УТВЕРЖДЕНО

RU.НКБГ.70009-02 92 - ЛУ

Клиент криптографического сервера доступа «DiSec-W»

Версия 6.0

Руководство пользователя

RU.НКБГ.70009-02 92

Листов 117

Содержание

1 Общие сведения

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	-	СКЗИ «Клиент криптографического сервера доступа «DiSec-W»
Краткое наименование изделия	-	«DiSec, версия 6.0» или «DiSec-W»
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 первом 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, и для обеспечения доступа удалённых пользователей к ресурсам сегментов глобальной вычислительной сети, защищённых сетевыми устройствами.

ПО DiSec совместно с Севером VPN реализует набор протоколов IPsec (IP Security) для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов, а также включает в себя протоколы для защищённого обмена ключами в сети Интернет. 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 Микрософт: 32-разрядных и 64-разрядных версий операционных систем Microsoft Windows Server 2012, Windows Server 2008, Microsoft Windows 10, Microsoft Windows 8.1, Windows 7, Windows Vista.

Далее по тексту, где не требуется детализация, будет использоваться общий термин "устройство пользователя 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).

В DiSec реализованы два протокола защиты данных в канале связи, что обеспечивает информационную совместимость DiSec с сетевыми устройствами разработки ФАКТОР-ТС: «Многоуровневый криптомаршрутизатор DioNIS TS/FW 16000/КВ2», «Многоуровневый криптомаршрутизатор DioNIS-LXM», «Программно-аппаратный комплекс Dionis-NX», а также с сетевыми устройствами, выполняющими требования документов «Методические рекомендации по использованию ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при управлении ключами IKE И ISAKMP», Методические рекомендации по использованию комбинированного алгоритма вложений IPSEC ESP на основе ГОСТ 28147-89» и «Техническая спецификация по использованию ГОСТ 28147-89, ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 в протоколах обмена ключами IKE и ISAKMP», разработанному Техническим комитетом по стандартизации «Криптографическая защита информации» (ТК-26) (несимметричная система распределения ключевой информации).

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 (туннель) между компьютером с установленным ПО DiSec и Сервером VPN. Компьютеры, подключенные к открытой сети и имеющие, как правило, «неопределенный» IP-адрес, называются Мобильными клиентами.

ПО DiSec, установленное на одном компьютере, доступно для использования всеми пользователями WINDOWS, которые работают независимо друг от друга, при этом настройки DiSec хранятся отдельно в персональных директориях пользователей WINDOWS.

DiSec выполняет также функции Межсетевого экрана (МЭ), обеспечивая фильтрацию сетевых пакетов в соответствии с заданными настройками. Фильтрация выполняется только для не туннелированных IP-пакетов.

Сводка основных функциональных возможностей ПО DISEC приведена в Приложении (см. раздел 13).

На общей схеме IP-доступа к ресурсам защищенных сетей (Рис. 1) представлено взаимодействие мобильных клиентов, 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 **Защищенной сети 1** и **Защищенной сети 2** имеют возможность взаимного доступа к ресурсам каждой сети путем организации средствами туннеля виртуальной частной сети (VPN). Такие туннели образуются между Серверами VPN в момент их включения и действуют постоянно до выключения узлов, поэтому они называются «статическими» (туннель VPN статический).

Вся информация (IP-пакеты) при передаче между ресурсами **Защищенной сети 1** и **Защищенной сети 2** через туннель шифруется, что делает возможным для пользователей компьютеров этих сетей обмен конфиденциальной информацией по каналам связи открытой сети.

Статические туннели могут использовать пользователи DiSec, имеющие постоянный статический IP-адрес.

Пользователи DiSec инициируют создание динамического туннеля.

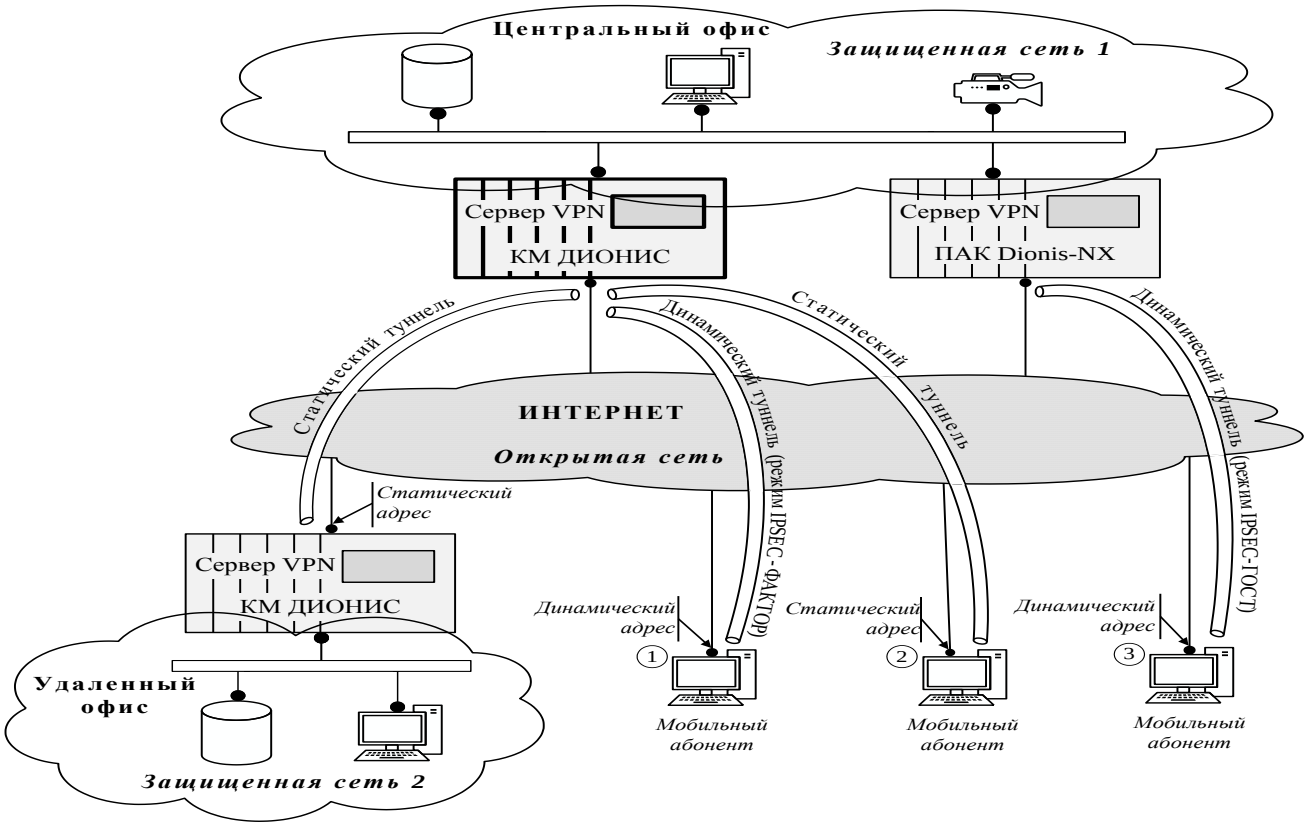


Рис. 1

1.2 Основные понятия IPSEC и способы организации туннелей

IPsec - это набор стандартов Интернет, который функционирует на сетевом уровне семиуровневой модели OSI и использует самый распространённый протокол этого уровня — IP, таким образом представляет собой «надстройку» над IP-протоколом. Ядро IPsec составляют три протокола:

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. При применении ESP в обязательном порядке должен указываться набор услуг по обеспечению безопасности: каждая из его функций может включаться опционально.

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, включая задание фиксированных ключей, или же использование таких протоколов, как Internet Key Exchange (IKE).

Ключевым понятием IPSec является Security Association (SA - Ассоциация Безопасности). SA представляет собой набор параметров, характеризующий соединение, в частности, используемые алгоритм шифрования и хэш-функция, секретные ключи.

В ПО DiSec существуют два режима IPSEC-ФАКТОР и IPSEC-ГОСТ, реализующие отличающиеся варианты (наборы) протокола IPSec. Режим IPSEC-ФАКТОР из вышеперечисленных протоколов IPSec использует только протокол ISAKMP, а режим IPSEC-ГОСТ - два последних протокола (IKE и ESP)

Режим IPSEC-ФАКТОР использует протокол ISAKMP с заранее распределенными ключами, а режим IPSEC-ГОСТ - использует протокол IKE для защищенного обмена ключами и для создания Ассоциаций Безопасности.

В режиме IPSEC-ФАКТОР выполняется согласование одной SA, в режиме IPSEC-ГОСТ - две SA (1-я фаза протокола IKE - согласование SA IKE, 2-я фаза протокола IKE - согласование SA ESP, при этом каждый вид SA имеет свой набор параметров - алгоритмов шифрования, имитовставки - хеш-функций, размеров ключей шифрования и проч.). Параметры для каждой SA хранятся в соответствующей политике (политика IKE и политика ESP).

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**.

Статический туннель. Оба конца туннеля должны иметь постоянный IP-адрес подключения к открытой сети. Параметры настройки противоположных концов туннеля согласуются администратором Сервера VPN и пользователем DiSec с помощью обычных каналов связи (телефон, e-mail …), т.е. без использования IP-сети и протокола ISAKMP. Запускается туннель в момент запуска Сервера VPN и существует до его остановки , либо до снятия туннеля по инициативе администратора сервера. DiSec может подключаться и отключаться от туннеля по инициативе пользователя DiSec.

Динамический туннель организуется между Сервером VPN и компьютером, оснащенным DiSec. Организуется динамический туннель только по запросу пользователя DiSec, и для его организации каждый раз требуется согласование параметров настройки противоположных концов туннеля посредством протокола ISAKMP.

В режиме IPSEC-ФАКТОР может использоваться как статический, так и динамический туннель. В режиме IPSEC-ГОСТ - только динамический.

Протокол IKE реализован на основе рекомендаций RFC 2407-2409 с использованием российских криптоалгоритмов ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94. 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 адреса IP-подсети в качестве доступного ресурса (целевой объект).

1.3 Туннелирование

Туннелированием называется процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов, 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);
- UDP (IP-протокол с номером 17);
- ESP (IP-протокол с номером 50);

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 заданного протокола инкапсуляции). При этом добавляется заголовок инкапсулирующего пакета, а в поле данных заносится информация, идентифицирующая туннель и другая служебная информация. Сформированный таким образом транспортный сетевой пакет при необходимости разбивается на фрагменты (фрагментируется) и отправляется в открытую IP-сеть.

