов (СОС).

Настройка PKI пользователя выполняется следующим образом.

После нажатия кнопки **Настроить** вкладки **Безопасность** на экран будет выведено окно **Настройка PKI пользователя**.

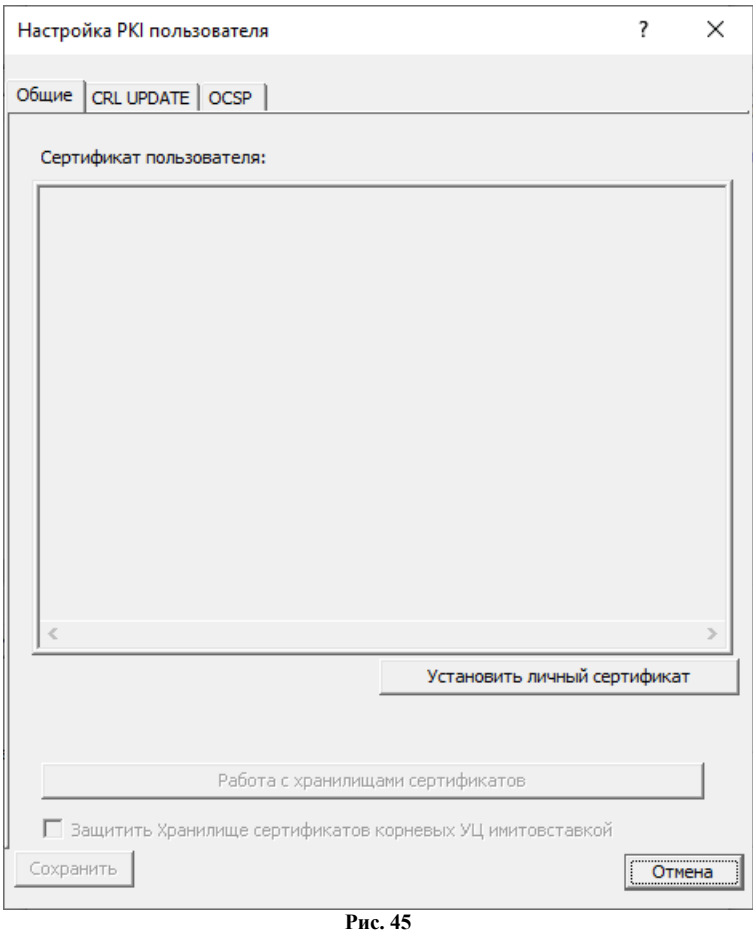
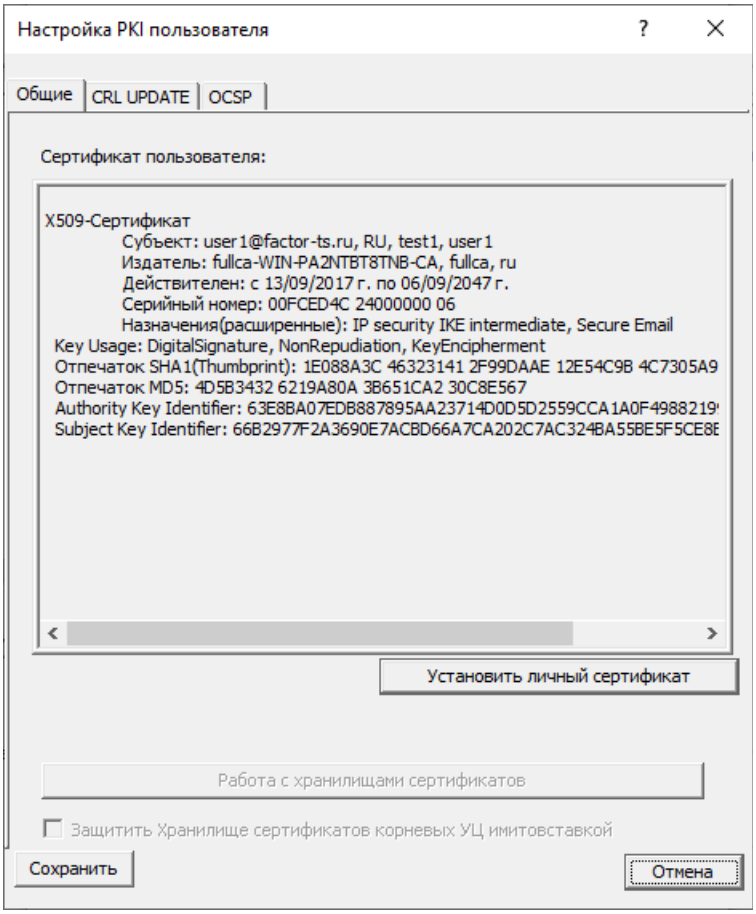


Рис. 45

Вставить ключевой носитель в считывающее устройство или в порт USB и нажать кнопку **Установить личный сертификат**, после чего автоматически начнется процедура последовательного выполнения перечисленных выше действий.



46

После того как будут выполнены все настройки, следует в окне **Настройка PKI пользователя** нажать кнопку **Сохранить**. При этом выполнится выход из окна в окно **Безопасность**.

Если сделаны все настройки, но по каким-либо причинам (например, не вставлен ключевой носитель) не выполнена инициализация, то система выдаст соответствующее сообщение и сделает активной кнопку **Инициализировать** на вкладке **Безопасность**.

После успешной инициализации рекомендуется снова зайти в окно **Настройка PKI пользователя**, добавить все необходимые сертификаты и списки отзыва, необходимые для построения цепочек доверия. Рекомендуется также выполнить защиту хранилища сертификатов доверенных корневых УЦ, т.е. установить флажок **Защитить Хранилище сертификатов корневых УЦ имитовставкой** и сохранить настройки.

7.4.1.1. УСТАНОВКА ЛИЧНОГО СЕРТИФИКАТА

Процедура установки личного сертификата состоит из последовательности запросов со стороны DISEC и ответов пользователя.

При прерывании процедуры пользователем, например, при отсутствии нужного носителя, следует устранить причину и начать ее заново.

На экран будет выведено окно **Выбора ключевого контейнера**, содержащее список съемных носителей, а для PKCS11-токенов список контейнеров.

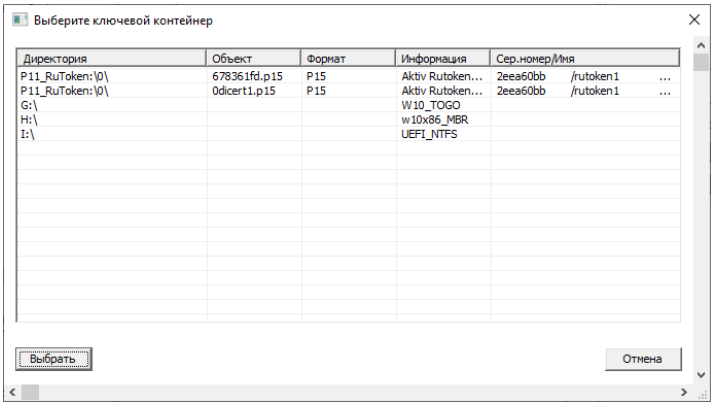


Рис. 47

Пользователю необходимо выбрать ключевой контейнер: в списке носителей следует выделить строчку с нужным контейнером (т.е. с тем контейнером, который содержит закрытый ключ пользователя DISEC) и нажать кнопку **Выбрать**.

Если ключевой контейнер защищен паролем, то будет выдан запрос на его ввод.

В случае выбора токена PKCS11 всегда последует запрос на ввод пароля:

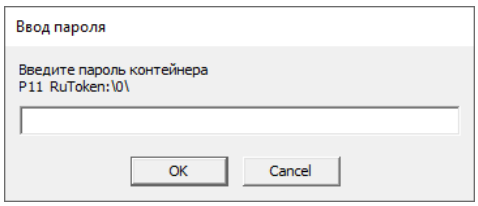


Рис. 48

Пользователю необходимо ввести известный ему пароль или ПИН-код для токена.

Затем будет выдан запрос на выбор соответствующего ключевому контейнеру сертификата. Программа перебирает имеющиеся в текущей директории файлы с расширением "`.cer`" и предлагает пользователю выбрать подходящий.

При положительном ответе в дальнейшем будет продолжена процедура обработки данного сертификата.

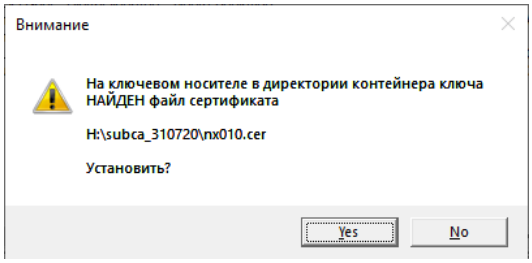


Рис. 49

Пользователь либо соглашается на предложенный вариант, либо отказывается. При отрицательном ответе будут последовательно предлагаться имеющиеся в данной директории носителя сертификаты.

Если на все предложенные варианты пользователь ответил отрицательно, предлагается вариант самостоятельного поиска сертификата.

При поиске сертификатов предоставляется выбор по всем доступным в системе носителям, в том числе по жестким внешним и внутренним дискам (HDD).

Пользователю необходимо перейти на нужный носитель и выбрать сертификат.

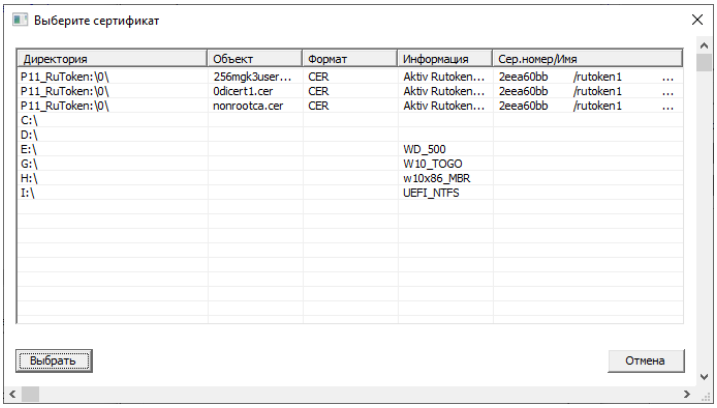


Рис. 50

После успешного выбора сертификата программа приступит к созданию ссылки на личный сертификат.

В случае несоответствия ключевой информации выбранному сертификату будет выдано сообщение об ошибке.

В этом случае следует прервать процедуру и начать сначала.

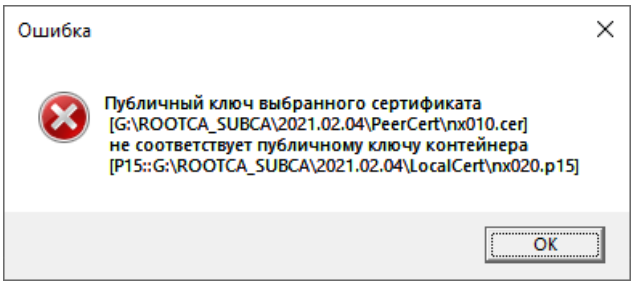


Рис. 50

Перед продолжением процедуры выдается запрос, отрицательный ответ на который позволяет закончить процедуру на замене личного сертификата.

При замене личного сертификата, предыдущий (замененный) сертификат удаляется из хранилища.

При создании нового ресурса подключения следует ответить положительно на этот запрос. Если выполняется только замена личного сертификата, например, после окончания срока его действия или отзыва по причине компрометации, то, ответив отрицательно, можно закончить процедуру.

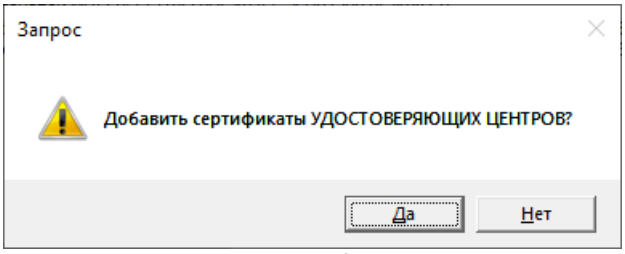


Рис. 50

Во время продолжения процедуры с целью построения цепочки сертификатов доверенных УЦ появится окно для выбора на любых доступных носителях.

Для носителей типа PKCS11 будут доступны только **публичные** зоны.

Для носителей типа PKCS11 с выбранным ключевым носителем будет доступна также **приватная** зона.

В данный момент можно выбрать только один сертификат УЦ, файловое хранилище SST или контейнер P7B. Остальные следует выбрать позже вручную при работе с хранилищами сертификатов.

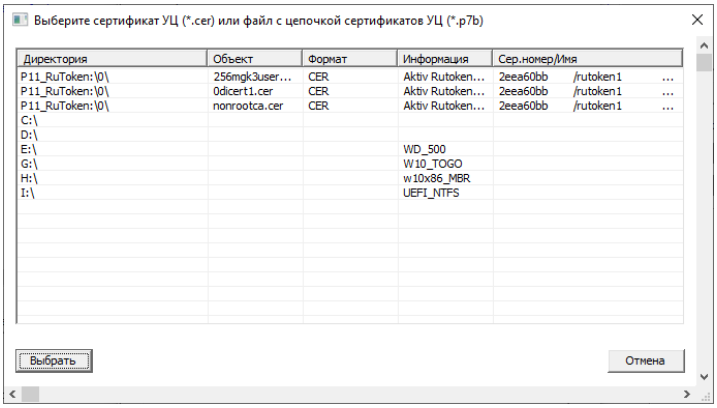


Рис. 51

После этого (при выборе файла P7B или SST) система выведет на экран информацию из очередного выбранного сертификата УЦ, которая позволит пользователю идентифицировать сертификат, и предложит добавить его в хранилище (или заменить, если сертификат уже находится в хранилище).

Пользователю необходимо сделать выбор.

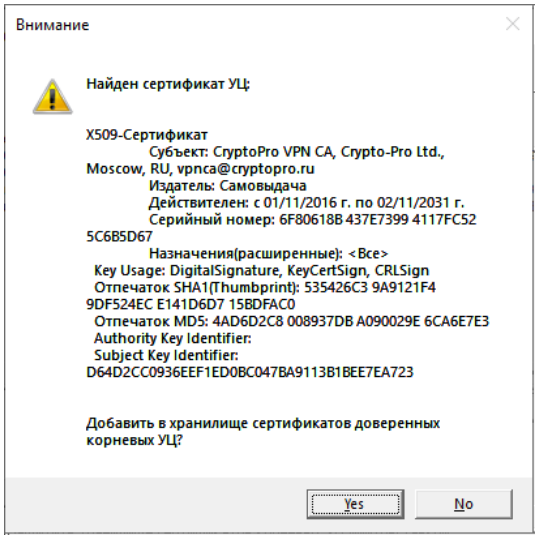


Рис. 52

После выбора сертификата УЦ программа будет выполнять поиск CRL, предлагая поочередно файлы с расширением ".crl".

Пользователю необходимо сделать выбор.

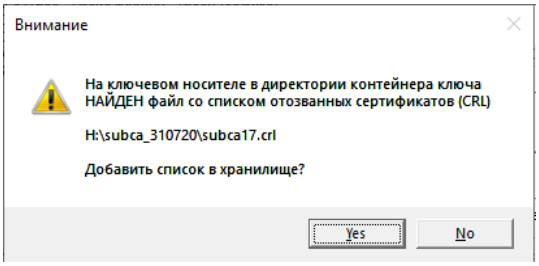


Рис. 53

При отказе от всех предложенных будет выведено окно для самостоятельного выбора CRL на всех носителях информации.

Для носителей типа токен будут доступны только **публичные** зоны.

Для токен с выбранным ключевым носителем будет доступна также **приватная** зона.

Пользователю необходимо сделать выбор.

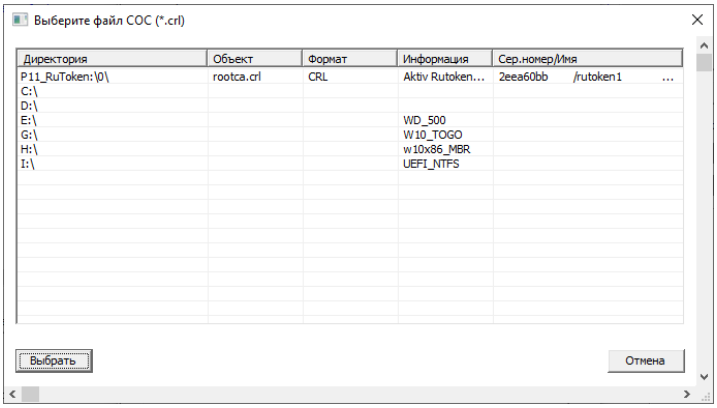


Рис. 54

Выбранные CRL считывается из файла и представляются на рассмотрение пользователю.

Пользователю необходимо сделать выбор.

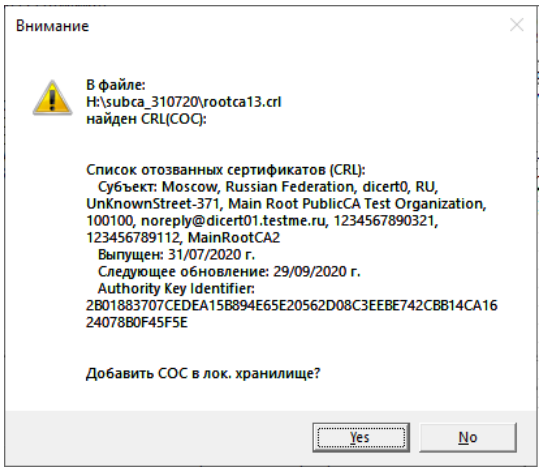


Рис. 55

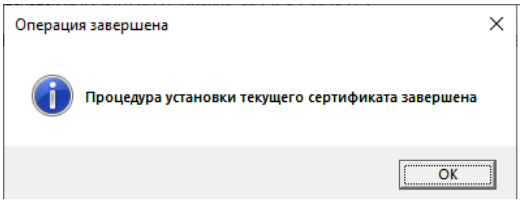


Рис. 56

Если вместе с заменой локального сертификата выполнялась также и замена сертификата УЦ и соответствующих CRL, то "устаревшие" сертификаты и CRL НЕ УДАЛЯЮТСЯ. Их рекомендуется удалить вручную. Однако их присутствие не будет мешать функционированию.

7.4.1.2. НАСТРОЙКА ПАРАМЕТРОВ ОБНОВЛЕНИЯ CRL

В окне **Настройки криптосистемы** имеется возможность настраивания параметров автоматического обновления списка отзыва (**CRL**) сертификатов УЦ, используемых в данном Подключении.

Автоматическое обновление **CRL** будет выполняться каждый раз в соответствии с настройками, а также по команде проверки сертификатов и при установке периодической проверки.

Настройка выполняется на вкладке **CRL.**

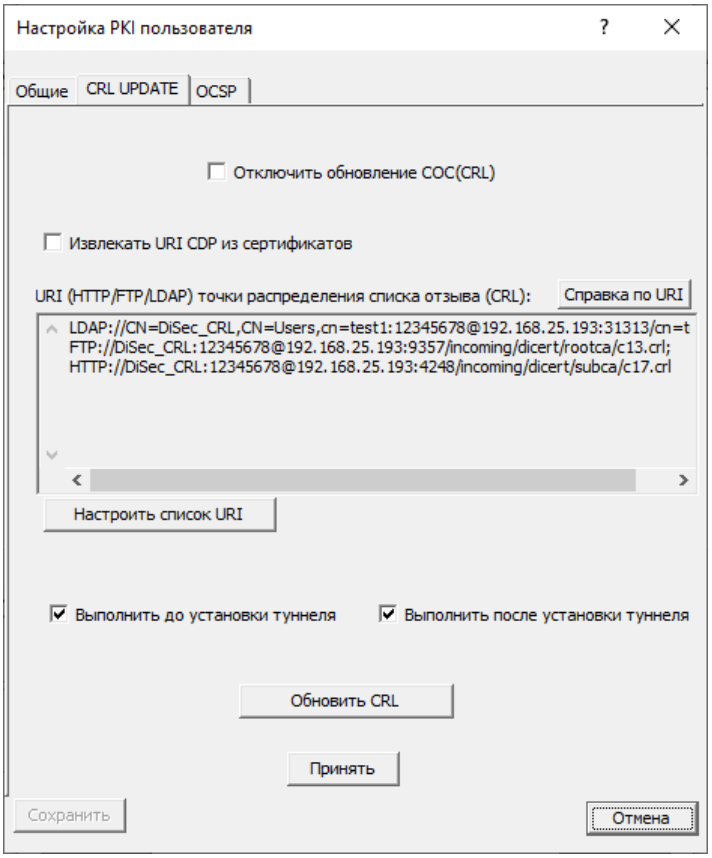


Рис. 57

На вкладке **CRL UPDATE** можно настроить автоматическое обновление списка отзыва.

Эта возможность позволяет повысить эффективность проверки статуса сертификатов, обеспечивая использование во время проверки сертификата (построения Цепочки Доверия) актуального COC (CRL), получаемого с соответствующего сервера. Адреса серверов задаются при помощи **URI** (Uniform Resource Identifier - унифицированный указатель информационного ресурса).
Автоматическое обновление списков отзыва позволяет загрузить из точки распространения актуальные CRL и поместить в хранилище сертификатов пользователя.

Отключить обновление COC

Опция **Отключить обновление COC** позволяет полностью отключить автоматическое обновление списков отозванных сертификатов. Если эта опция включена, то обновление списков отзыва не будет выполняться, другие опции этого раздела станут не доступными для изменения.
При снятии флажка **Отключить обновление COC** становятся доступными элементы управления в данной секции.

URI(HTTP(s)/FTP/LDAP) точки распределения списка отзыва (CRL):

Данное поле задает один или несколько идентификаторов сетевых ресурсов разделенных символом ";". предназначенных для выполнения обновления списков отзыва. Формат URI соответствует синтаксису протоколов http, ftp, ldap (регистр написания не имеет значения)б формат которых может быть уточнен по нажатию кнопки **Справка по URI**:

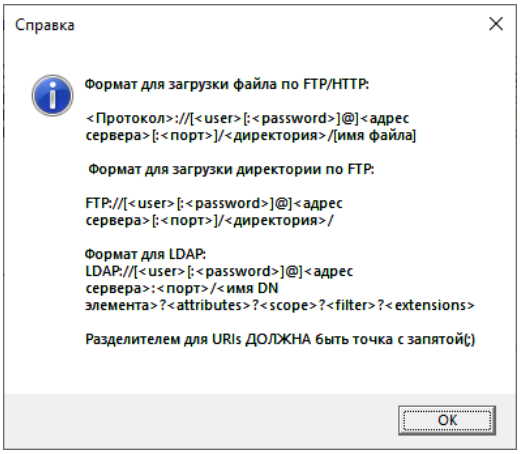


Рис. 58

Данное поле может оставаться пустым, в этом случае обновление CRL будет выполняться по URI, указанным в сертификате пользователя и сертификатах УЦ:

Извлекать URL CDP из сертификатов

При установке флажка **Извлекать URL CDP из сертификатов** помимо адреса в поле "**URI(HTTP(s)/FTP/LDAP) точки распределения списка отзыва (CRL)**" будут использоваться адреса точек распределения списков отзыва, указанные в сертификате (поле "*CRL Distribution Point*").
Точки распределения списков отзыва могут отсутствовать в сертификате.

Кнопка **Список URI** - позволяет вывести список URI в виде таблицы, а также позволяет добавлять, удалять и изменять отдельные элементы, а также состав списка.

Обновить CRL

Кнопка **Обновить CRL** позволяет обновить список отзыва вручную с соответствующего сервера, указанного в поле "**URI(HTTP(s)/FTP/LDAP) точки распределения списка отзыва (CRL):**".

Выполнить до установки туннеля

Флажок **Выполнить до установки туннеля** определяет выполнение обновления COC (CRL) в начале процедуры установки данного Подключения. Если COC (CRL), необходимый для построения цепочки доверенных сертификатов для сертификата пользователя и\или сертификата оппонента, не является действующим, а обновление COC (CRL) закончилось неудачей либо не выполнялось, процедура подключения прерывается.

Выполнить после установки туннеля

Флажок **Выполнить после установки туннеля** определяет выполнение обновления COC (CRL) после установки туннеля после запуска данного Подключения. Этот режим используется, если сервер находится в защищенной сети. Обновление COC (CRL) будет выполняться каждый раз при проверке сертификатов Подключения перед обновлением 1-й Фазы IKE, выполняемой периодически в соответствии с параметром "Период смены ключей Ike" в настройках.

7.4.1.3. НАСТРОЙКА ПАРАМЕТРОВ ПРОВЕРКИ ПО OCSP

Использование OCSP-сервера позволяет в реальном времени проверить статус сертификата.

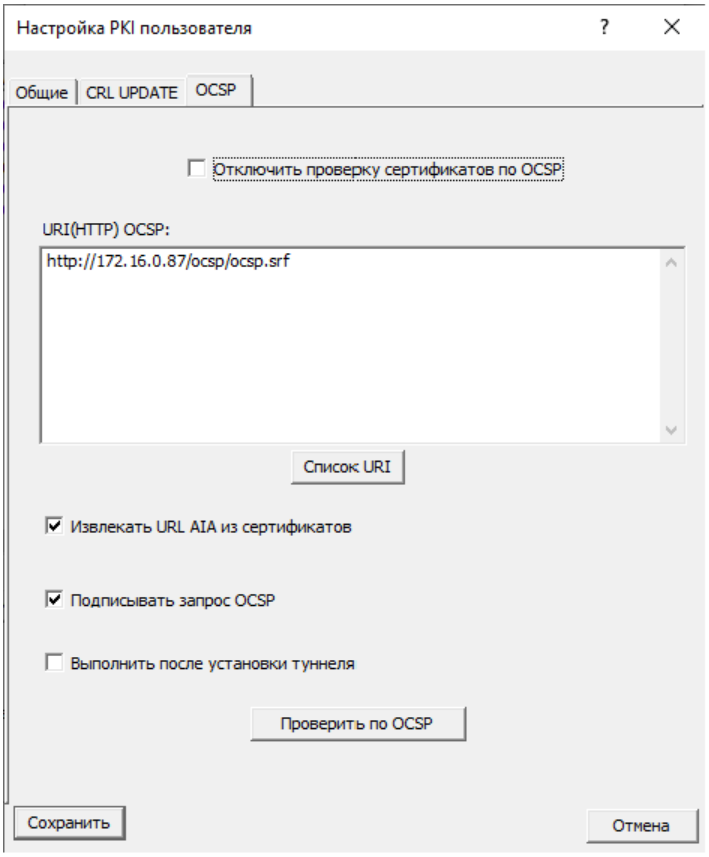


Рис. 59

Отключить проверку сертификатов по OCSP

Опция **Отключить проверку сертификатов по OCSP** позволяет полностью отключить или включить проверку сертификатов по OCSP протоколу. Если эта опция включена, то проверка сертификатов по OCSP протоколу не будет осуществляться, другие опции этого раздела станут не доступными для изменения, но их значения сохраняются, если были установлены ранее. При снятии флажка **Отключить проверку сертификатов по OCSP** становятся доступными элементы управления в данной секции.

URI(HTTP) OCSP

Поле **URI(HTTP) OCSP** - это адрес и атрибуты OCSP сервера, с помощью которого будет происходить проверка статусов сертификатов.

Список URI

Кнопка **Список URI** - позволяет вывести список URI в виде таблицы, а также позволяет добавлять, удалять и изменять отдельные элементы, а также состав списка.

Извлекать URL AIA из сертификатов

Опция **Извлекать URL AIA из сертификатов** позволяет использовать при проверке статуса сертификата адрес OCSP сервера, указанный в проверяемом сертификате. Этот адрес извлекается из соответствующего сертификата X509 из поля *Authority Information Access (AIA)*. Если в проверяемом сертификате данный адрес отсутствует, то будет использовать адрес из поля "**URI(HTTP) OCSP**" (если задан).

Подписывать запрос OCSP

Опция **Подписывать запрос OCSP** определяет, что каждый запрос будет подписываться собственным ключом. Эта специфическая опция может иметь существенное значение, если сервер OCSP не принимает подписанные запросы или, наоборот, принимает только подписанные запросы.

Выполнить после установки туннеля

Флажок **Выполнить после установки туннеля** определяет выполнение проверки сертификата по OCSP ТОЛЬКО после установки туннеля после запуска данного Подключения. Этот режим используется, если сервер OCSP находится в защищенной сети. При получении отрицательного результата подключение отключается.
При снятом флажке проверка сертификатов по OCSP будет выполняться в начале процедуры установки Подключения. Только после успешной проверки сертификатов будет выполняться подключение.

Проверить по OCSP

Кнопка **Проверить по OCSP** позволяет выполнить проверку текущего сертификата пользователя для данного Подключения.

7.4.1.4. НАСТРОЙКА СПИСКА URI

В окне **Настройка списка URI** в виде таблицы приведены используемые URI - Uniform Resource Identifier (унифицированный идентификатор ресурса).
Данные элементы списка предназначены либо для обновления CRL - списков отозванных сертификатов, либо для проверки сертификатов по протоколу OCSP для PKI-подключения.

URI для OCSP

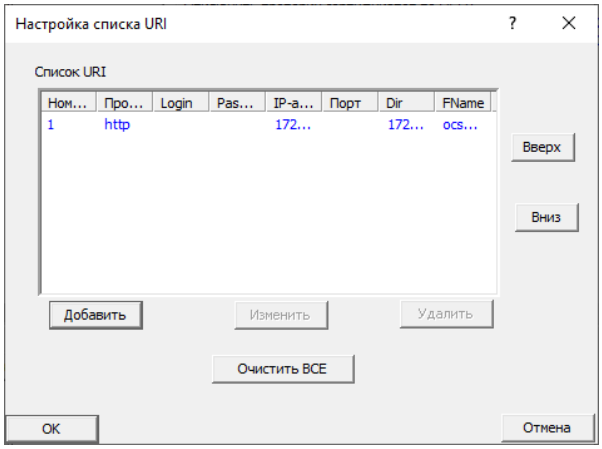


Рис. 60

URI для CRL Update

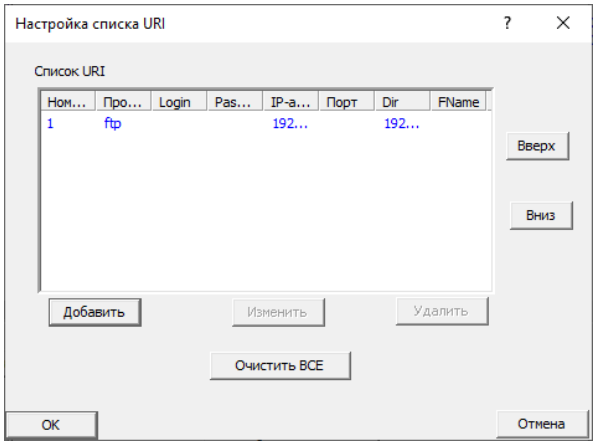


Рис. 61

По кнопке **Добавить** будет открыто окно **Настройка URI** для добавления нового элемента в список:

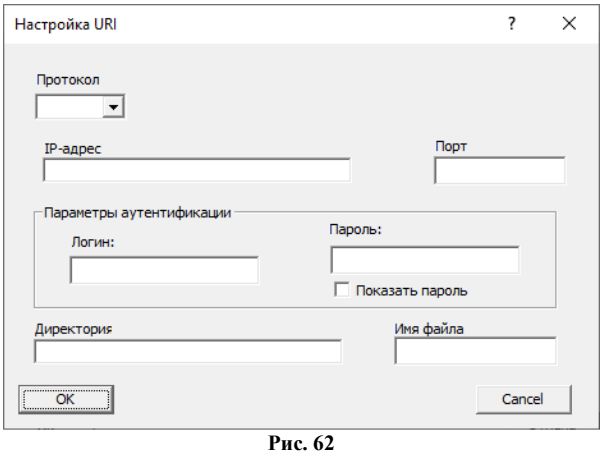


Рис. 62

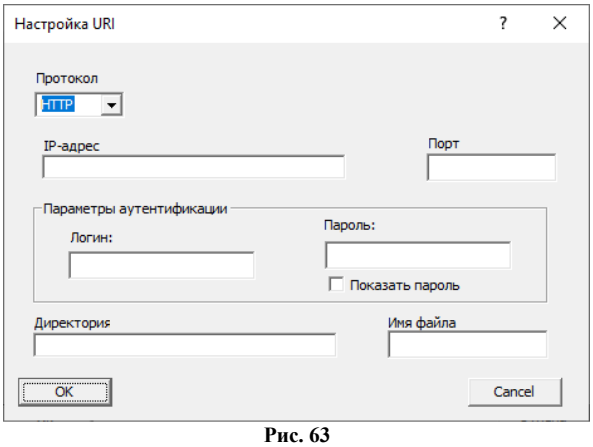


Рис. 63

Поскольку для проверки по протоколу OCSP используется только сетевой протокол HTTP, то он сразу будет отображен в соответствующем поле окна.
При выделении уже существующего элемента в списке URI и нажатии кнопки **Изменить** будет открыто окно **Настройка URI** с заполненными полями.

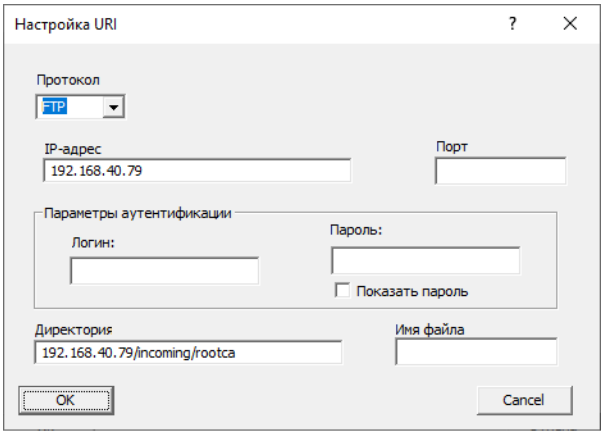


Рис. 64

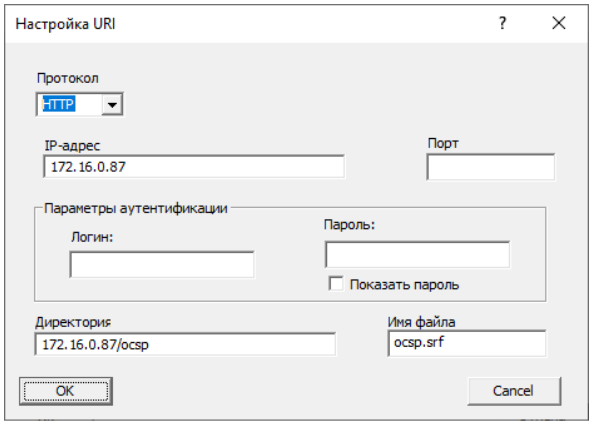


Рис. 65

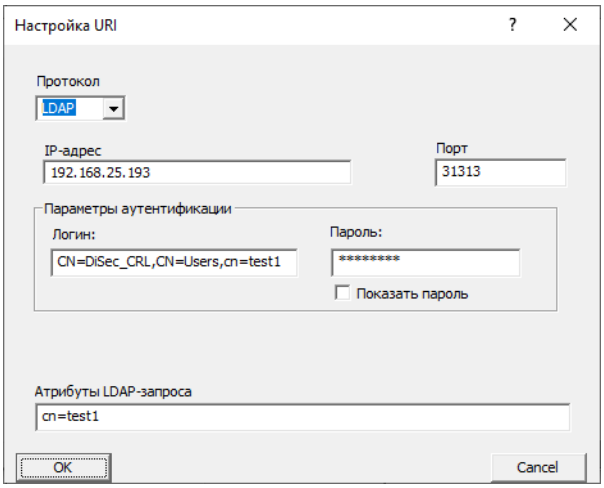


Рис. 64

Из выпадающего списка Протокол можно выбрать допустимое значение: для обновления CRL доступны три значения - FTP, HTTP и LDAP.

Группа **Параметры аутентификация** позволяют задать логин и пароль необходимый для аутентификации на серверах, где размещены точки распределения в соответствии со значением в поле **URI(HTTP(s)/FTP/LDAP) точки распределения списка отзыва (CRL)"**. Поля могут оставаться пустыми, если сервер не требует аутентификации. Для FTP-сервера будут автоматически подставляться значения для анонимного входа.

При заполнении поля **Директория** начальный и конечный слэши можно не добавлять - они добавятся автоматически.

После изменения или заполнении недостающих полей в составе URI и нажатия кнопки OK в секции Список URI соответствующей вкладки настройки обновления CRL или настройки проверки по протоколу OCSP появится список URI, каждый элемент которого сформируется автоматически из заданных полей.