При получении сетевого пакета выполняется процедура деинкапсуляции, то есть процесс восстановления данных в соответствии с заданным протоколом инкапсуляции из поля информационных данных транспортного протокола, его расшифрование и 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 "верх" по стеку TCP\IP получателю - прикладной программе. Процедуре деинкапсуляции может предшествовать процедура дефрагментирования пакетов (сборки одного пакета из нескольких принятых), также проверка корректности заголовков пакета.

1.3.1 Режим IPSEC-ФАКТОР

В качестве инкапсулирующего (транспортного) протокола используется IP-протокол IP-in-IP (номер 4).

В случае статического туннеля "поверх" протокола IP-in-IP может быть использован протокол UDP с произвольными, но согласованными номерами портов источника и назначения.

В динамическом туннеле 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 и т.п, устанавливаемые на сетевом интерфейсе устройства пользователя DiSec.

Примечания. После закрытия туннеля эти настройки снимаются и возвращаются прежние значения.

1.3.2 Режим IPSEC-ГОСТ

При туннелировании в режиме IPSEC-ГОСТ 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 IPSEC-ГОСТ реализованы два режима ESP-инкапсуляции: транспортный и туннельный.

В транспортном режиме шифруются (или подписываются) только данные IP-пакета, исходный заголовок сохраняется. Транспортный режим, как правило, используется для установления соединения между хостами.

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.

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 34.10-2001, ГОСТ Р 34.11-94. Встраивание российских криптоалгоритмов в указанные протоколы производилось в соответствии с рекомендациями технического комитета по стандартизации «Криптографическая защита информации» (ТК26) (www.tk26.ru).

1.4 Межсетевое экранирование

Межсетевой Экран (МЭ), входящий в состав DiSec, обеспечивает фильтрацию трафика на сетевом уровне.

Решение по фильтрации принимается для каждого сетевого пакета на основе сетевых адресов отправителя и получателя, а также на основе атрибутов, таких как порт протокола TCP/IP получателя и/или отправителя, флагов в TCP-заголовках сетевых пакетов, значения заданных полей в любом месте сетевого пакета.

Фильтрация выполняется с учетом входного и выходного сетевого интерфейса независимо для входящего и исходящего трафика для каждого сетевого интерфейса.

Проверка соответствия характеристик сетевого пакета правилам фильтрации выполняется ТОЛЬКО для открытых (не туннелированных) данных как при наличии туннеля, так и при его отсутствии.

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 (раздел 2.1, с. 10); сведения об общих принципах функционирования ПО DiSec и о взаимодействии с Серверами VPN (раздел 2.2, с. 11), а также об основных терминах и принципах системы криптографической защиты информации, используемых в DiSec (раздел 2.4, с. 13).

2.1 Взаимодействие компонентов DiSec с компонентами WINDOWS

Клиент Криптографического сервера доступа DiSec состоит из следующих основных компонентов (Рис. 2):

- на уровне приложений - приложение DiSec (**`DiSec.exe`**) и комплект динамически подгружаемых крипто-библиотек;
- на уровне сервиса операционной системы (службы) – служба DiSecSrv (**`DiSecSrv.exe`**) и вспомогательная служба DiSecIsm;
- 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 и останова службы DiSecSRV, инсталляции драйверов ruToken\eToken.

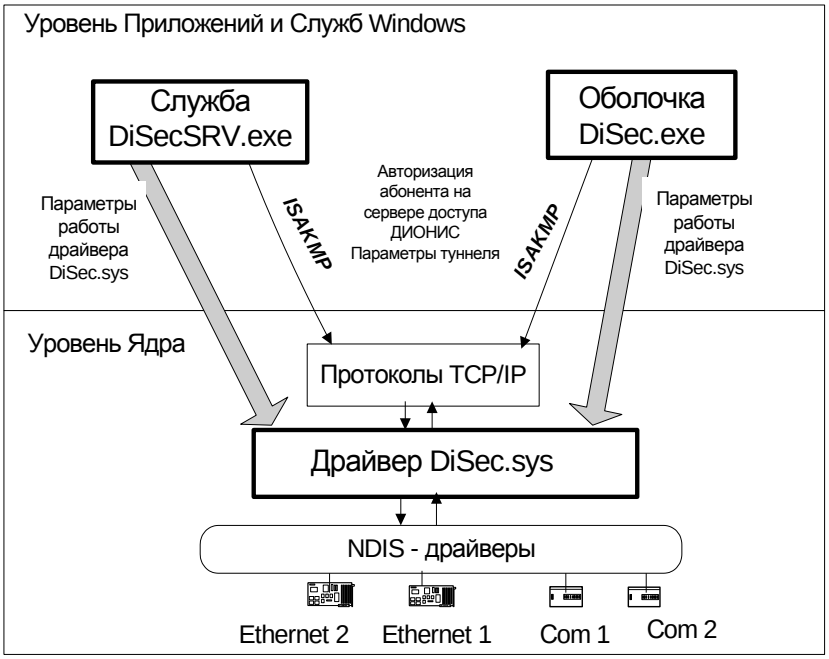


Рис. 2

Приложение DiSec выполняет главную задачу - организации и удаления 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, о текущем состоянии IP-компонентов WINDOWS;

- выполнить различные диагностические функции;

- останавливать, запускать и следить за работой службы DiSecSrv.

Помимоэтого 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 DiSecIsm обеспечивает доступ к глобальным объектам (сокетам), прием и диспетчеризацию полученных от сокетов сообщений, выполняет вспомогательные функции изменения настроек интерфейсов по "заданию" приложения и службы при установке туннелей. 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, компонентом «Удаленный доступ» (RAS) 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.

Драйвер также выполняет функции межсетевого экрана (МЭ), анализируя пакеты на соответствие правилам фильтрации.

При обнаружении ошибок в процедурах фрагментирование\дефрагментирования, инкапсуляции\деинкапсуляции, зашифрования\расшифрования, а также при обнаружении некоторых видов сетевых атак (например, AntiReplay) 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 (Рис. 3).

1-й этап – организация туннеля.

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

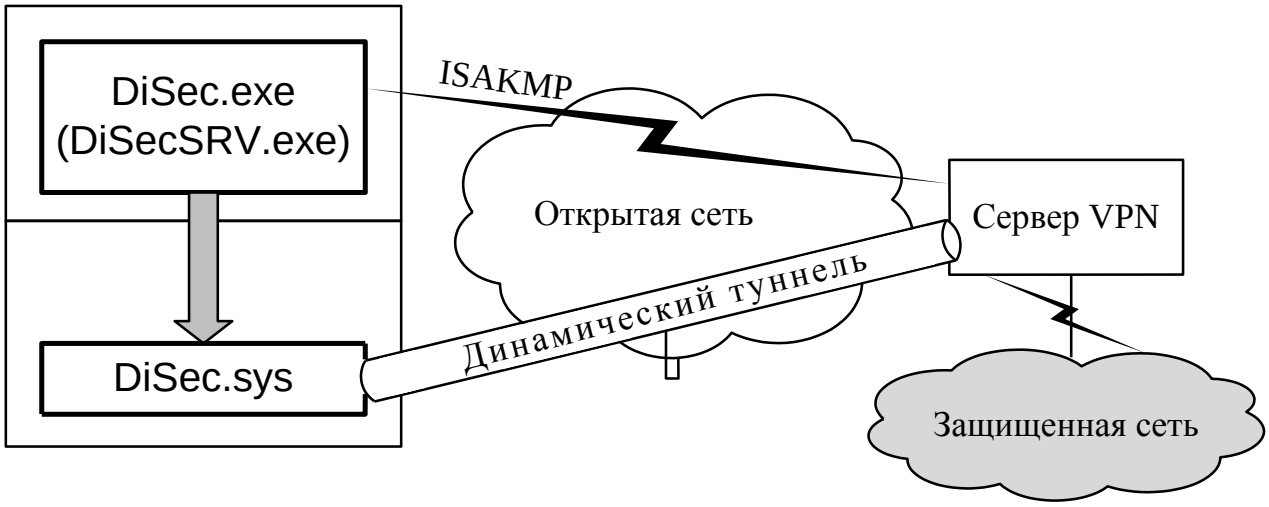


Рис. 3

Выполнение 1-го этапа осуществляется по-разному для статических (см. 2.2.2) и динамических туннелей (см. 2.2.1).

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 и с помощью приложения DiSec (или посредством службы DiSecSrv).
2) Пользователь DiSec посылает запрос на подключение к Серверу VPN.

   Для режима IPSEC-ФАКТОР запрос посылается по протоколу ISAKMP и содержит аутентификационные данные абонента, соответствующие его ключевой информации, необходимые для создания динамического туннеля.

   Для режима IPSEC-ГОСТ посылается запрос в соответствии с протоколом IKE версии 1.
3) Выполняется взаимная аутентификация.

   Для режима IPSEC-ФАКТОР Сервер доступа VPN выполняет аутентификацию и частичную авторизацию абонента, т.е. проверяет, имеет ли данный абонент право на создание личного туннеля.

   Для режима IPSEC-ГОСТ 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.

   Для режима IPSEC-ФАКТОР в случае успешной аутентификации и авторизации абонента выполняется проверка ключевой информации пользователя DiSec (окончательная авторизация абонента) и согласование параметров динамического туннеля, в том числе правил отбора в туннель, которые присылаются на DiSec Сервером VPN и формирование ключей для шифрования и расшифрования сетевых пакетов в туннеле.

   Для режима IPSEC-ГОСТ 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) Согласованные параметры работы туннеля загружаются в драйвер DiSec.

   Для режима IPSEC-ГОСТ 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.
6) В режиме IPSEC-ГОСТ 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.

   Примечание - Входной рекиинг, то есть обновление SA IKE и SA ESP по инициативе Сервера VPN не поддерживается (см. п. 3.4.2).

2.2.2 Организация статического туннеля

Для статического туннеля согласования параметров не выполняется, DiSec загружает с ключевого носителя ключи шифрования и переходит в состояние готовности передачи и приема зашифрованного трафика.

При настройке параметров статического туннеля имеется возможность выбора протокола инкапсуляции (IP-in-IP или 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 (напомним, что для динамического туннеля правила отбора устанавливаются во время процедуры организации туннеля).

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, а также с ресурсами всех сетей, с которыми у данного Сервера существуют статические или динамические туннели.

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 и DiSec (см. раздел 8.3, с. 91).