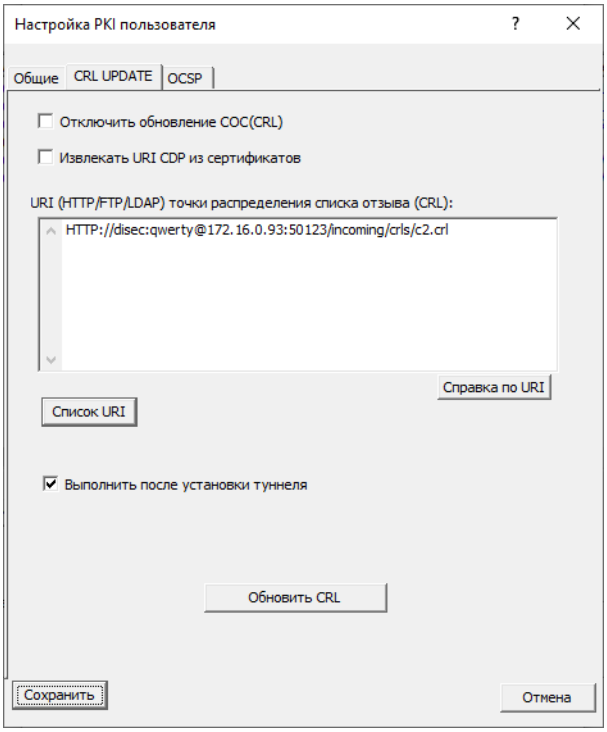


Рис. 66

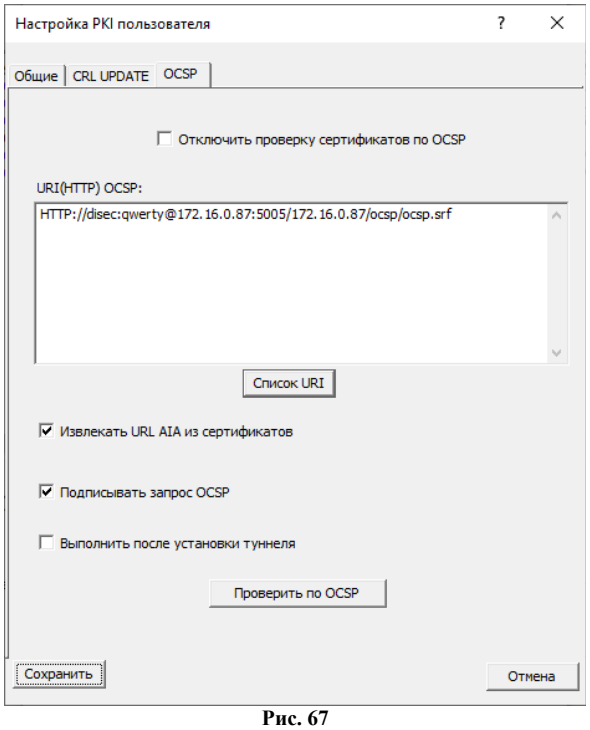


Рис. 67

7.4.2. Выбор сертификата оппонента

Пользователь DISEC должен иметь сертификат оппонента, с которым предполагается взаимодействие, на ключевом или другом носителе.
В процессе настройки Подключения его необходимо поместить в локальное хранилище сертификатов, а также всю цепочку УЦ, начиная с издателя вплоть до корневого, и их CRL.
В процессе переговоров по протоколу IKE выполняется проверка присланной идентификационной информации (имя субъекта сертификата и сам сертификат) с хранящимся в хранилище сертификатом оппонента.
Для выбора сертификата оппонента на вкладке **Безопасность** имеется кнопка **Выбор сертификата оппонента**.
После ее нажатия открывается окно **Работа с хранилищем сертификатов**.

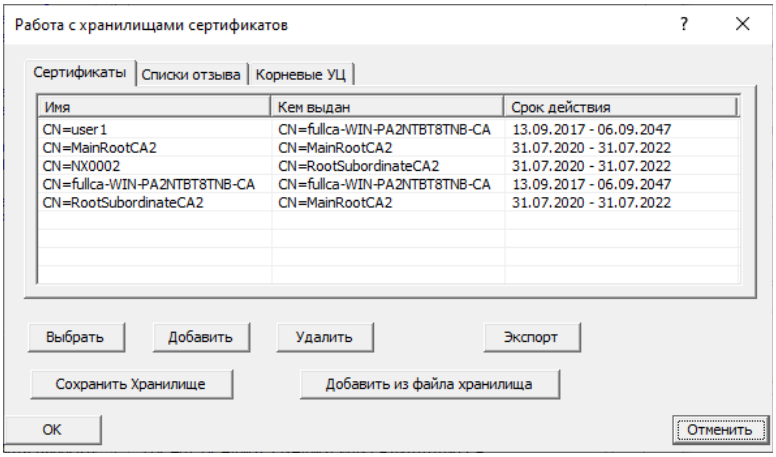


Рис. 68

Если необходимый сертификат оппонента отсутствует в списке, необходимо нажать кнопку **Добавить** на вкладке **Сертификаты**, и в открывшемся списке выбрать нужный сертификат. При необходимости следует выполнить поиск на нужном съемном носителе в нужной поддиректории и выбрать сертификат.

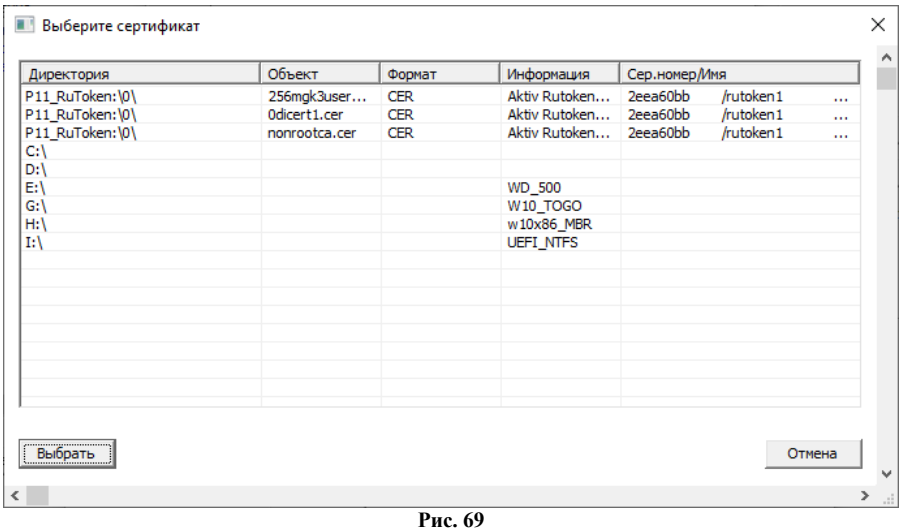


Рис. 69

После помещения сертификата оппонента в хранилище следует удостовериться, что ВСЕ сертификаты из цепочки сертификатов, подписавших этот сертификат, и соответствующие им CRL присутствуют в хранилищах (они могут присутствовать, если сертификат пользователя и оппонента выпущены одним и тем же УЦ).

При отсутствии каких-либо объектов НЕОБХОДИМО добавить их посредством процедуры **добавления** с носителей.

> *Примечание*. Данная процедура заметно упрощается, если все необходимые объекты помещены в файловое хранилище **SST** или контейнер **P7B**.

Далее следует выбрать сертификат оппонента посредством кнопки **Выбрать**.

В качестве сертификата оппонента может быть выбран сертификат УЦ. В этом случае в переговорах по протоколу IKE от оппонента будут приниматься любые сертификаты пользователя, подписанные данным УЦ.

> *Примечание*. Сам сертификат УЦ не может быть использован в переговорах IKE, поскольку, как правило, не имеет разрешения на использование в этом качестве.

Окно закроется, а реквизиты выбранного сертификата будут отображены в окне **Безопасность**.

7.4.2.1. ПОИСК СЕРТИФИКАТА ИЛИ CRL НА НОСИТЕЛЯХ

Окно выбора объекта (контейнера ключа, сертификата или CRL) на носителях открывается при необходимости выбора пользователем соответствующих объектов. При этом в зависимости от типа объекта отображается список разных типов носителей. Так для ключевого контейнера отображается список съемных носителей, зарегистрированных ОС Windows. Токены отображаются только те, для которых инсталлированы драйверы, независимо от инсталляции ПО DISEC, и которые поддерживаются ПО DISEC.

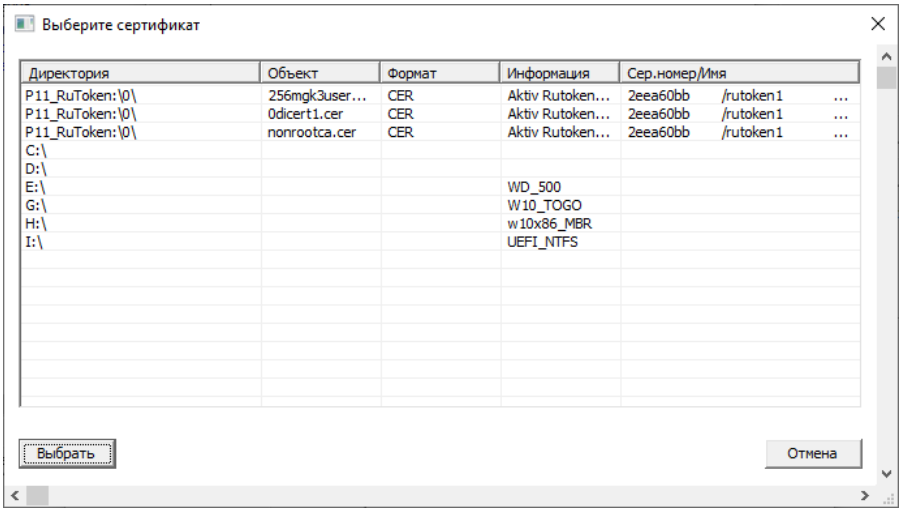


Рис. 70

Можно двойным щелчком мыши либо выбрать контейнер, либо перейти в список объектов и поддиректорий на любом съемном носителе.

Продолжая переходы по поддиректориям, следует выбрать нужный объект.

7.4.3. Настройка пересылки сертификатов

Посылка локального сертификата

В поле под этим заголовком имеется выпадающий список с тремя опциями:

- *Не посылать*
- *Посылать*
- *По запросу*

Данная настройка должна быть согласована с сервером VPN. Стандартное значение - «*Не посылать*» - для уменьшения накладных расходов на пересылку, поскольку рекомендуется, чтобы сертификат пользователя уже был помещен на сервер. Однако, IPSEC-соединение может быть настроено на «шаблон» имени субъекта или издателя сертификата, в этом случае, Сервер VPN пришлет запрос, в ответ на который необходимо отправить сертификат. Поэтому рекомендуемое значение - «*По запросу*».

7.4.4. Настройка запроса сертификата оппонента

Флажок **Запросить сертификат оппонента** служит для включения или отключения формирования запроса сертификата (CR) в процессе процедуры взаимной аутентификации протокола IKE сертификата оппонента для сравнения с имеющимся у пользователя DISEC сертификатом.

> *Примечание.* Сертификаты всех Серверов VPN, с которыми предполагается создавать туннели, предварительно должны быть помещены в хранилище пользователя DISEC (см. раздел Подготовка к работе в режиме динамического туннеля).

7.4.5. Хранилища сертификатов

Для хранения сертификатов, необходимых пользователю DISEC, используется хранилища сертификатов - общее и хранилище корневых (самоподписанных сертификатов УЦ), отдельные для каждого ресурса подключения. В хранилищах подключения содержатся два типа объектов, которые размещаются в них в процессе настройки Подключения:

1. **Сертификаты** - сертификат(ы) открытых ключей пользователя DISEC, сертификаты открытых ключей всех Серверов VPN, с которыми предполагается устанавливать туннели, и сертификаты доверенных удостоверяющих центров, включая корневые.
2. **Списки отзыва** - списки отозванных сертификатов всех УЦ, необходимые для построения цепочки доверия.

Помещение объектов в хранилища выполняются либо автоматически в процессе настройки личного сертификата пользователя DISEC, либо может быть выполнено вручную для добавления, просмотра и удаления объектов.

Переход в окно работы с хранилищами может быть выполнен:

1) либо из окна **Настройка PKI пользователя** становится активной кнопка **Работа с хранилищем сертификатов** после того как будет закончена установка личного сертификата пользователя,

2) либо с вкладки **Безопасность** по кнопке **Выбор сертификата оппонента**.

После нажатия одной из этих кнопок на экран будет выведено окно **Работа с хранилищами сертификатов**, открытое на вкладке **Сертификаты**.

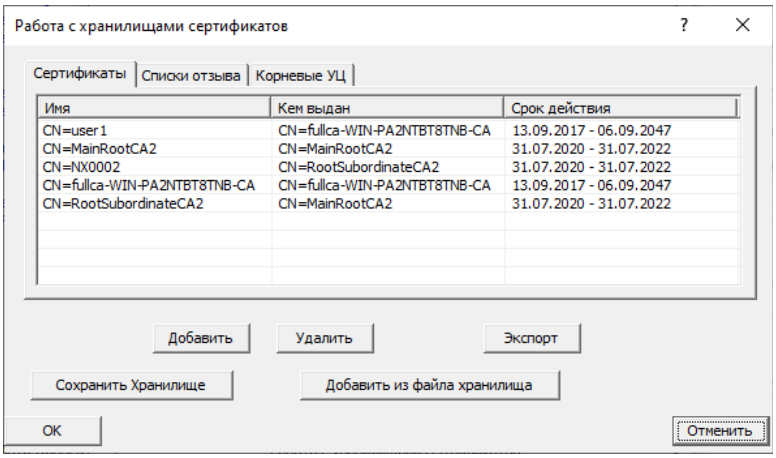


Рис. 71

Во втором случае (по кнопке **Выбор сертификата оппонента**) в окне **Работа с хранилищами сертификатов** добавится дополнительная кнопка **Выбрать**.

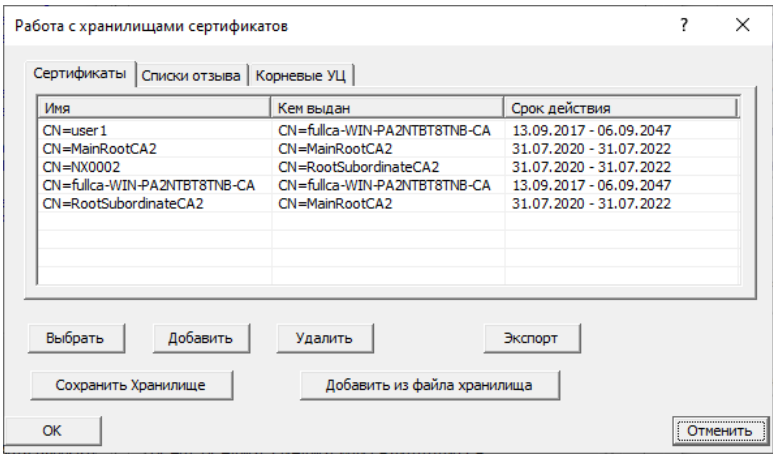


Рис. 72

В окне **Работа с хранилищами сертификатов** выводится информация обо всех объектах в обоих хранилищах. На первых двух вкладках отображаются объекты из ОБЩЕГО хранилища, а сертификаты Корневых УЦ отображаются на 3-ей вкладке (Корневые УЦ). Действия кнопок под списком относятся к соответствующему хранилищу. Т.е. для работы с Корневыми сертификатами УЦ необходимо перейти на 3-ю вкладку.

Пользователь имеет возможность выполнить следующие действия:
1) добавить в хранилище новый объект (сертификат или СОС, в соответствии с вкладкой),
2) удалить имеющийся,
3) просмотреть более подробную информацию об объекте, выведя его содержимое на экран.
4) Записать объект в файл (экспорт).

Для выполнения одного из перечисленных действий необходимо перевести курсор на строчку в таблице и либо щелкнуть правой кнопкой мыши - на экран будет выведено меню для выбора требуемого действия, либо выполнить действия при помощи соответствующих кнопок, расположенных под списком.
Просмотр осуществляется по двойному клику на строке с объектом.

Примечание. Функция экспорта для корневых сертификатов не поддерживается. Вследствие этого при переходе на 3-.ю вкладку кнопка **Экспорт** отсутствует.

Вкладка Сертификаты

Вкладка **Сертификаты** содержит таблицу со списком сертификатов. В списке отображаются как сертификаты пользователей, так и сертификаты УЦ, в том числе, сертификаты корневых УЦ.

В таблице информация о каждом сертификате занимает одну строку. В первой графе таблицы выводится имя владельца сертификата, во второй - имя удостоверяющего центра, выдавшего сертификат, в третьей - срок действия сертификата.

Чтобы просмотреть сертификат, надо выделить соответствующую строчку в таблице и дважды щелкнуть левой кнопкой мыши, либо в меню выбрать команд **Просмотреть сертификат**. На экран будет выведено стандартное окно **Сертификат**, открытое на вкладке **Общие**. На этой вкладке содержатся общие сведения о сертификате: имя владельца сертификата, имя УЦ, выдавшего сертификат и время действия сертификата.

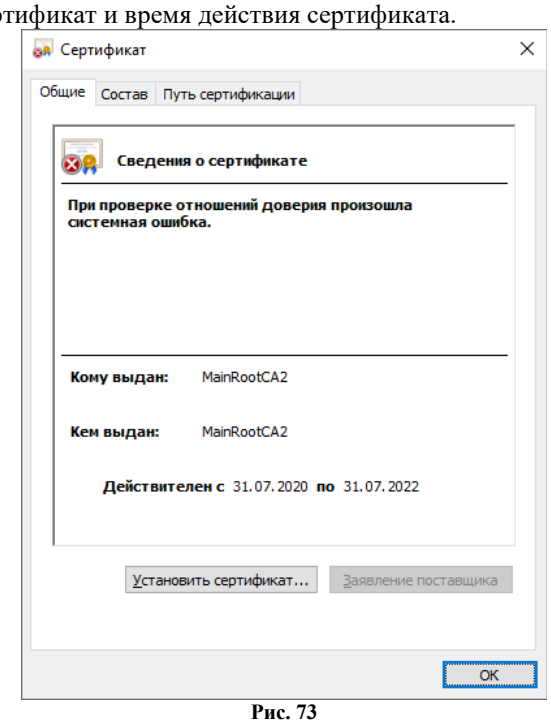


Рис. 73

На вкладке **Состав** содержатся данные всех полей сертификата. В верхнем окне - название поля и его значение; в нижнем окне - более подробное значение того поля, на котором установлен курсор в верхнем окне.

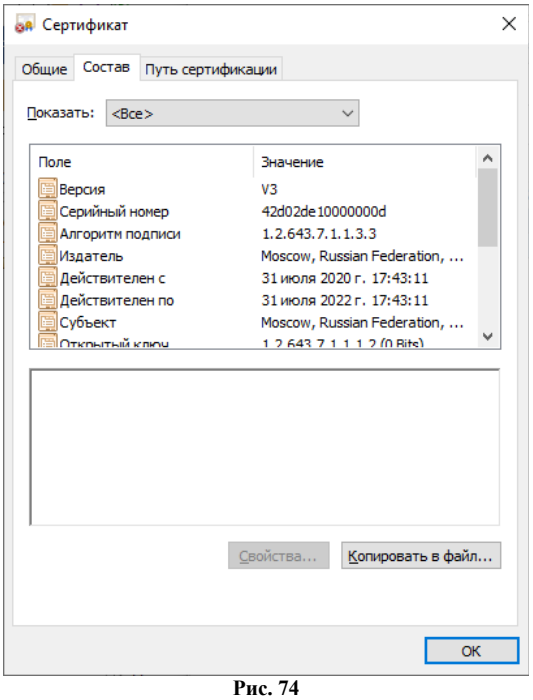


Рис. 74

Вкладка Списки отзыва

Вкладка **Списки отзыва** окна **Работа с хранилищами сертификатов** содержит все CRL для всех сертификатов УЦ - и корневых и не корневых.

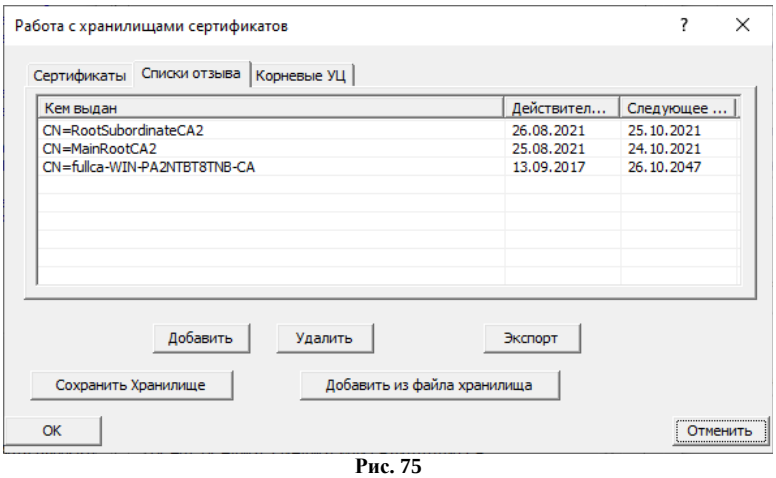


Рис. 75

В таблице каждый список занимает одну строку. В 1-й графе таблицы выводится имя удостоверяющего центра, выпустившего список, во 2-й - дата выпуска списка, в 3-й - срок действия списка.

При просмотре списка на экран выводится окно **Список отзыва сертификатов**, содержащее две вкладки и открытое на вкладке **Общие**. На этой вкладке содержатся сведения о списке отзыва: в верхнем окне - название поля и его значение; в нижнем окне - более подробное значение того поля, на котором установлен курсор в верхнем окне.

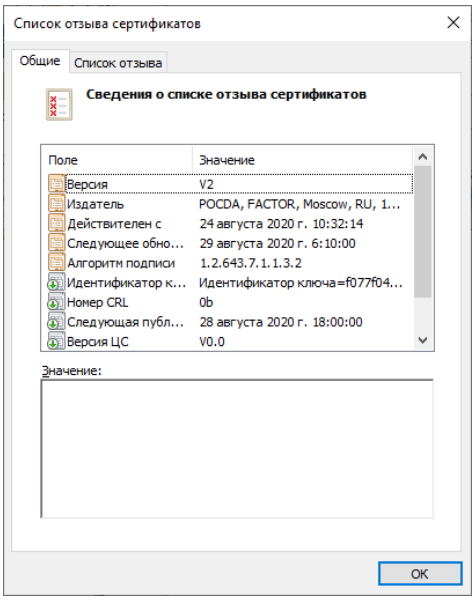


Рис. 76

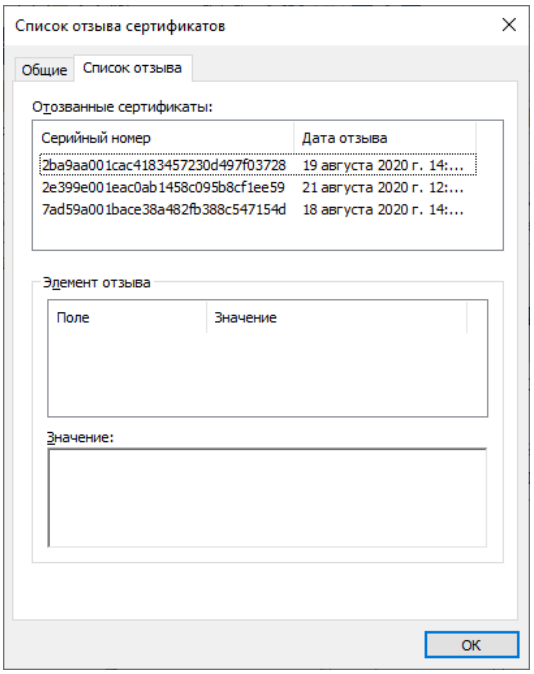


Рис. 77

На вкладке **Список отзыва** перечислены все отозванные сертификаты указанного списка. В верхнем окне - серийный номер и дата отзыва сертификата; во втором окне - информация о том сертификате, на котором установлен курсор в верхнем окне; в нижнем окне - более подробная информация о значении того поля, на котором установлен курсор в среднем окне.

Вкладка Корневые УЦ

Вкладка **Корневые УЦ** содержит корневые сертификаты удостоверяющих центров.
В таблице каждый сертификат занимает одну строку. Формат записей полностью совпадает с рассмотренным выше форматом записей для вкладки **Сертификаты**. Сертификаты корневых УЦ являются «самоподписанными», поэтому для них совпадают значения в первых двух графах: **Имя** и **Кем выдан**.

Пользователь может добавить в хранилище новый сертификат, удалить имеющийся и получить более подробную информацию о сертификате. Эти действия выполняются так же, как и для вкладки **Сертификаты**.

Кнопка Добавить

Кнопка **Добавить** в нижней части экрана также служит для добавления объекта, соответствующего вкладке, в хранилище; кнопка **Удалить** - для удаления.

При *добавлении* сертификата по кнопке **Добавить** на экран выводится окно, позволяющее выбрать файл с нужным сертификатом. При вызове окна оно содержит список файлов на всех доступных носителях (имена файлов, как правило, имеют расширение **cer**), в столбце **Формат** отображается "CER".

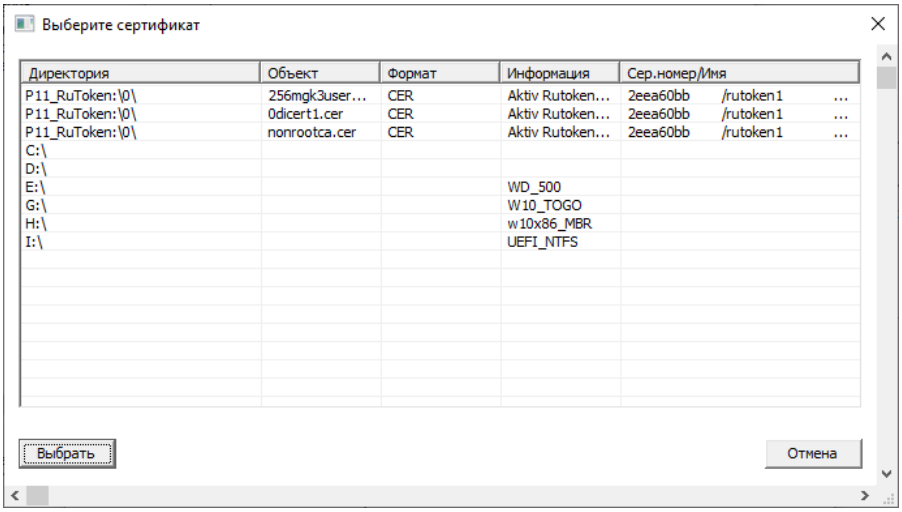


Рис. 78

Если требуется добавить корневой сертификат УЦ, то необходимо перейти на вкладку **Корневые УЦ** и выполнить команду добавления или нажать кнопку **Добавить**. В результате появится окно для поиска сертификатов УЦ (файлы с расширением **cer**) или контейнеров с сертификатами УЦ (файлы с расширением **p7b** или **sst**).

Примечание. На токенах доступны и отображаются объекты PKCS11, размещенные в публичных зонах, а также для текущего ключевого носителя объекты, размещенные в приватной зоне.

В списке надо перевести курсор на требуемый файл и, либо при помощи двойного щелчка мышью, либо кнопкой **Выбрать** указать файл, содержимое которого (один или несколько сертификатов) будет добавлен в локальное хранилище. В хранилище корневых сертификатов будут добавляться ТОЛЬКО самоподписанные сертификаты.

Кнопка Удалить

При *удалении* объекта из хранилища будет выдан дополнительный запрос и после подтверждения объект будет удален.

Кнопка Экспорт

Для экспорта объекта в файл необходимо выбрать соответствующую строку в списке м нажать кнопку **Экспорт**. При этом будет выдан запрос для выбора директории в файловой системе и после этого в выбранной директории будет сформирован файл с именем, соответствующем имени CN объекта (Common Name), и расширением "**.cer**" для сертификата и "**.crl**" - для списка отзыва.

Кнопка Сохранить хранилище

По нажатию кнопки **Сохранить хранилище** будет выдан запрос на выбор имени файла для сохранения в файловой системе Общего хранилища сертификатов. Откроется окно выбора директории. После перехода в требуемую директорию следует выбрать либо существующий файл, либо ввести с клавиатуры желаемое имя. После этого содержимое хранилище будет записано в указанный файл с расширением "**.sst**".

Примечание. Экспорт Хранилища корневых сертификатов в файл не поддерживается.

Кнопка Добавить из файла хранилища

По нажатию кнопки **Добавить из файла хранилища** будет выдан запрос на выбор имени файла с расширением ".sst" в файловой системе. Откроется окно поиска и выбора файла. После перехода в требуемую директорию следует выбрать существующий файл. После этого содержимое файла будет перенесено в Общее хранилище сертификатов.

Для каждого найденного в файле объекта будет выдан запрос на подтверждение операции.

7.4.6. Защита хранилища доверенных корневых УЦ

Иногда в соответствии с требованиями безопасности для хранилища доверенных корневых УЦ необходимо установить такой режим, при котором каждый раз при инициализации криптосистемы будет выполняться проверка имитовставки этого хранилища.
Чтобы установить требуемый режим, надо на вкладке **Безопасность** нажать кнопку **Настроить** и установить флажок **Защитить Хранилище сертификатов корневых УЦ имитовставкой** - система сформирует имитовставку хранилища **корневых сертификатов** на текущем закрытом ключе пользователя и сохранит ее. Имитовставка будет проверяться каждый раз при инициализации крипто-контекста Подключения.
Защиту хранилища можно отменить (снять флажок **Защитить Хранилище сертификатов корневых УЦ имитовставкой**), после этого имитовставка удаляется.

7.5. Вкладка Безопасность для режима статического туннеля

С помощью переключателя под заголовком **Ключевой носитель** следует указать тип ключевого носителя с персональной ключевой информацией пользователя DISEC, необходимой для организации туннеля с Сервером VPN (см. раздел Ключевые носители).

Параметры ключей

Группа параметров **Параметры ключей** содержит всю необходимую информацию о симметричных ключах.

Криптодиректория

Поле **Криптодиректория** предназначено для ввода имени директории на ключевом носителе, в которой записана ключевая информация (КИ). Поле необходимо заполнить, если ключевая информация сформирована не в корневой директории носителя. Если значение не установлено, то поиск КИ будет выполняться только в корневой директории.
Для ключевого носителя **ruToken** и **eToken** значение поля должно быть числовым и не превышать значения «*65535*».

Номер серии и **Локальный криптономер**

Значения полей **Номер серии** и **Локальный криптономер** должны соответствовать настройкам статического туннеля (**ditun**) на Сервере VPN. Эти поля можно оставить не заполненными. В этом случае будет сделана попытка подключиться к Серверу VPN с использованием ключевой информации, считанной с указанного ключевого носителя - пользователь должен следить, чтобы был установлен правильный ключевой носитель.

Удаленный криптономер

Поле **Удаленный криптономер** должно быть заполнено. В поле надо занести криптографический номер ключа удаленного конца туннеля.

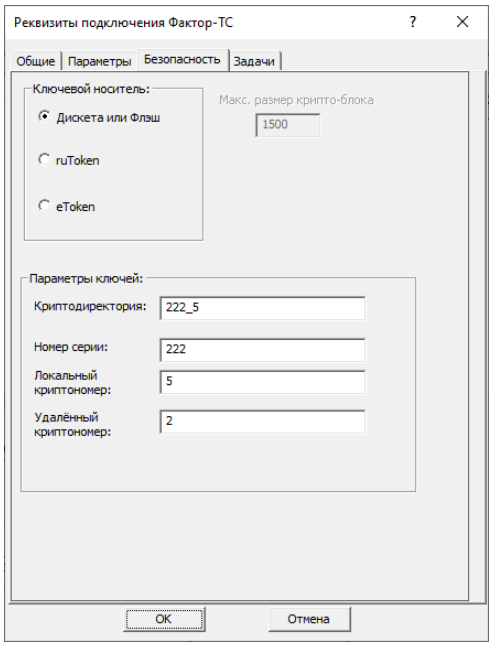


Рис. 79

ПИН

Для ключевого носителя типа Токен присутствует дополнительное поле для введения ПИН-кода. ПИН-код вводится на этапе настройки и хранится в системе для его использования в процедуре подключения.

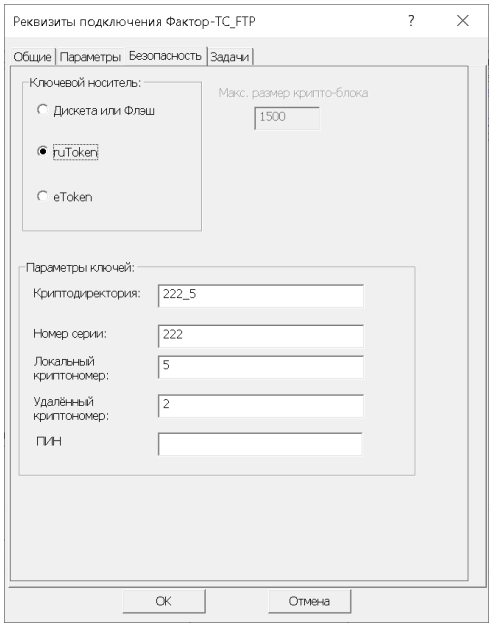


Рис. 80

7.6. Вкладка Задачи

На вкладке **Задачи** назначается выполнение определенных действий для автоматизации некоторых рутинных операций, которые требуется выполнять каждый раз на определенном этапе подключения и установления туннеля.

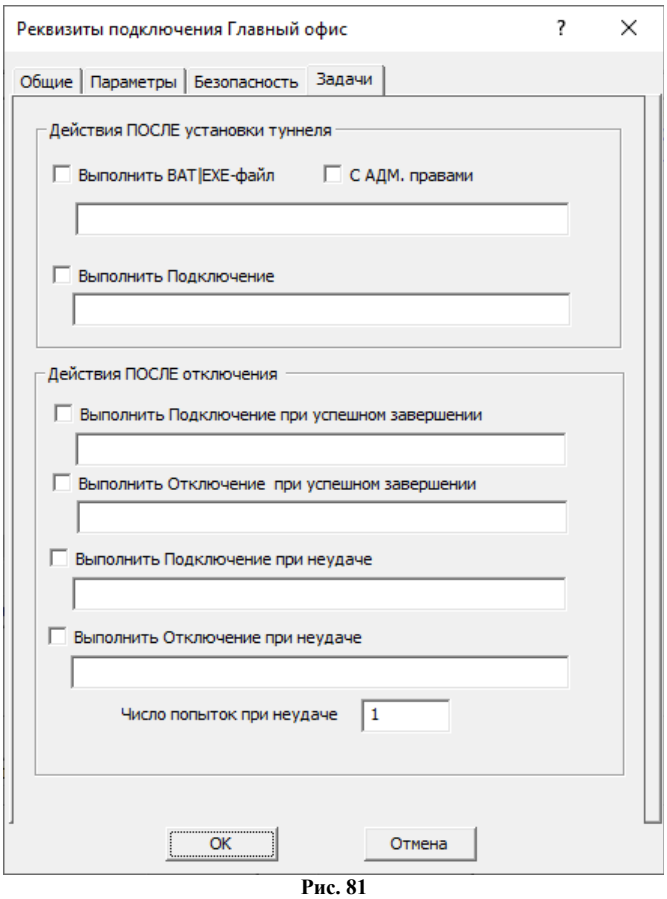


Рис. 81

Действия ПОСЛЕ установки туннеля

Группа параметров **Действия ПОСЛЕ установки туннеля** содержит две задачи.

Выполнить BAT-файл

Флажок **Выполнить BAT-файл** позволяет автоматически после установки туннеля выполнить любой скрипт, сформированный в форме командного файла (BATCH или BAT-файла). При этом выбранный BAT-файл может быть любой сложности и содержать другие скрипты, написанные на любом языке скриптов. При установке флажка открывается стандартное окно файловой системы и предоставляется возможность выбора командного файла в любой директории.

Выполнить Подключение

Флажок **Выполнить Подключение** позволяет автоматически после установки туннеля выполнить еще одно Подключение.

Действия ПОСЛЕ отключения

Группа параметров **Действия ПОСЛЕ отключения** содержит несколько вариантов, смысл которых очевиден из названий.

Заданные при настройке параметры **Выполнить Подключение при неудаче**, а также параметр **Число попыток при неудаче** могут быть изменены при выполнении команды Подключиться, как описано в разделе.

8 Вкладка Обслуживание

Вкладка **Обслуживание** окна **Настройка** предоставляет возможность выполнения команд по настройке и запуску отдельных компонент ПО DISEC, а также сервисные команды:

- команды обслуживания драйвера DiSecDRV;
- команды обслуживания службы DiSecSRV;
- команды обслуживания службы DiSecAGENT;
- команда проверки Контрольных сумм;
- команда проверки сертификатов Подключений

Кнопки запуска команд, требующих привилегированных полномочий помечены символом "**".