Во время работы туннеля его «жизнеспособность» может контролироваться или Сервером VPN, или DiSec, или тем и другим. Имеется возможность настройки параметров проверки жизнеспособности туннеля (значения интервала посылок, таймаутов ожидания ответа, предельных значений количества ошибок).

Одновременно с защищенными ресурсами пользователь DiSec может работать с открытыми ресурсами при соответствующей настройке (см. п. 6.4.1.1, с. 69).

По окончании работы с защищенными ресурсами пользователь DiSec выполняет закрытие туннеля и отсоединение от Сервера VPN (см. раздел 7.3, с. 87).

Закрыть туннель может сам пользователь DiSec по завершении работы с защищенными ресурсами; закрыть туннель может Сервер VPN при обнаружении разрыва соединения с клиентом, а также DiSec при отсутствии ожидаемых ответов от Сервера VPN.

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 (см. Команда Подключиться).

После закрытия туннеля драйвер DiSec продолжает работать в «прозрачном» режиме.

Подключение к сети Интернет сохраняется, в том числе посредством Dial-UP соединения.

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 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).

2.4 Система криптозащиты в DiSec

Как было сказано выше, 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 DiSec.

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.

Далее в процессе согласования с Сервером VPN параметров туннеля осуществляется проверка корректности ключевой информации (соответствие настроек на DiSec настройкам на Сервере). При обнаружении ошибок пользователю DiSec выводится сообщение об ошибке, и процедура подключения прекращается.

Режим организации туннеля IPSEC-ФАКТОР 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 туннеля IPSEC-ГОСТ 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 расшифрования 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 режиме IPSEC-ГОСТ Сервер VPN и DiSec могут пересылать друг другу сертификаты в процессе согласования SA IKE (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. Наивысший сертификат в цепочке называется **корневым** (Root certificate).

В процессе согласования SA IKE **Цепочка Доверия** строится каждой стороной для проверки 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, выполняя обращение к серверам LDAP для загрузки обновленного COC(CRL), а также выполнять оперативную проверку актуальности сертификата по протоколу OCSP (Online Certificate Status Protocol).

Используются алгоритмы шифрования, длина ключей и т.п. в соответствии с документами ТК26.

2.4.1 Ключевые носители

Пользователь DiSec должен иметь в своем распоряжении ключевой носитель с персональной ключевой информацией.

В качестве ключевых носителей могут быть использованы любые носители, которые ОС WINDOWS может определить как съемные (дискета НГМД, съемный USB-носитель и.т.п.).

В качестве ключевых носителей также могут использоваться устройства типа ТОКЕН:

- **ruToken** производства компании Актив (тип «ruToken» и «ruToken S»);

- **eToken** производства компании Aladdin.

В процессе установки DiSec пользователь может при необходимости выполнить установку ПО, обеспечивающего функционирование этих устройств в ОС WINDOWS.

> *Примечание* - ООО «Фактор-ТС» не является разработчиком ПО поддержки носителей типа ТОКЕН, а только обеспечивает возможность их использования в качестве ключевых носителей.

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.

> *Внимание!* Ключевой носитель содержит закрытую 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 в режиме IPSEC-ФАКТОР (используется симметричная ключевая система) на ключевом носителе содержится сетевой набор ключей определенной серии. На ключевом носителе может быть несколько сетевых наборов, размещенных в разных директориях.

При работе в режиме IPSEC-ГОСТ (используется несимметричная ключевая система) пользователь DiSec должен получить на ключевом носителе свой закрытый ключ вместе с сертификатом открытого ключа.

Закрытый ключ (и необходимая для его использования информация) помещается на съемном ключевом носителе в так называемом «контейнере».

DiSec поддерживает два формата «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; это значение следует выбирать, если ключ предполагается использовать в изделиях, от которых требуется такая совместимость.
- **Фактор ТС 1.0** – формат, разработанный в рамках технологии «ДИОНИС»; это значение следует выбирать, если ключ предполагается использовать в изделиях, не поддерживающих формат PKCS#15;

На ключевой носитель может быть помещен сертификат ключа пользователя.

Кроме того, для организации туннеля в режиме IPSEC-ГОСТ пользователь DiSec должен иметь сертификаты ключей всех Серверов VPN, с которыми предполагается устанавливать туннель, сертификаты всех необходимых Удостоверяющих Центров (УЦ), а также списки отозванных сертификатов (СОС). Эти сертификаты и списки можно разместить на этом же ключевом носителе, в том числе и на носителях типа ТОКЕН, если они поддерживают интерфейс PKCS11.

> *Примечание.* В реквизитах подключения в режиме IPSEC-ГОСТ имеется возможность автоматической загрузки актуальной информации о СОС.

Если в качестве ключевых носителей используются токены, то сертификаты и списки отозванных сертификатов размещаются на другом носителе.

Ключевой носитель должен быть доступен для записи, поскольку в процессе настройки криптосистемы на него записывается необходимая для дальнейшей работы информация (см. раздел 6.3.5.1, с. 50).

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.

Режим IPSEC-ФАКТОР. Для генерации симметричных ключей и формирования ключевых носителей могут использоваться изделия производства ООО «ФАКТОР-ТС»:

- Автоматизированное рабочее место генерации ключей (АРМ ГК-3) (НКБГ.501430.735) - в режиме «IPsec-Фактор»;

Режим IPSEC-ГОСТ. Для генерации несимметричных ключей и формирования ключевых носителей могут использоваться изделия производства ООО «ФАКТОР-ТС»:

- Модуль генерации ключей МГК-2 (НКБГ.501430.774) совместно с программно-аппаратными средствами Удостоверяющего центра, поддерживающими формат сертификатов, соответствующий рекомендациям X.509 - в режиме «IPsec-ГОСТ».

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.

3 Условия применения программы

ПО DiSec обеспечивает выполнение решаемых им задач при выполнении требований данного документа, документов «СКЗИ Клиент криптографического сервера доступа «DiSec» Правила пользования» RU.НКБГ.70009-02 90 (далее по тексту ПРАВИЛА) и «СКЗИ Клиент криптографического сервера доступа «DiSec» Формуляр» RU.НКБГ.70009-02 30 (документы входит в комплект поставки DiSec).

Ниже приведены требования:

- к оборудованию компьютера пользователя DiSec (раздел 3.1, с. 16),
- к операционной среде – настройке программных компонентов ОС WINDOWS (раздел 3.2, с. 16) и программных средств, работающих под ее управлением,
- к программно-аппаратным средствам подключения к сети Интернет (раздел 3.3, с. 16),
- к настройкам Сервера VPN (раздел 3.4, с. 17),
- к ключевой информации (раздел 3.5, с. 18).

3.1 Требования к оборудованию

ПО DiSec устанавливается на IBM-совместимом компьютере, функционирующем под управлением 32 и 64-разрядных версий операционных систем Microsoft: Microsoft Windows Server 2012, WINDOWS Server 2008, Microsoft Windows 10, Microsoft Windows 8.1, Windows 7, Windows Vista.

DiSec функционирует на сетевых интерфейсах типа Ethernet, интерфейс беспроводной связи WiFi, 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 (НГМД либо USB-порт).

3.2 Требования к программному окружению

Настройки ОС WINDOWS должны быть произведены в соответствии с ПРАВИЛАМИ.

Требуется выполнять регулярное обновление ОС WINDOWS, а также программного обеспечения (драйверов) сетевых плат Ethernet, адаптеров и модемов.

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 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 UDP-пакеты с портом 500 и 4500 (портом источника а и портом назначения для исходящего) и туннелированные пакеты (протокол IP in IP – номер 4) - для режима IPSEC-ФАКТОР), и протокол ESP (номер 50) для режима IPSEC-ГОСТ.

При использовании для выхода в сеть Интернет WINDOWS-ресурса сервиса удаленного доступа (**DialUP**) следует выполнить следующие предварительные действия:

- подключить к компьютеру и настроить модем в соответствии с инструкцией по эксплуатации модема и с требованиями сервера удаленного доступа.
- создать WINDOWS-ресурс удаленного доступа стандартными средствами операционной системы, при необходимости разрешить его использование всеми пользователями компьютера.
- проверить подключение к серверу удаленного доступа с соответствующими именем пользователя этого ресурса и паролем.

  Примечание - Имя пользователя и пароль можно в дальнейшем изменить при настройке DiSec для конкретного пользователя.

DiSec можно настраивать на автоматическое установление соединения с сервером удаленного доступа с использованием созданного ресурса удаленного доступа во время процедуры организации туннеля. В этом случае необходимо заранее создать **DialUP**-ресурс и разрешить его использование пользователями компьютера.

3.4 Настройки на Сервере VPN

Для того чтобы пользователь DiSec мог организовать туннель, на Сервере VPN должны быть выполнены необходимые настройки. Эти настройки зависят от типа туннеля (динамический или статический), от режима организации туннеля (IPSEC-ФАКТОР или IPSEC-ГОСТ), а также от многих других факторов (от топологии сети, от требований, предъявляемых к криптографическим и технологическим параметрам туннелей, и т.п.).

Ниже (раздел 3.4.1, с. 17) приведена типовая настройка Сервера VPN для организации туннеля в режиме IPSEC–ФАКТОР. Так могут быть настроены все перечисленные в разделе 1.1 (с. 5) криптомаршрутизаторы.

В разделе 3.4.2, с. 17 приведена настройка Сервера VPN для организации туннеля в режиме IPSEC-ГОСТ на примере настройки криптомаршрутизатора «ПАК Dionis-NX».

3.4.1 Настройки на Сервере VPN для организации туннеля в режиме IPSEC–ФАКТОР

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

1. Должно быть разрешено прохождение входящих пакетов протокола UDP с портом назначения 500 и исходящих пакетов с портом источника 500, а также разрешено прохождение туннелированных сетевых пакетов (транспортный протокол TNL (IP in IP) - номер протокола 4).
2. Должна быть проинициализирована подсистема **Криптозащита** и введена ключевая информация.
3. Пользователь ПО DiSec должен быть зарегистрирован на Сервере VPN, т.е. иметь на нем учетную запись (являться АБОНЕНТОМ) и иметь право на создание личного туннеля.
4. Должно быть обеспечено соответствие ключевой информации на Сервере VPN и ключевой информации пользователя DiSec.
5. В параметрах **Ограничения доступа** личного туннеля абонента Сервера VPN, соответствующих **правилам отбора в туннель**, должны присутствовать правила, разрешающие прохождение сетевых пакетов, обеспечивающие контроль функционирования туннеля - протокола ISAKMP и Ping-пакетов. При отборе сетевых пакетов в туннель и при извлечении их из туннеля правила просматриваются по порядку, начиная с первого, и просмотр заканчивается, как только будет обнаружено соответствие параметров сетевого пакета с параметрами правила, поэтому список правил следует формировать таким образом, чтобы правила с меньшим диапазоном действия предшествовали правилам с большим диапазоном.
6. В параметрах **Ограничения доступа** личного туннеля абонента Сервера VPN, соответствующих **правилам отбора в туннель**, при неизвестном заранее IP-адресе клиента DiSec необходимо указывать значение параметра **Адрес** равным *0.0.0.0*, а параметра **Зн.бит** равным *0*.

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. Должна быть проинициализирована подсистема **Криптозащита** и введена ключевая информация.
5. Статический туннель должен быть настроен на загруженные ключи шифрования.
6. Пользователю DiSec должен быть передан идентификатор статического туннеля и номер ключа удаленного конца туннеля.
7. 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).

3.4.2 Настройки на Сервере VPN для организации туннеля IPSEC–ГОСТ

Для обеспечения возможности организации динамического туннеля IPSEC–ГОСТ 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:

- необходимо отключить рекиинг (обновление сессионных ключей по инициативе Сервера VPN);

- установить максимально допустимые времена жизни SA фазы 1 и фазы 2;

- назначить согласованные параметры для SA фазы 1 и фазы 2, либо позволить ПО DiSec выбирать эти параметры (режим "no strict").

Примерная последовательность настройки приведена в Приложении (раздел 14, стр. 115). Следует учитывать, что состав и формат команд может меняться в зависимости от версии «ПАК Dionis-NX». Для уточнения следует обращаться к документации «ПАК Dionis-NX».

3.5 Требования к ключевой информации

Для организации туннеля в режиме IPSEC-ФАКТОР должны выполняться следующие требования:

- ключи взаимодействующих сторон должны быть сформированы одним средством генерации ключей;
- ключевая информация на DiSec и на Сервере VPN должна иметь одну и ту же серию;
- номер ключа (криптономер) в настройках туннеля на DiSec должен совпадать с номером, указанным в настройках личного туннеля для данного абонента на Сервере VPN.

Для организации туннеля в режиме IPSEC-ГОСТ должны выполняться следующие требования:

- ключевая информация на DiSec должна соответствовать сертификату пользователя;
- сертификат пользователя DiSec должен быть выпущен Удостоверяющим Центром. Поле «**Enhanced Key Usage**» сертификата должно содержать *OID 1.3.6.1.5.5.8.2.2*;
- сертификат пользователя DiSec должен быть выпущен в формате x.509.

Формат ключевых носителей должен соответствовать требованиям, приведенным в п. 2.4.1, стр. 14.

3.6 Подготовка и порядок работы с DiSec

Перед началом выполнения процедуры настройки туннелей пользователю DiSec следует выполнить подготовительные действия и получить ВСЮ необходимую для этого информацию о настройках Сервера VPN (см. раздел 3.4, с. 17) и получить криптографический материал, необходимый для зашифрования и расшифрования данных туннеля. Подготовительные действия и состав необходимой информации различен для режимов туннелирования в режиме IPSEC-ФАКТОР и в режиме IPSEC-ГОСТ.

3.6.1 Подготовка к работе в режиме IPSEC-ФАКТОР

Для организации динамического или статического туннеля в режиме IPSEC-ФАКТОР пользователь DiSec должен иметь информацию, необходимую для подключения к Серверу VPN:

- IP-адрес или доменное имя Сервера VPN в сети Интернет (IP-адрес должен совпадать с локальным адресом интерфейса Сервера, к которому осуществляется подключение);
- 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 организации ***динамического*** туннеля в режиме IPSEC-ФАКТОР пользователь DiSec должен знать имя, под которым он был зарегистрирован на Сервере VPN и получил право на создание личного туннеля - параметр **имя абонента**.

Для организации *динамических* туннелей в режиме IPSEC-ФАКТОР необходимо зарегистрироваться на каждом из Серверов VPN для работы с защищаемыми ими сетевыми ресурсами. Регистрация выполняется следующим образом:

- администратор Сервера VPN создает нового абонента, и имя этого абонента сообщает пользователю DiSec (обратите внимание, что пароль для регистрации на Сервере не требуется, так как аутентификация и авторизация при работе DiSec идет по криптографическим ключам);
- администратор Сервера VPN дает абоненту разрешение на работу с личным туннелем (динамическим) и указывает номер ключа, который будет использовать абонент для создания туннеля.

Для организации *статического* туннеля в режиме IPSEC-ФАКТОР пользователь DiSec должен знать:

- **идентификатор** (**номер**) статического туннеля и IP-адрес (или доменное имя) Сервера VPN;
- **криптономер** ключа сервера VPN из той же серии, что и ключ пользователя;

- метод **инкапсуляции** трафика;
- IP-адреса доступных защищенных ресурсов (**правила отбора**). В случае настройки IPSEC-соединения на сервере, обеспечивающей IP-адресов подсети, эта информация не требуется.

3.6.2 Подготовка к работе в режиме IPSEC-ГОСТ

Для организации туннелей в режиме IPSEC-ГОСТ надо предварительно выполнить следующее.

- 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.
- Получить от администратора Сервера VPN следующие данные:
  - IP-адрес (или доменное имя) Сервера VPN, с которого 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, эта информация не требуется.
- Получить от службы безопасности организации или от ответственного лица:
  - сертификаты всех Серверов VPN, с которыми предполагается устанавливать;
  - сертификаты всех доверенных УЦ и списки отозванных сертификатов, необходимые для корректного построения цепочек доверия для сертификатов Серверов VPN.

  Все полученные сертификаты и списки должны быть помещены в соответствующие хранилища DiSec (см. п. 6.3.5.6, с. 63).

  Примечание. Сертификаты доверенных УЦ присылаются на DiSec по доверенному каналу связи, остальные – произвольным способом.

Для организации туннелей в режиме IPSEC-ГОСТ требуется, чтобы значения перечисленных ниже криптопараметров на DiSec соответствовали значениям соответствующих параметров на Сервере VPN:

- узел замены (алгоритм ГОСТ 28147-89), используемый для шифрования протокола IKE (см. 14, п. 19) (необязательно в случае использования политики "no strict");
- параметры алгоритма ГОСТ Р 3410-2001, используемые для выработки сессионного ключа фазы 1 протокола IKE (см. 14, п. 19) (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 (см. 14, п. 22) (необязательно в случае использования политики "no strict");
- узел замены (алгоритм ГОСТ 28147-89), используемый для шифрования данных в протоколе ESP (см. 14, п. 20) (необязательно в случае использования политики "no strict");
- преобразование ESP - туннельное или транспортное (см. 14, п. 20);
- режим ***Perfect Forward Secrecy*** (PFS) (см. 14, п. 21);
- для устойчивости соединения надо, чтобы значения времен жизни 1-й и 2-й фазы протокола IKE не превышали соответствующих значений на Сервере VPN.

3.6.3 Порядок работы с DiSec

Для работы с DiSec необходимо выполнить следующие действия.

1. Инсталлировать DiSec (раздел 4, с. 21).
2. После выполнения перезагрузки WINDOWS запустить приложение DiSec (раздел 5.2, с. 27).
3. При необходимости 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 (Рис. 14) и заполнить список **Защищенные сети (ресурсы подключения)** (раздел 6.2, с. 35).
5. Штатными средствами WINDOWS (или средствами, предоставленными провайдером услуг доступа в сеть Интернет) выполнить подключение к IP-сети. Этот шаг может быть пропущен при использовании **DialUP**-соединения.
6. Дать команду **Подключиться** из Главного меню приложения (Рис. 14) и, выбрав необходимый ресурс (ресурсы) из списка, отправить ему запрос для подключения к Серверу VPN (см. раздел 7.1, с. 84).

7. После успешного тестирования подключения возможно назначение его (или всего списка) для автоматического запуска при запуске ОС WINDOWS (раздел 6.3.1, с. 39).

4 Инсталляция и удаление DiSec

Инсталляция состоит из двух этапов: инсталляция основного ПО – инсталляция собственно DiSec (раздел 4.2, с. 21) и инсталляция дополнительного ПО поддержки носителей eToken и ruToken, используемых в работе ПО DiSec в качестве ключевых носителей.

В результате инсталляции основного ПО на компьютере будут установлены все основные и служебные программы, а также документация.

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 опциональную установку ПО поддержки (драйверов) носителей eToken и ruToken;
- 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 необходимо предыдущую версию деинсталлировать (см. раздел 4.4, с. 25).

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 Микрософт, 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 Микрософт, которой можно воспользоваться, например, при отсутствии по какой-либо причине доступа в Интернет или к сайту Микрософт.

Начинается установка с предупреждающего сообщения (Рис. 4).

Рис. 4

Затем программа установки выводит на экран окно (Рис. 5) с информацией о необходимости деинсталлировать предыдущую версию DiSec и возможной несовместимости DiSec с другими программами.

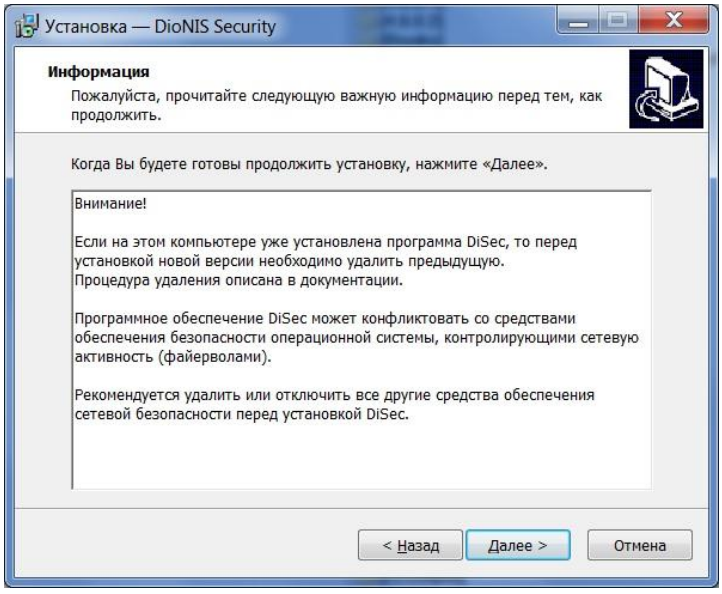


Рис. 5

Далее программа установки проверяет наличие свободной памяти на компьютере и запрашивает имя папки, в которую будет установлено ПО DiSec (стандартное значение `<системный_диск>:\`**`Program Files\Factor-TS\DioNIS Security`**).