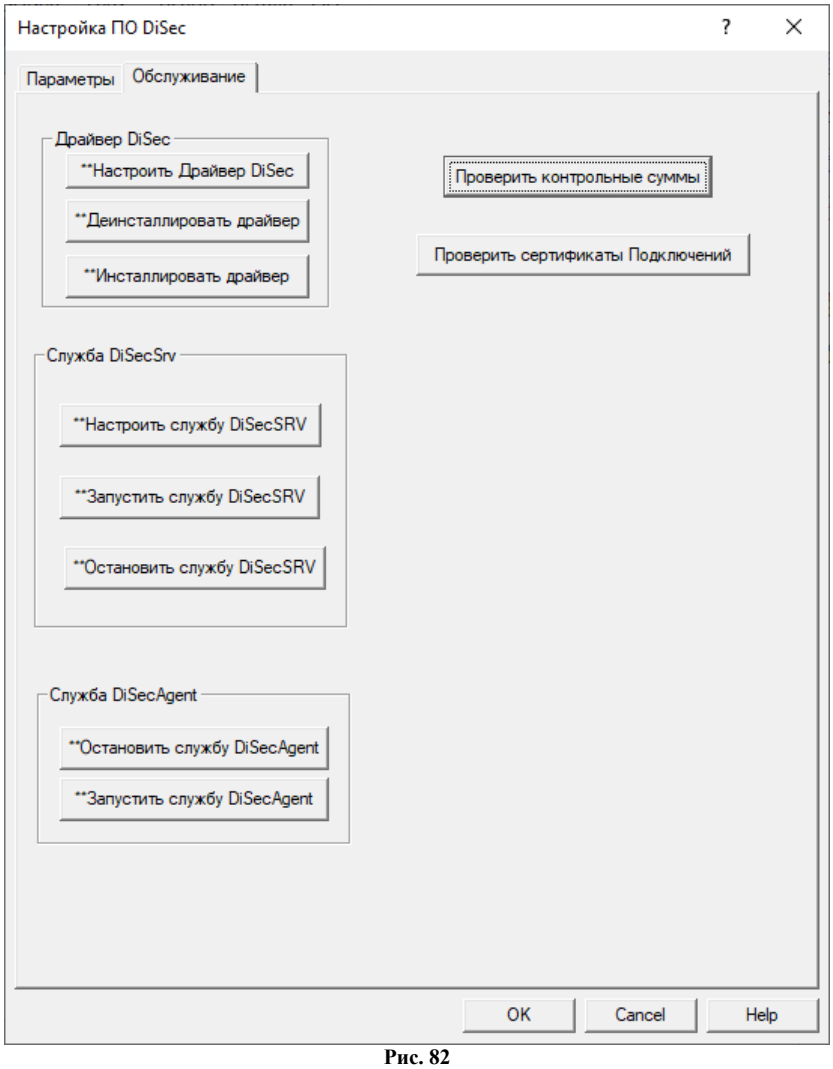


Рис. 82

8.1. Проверка контрольных сумм

По нажатию кнопки **Проверить контрольные суммы** вызывается программа, входящая в состав ПО DISEC, и выполняется проверка контрольных сумм всех компонент.
При положительном результате будет выдано окно:

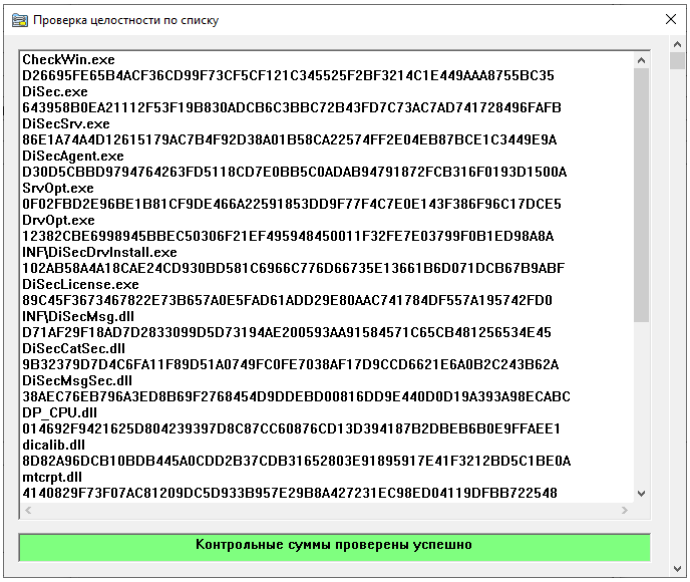


Рис. 83

При отрицательном результате будет выдано, например, сообщение:

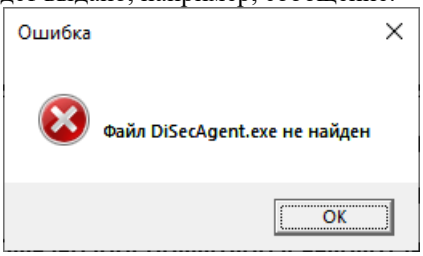


Рис. 84

или

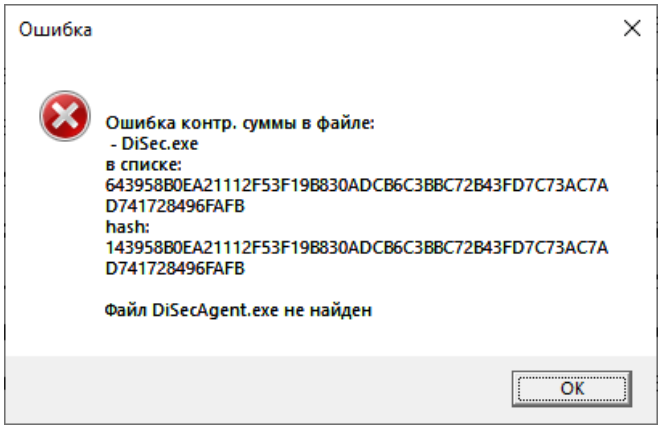


Рис. 85

8.2. Проверить сертификаты Подключений

По кнопке **Проверить сертификаты Подключений** выполняется просмотр списка подключений текущего пользователя и для подключений, использующих ключи PKI (динамические туннеля), выполняются следующие действия сначала для локальных сертификатов, а затем и для сертификатов оппонента (Сервера VPN):

1. Выполняется обновление CRL (СОС) в соответствии с настройками в подключении.
2. Выполняется проверка сертификата по протоколу OCSP в соответствии с настройками в подключении.
3. Выполняется "локальная" проверка сертификата участника подключения и всей цепочки сертификатов издателей до корневого включительно.

Примечание. С целью экономии времени обновление CRL не выполняется для сертификата оппонента в случае, когда его издатель является издателем локального сертификата.

Результат отображается в окне **Диагностика** и Журнале.

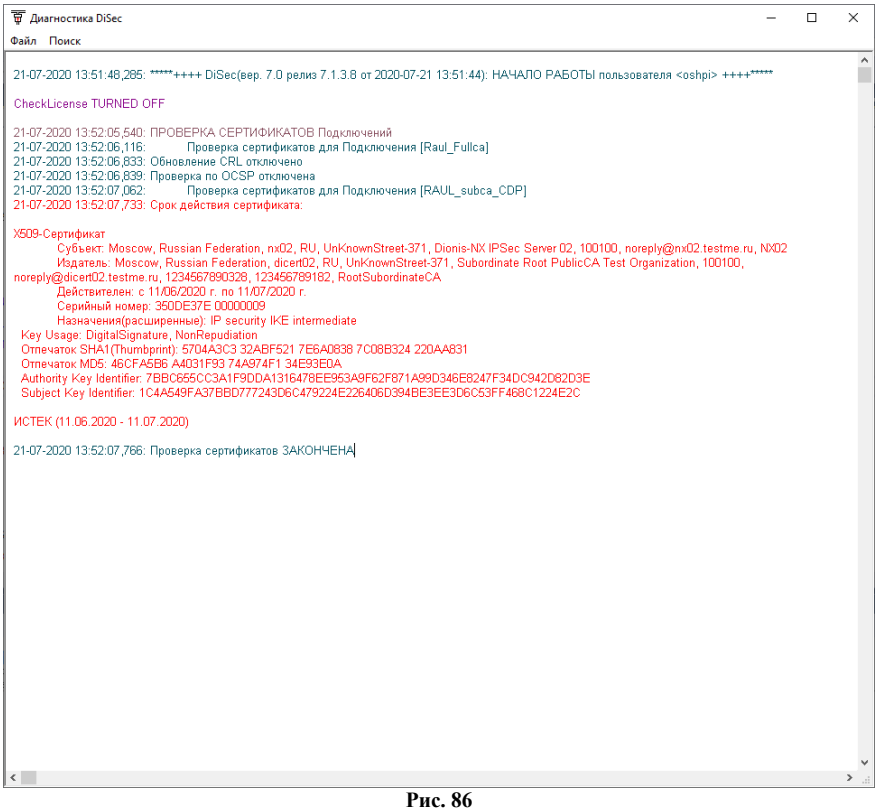


Рис. 86

8.3. Обслуживание драйвера DiSec

В группе команд обслуживания драйвера DiSec имеются три команды:

- Настроить драйвер DiSec
- Деинсталлировать драйвер DiSec
- Инсталлировать драйвер DiSec

8.3.1. Настройка драйвера DiSec

По кнопке **Настроить Драйвер DiSec** выполняются настройки режима работы драйвера и устанавливаются или отменяются параметры протоколирования сети.

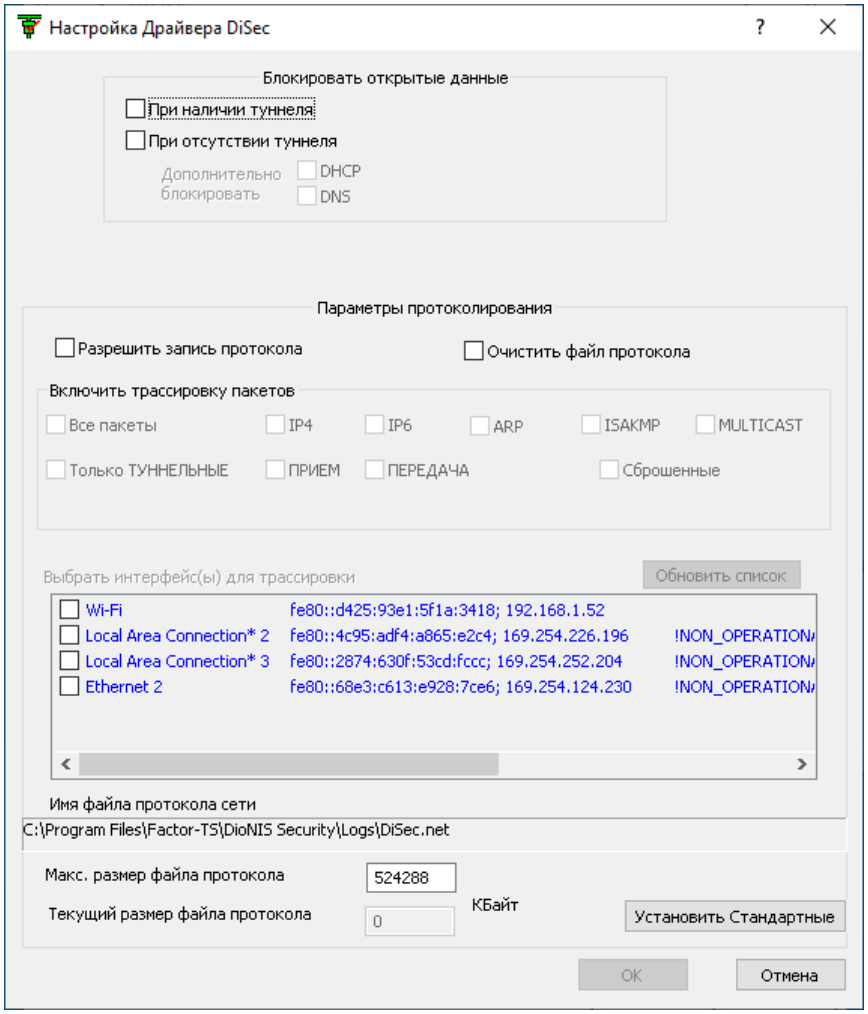


Рис. 87

В данном окне имеются несколько групп параметров:

- Блокировать открытые данные;
- Параметры протоколирования;
- Параметры файла протокола сети.

8.3.1.1. РЕЖИМ БЛОКИРОВКИ ОТКРЫТЫХ ДАННЫХ

Группа параметров **Блокировать открытые данные** определяют действия, которые будет выполнять драйвер с нетуннелированными пакетами («открытыми данными»).

Примечание. Блокировка открытых данных значительно ограничивает доступ компьютера к сетевым ресурсам и, следовательно, повышает его защищенность от сетевых угроз.

При наличии туннеля

Установленный флажок **При наличии туннеля** указывает драйверу DiSec, что после подключения к защищенной сети и установки туннеля (см. раздел Команда Подключиться) необходимо блокировать весь открытый трафик, т.е. отбрасывать сетевые пакеты, не соответствующие правилам отбора в туннель. Другими словами, в этом случае пользователь сможет работать только с ресурсами сети, защищенными Сервером VPN, с которым организован туннель. Блокировка открытых данных выполняется следующим образом:

- ***прием*** - принимаются (и обрабатываются) только сетевые пакеты, пришедшие через туннель; все остальные сетевые пакеты отбрасываются, в том числе пакеты протокола IPv6;
- ***отправка*** - сетевые пакеты будут отправляться только через туннель; те сетевые пакеты, которым не разрешено прохождение через туннель (не соответствуют правилам отбора в туннель), отбрасываются (в том числе, по сетевым интерфейсам, по которым туннелирование не выполняется).

При снятом флажке драйвер пропускает все сетевые пакеты, таким образом, пользователь, работая с защищенными ресурсами по туннелю, может одновременно работать и с незащищенными сетевыми ресурсами.

При отсутствии туннеля

Установленный флажок **При отсутствии туннеля** указывает драйверу, что до установления туннеля и после его снятия весь сетевой трафик должен быть заблокирован (отброшен). При этом пропускаются только сетевые пакеты, необходимые для установки туннеля, то есть для взаимодействия с Сервером VPN по протоколу ISAKMP.

Дополнительно блокировать

Одновременно с флажком **При отсутствии туннеля** можно установить дополнительно два флажка: **DHCP** и **DNS**, каждый из которых указывает на необходимость блокировки пакетов соответствующего протокола. В случае их установки сетевое подключение, используемое для создания туннеля, должно использовать статический IP-адрес, а в реквизитах подключения должен быть указан IP-адрес Сервера VPN, а не доменное имя.

8.3.1.2. ПАРАМЕТРЫ ПРОТОКОЛИРОВАНИЯ

Протокол сети необходим, как правило, для диагностики, настройки и отладки взаимодействия с сетевыми компонентами компьютера, а также с Сервером VPN.
Ведение протокола можно включить или отключить, а также можно назначить состав информации, которая будет заноситься в него.

Разрешить запись протокола

При установленном флажке информация о сетевых пакетах, проходящих через драйвер, будет записываться в протокол. После установки флажка становятся доступными для изменения параметры трассировки (становятся активными флажки под заголовком **Включить трассировку пакетов**. При снятом флажке параметры трассировки становятся недоступными для изменения.

Очистить файл протокола

При установке флажка после нажатия кнопки **ОК** (или **Принять**) вся информация из протокольного файла будет удалена, и после очистки запись в файл начнется снова. При снятом флажке информация будет записываться в конец протокольного файла.

После включения протоколирования сете необходимо установить параметры для выбора типа пакетов и сетевых интерфейсов:

- Включить трассировку пакетов
- Выбрать трассировку интерфейсов

Включить трассировку пакетов

Группа флажков **Включить трассировку пакетов** определяет тип пакетов, которые будут фиксироваться в протоколе. Флажки активны только при установленном флажке **Разрешить запись протокола**. При протоколировании (фиксировании) пакета в протокол записывается информация, полученная при расшифровке заголовка IP-пакета, протоколов прикладного уровня (UDP, TCP, ICMP) и туннельного заголовка (для туннелированных пакетов). Запись о каждом заголовке начинается с новой строки и помечается именем протокола.
При записи туннелированных пакетов в протокол записывается исходный пакет (ORIGINAL)с расшифровкой всех заголовков и туннельный пакет, также с расшифровкой всех заголовков инкапсулирующих протоколов.

Флажок Все пакеты

Флажок определяет запись в протокол (трассировку) информации обо всех IP и ARP-пакетах, проходящих через выбранные для трассировки интерфейсы. При установке данного флажка включаются остальные флажки, кроме флажка "Только ТУННЕЛЬНЫЕ". Для выбора отдельных категорий пакетов данный флажок следует снять.

Флажок IP4

Флажок управляет протоколированием IPv4-пакетов, проходящих через выбранные для трассировки интерфейсы. Расшифровка заголовка в протоколе начинается с префикса «IPv4:».

Флажок IP6

Флажок управляет протоколированием IPv6-пакетов, проходящих через выбранные для трассировки интерфейсы. Расшифровка заголовка в протоколе начинается с префикса «IPv6:».

Флажок ARP

Флажок управляет протоколированием ARP-пакетов, проходящих через выбранные для трассировки интерфейсы, при этом для каждого фиксируемого пакета выполняется расшифровка ARP-заголовка. Расшифровка заголовка ARP-пакета в протоколе начинается с префикса «ARP:». В режиме IPv6 протокол ARP оне используется.

Флажок ISAKMP

Флажок управляет протоколированием ISAKMP-пакетов, проходящих через выбранные для трассировки интерфейсы, т.е. пакетов протокола UDP, а один из портов равен 500 или 4500.

Флажок MULTICAST

Флажок включает протоколирование всех мультикастовых пакетов, проходящих через выбранные для трассировки интерфейсы, т.е. пакетов, адреса которых соответствуют определению мультикастовых пакетов для IPv4 и\или IPv6.

Флажок Только Туннельные

При установке флажка в протокол сети будут записываться только туннелированные пакеты.

Флажок Сброшенные

Флажок задает протоколирование всех пакетов, сброшенных (заблокированных) в соответствии с настройками блокировки открытых данных. При этом в протокол выводится расшифровка IP- и TCP/UDP/ICMP/ICMP6-заголовков.

Выбрать трассировку интерфейсов

Секция **Выбрать трассировку интерфейсов** содержит список имеющихся в данный момент на компьютере пользователя IP-интерфейсов, зарегистрированных драйвером DiSec. Трассировку можно задать по любому числу интерфейсов, установив флажки слева от названия интерфейса. Если не установлен ни один флажок, то ведение протокола не выполняется.
После перезагрузки системы выбор интерфейсов и параметры расшифровки протоколирования сохраняются.
Кнопка **Обновить список** позволяет заново получить список зарегистрированных драйвером DiSec сетевых интерфейсов без выхода из программы. Использование данной кнопки рекомендуется, если во время работы с программой были выполнены изменения состава и/или свойств сетевых интерфейсов компьютера, например, изменение статического IP-адреса сетевого интерфейса, а также переход со статического адреса на динамический и наоборот.

8.3.1.3. ПАРАМЕТРЫ ФАЙЛА ПРОТОКОЛА СЕТИ

Имя файла протокола сети

В поле под этим заголовком отображено полное имя файла протокола сети. Пользователь не может изменить данное значение. Данная информация необходима, чтобы переслать Протокол сети разработчикам или администраторам для разрешения ошибочных ситуаций.

Макс. размер файла протокола

В поле под этим заголовком можно задать максимальный размер файла в килобайтах, при этом следует учитывать, какой программой будет просматриваться этот файл, поскольку у каждой программы имеются свои ограничения. Например, стандартная программа для просмотра текстовых файлов ***Notepad*** имеет ограничение меньше 500 Мбайт, однако существуют программы, которые позволяют просматривать файлы практически любых размеров. По достижении размера, заданного данным параметром, запись в Протокол сети прекращается.

Примечание. Разработчик ПО DISEC не предоставляет специальные программы для просмотра файлов большого размера. Команда Протокол сети позволяет просмотреть последний мегабайт протокола.

Текущий размер файла протокола

В этом поле в соответствии с названием отображается текущий размер файла.

Установить стандартные

При нажатии этой кнопки устанавливается стандартное значения для максимального размера файла протокола: (524288 Кбайт, т.е. 512 мегабайт).

8.3.2. Деинсталляция драйвера DiSec

По нажатию кнопки **Деинсталлировать драйвер** вызывается программа, входящая в состав ПО DISEC, и выполняется удаление драйвера **DiSec** после запроса авторизационных данных привилегированного пользователя.
Действия аналогичны вызову соответствующей программы из стартового меню Windows.