Если для установки DiSec пользователь укажет новую папку, то она будет создана; если будет указана уже существующая папка, то будет выдан дополнительный запрос на подтверждение данного выбора.

Затем программа установки предложит выбрать имя папки в стартовом меню WINDOWS для размещения ярлыков программ, входящих в состав DiSec. Будет создана папка **`FACTOR Applications\DioNIS Security`**.

В следующем окне (Рис. 6) программа инсталляции предложит выбрать комплект установки: пользователь может отказаться от предложенной установки драйверов ruToken и/или eToken, а также снять флажок автоматической инициализации службы DiSecSrv.

Рис. 6

Далее программа установки выведет на экран окно с полученной от пользователя информацией для инсталляции и после нажатия кнопки **Установить** выполнит разархивацию и копирование файлов с дистрибутивного носителя в указанную папку.

При работе в операционной системе WINDOWS VISTA и выше будет выдано сообщение системной службы безопасности, запрашивающее разрешение на установку драйвера DiSec.

Рис. 7

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

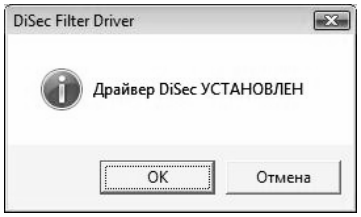


Рис. 8

В окне установки появится сообщение «**Завершение установки**» и, если это было задано (см. Рис. 6), будут установлены драйверы устройств считывания ключевых носителей eToken и ruToken. Процесс установки драйверов не требует вмешательства пользователя.

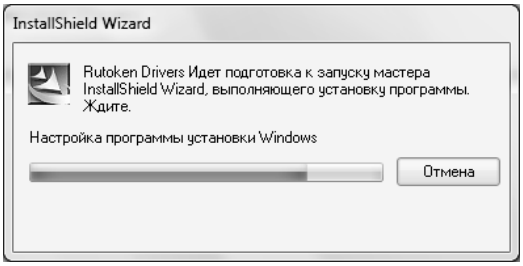


Рис. 9

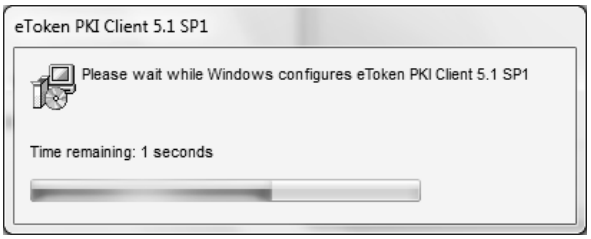


Рис. 10

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

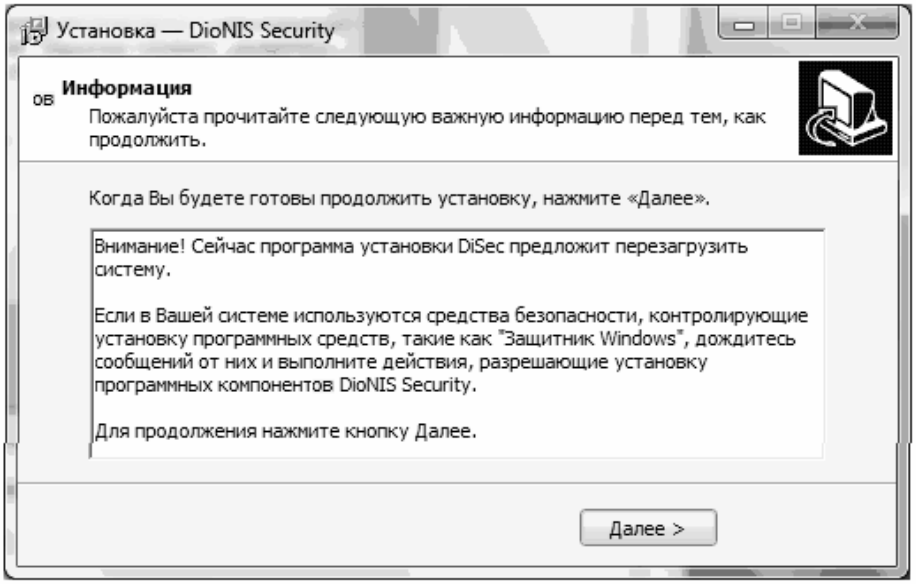


Рис. 11

По окончании инсталляции будет предложено перезагрузить компьютер.

Перезагрузку выполнить необходимо, поскольку в процессе перезагрузки выполняются действия по регистрации (формировании записей в системном реестре) сетевых IP-интерфейсов (Ethernet, Удаленный доступ и пр.) драйвером DiSec. Затем надо 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:

- папка **Служба DiSecSrv** с ярлыками программ работы со службой (инициализация, настройка, удаление, запуск и останов службы);
- папка **Драйвер DiSec** с ярлыками программ работы с драйвером (инсталляция, настройка и деинсталляция);
- папка **Ключи**, содержащая команды инсталляции драйверов ключевых носителей ruToken и eToken;
- папка **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 ОС драйвер DiSec будет автоматически запускаться каждый раз при старте операционной системы и функционировать в «прозрачном» режиме до загрузки в драйвер DiSec параметров динамического туннеля, т.е. драйвер будет пропускать все пакеты по всем IP-интерфейсам, имеющимся в системе, не выполняя никаких преобразований.

4.3 Проверка контрольных сумм

ПО DiSec предназначено для работы с конфиденциальной информацией, поэтому перед тем как начинать работать с изделием, пользователь должен проверить целостность полученного программного обеспечения.

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 (обычно в папке <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» RU.НКБГ.70009-02 90 (комплектации 1.1, 1.2, 1.3) или RU.НКБГ.70009-02 91 (комплектации 2.1, 2.2).

При первом включении DiSec для проверки целостности полученного программного обеспечения: пользователь должен запустить программу **Контрольные суммы**: **Пуск ⇨ Программы ⇨ FACTOR Applications ⇨ DioNIS Security ⇨ Контрольные суммы.**

Программа **Контрольные суммы** вычислит контрольные суммы на файлы, приведенные в списке, сравнит их с эталонными значениями и выведет на экран список проверенных файлов 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 (раздел 4.4, с. 25).

В дальнейшем контроль целостности ПО будет проводиться с периодичностью, заданной в настройках программы (см. 6.1.4, стр. 35). Периодичность проверки зависит от условий эксплуатации и определяется политикой безопасности эксплуатирующей организации. Периодический контроль выполняется автоматически, если программа DiSec запущена. Если программа DiSec не запущена, то проверка выполнится при ее запуске.

4.4 Удаление DiSec

Для выполнения удаления (деинсталляции) DiSec полностью либо для удаления службы DiSecSrv необходимо обладать правами администратора WINDOWS.

При удалении DiSec полностью служба DiSecSrv удаляется автоматически вместе с файлом настроек службы.

4.4.1 Удаление службы DiSecSrv

Удаление службы из списка служб WINDOWS может быть выполнено только после ее останова. Остановить службу можно либо командой **Останов службы DiSecSrv** из программной папки **Dionis Security** стартового системного меню (**Пуск**), либо кнопкой **СТОП** на вкладке **Служба DiSecSrv** окна **Тестирование** (см. раздел 9.5, с. 98).

Удаление службы DiSecSrv выполняется командой **Удаление службы DiSecSrv** из программной папки **DiSec** стартового системного меню (**Пуск**).

4.4.2 Удаление всех компонентов ПО DiSec

При необходимости перед удалением ПО DiSec можно сохранить **Журналы событий**, которые находятся в поддиректории **Logs** программной директории **DiSec** (как правило, это директория «<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;
- активизировать в **Главном меню** приложения (Рис. 14) команду **Настройка**, получить окно **Настройка**, открытое на вкладке **Реквизиты подключений** (раздел 6.2, с. 35), и снять флажок **Авто-коннект** во всех элементах списка;

- на вкладке **Драйвер DiSec** окна **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 **DioNIS Security** стартового системного меню.

В процессе деинсталляции DiSec выполняются следующие процедуры:

- останов и деинсталляция службы DiSecSrv**;**
- удаление драйвера DiSec, 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 в персональных директориях пользователей, работавших с DiSec, соответствующую рабочую папку. В разных ОС WINDOWS эти папки имеют разные названия, например, в WINDOWS 7 имя персональной директории имеет следующий вид:

<системный диск>**:\Users**<имя пользователя>**\Application Data\Factor-TS\DioNIS Security**.

либо:

<системный диск>**:\Users**<имя пользователя>**\AppData\Roaming\Factor-TS\DioNIS Security**.

В процессе деинсталляции выполняется удаление драйверов ключевых носителей ruToken и eToken автоматически, если они устанавливались при установке DiSec. Если они устанавливались отдельно, то их деинсталляция не будет выполнена.

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 DiSec, использования DiSec и обслуживания (раздел 5.1, с. 27);
- возможность использования ПО различными пользователями ОС WINDOWS компьютера независимо друг от друга в режиме работы с приложением DiSec (раздел 5.2, с. 27);
- работа в режиме службы WINDOWS (раздел 5.3, с. 31).

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`**), а для WINDOWS VISTA и ***выше*** дополнительно необходимо обладать «повышенными» (**`elevated`**) административными правами.

Работы по обслуживанию DiSec должны выполняться пользователем, обладающим административными правами в операционной системе WINDOWS. К таким работам относятся инсталляция и деинсталляция всего ПО или его части (службы, драйвера). Проверка контрольных сумм не требует наличия у пользователя административных прав.

После инсталляции DiSec любой пользователь данного компьютера, в том числе не имеющий административных прав в ОС WINDOWS, 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.

Настройка режимов работы **драйвера**, включая настройку режимов протоколирования сети, должна выполняться пользователем, обладающим административными правами в операционной систем WINDOWS.

Настройка и тестирование службы DiSecSrv**,** а также ее запуск и останов посредством команд из программной папки **`DioNIS Security`** стартового системного меню должны выполняться пользователем, обладающим административными правами в операционной системе WINDOWS.

Элементы управления (кнопки) окон настройки и тестирования, при активизации которых выполняются действия, требующие административных прав в операционной системе WINDOWS VISTA или выше, помечаются значком (или аналогичным). При инициировании соответствующих операций будет выдан запрос на разрешение выполнения привилегированных действий в системе.