8.3.3. Инсталляция драйвера DiSec

По нажатию кнопки **Инсталлировать драйвер** вызывается программа, входящая в состав ПО DISEC, и выполняется инсталляция драйвера **DiSec** после запроса авторизационных данных привилегированного пользователя.
Действия аналогичны вызову соответствующей программы из стартового меню Windows.

8.4. Служба DiSecSRV

В группе команд обслуживания службы DiSecSRV имеются три команды:

- Настроить службу DiSecSRV;
- Запустить службу DiSecSRV;
- Остановить службу DiSecSRV.

8.4.1. Настройка службы DiSecSRV

По кнопке **Настроить Службу DiSecSRV** выполняются настройки режима ее работы .

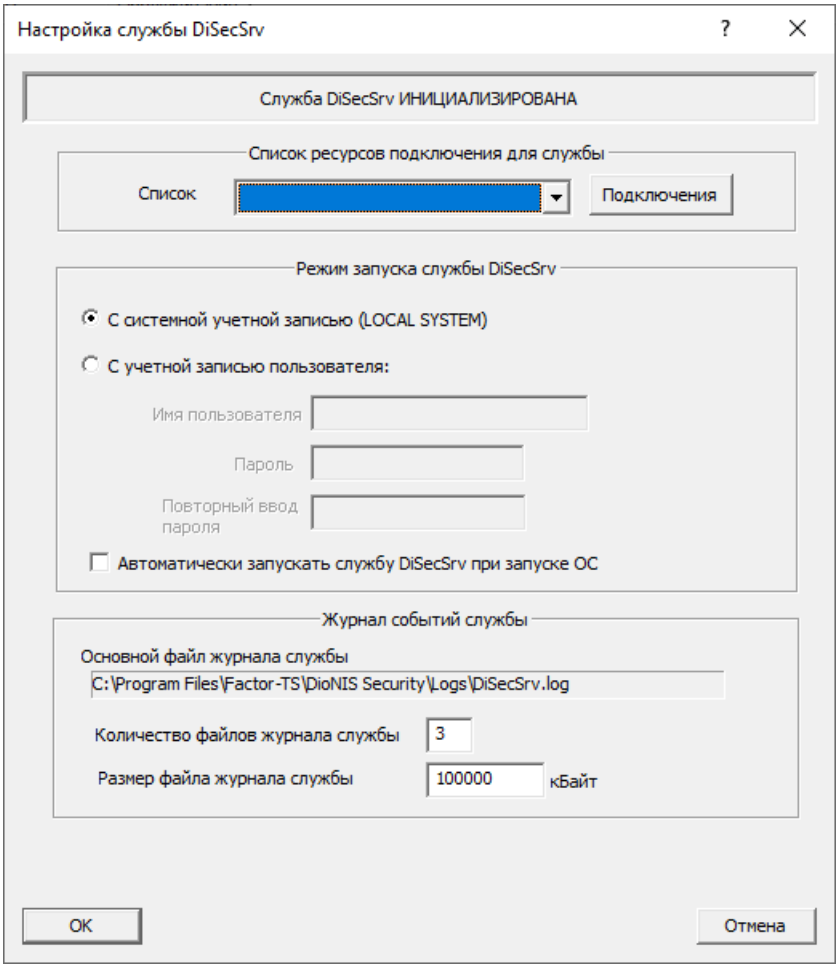


Рис. 88

В данном окне имеются несколько групп параметров:

- Список ресурсов подключений
- Режим запуска службы DiSecSRV
- Журнал событий службы

8.4.1.1. СПИСОК РЕСУРСОВ ПОДКЛЮЧЕНИЙ ДЛЯ СЛУЖБЫ

Группа параметров **Список ресурсов подключения для службы** позволяют создать (настроить) один или несколько ресурсов подключения для службы и выбрать один или несколько из них в качестве текущего списка, а также настроить параметры цикла. Цикл для службы выполняется бесконечно до вмешательства пользователя, который может прервать его командой отключения службы.

Список

Параметр позволяет выбрать из списка ресурсов подключений тот (или те), которое будет использоваться при работе службы DiSecSrv. Выпадающий список содержит все подключения для службы, если их описания были созданы ранее при помощи кнопки **Подключения** данного окна. Может быть выбрано несколько подключений, составляющие ЦИКЛ. Переход к следующему в цикле выполняется после разрыва предыдущего подключения.

Подключения

Кнопка предназначена для создания или модификации списка подключений для службы, после ее нажатия откроется окно **Подключения**.

В отличие от окна списка подключений для приложения в данном окне имеется кнопка **Импорт от пользователя**, которая позволяет существенно упростить процесс настройки реквизитов подключения для службы, импортируя настроенное и протестированное в режиме пользователя подключение в службу.

После выхода из окна по кнопке **OK** в окне **Настройка службы DiSecSRV** следует выбрать из выпадающего списка нужные ресурсы:

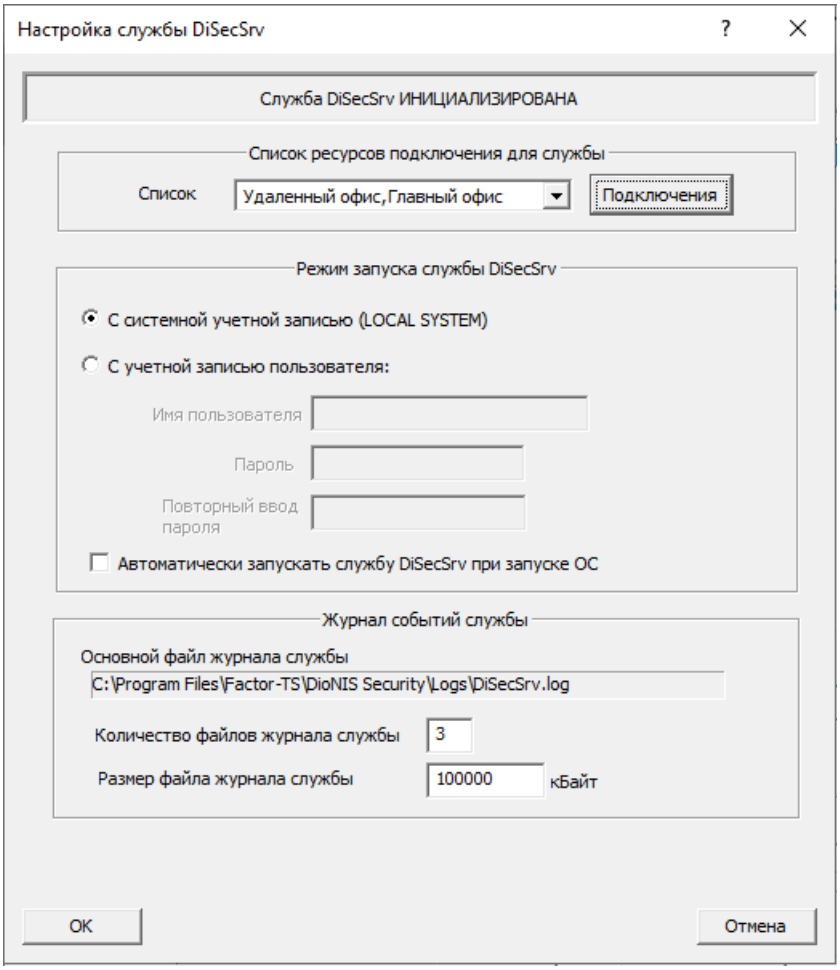


Рис. 89

8.4.1.2. РЕЖИМ ЗАПУСКА СЛУЖБЫ DISECSRV

Группа параметров под этим заголовком позволяет установить (или отменить) автоматический запуск службы DiSecSrv после перезагрузки компьютера, а также назначить учетную запись пользователя WINDOWS для ее работы.

С системной учетной записью (LOCAL SYSTEM)

Переключатель устанавливает соответствующий режим запуска службы; это значение установлено по умолчанию. Не рекомендуется его менять.

С учетной записью пользователя

Переключатель устанавливает соответствующий режим запуска службы, при этом активизируются элементы управления для ввода данных о пользователе.

Имя пользователя

Поле предназначено для указания имени пользователя WINDOWS, учетная запись которого будет использоваться при запуске службы DiSecSrv. Имя пользователя должно присутствовать в списке пользователей WINDOWS, и ему должны быть предоставлены права входа в систему в качестве службы.

Имя пользователя может содержать имя домена в формате: <Домен Windows>\<Имя пользователя> (угловые скобки при вводе отсутствуют). Для пользователя данного компьютера к имени автоматически добавляется префикс из двух символов:. \ . Требования в учетной записи приведены в разделе.

Пароль

Поле предназначено для указания пароля пользователя WINDOWS, учетная запись которого будет использоваться при запуске службы.

Повторный ввод пароля

В поле необходимо повторить пароль, совпадающий с паролем, введенным в предыдущем поле. При переходе на любой другой элемент окна (что означает завершение повторного ввода пароля) программа проверит совпадение паролей.

Автоматически запускать службу DiSecSrv при запуске ОС

Флажок управляет режимом запуска службы DiSecSrv. Сразу после инсталляции службы флажок сброшен - это означает, что служба запускается вручную - либо при помощи команды запуска службы из программной папки **Dionis Security** системного стартового меню, либо через консоль управления службами WINDOWS. Установленный флажок задает автоматический запуск службы после загрузки WINDOWS - данный режим является рабочим, его рекомендуется устанавливать после полной настройки службы и проверки ее работоспособности.

8.4.1.3. ЖУРНАЛ СОБЫТИЙ СЛУЖБЫ

Журнал событий служит для записи сообщений, выдаваемых в процессе работы службы DiSecSrv. Журнал должен обязательно храниться на диске компьютера и, как правило, достаточно длительное время.

Основной файл журнала службы

Имена файлов, в которых хранится журнал службы, задаются программой, и изменить их нельзя. Имя основного (первого) файла - **DiSecSrv.log**. Имена второго и последующих файлов образуются из имени основного добавлением двух цифр: **DiSecSrv01.log**, **DiSecSrv02.log** и т.д.

Все файлы журнала размещаются в поддиректории **Logs** программной директории ПО DISEC.

Двум следующим параметрам необходимо задать оптимальные значения, с точки зрения экономии дисковой памяти и срока хранения записанных в журналах данных. Рекомендуется не менять установленные по умолчанию значения.

Количество файлов журнала службы

Параметр задает количество файлов, в которые будет записываться информация. Если параметр имеет значение *0* или *1*, то журнал занимает один файл неограниченного размера (значение следующего параметра не имеет значения).

Размер файла журнала службы

Параметр определяет размер каждого из файлов журнала.

Информация всегда записывается в основной файл. Когда основной файл превысит установленный размер, вся информация из него будет перенесена во второй файл, и запись в основной файл начнется сначала. Если во втором файле была информация, то она будет перенесена в третий и т.д. Информация из последнего файла при перемещении будет утеряна.

8.4.2. Запустить службу DiSecSRV

Кнопка **Запустить службу DiSecSRV** на вкладке **Обслуживание** окна **Настройка** позволяет протестировать настройку службы.

Примечание. Следует учитывать, что для выполнения этой функции потребуются привилегированные права.

В результате запуска должны установиться заданные в настройках подключения и измениться значок программы DiSec в области уведомлений Windows (SYSTEM TRAY).

В случае неудачи следует изучить Журнал событий службы.

8.4.3. Остановить службу DiSecSRV

Кнопка **Остановить службу DiSecSRV** на вкладке **Обслуживание** окна **Настройка** позволяет остановить запущенную ранее службу **DiSecSRV**.

Примечание. Следует учитывать, что для выполнения этой функции потребуются привилегированные права.

В результате останова будут отключены все запущенные службой подключения.

8.5. Служба DiSecAgent

Группа элементов управления **Служба DiSecAgent** содержит кнопки останова и запуска соответствующей службы, входящей в состав ПО DISEC. Пользоваться командами данной группы не следует без крайней необходимости - использовать их следует только при возникновении подозрений в неправильном функционировании службы, например, при получении сообщения об ошибке при запуске приложения **DiSec**.

Для выполнения обеих команд требуются привилегированные полномочия, поэтому при нажатии кнопок выдается запрос на ввод авторизационных данных администратора. Далее команды выполняются без дополнительных запросов.

После перезапуска службы **DiSecAgent** следует перезапустить приложение **DiSec**.

9 Команды Подключиться/Отключиться

Команда **Подключиться** Главного меню приложения DiSec служит для установки туннеля с конкретной защищенной сетью, после ее выбора на экран выводится окно в котором выбирается один или несколько ресурсов и инициируется процедура подключения.
Команда **Отключиться** Главного меню приложения DiSec служит для снятия ранее установленного средствами приложения DiSec туннеля. Подробнее ниже.

9.1. Команда Подключиться

Команда **Подключиться** предназначена для организации туннеля между DISEC и Сервером VPN в соответствии с заданными реквизитами ресурса подключения.
После активизации команды **Подключиться** на экран будет выведено окно, содержащее элементы управления, необходимые для выбора одного подключения или нескольких подключений; кнопки для запуска и прерывания процедуры подключения.

9.1.1. Выполнение процедуры подключения

Для запуска процедуры подключения необходимо в появившемся после выбора команды **Подключиться** окне выполнить следующие действия:

- сформировать список ранее настроенных ресурсов подключений из выпадающего списка **Список ресурсов подключения**,
- настроить параметры цикла (установить значения **Число попыток**, **Число циклов** и флажок **По очереди**);
- после чего нажать кнопку **Начать**.

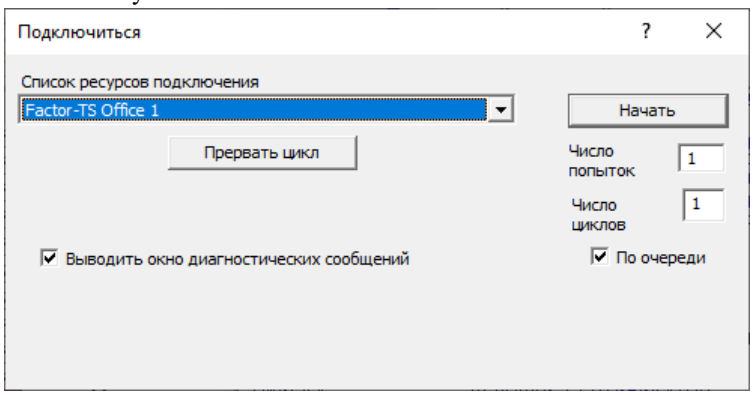


Рис. 90

Список ресурсов подключения

В текстовом поле элемента **Список ресурсов подключения** отображается название одного или нескольких ресурсов, к которым будет выполняться подключение. Список ресурсов можно выбрать (изменить), посредством установки или снятия флажков в раскрывающемся списке. Перечень и последовательность ресурсов в выпадающем списке содержит все созданные заранее на этапе настройки системы ресурсы. При нажатии правой кнопки мыши на выпадающем списке будут выбраны все ресурсы.

Число попыток

Числовое значение в поле **Число попыток** определяет число попыток подключения к КАЖДОМУ ресурсу в списке до перехода к следующему. Стандартное значение - 2. Попытки повторного подключения осуществляются в случае возникновения ошибок. В случае некоторых ошибок, когда повторная попытка не конструктивна, например, ключевой носитель отсутствует, повторные попытка не осуществляются.

Число циклов

Числовое значение в поле **Число циклов** определяет число выполнений заданной в списке последовательности. После достижения заданного значения процедура подключений за-

канчивается с выдачей диагностического сообщения об этом факте (в окно **Диагностика DiSec** и журнал **DiSec.log**. Стандартное значение - 1.

По очереди

Флажок определяет режим запуска подключений из списка. При установленном флажке переход к следующему подключению в списке выполняется ТОЛЬКО при ошибочном завершении предыдущего. При этом, если в настройках какого-либо подключения установлены **параметры Задачи** (**Workflow**), такие как **Выполнить подключение при неудаче** и **Число попыток при неудаче**, то они заменяются на значения, установленные в данном окне.
При снятом флажке все подключения из списка запускаются без ожидания результатов предыдущего, фактически сразу после считывания и обработки реквизитов одного Подключения происходит переход к запуску следующего.

Начать

Кнопка **Начать** инициирует процедуру выполнения цикла подключений по сформированному списку.

Прервать цикл

Кнопка **Прервать цикл** позволяет прервать цикл подключений.

Выводить окно диагностических сообщений

Установка флажка приводит к выводу на экран окна **Диагностика DiSec**, которое позволяет оперативно наблюдать за диагностическими сообщениями в процессе подключения. Снятие флажка не отменяет вывод диагностических сообщений, просмотр которых возможен по команде **Диагностика** Главного меню приложения DiSec.

Статический туннель. После запуска считывается ключевая информация с указанного в настройках подключения ключевого носителя, на ее основе формируется ключевой материал, который вместе с параметрами туннеля передается в драйвер DiSec. Туннель переходит в состояние готовности передачи и приема зашифрованного трафика.

Динамический туннель. При успешном считывании ключевой информации начинается процесс соединения с Сервером VPN, во время которого DiSec передает данные на сервер для криптографической аутентификации и авторизации пользователя и получает от Сервера VPN данные о динамическом туннеле (в частности, получает от Сервера VPN список доступных целевых объектов, на базе которых формирует правила отбора в туннель). Согласованные параметры работы туннеля загружаются в драйвер DiSec. Обмен данными между Сервером VPN и DISEC выполняется по протоколу IKE.
Процесс выполнения процедуры подключения в виде последовательных сообщений отражается в информационном окошке (нижняя части окна), там же будет выведено сообщение об ошибке, если она произойдет при выполнении соединения. Дополнительную информацию можно получить в окне **Диагностика** DiSec и Журнале.

Примечание. Диагностические сообщения сохраняются в оперативной памяти компьютера, их можно просмотреть и позднее до окончания сеанса работы с приложением DiSec с помощью **команды Диагностика Главного меню** приложения DiSec.

При отсутствии ошибок в информационное окошко будет выведено сообщение о том, что подключение установлено, и после небольшой паузы окно **Подключиться** свернется. Значок вызова **Главного меню** приложения DiSec (расположенный на панели задач в области уведомлений SYSTEM TRAY) изменит цвет на зеленый.
Зеленый цвет значка означает:

- драйвер DiSec находится в состоянии соединения с сервером;
- параметры туннеля загружены в драйвер DiSec;
- можно начинать разрешенные правилами отбора в туннель работы с защищаемыми им ресурсами.