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.

5.2 Работа с приложением DiSec

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

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.

Версия DiSec 6.0 защищена от несанкционированного копирования, т.е. для каждой ее инсталляции на отдельном устройстве необходимо получить ключ регистрации от фирмы-разработчика.

При первом запуске программы 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, приведенное на рис.

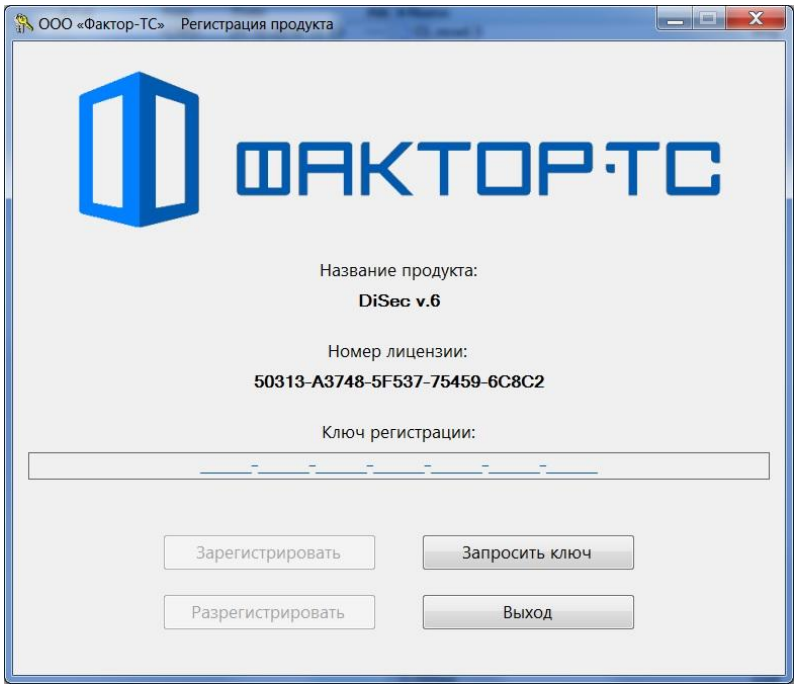


Рис. 12

Необходимо нажать кнопку Запросить ключ. При этом на экран будет выдана форма, приведенная на рис.

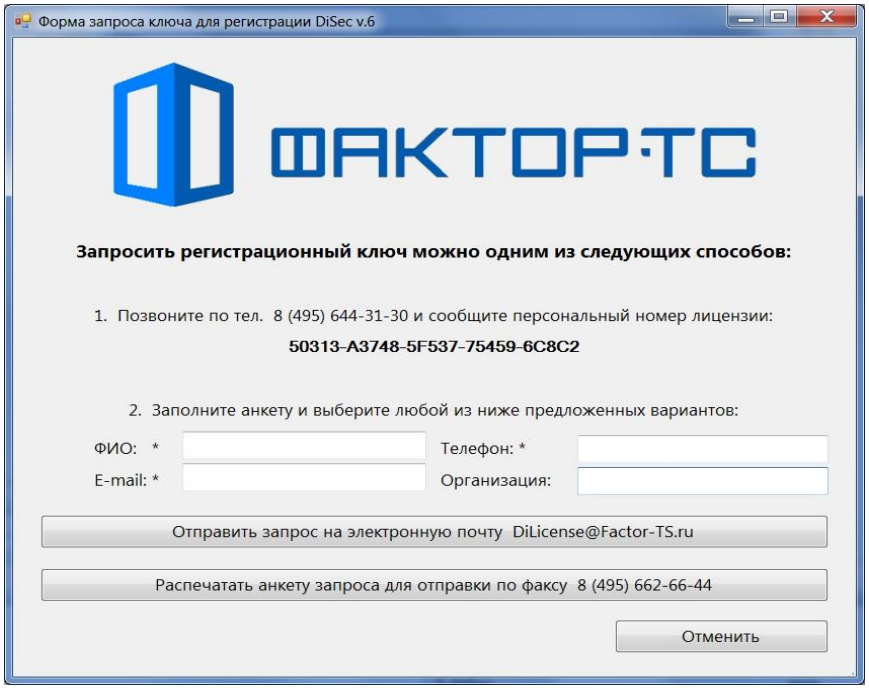


Рис. 13

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**.

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. Наличие фона (оранжевого цвета) показывает, что инициатором установки туннеля была служба DiSecSrv (см. раздел 5.3, стр. 31).

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 вызова приложения при старте операционной системы, в противном случае флажок автоматического запуска следует снять (см. п. 6.1.1, с. 34).

При постоянной работе с какими-либо ресурсами (подключениями) рекомендуется выполнить настройку автоматического установления соединения при запуске приложения (см. раздел 6.2, с. 35). 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,
- а также сообщения, выдаваемые в процессе установления и отключения соединения с Сервером VPN.

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 установленного туннеля для предотвращения его несанкционированного использования.

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.

5.2.2 Команды приложения DiSec

Работа с приложением DiSec выполняется посредством команд Главного меню приложения (Рис. 14). 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 (Рис. 14) 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 и тестирование сетевых компонентов;
- 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.

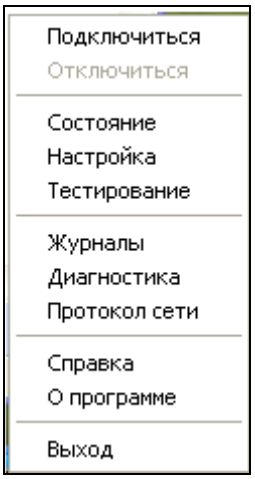


Рис. 14. Главное меню приложения DiSec

По команде **Подключиться** выполняется процедура организации туннеля с одним из Серверов VPN для работы с сетевыми ресурсами соответствующей защищенной сети. Команда **Подключиться** также активизируется при двойном щелчке мышью на значке в системной области. Действия, выполняемые при этом DiSec, зависят от типа туннеля и режима его организации (см. разделы 7.1, с. 84 и 7.2, с. 87).

По команде **Отключиться** выполняется разъединение с выбранным из списка Сервером VPN. Команда доступна только при наличии связи с Сервером VPN, либо если запущен цикл подключений (п. 2.3, стр. 13). Действия DiSec, выполняемые при активизации команды, зависят от типа туннеля и режима его организации (см. раздел 7.3, с. 87). Если одновременно установлены несколько подключений, то при наведении курсора мыши на команду **Отключиться** выдается список, из которого можно выбрать одно или ВСЕ подключения.

Команда **Состояние** позволяет просмотреть текущее состояние параметров работы драйвера DiSec, в том числе, информацию об установленном туннеле и статистические данные по сетевым интерфейсам (раздел 8, с. 88), а также информацию о настройке драйвера DiSec.

Команда **Настройка** обеспечивает выполнение следующих функций (раздел 6, с. 33):

- 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.

Несмотря на то, что команда активна при установленном подключении, ее вызов позволяет только просмотреть основные настройки, но изменить из невозможно.

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 **Тестирование** предназначена для проверки состояния IP-компонентов WINDOWS, а также для тестирования доступности сетевых ресурсов (раздел 9, с. 94). Также можно определить состояние службы DiSecSrv, протестировать ее запуск и останов (только для пользователей WINDOWS с административными правами).

Команда **Журналы** позволяет просмотреть на экране журнал работы приложения DiSec, журнал работы службы DiSecSrv (раздел 10, с. 102) и журнал вспомогательной службы DiSecIsm.

Команда **Диагностика** служит для просмотра накопленных во время сеанса работы DiSec диагностических сообщений, которые выдает приложение DiSec при подключении к Серверу VPN (раздел 10.1, с. 102). 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 (раздел 10.3, с. 104) – заданную при настройке информацию о проходящих через драйвер DiSec сетевых пакетах.

Команда **Справка** позволяет получить полную справочную информацию по работе с DiSec (раздел 11, с. 108).

Команда **О программе** позволяет получить информацию о составе и версиях компонентов ПО DiSec (раздел 11, с. 108).

Команда **Выход** позволяет завершить работу с приложением DiSec. Данная команда используется при удалении ПО DiSec с компьютера (см. раздел 4.4, с. 25), а также при работе в режиме ручного запуска приложения (раздел 12, с. 109). При выходе из программы автоматически выполняется отключение от Сервера VPN, если подключение было выполнено командой **Подключиться** (драйвер DiSec переходит в исходный режим).

> *Замечание*. 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 соединение с защищенным ресурсом (туннель) 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 некоторые предварительные действия.

1) Инициализировать компонент ПО DiSec – службу DiSecSrv, если она не была инициализирована при установке DiSec (по умолчанию после инсталляции DiSec служба DiSecSrv инициализирована) или была по какой-то причине удалена.
2) Назначить пользователя, от имени которого будет запускаться служба.
3) Настроить реквизиты подключения, с которым будет работать служба DiSecSrv, и назначить его для использования службой (см. п. **Ошибка! Источник ссылки не найден.**, с. **Ошибка! Закладка не определена.**).

Инициализация службы DiSecSrv, т.е. добавление ее к списку сервисов (служб) операционной системы, может быть выполнена автоматически во время инсталляции DiSec (раздел 4.2, с. 21). Если впоследствии служба была удалена, то ее можно вновь инициализировать вызовом из программной папки стартового системного меню команды **DioNIS Security ⇨ DiSecSrv ⇨ Инсталляция службы DiSecSrv**.

По окончании инсталляции службы будет выведено окно (Рис. 15).

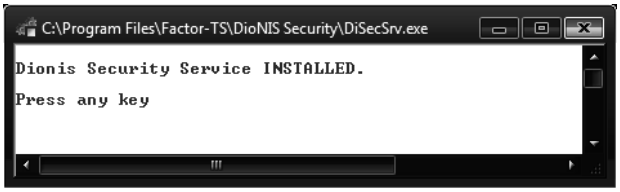


Рис. 15

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);
- 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.

Далее следует настроить службу (см. раздел 6.5, с. 78), то есть назначить ей ресурс для подключения и задать режим ее запуска.

Настроить режим запуска службы можно также средствами WINDOWS, для этого следует открыть окно списка служб WINDOWS: **Панель управления ⇨ Администрирование ⇨ Службы,** выбрать из списка службу **Dionis Security Service**, и в окне свойств на вкладке **Вход в систему** выбрать пользователя.

Рекомендуется проверить работу службы в окне **Тестирование** (см. раздел 9.5, с. 98).

После полной настройки службы и проверки ее запуска в окне **Тестирование** следует включить автоматический запуск службы при загрузке ОС и перезагрузить компьютер.

После перезагрузки ОС служба автоматически начнет работу в соответствии с произведенными настройками, при этом она выполняет поиск и считывание ключевой информации пользователя на съемных носителях без выдачи каких-либо сообщений.

В случае корректного ввода ключевой информации и успешного установления 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  . Над этим значком появится всплывающая надпись с именем активизированного службой подключения.

При невозможности выполнить подключение к Серверу VPN служба остается в «рабочем» состоянии и через определенные интервалы делает попытку поиска ключевого носителя и подключения к заданному ресурсу. В этом случае после входа пользователя в систему значок программы DiSec имеет белый цвет на оранжевом фоне. Рекомендуется отключить службу и изучить журнал службы с целью определения причины неудачного подключения (см. п. 10.1, стр. 102).

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 **СТАРТ** на вкладке **Служба DiSecSrv** окна **Тестирование** (см. п. 9.5, с. 98).

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 **СТОП** на вкладке **Служба DiSecSrv** окна **Тестирование** (см. п. 9.5, с. 98).

Для диагностирования проблем с запуском службы следует просмотреть журнал событий **DiSecSrv.log** при помощи соответствующий команды Главного меню приложения ПО DiSec (см. п. 10.2, с. 103).

6 Команда Настройка

Команда Главного меню приложения (Рис. 14) **Настройка** позволяет установить параметры работы для всех компонентов DiSec - драйвера, службы и приложения. Команда позволяет:

- задать список ресурсов подключений (защищенных сетей) и указать необходимые для подключения реквизиты;
- задать режимы работы драйвера (доступно только пользователю, обладающему административными правами в операционной системе WINDOWS), в частности, задать режим протоколирования сетевой активности, настроить и активировать МЭ;
- задать режим запуска приложения и параметры ведения журнала событий;
- задать периодичность проверки целостности ПО;
- задать режим запуска службы DiSecSrv (доступно только пользователю, обладающему административными правами в операционной системе WINDOWS).

По команде **Настройка** открывается окно, содержащее четыре вкладки, каждая из которых содержит параметры, относящиеся к соответствующей группе, обозначенной в названии вкладки.

Чтобы сохранить выполненные на всех вкладках изменения настроек, надо выйти из окна, нажав кнопку **ОК**.

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

Кнопка **Принять** позволяет применить выполненные на данной вкладке изменения настроек, после чего использование кнопки **Отмена** не окажет на них влияния. Окно остается открытым на текущей вкладке.

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

6.1 Вкладка Общие (Настройка ПО DiSec)

После активизации команды **Настройка** на экран будет выведено окно **Настройка ПО DiSec**, открытое на вкладке **Общие** (Рис. 16).

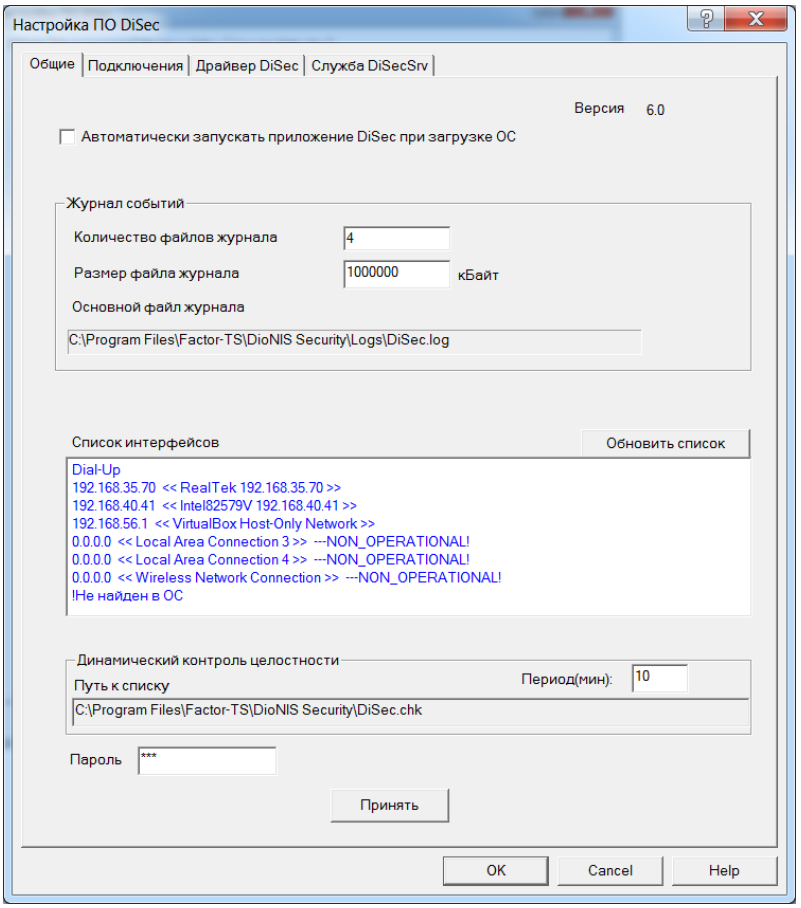


Рис. 16

Вкладка позволяет задать режим запуска приложения DiSec, задать параметры ведения журнала событий, а также просмотреть состояние зарегистрированных драйвером DiSec сетевых интерфейсов

6.1.1 Режим запуска приложения DiSec

Флажок Автоматически запускать приложение DiSec при загрузке ОС обеспечивает автоматический запуск приложения DiSec при старте операционной системы. При этом 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) **DioNIS Security** стартового системного меню WINDOWS.

6.1.2 Журнал событий

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

1. **Количество файлов журнала** - 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 играет роли).
2. **Размер файла журнала** - параметр 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.
3. **Основной файл журнала** – имя первого (единственного) файла журнала оболочки; имя задается программой, и изменить его нельзя: основной файл журнала оболочки DiSec - **DiSec.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.

6.1.3 Список интерфейсов

В секции под заголовком **Список интерфейсов** отображаются активные сетевые интерфейсы TCP/IP (интерфейсы, соответствующие платам Ethernet, беспроводным соединениям WiFi, 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, а также имя **Dial-UP** для интерфейса службы удаленного доступа WINDOWS (RAS).

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 неуспешна, 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, работоспособность COM-портов компьютера и т.п.).

Кнопка **Обновить список** позволяет заново получить список зарегистрированных драйвером DiSec сетевых интерфейсов без закрытия окна **Настройка ПО DiSec**. Использование данной кнопки рекомендуется, если во время работы с окном **Настройка ПО DiSec** 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.

6.1.4 Динамический контроль целостности

В секции под заголовком **Динамический контроль целостности** отображаются параметры контроля. один из которых Период (мин.) может быть изменен. 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 закрывается с отключением всех активных туннелей.

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

6.2 Вкладка Подключения (Настройка ПО DiSec)

Вкладка **Подключения** (Рис. 17) позволяет создать список защищенных сетей, с ресурсами которых пользователю DiSec необходимо взаимодействовать. Список содержит реквизиты подключения к защищенным сетям, необходимые для создания туннелей с Серверами VPN.

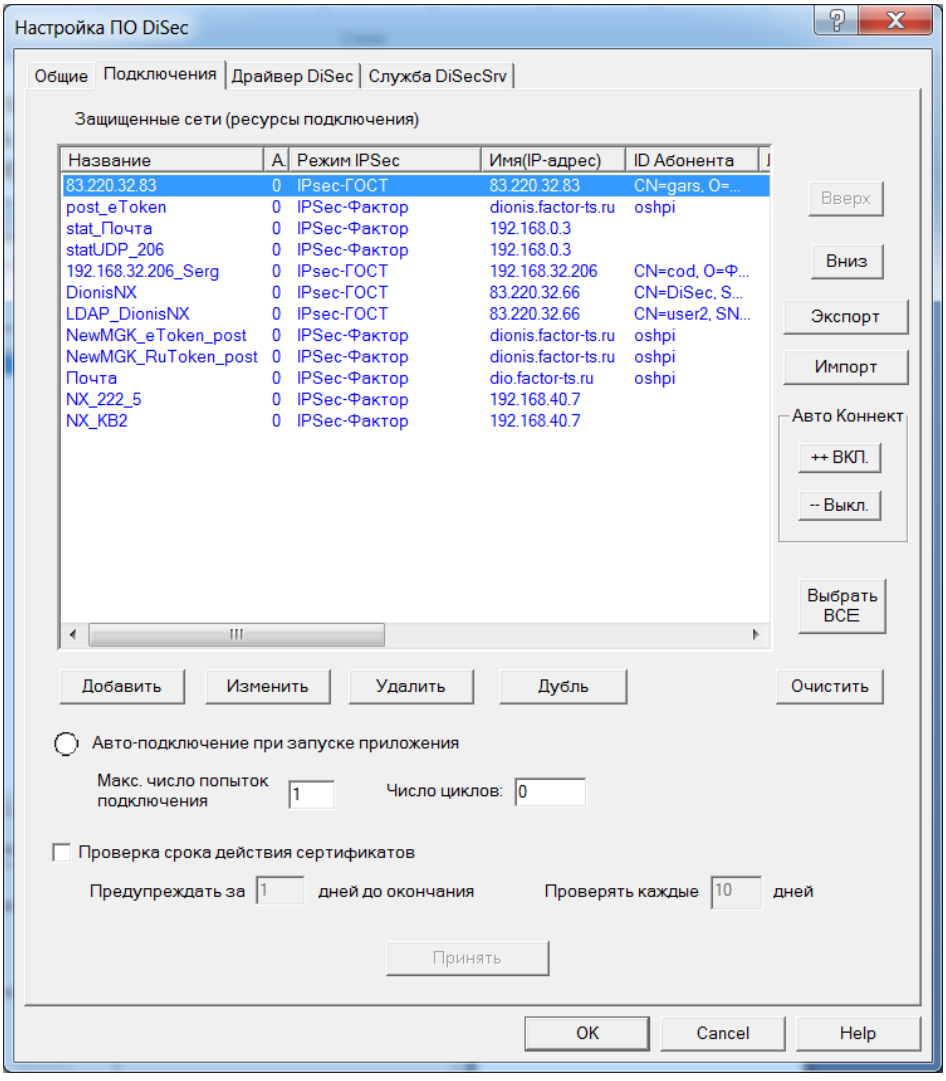


Рис. 17

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 – раздел 6.3, с. 38.