9.2. Команда Отключиться

Команда **Отключиться Главного меню** приложения DiSec становится доступной после того, как будет выполнено соединение хотя бы с одним Сервером VPN. По команде Отключиться появляется контекстное меню, содержащее список установленных или устанавливаемых подключений и позицию "ВСЕ". Пользователь может выбрать одну из позиций. После этого начинается процедура отключения, при этом выполняются следующие действия:

- в драйвере DiSec удаляются данные туннелей, соответствующие данному подключению, в том числе ключевой материал;
- для динамического туннеля выполняется удаление всех SA ESP и SA IKE, функционирующих на данный момент для данного подключения, при этом на Сервер VPN посылаются сообщения IKE для удаления SA
- связь с Сервером VPN корректно разрывается, подключение к IP-сети сохраняется.

Статический туннель на стороне Сервера VPN остается в рабочем состоянии.

10 Команда Состояние

Команда **Состояние Главного меню** приложения DiSec позволяет просмотреть статистику прохождения и обработки сетевых пакетов драйвером DiSec. После активизации команды **Состояние** выполняется обращение к драйверу DiSec для получения текущих значений параметров и счетчиков пакетов. На экран выводится окно.

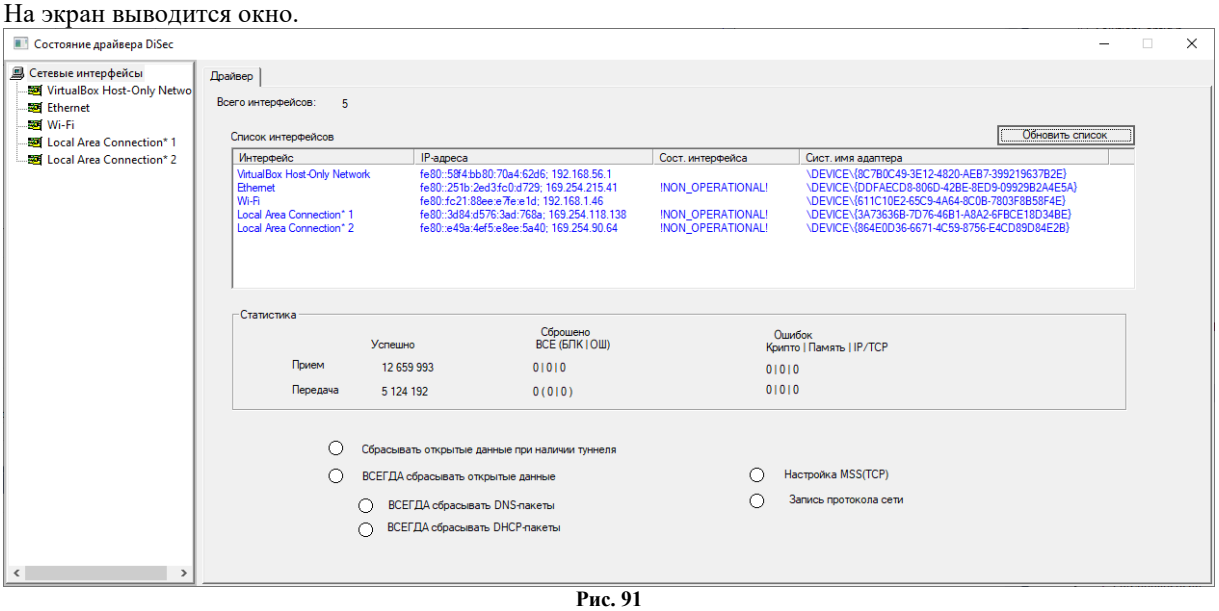


Рис. 91

В левой части окна под заголовком Сетевые интерфейсы выводится список всех зарегистрированных в операционной системе и активных сетевых интерфейсов компьютера, через которые возможно подключение к IP-сети и которые взял на обслуживание драйвер DiSec.
В правой части окна - набор вкладок, позволяющих получить информацию о текущем состоянии драйвера DiSec для каждого сетевого интерфейса, а также статистику для всех интерфейсов в целом.
Если в левой части окна курсор установлен на первой строке **Сетевые интерфейсы**, то в правой части окна только одна вкладка - **Драйвер** .
Если в левой части окна курсором выделена строка с названием одного из интерфейсов, то в правой части окна появляется набор из четырех вкладок **Драйвер**, **Интерфейс**, **Туннель** и **Трафик**.

10.1. Вкладка Драйвер

Вкладка содержит информацию о количестве зарегистрированных драйвером DiSec сетевых интерфейсов и суммарную статистику прохождения пакетов через драйвер DiSec по всем интерфейсам.

Всего интерфейсов:

Количество зарегистрированных драйвером DiSec сетевых интерфейсов (перечислены в левой панели окна). Регистрация сетевых интерфейсов выполняется во время первой загрузки драйвера DiSec при старте операционной системы.

Статистика

В секции под этим заголовком на экран выводится число пакетов, принятых и отправленных, с указанием результата обработки их драйвером DiSec.

Успешно

Количество пакетов, которые прошли успешно (отправлены или приняты драйвером DiSec соответственно).

Сброшено ВСЕ (БЛК|ОШ)

Количество пакетов, отвергнутых драйвером:

- БЛК - не соответствующих правилам отбора в туннель и сброшенных драйвером DiSec в соответствии с настройкой блокировки открытых данных.
- ОШ - полученным с ошибками

Ошибок (Крипто | Память | IP\TCP)

Количество пакетов, сброшенных драйвером DiSec:

- Крипто - или из-за ошибок в процессе зашифрования (в строке Передача) или расшифрования (в строке Прием);
- Память - из-за возникновения ситуации нехватки ресурсов в драйвере DiSec для передачи\приема пакета.
- IP\TCP - из искажения в заголовках пакета, ошибках контрольной суммы.

В нижней части экрана размещены индикаторы информирующих о настройках драйвера DiSec. Зеленый цвет индикатора свидетельствует о включении соответствующей настройки.

10.1.1. Список интерфейсов

В секции под заголовком **Список интерфейсов** отображаются активные сетевые интерфейсы TCP/IP (интерфейсы, соответствующие платам Ethernet, беспроводным соединениям Wi-Fi, VPN-соединениям и службе удаленного доступа WINDOWS), обслуживаемые драйвером DiSec, т.е. зарегистрированные им во время загрузки ОС.

Названия интерфейсов содержат IP-адрес данного интерфейса, его имя в системе, и, возможно (в случае неисправности), его статус.

При успешной загрузке драйвера DiSec в списке интерфейсов присутствуют IP-адреса сетевых интерфейсов, в общем случае в формате IPv4 и IPv6, разделенные точкой с запятой.

Имя интерфейса помещается в двойных угловых скобках, оно присваивается операционной системой, например, <<**Подключение по локальной сети**>>, но может быть изменено пользователем при помощи системных средств управления сетевыми подключениями.

В названиях интерфейсов, которые по каким-либо причинам не функционируют (например, не подключен сетевой кабель) присутствует текст "**NON OPERATIONAL!**"

Список интерфейсов может оказаться пустым, если загрузка драйвера DiSec была не успешна, например, после инсталляции не была выполнена перезагрузка ОС.

Примечание. Драйвер DiSec всегда запускается во время загрузки операционной системы.

При отсутствии какого-либо интерфейса в списке необходимо проверить настройку ОС (наличие драйверов плат локальной сети, включение WiFi и т.п.).

Кнопка **Обновить список** позволяет заново получить список зарегистрированных драйвером DiSec сетевых интерфейсов без закрытия окна **Состояние DiSec**. Использование данной кнопки рекомендуется, если во время работы с окном **Состояние** были выполнены изменения состава и/или свойств сетевых интерфейсов компьютера, например, изменение IP-адреса сетевого интерфейса, подключение или отключение сетевого адаптера.

10.2. Вкладка Интерфейс

Вкладка **Интерфейс** содержит параметры и информацию о текущем состоянии конкретного интерфейса.

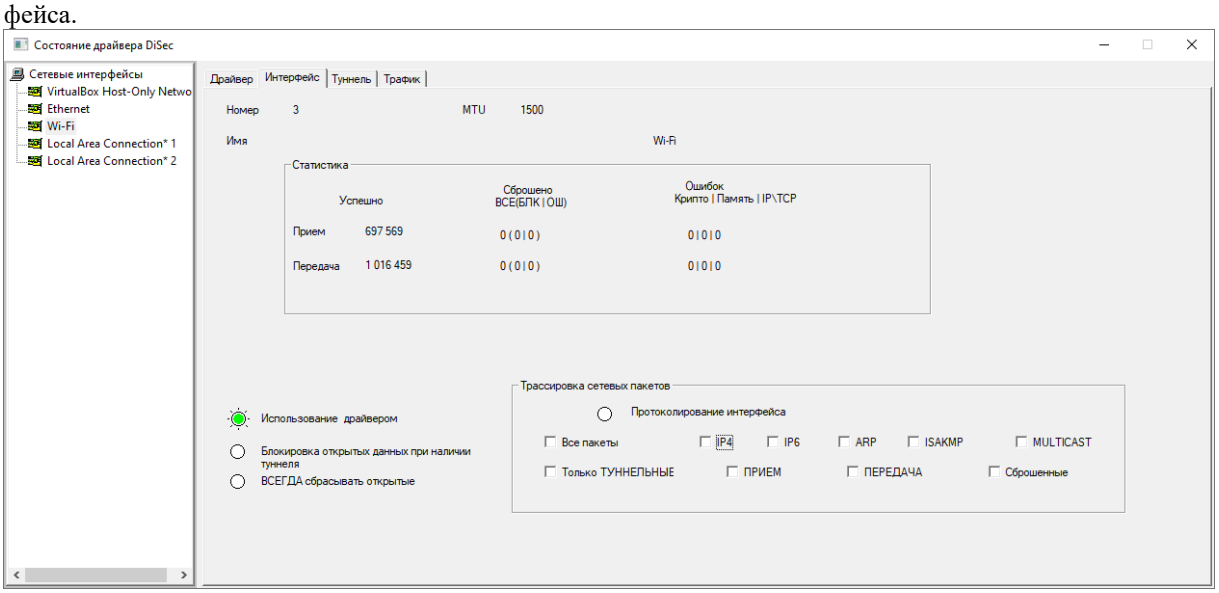


Рис. 92

Номер

Порядковый номер интерфейса, присвоенный драйвером **DiSec** в процессе регистрации интерфейсов.

Имя

Имя интерфейса.

MTU

Значение **MTU** (Maximum-Transmission-Unit), установленное на данном интерфейсе.

Статистика

В секции под этим заголовком на экран выводится число пакетов, принятых и отправленных по данному интерфейсу с указанием результата обработки их драйвером **DiSec**. Статистика выводится в том же формате, что и суммарная статистика по всем интерфейсам.

В нижней части экрана размещены индикаторы, отображающие режимы работы драйвера.

Использование драйвером

Зеленый цвет индикатора означает, что драйвером **DiSec** организован туннель по данному интерфейсу и/или задано протоколирование пакетов для данного интерфейса.

Блокировка открытых данных при наличии туннеля

Индикатор имеет зеленый цвет, если прохождение открытых данных заблокировано соответствующей настройкой.

ВСЕГДА сбрасывать открытые данные

Индикатор имеет зеленый цвет, если прохождение открытых данных заблокировано соответствующей настройкой.

Трассировка сетевых пакетов

Данная группа индикаторов отображает параметры протоколирования сети.

Протоколирование интерфейса

Индикатор имеет зеленый цвет, если для данного интерфейса ведется протоколирование.

Информация, отображаемая на данной вкладке автоматически обновляется через каждые 5 сек.

10.3. Вкладка Туннель

Вкладка **Туннель** позволяет просмотреть текущее состояние параметров туннелей, установленных на данном интерфейсе.

Для двух установленных подключений

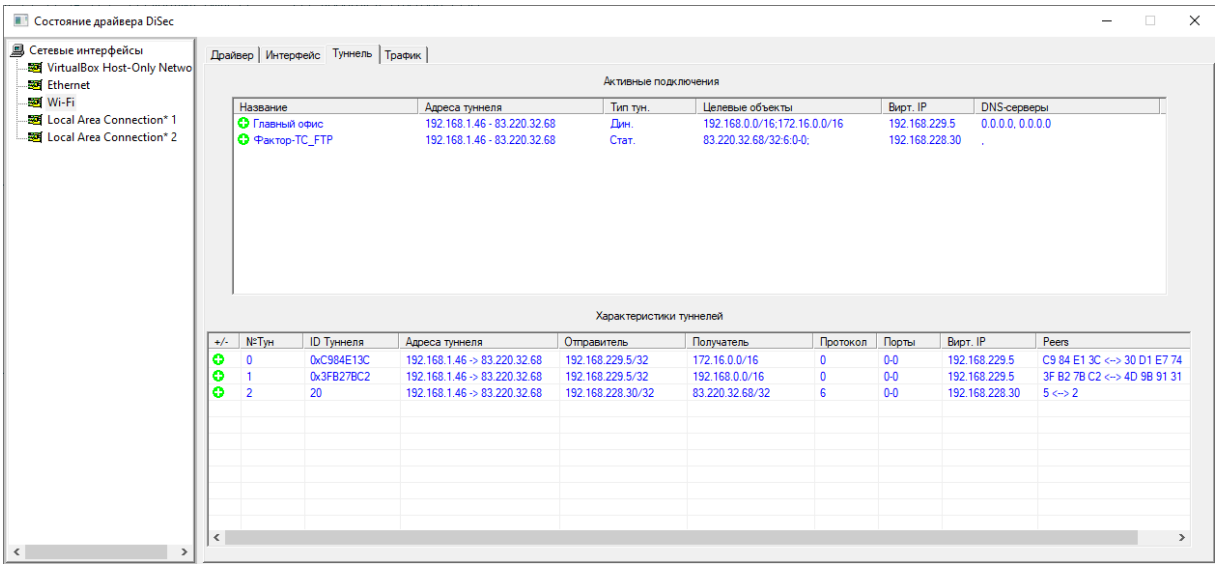


Рис. 93

В секции **Активные подключения** отображаются запущенные из Приложения **DiSec** подключения и их основные параметры.
В секции **Характеристики туннеля** отображаются все активные в данный момент туннели, созданные как Приложением **DiSec**, тк и службой **DiSecSRV**.
При этом в каждой строке таблицы отображается одно правило отбора (целевой объект). Те правила, у которых совпадает номер туннеля во 2-м столбце и идентификатор - в 3-ем столбце, относятся к одному подключению.
В столбце **№Тун** отображается номер туннеля, присвоенный ему драйвером **DiSec**.
В столбце **ID Туннеля** отображается идентификатор туннеля. Для динамического туннеля идентификатор присваивается в процессе согласования SA ESP по протоколу IKE и фактически являются ее локальным идентификатором (индекс параметров безопасности - Security Parameters Index, SPI_I).
В столбце **Адреса туннеля** отображаются IP-адреса "концов" туннеля: первый адрес - IP-адрес сетевого интерфейса устройства пользователя, с которого отправляются и на который принимаются туннелированные пакеты, второй адрес - IP-адрес сетевого интерфейса Сервера VPN, с которого отправляются и на который принимаются туннелированные пакеты от DISEC.
Следующие четыре столбца (**Отправитель**, **Получатель**, **Протокол**, **Порт**) содержат собственно правило отбора с учетом заданной в настройках подмены адреса (MODE_CFG для динамического туннеля, или IP-адрес клиента при интеграции в удаленную сеть для статического туннеля). При этом в самом 1-м столбце отображается признак разрешающего или запрещающего правила (для динамического туннеля правила всегда разрешающие, поскольку соответствуют доступным защищенным ресурсам).
Столбец **Вирт.IP** отображает "новый" подставляемый в сетевые пакеты IP-адрес (MODE_CFG для динамического туннеля, или IP-адрес клиента при интеграции в удаленную сеть для статического туннеля).
Столбец **Peers** содержит разную по смыслу информацию для динамического и статического туннелей. Для статических туннелей содержит пару симметричных ключей (первое значение соответствует локальному ключу, второе - ключу оппонента. Для динамического туннеля отображаются значения **SPI_I** и **SPI**. - идентификаторы SA ESP. В таблице могут присутствовать несколько строк с разными **SPI_I** и **SPI_R** и одинаковыми номером и идентификатором туннеля. Это соответствует ситуации смены SA ESP по окончании времени жизни, задаваемом в настройках политики ESP, поскольку согласование новой SA ESP выполняется заранее.
Информация, отображаемая на данной вкладке ***автоматически обновляется*** через каждые 5 сек.

10.4. Вкладка Трафик

На данной вкладке приведена информация о прохождении данных по туннелю, такие как тип инкапсуляции и статистика ошибок, фиксируемая драйвером.
Первые два столбца идентифицируют правила отбора и туннель, аналогично вкладке **Туннель**.

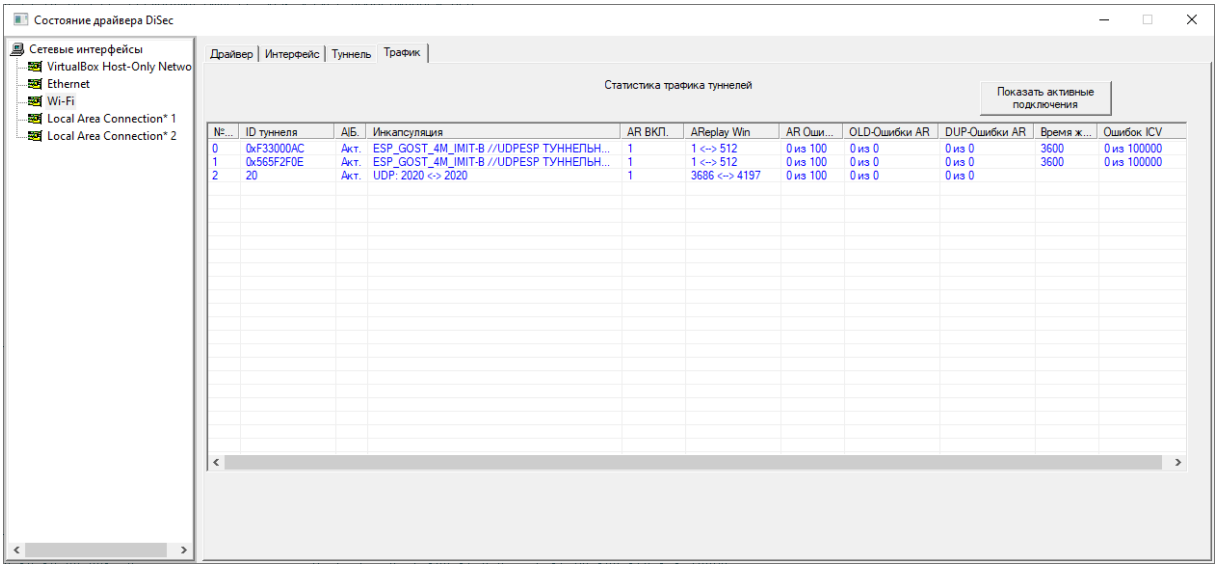


Рис. 94

Последний столбец **А|Б** - отображает состояние активности туннеля: активен или заблокирован в результате обнаружения ошибок, приводящих к блокировке туннеля. Такими ошибками являются обнаружение значительных нарушений нумерации входящих пакетов, а также значительное число отрицатель-

ных результатов контроля целостности пакетов - превышено заданное при настройке политики ESP допустимое число искаженных, т.е. имеющих неверную имитовставку, туннелированных сетевых пакетов (Integrity Fail).

В столбце **Инкапсуляция** отображается протокол туннелирования и номера используемых портов для UDP-инкапсуляции, а также режим ESP, т.е. отображается либо слово "*Транспортный*", либо "*Туннельный*".

Для обоих типов подключения приведены параметры защиты от атак (AntiReplay- защита) и статистика ошибок данного типа.

- в столбце **AR ВКЛ**. отображается состояние защиты от атак: *1* - если включена, *0* - выключена.
- в столбце **AReplayWin** отображается состояние текущего окна: 1-е значение - минимальный контролируемый номер, 2-е - максимальный.
- в столбце **AR Ошибки** отображается количество ошибок на текущий момент времени и максимально допустимое число ошибок (2-е значение).
- в столбце **OLD-ОшибкиAR** - отображается число слишком "старых" пакетов, т.е. номер которых выходит за нижнюю границу окна.
- в столбце **DUP-ОшибкиAR** - отображается число пакетов с повторяющимися номерами.

В столбце **Время жизни** отображается соответствующее значение для SA ESP, по истечении которого будет выполняться рекиинг (обновление ключей) для 2-й фазы протокола IKE (для туннеля СТАТИЧЕСКОГО туннеля значение отсутствует).

В столбце **Ошибок ICV** отображается соответствующее количество ошибок контрольной суммы принятого туннельного пакета (режим ДИНАМИЧЕСКОГО туннеля) на текущий момент времени и максимально допустимое число ошибок (2-е значение).

Информация, отображаемая на данной вкладке автоматически обновляется через каждые 20 сек.

11 Информационные команды

Информационные команды позволяют получить дополнительную информацию, необходимую для диагностики ситуаций невозможности установки подключения и/или возможных причин неработоспособности туннеля посредством изучения информации, выведенной в процессе установки и функционирования туннеля в окно **Диагностика** и **Протокол Сети**, либо при нарушении регламента безопасности в Журнале работы DISEC.

11.1. Команда Диагностика

Активизация команды **Диагностика Главного меню** приводит к выводу на экран окна с заголовком **Диагностика DiSec**, содержащего диагностическую информацию, в том числе, информацию о сообщениях, передаваемых между DISEC и Сервером VPN в процессе установки и разрыва туннеля .

Примечание. Такое же окно выводится на экран при организации туннеля после установки флажка **Выводить окно диагностических сообщений** в окне **Подключиться**.

В окно **Диагностика DiSec** выводятся только основные сообщения, а более подробная информация записывается в файл **Diagnostika.txt**, формируемый в поддиректории **Logs** директории установки программы.

Диагностическая информация требуется, как правило, для разбора ошибочных ситуаций.

В строке меню окна **Диагностика DiSec** два пункта **Файл** и **Правка**:

- команды меню **Файл** позволяют сохранить все содержимое окна в файле в формате (***.rtf**) или распечатать его;
- по команде **Закрыть файл Diagnostika** вся накопленная в памяти компьютера, но не записанная на диск диагностическая информация будет записана в файл **DiSecAPP.txt**;
- команды меню **Правка** позволяют найти нужный фрагмент текста, выделить его и скопировать в другое приложение, например, в стандартный редактор текстовых файлов NotePad.

При возникновении проблемы при подключении к Серверу VPN для создания туннеля или в процессе работы туннеля можно записать сеанс работы DISEC в файл (командой **Сохранить** или **Сохранить как**), сформировать файл **Diagnostika.txt** (командой **Закрыть файл Diagnostika**) и переслать ОБА файла администратору Сервера VPN или разработчикам ПО DISEC.

11.2. Команда Журналы

Команда **Журналы Главного меню** приложения DiSec позволяет просмотреть на экране журнал работы приложения DiSec, журнал работы службы DiSecSrv и журнал вспомогательной службы DiSecAgent.
В журналы записываются основные события, происходящие в процессе работы.
Журналы представляют собой текстовые файлы (UNICODE) и хранятся на диске в директории установки программы в одном или нескольких файлах в зависимости от настройки.
Журнал службы DiSecAgent содержит информацию, которая может понадобиться разработчикам ПО DISEC для выяснения причин неработоспособности.
В командном меню окна находятся команды навигации по журналам.

Файл

Команда **Файл** служит для переключения между файлами, содержащими журналы работы приложения DiSec, службы DiSecSrv и службы DiSecAgent, а также журналы Обновления CRL и проверки сертификатов по протоколу OCSP для подключения динамических туннелей.
При активизации команды **Журналы** всегда открывается текущий файл работы приложения DiSec - тот, в который ведется запись в настоящий момент.

Поиск

Меню **Поиск** содержит команды, которые позволяют:

- команда **Найти** (или клавиши **Ctrl+F**) - выполнить контекстный поиск в файле;
- команда **Найти далее** (или клавиша **F3**) продолжить поиск;

- команда **Найти назад** (или клавиши **Shift+F3**) - изменить направление контекстного поиска;
- команда **Копировать** (или клавиши **Ctrl+C**) - скопировать фрагмент журнала в системный буфер обмена;
- команда **Выделить все** (или клавиши **Ctrl+A**) - выделить и скопировать весь текст в системный буфер обмена.

Обновить (F5)

Команда **Обновить** обновляет окно просмотра, т.е. выводит те записи, которые накопились в журнале с момента активизации команды **Журналы**. Обновляется информация просматриваемого журнала.

События

Команда **События** позволяет просмотреть сообщения (события Безопасности - криптографической подсистемы) из системного журнала WINDOWS ***EventLog***, которые программа DiSec записывает в процессе работы. Сообщения выводятся в порядке убывания даты и времени событий, то есть в верхней части окна помещаются более поздние события.

11.3. Команда Протокол сети

Команда **Протокол сети Главного меню** приложения DiSec позволяет просмотреть на экране файл, содержащий протокол сетевой активности.

Примечание. Протокол сети, как правило не ведется. Включать следует только в целях определения причины ошибочного функционирования туннеля по запросу компетентных в этих вопросах лиц.

В протокол записывается информация о прохождении через драйвер DiSec пакетов данных. Протокол представляет собой текстовый файл **DiSec.net**, помещенный в директории установки программы в поддиректории **Logs**.

Количество и тип записываемой в протокол информации определяется настройкой (см. раздел Параметры протоколирования сетевых пакетов).

В верхней строке после названия окна выводится имя файла, содержащего протокол, и его размер.

В командной строке окна находятся команды.

Файл

Команда **Файл** служит для вывода в окно просмотра основной файл Протокола Сети, например, после просмотра системного журнала по команде **Драйвер** из меню **События**.

Поиск

Меню **Поиск** содержит пять команд, которые позволяют:

- команда **Найти** (или клавиши <Ctrl+F>) - выполнить контекстный поиск в файле;
- команда **Найти далее** (или клавиша <F3>) - продолжить поиск;
- команда **Найти назад** (или клавиши <Shift+F3>) - изменить направление контекстного поиска;
- команда **Копировать** (или клавиши <Ctrl+C>) - скопировать фрагмент протокола в системный буфер обмена;
- команда **Выделить все** (или клавиши <Ctrl+A>) - скопировать весь текст в системный буфер обмена.

Обновить (F5)

Команда **Обновить** обновляет окно просмотра, т.е. выводит те записи, которые накопились в Протоколе сети с момента активизации команды **Протокол сети**.

События -> Драйвер

В меню **События** находится одна команда Драйвер, которая позволяет просмотреть сообщения из системного журнала WINDOWS ***EventLog***, которые драйвер DiSec записывает в процессе работы. Сообщения выводятся в порядке убывания даты и времени событий, то есть в верхней части окна помещаются более поздние события.

Системный журнала событий также можно просмотреть встроенными в ОС WINDOWS средствами. Для этого применяется следующая последовательность действий:

- нажать правой кнопкой мыши на значке Computer;
- выбрать контекстную команду Управление (Manage);
- выбрать последовательно System Tools, Event Viewer, Windows Logs, System.
- применить фильтр по значению "DiSec".

12 Справочная информация

Справочная информация может быть выведена на экран либо по команде **Справка**, либо по значку контекстной справки в диалоговых окнах.

12.1. Справка

Приложение DiSec снабжено стандартной для программ под управлением WINDOWS справочной подсистемой, вызываемой по команде **Справка Главного меню**. Кроме того, есть возможность использовать контекстную справку для всех элементов окон и команд меню
Для вызова контекстной справки следует после нажатия знака вопроса (**?**) в верхнем правом углу активного окна «подтянуть» его к интересующему элементу окна или кликнуть на нем правой кнопкой манипулятора «мышь» или нажать клавишу F1.
Для получения контекстной справки по команде меню следует подвести курсор мыши к интересующей команде и нажать правую кнопку манипулятора «мышь» или клавишу F1.

12.2. О программе

По команде **О программе Главного меню** на экран выводится краткая информация о версии и компонентах ПО DISEC, а также о фирме-разработчике.

13 Команда Выход

По команде **Выход** Главного меню приложения DiSec выполняются только после отключения всех активных подключений по команде Отключить.
При выходе удаляется значок программы из области уведомлений строки состояния рабочего стола (SYSTEM TRAY).
Драйвер DiSec переходит в «прозрачный» режим.
Служба DiSecSrv и организованный ею туннель продолжают функционировать.

14 Приложение 1. Функциональные возможности ПО DISEC версии 7.0

Основные характеристики	
Категория программы	VPN-клиент, реализующий набор протоколов IPSEC (IPSecurity)
Назначение программы	Создание виртуального канала между компьютером пользователя и VPN-сервером для доступа к ресурсам защищенной сети.
Тип виртуального канала	IPSec с шифрованием и контролем целостности передаваемого трафика
Тип VPN-сервера	программно-аппаратный комплекс **Dionis-NX**
Операционная платформа (ОС Windows)	Десктоп-компьютеры Серверы Ноутбуки Планшеты
Сетевые конфигурации	Совместимость с любыми сетевыми интерфейсами, в том числе с Wi-Fi (статический и динамический IP-адрес), мобильные широкополосные модемы GSM
Количество одновременных подключений	не более 10
Типы подключений (по способу организации)	**Статический** с настройками правил отбора и выбором типа инкапсуляции **Динамический** (IKE v1)
Количество туннелей в подключении (каждый туннель предоставляет доступ к одному целевому объекту из списка в настройках подключения или соответствует одному правилу отбора)	Не ограничено на стороне DiSec
Настройка доступа к защищенным ресурсам	**Динамический:** 1) целевые объекты задаются на сервере и передаются клиенту в процессе переговоров по протоколу IKE (MODE_CONFIG) 2) целевые объекты согласовываются заранее и устанавливаются "вручную" при настройке клиента. Несколько правил в одном подключении соответствуют нескольким IPSEC-соединениям (***Connection)*** на стороне сервера VPN. **Статический** - целевые объекты согласовываются заранее и устанавливаются "вручную" при настройке клиента
Режимы взаимной аутентификации клиента и сервера	**Динамический:** инфраструктура PKI (асимметричные ключи шифрования). Режим "Preshared key" - не реализован **Статический:** симметричные ключи шифрования
Интегрированный межсетевой экран (МЭ)	Отсутствует
Контроль целостности	По инициативе пользователя клиента Периодический в процессе работы приложения, отключение туннелей и выход из программы при нарушении целостности ПО.
Состав ПО	Приложение Windows - DiSec.exe Службы Windows - DiSecSRV.exe, DiSecAgent.exe. Драйвер Kernel Mode - DiSec.sys Крипто-библиотека - динамически подгружаемые модули DLL

	Дополнительные программы и службы: инсталляция, деинсталляция драйвера; настройка настройка, запуск и останов служб; Сбор информации о системе, Лицензирование).
Лицензирование	Защита ключом регистрации - разрешена установка на одном компьютере. Возможно использование Лицензии на ограниченный срок действия
Программная операционная среда	
Поддерживаемые операционные системы: Microsoft Windows (x64)	Microsoft Windows 10 Microsoft Windows Server 2016
Совместимость со средствами защиты	- Функционирует при наличии установленного антивирусного ПО - требуется тестирование при наличии средств VPN
Совместимость со средствами мониторинга сети (анализаторы трафика)	да
Многопользовательская среда	Обеспечивает независимую настройку виртуальных туннелей каждого пользователя одного компьютера, а также защиту от несанкционированного использования туннелей при переключении сессий.
Вход в домен Windows по защищенному каналу (установление виртуального канала ДО входа пользователя в систему)	Автоматическая установка туннеля в режиме службы Windows (служба DiSecSRV)
Возможность авто-подключения при входе пользователя в систему	1) Несколько подключений одновременно 2) Несколько подключений последовательно, переход на следующий при разрыве соединения.
Авторизация для выполнения настроек	1. Запрашивается идентификационные данные администратора для настройки защищенного (критичного) функционала: - настройка службы; - настройка драйвера; - Экспорт конфигурации 2. Защита паролем процедуры выполнения настроек.
Сетевые конфигурации	
Сетевые интерфейсы	Ethernet Wi-Fi Модем телефонной линии Mobile Broadband modem
Стек TCP\IP	IPv4 IPv6 - поддерживается для статических туннелей
Поддержка нескольких сетевых интерфейсов	- Автоматическое определение сетевого интерфейса для туннеля и маршрутизация трафика
	- возможность блокирования "открытого" трафика при наличии\отсутствии туннеля
Работа через NAT (NAT Traversal)	**Динамический:** NAT Traversal **Статический:** UDP-инкапсуляция - настраиваемые порты
Интеграция в существующую сетевую инфраструктуру	**Динамический**: MODE_CONFIG - динамическое получение адреса из пула IP-адресов защищенной сети, а также адреса DNS и адрес IP-подсети в качестве целевого объекта. **Статический**: RLAN - назначение статического заранее согла-

	сованного IP-адреса, а также адреса DNS.
Свойства Ethernet-адаптеров	Работа на адаптерах, поддерживающих TaskOffload - автоматическое отключение при инсталляции ПО DISEC.
	Динамический: поддержка Jumbo-фреймов **Статический**: поддержка Jumbo-фреймов
Изменение сетевой конфигурации компьютера	Отслеживает отключение и подключение сетевых адаптеров - автоматически отключает туннель.
Особенности реализации	
Шифрование и контроль целостности передаваемого трафика	**Динамический**: Протоколы IPsec ESP (RFC2401-2412), с использованием (только) ***российских*** криптографических алгоритмов. **Статический**: Протоколы IPsec: "IP Encapsulation within IP" (RFC 2003), с использованием (только) ***российских*** криптографических алгоритмов.
Аутентификация взаимодействующих сторон	**Динамический**: по протоколу IKE (RFC 2407-2409 и RFC 4303) с использованием сертификатов X509 (RFC 5280). **Статический**: Использование симметричных ключей.
Режимы туннелирования	**Динамический**: - транспортный и туннельный режимы ESP-инкапсуляции. **Статический**: - туннельный режим "IP-in-IP" - UDP-инкапсуляция пакет (поверх IP-in-IP)
Режимы инкапсуляции	**Динамический**: -ESP_GOST-4M-IMIT, -ESP_GOST-1K-IMIT - UDP\ESP-инкапсуляция (NAT-Traversal) **Статический**: UDP-инкапсуляция пакет (поверх IP-in-IP). Настройка портов по согласованию с оппонентом (Сервером VPN)
Информационные обмены протокола ISAKMP\IKE	**Динамический**: IKEv1 - Main mode - Quick mode - Informational Exchanges - Transaction Exchanges (MODECFG) IKEv2 - **не реализован** **Статический**: отсутствуют
Алгоритмы выработки сессионных ключей	**Динамический**: - VKO ГОСТ Р 34.10-2012 - VKO_GOSTR3410_2012_256, - VKO_GOSTR3410_2012_512 **Статический**: ГОСТ28147-89
Алгоритмы шифрования	- ГОСТ28147-89
Алгоритмы контроля целостности сетевых пакетов	**Динамический**: - ГОСТ Р 34.11-2012 - ESP_GOST-4M-IMIT, - ESP_GOST-1K-IMIT **Статический**: ГОСТ Р 34.11-94
Алгоритмы электронной цифровой подписи (ЭЦП)	**Динамический:** - ГОСТ Р 34.10-2012

Мониторинг доступности удаленного узла (жизнеспособности туннеля)	**Динамический**: Dead Peer Detection (DPD) протокол (RFC 3706) с настройкой параметров и предпринимаемых действий **Статический**: посылка пинг-проб клиентом сервера (с возможностью отключения и настройки параметров)
Обновление сессионных ключей (re-keying)	**Динамический**: в соответствие с настройками политики IKE\ESP **Статический**: отсутствует
Обработка искаженных пакетов (Integrity Fail)	**Динамический**: реализована в соответствии с настройками политики ESP **Статический**: отсутствует
Защита от Replay-атак	Реализовано с использованием алгоритма сдвига окна (bit-shifting) с настройкой параметров окна и порога ошибок. Возможно отключение.
Журналирование и протоколирование	
Журнал действий пользователя	- начало\окончание сеанса пользователя с указанием имени пользователя - основные этапы установки подключения, возникшие ошибки - смена пользователя Windows
Протоколирование сетевого трафика	Опционально при включении данной опции администратором.
Системный журнал (Event Log, System Log)	Фиксируются ошибки функционирования виртуального канала драйвером (источник данных DISEC). Для приложения и службы - фиксируются события безопасности (положительные и отрицательные). Источник данных DISECAPP.
Сбор статистики сети в целом, а также по интерфейсам	Начиная от загрузки ОС: - количество пакетов принятого и переданного трафика; - количество сброшенных пакетов с разбивкой по причинам (блокировка, ошибки); - количество ошибочных пакетов с разбивкой по типу ошибок (крипто, нехватка памяти, искаженные IP\TCP-пакеты)
Статистика Туннелей	**Динамический:** - число пакетов с искаженной контр. суммой (Integrity Fail); - статистика нарушения нумерации пакетов (Replay атаки). **Статический:** статистика нарушения нумерации пакетов (Replay атаки).
Криптография	
Криптографические библиотеки	Встроенные библиотеки разработки ООО "Фактор-ТС"
Ключевые носители	- флэш-память USB - Токены производства компании Aladdin: eToken PRO32k – при наличии драйверов производителя - Токены производства компании Актив: Рутокен, Рутокен S - при наличии драйверов производителя
Формат ключевого контейнера	**Динамический:** - PKCS#15 - объекты PKCS#11 с контейнером ключа PKCS#15 **Статический:** контейнер
Формат сертификатов публичных ключей	X.509 v.3 (ГОСТ)
Поддержка списка отозванных сертификатов	Обновление и обработка Certificate Revocation List (CRL). Поддерживается CRL v.2. Способ получения CRL – протокол LDAP v.3, FTP, HTTP
Контроль валидности сертификатов	Опционально.

по протоколу OCSP.	