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

- кнопка **Добавить** позволяет внести в список новый ресурс; после ее нажатия открывается окно **Реквизиты подключения** (см. п. 6.3, стр. 38), и пользователю предоставляется возможность ввести все необходимые данные; ресурс будет добавлен в конец списка;
- 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 то же окно **Реквизиты подключения** с установленными ранее значениями реквизитов, и пользователю предоставляется возможность изменить данные;
- нажатие кнопки **Удалить** без дополнительного запроса удаляет выделенный курсором ресурс.
- сдублировать подключение кнопкой **Дубль**. При этом новому ресурсу присваивается новое имя, которое можно изменить отредактировав реквизиты (кнопка **Изменить**).
- удалить ВСЕ подключения кнопкой **Очистить.**

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.

- назначение для каждого ресурса авто-подключения при запуске приложения (**Авто-коннект**; **++Вкл.**; **--Выкл.**)

- 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*.

Экспорт

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

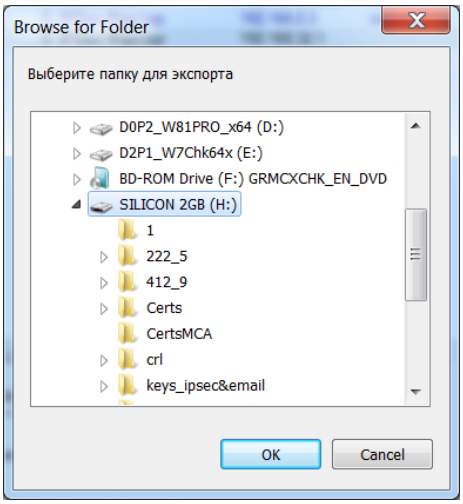


Рис. 18

После выбора директории на любом носителе и нажатия кнопки OK выводится сообщение, приведенное на Рис. 19.

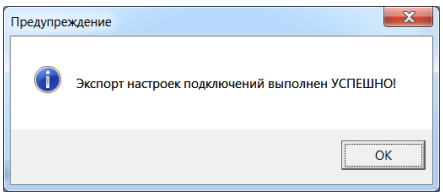


Рис. 19

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

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

Импорт

При нажатии кнопки **Импорт** открывается окно для выбора файла импортируемого ресурса:

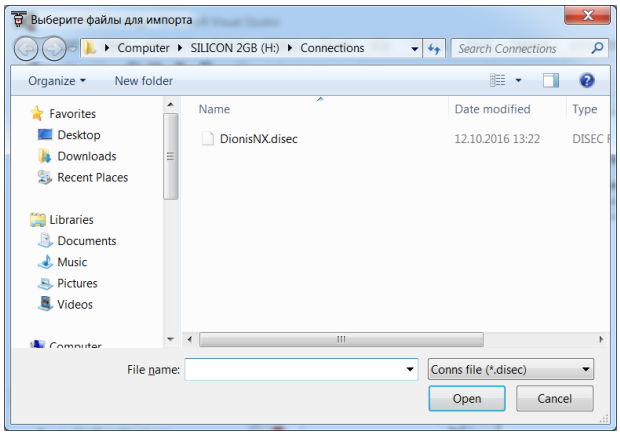


Рис. 20

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.

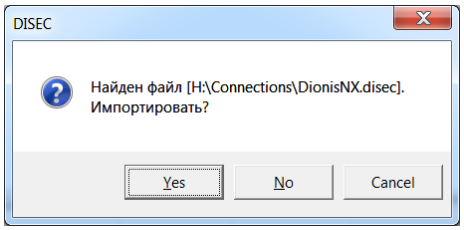


Рис. 21

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

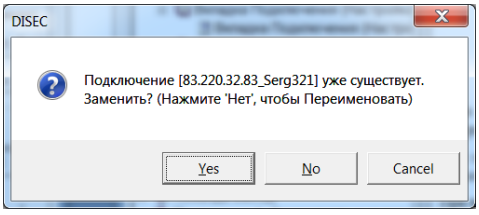


Рис. 22

При нажатии "*No*" ("Нет") будет выполнен импорт настроек из выбранного файла, новое подключение будет переименовано (добавится суффикс ".1") и будет выдано сообщение:

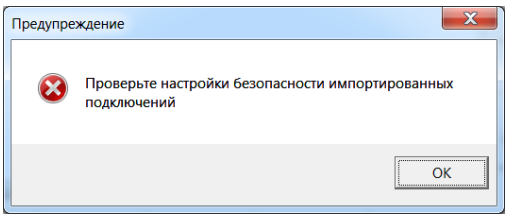


Рис. 23

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

После окончания будет предложено проверить настройки безопасности.

Авто-подключение при запуске приложения

Индикатор **Авто-подключение при запуске приложения** отображает настройку авто-подключения и имеет зеленую окраску, если хотя бы одного ресурса задано свойство ***Авто-коннект,*** равное 1.

Макс. число попыток 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).

Проверка срока действия сертификатов

Флажок **Проверка срока действия сертификатов** позволяет выполнять периодический контроль валидности сертификатов (как локальных, так и удаленных - сертификатов оппонентов) для ВСЕХ ресурсов с режимом IPSEC-ГОСТ и превентивно извещать об истечении срока годности. Соответствующее сообщение будет выведено в окно Диагностика DiSec и в журнале. Стандартное значение - включено.

Предупреждать за ... дней до окончания

Числовой параметр **Предупреждать за** позволяет назначить время (в днях) до окончания действия сертификата для вывода диагностического сообщения об этом факте (в окно Дианостика DiSec и журнал Disec.log, а также в системный журнал WINDOWS).

Проверять каждые ... дней

Числовой параметр **Проверять каждые** позволяет назначить интервал (в днях) проверки сертификатов.

6.3 Реквизиты подключения

При добавлении нового подключения к списку и при изменении реквизитов созданного ранее подключения выводится окно **Реквизиты подключения**. Для удобства параметры распределены по нескольким вкладкам. Содержание вкладок **Параметры** и **Безопасность** зависит от выбранного режима организации туннеля – IPSEC-ФАКТОР или IPSEC-ГОСТ, а также от типа туннеля - динамического или статического.

Открывается окно на вкладке **Общие**.

6.3.1 Вкладка Общие (Реквизиты подключения)

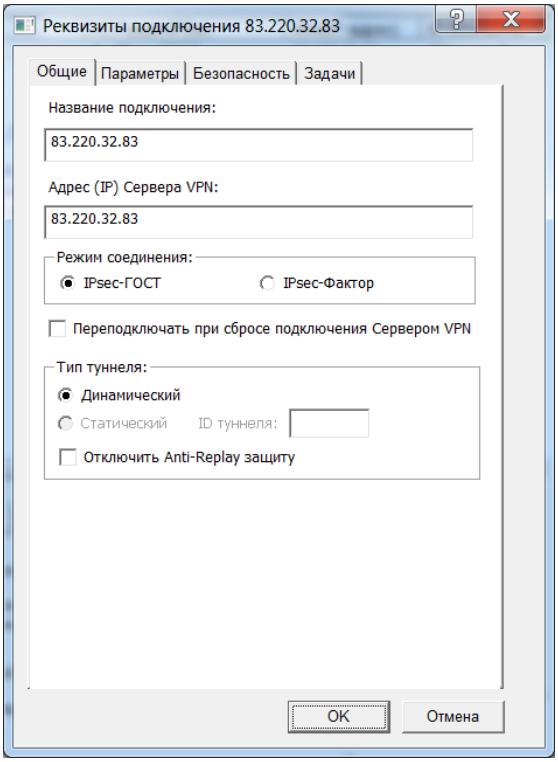


Рис. 24

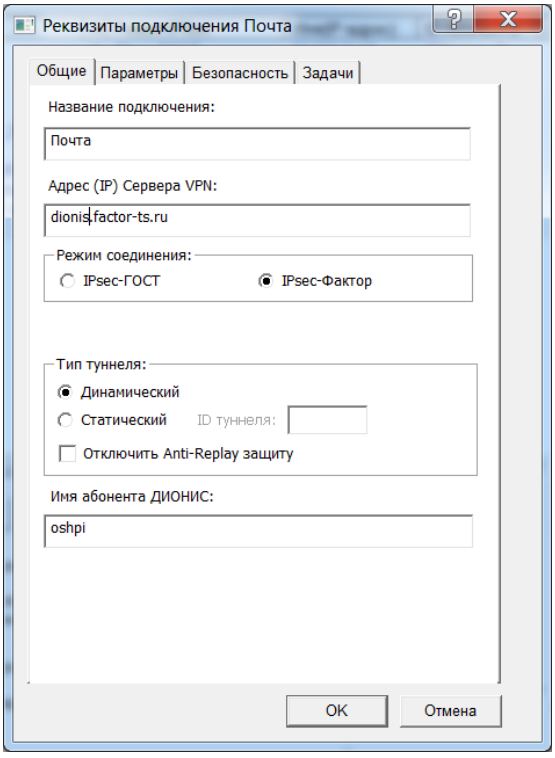


Рис. 25

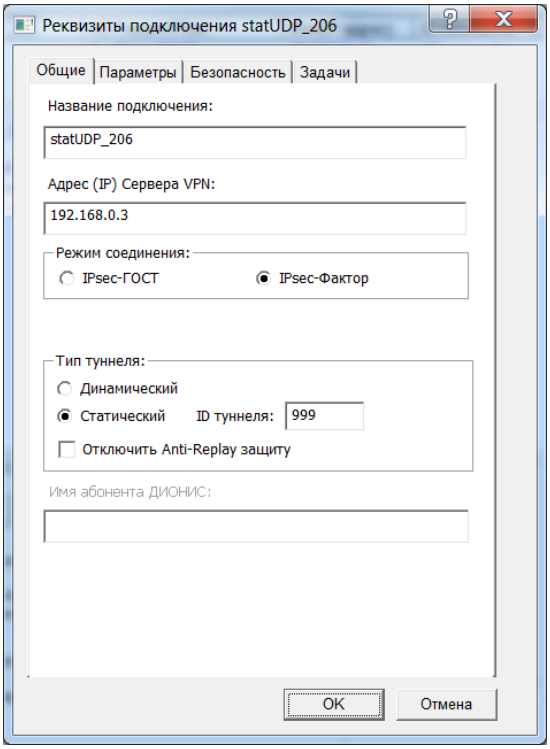


Рис. 26

На вкладке **Общие** назначаются основные параметры, которые определяют содержание остальных вкладок.

Название подключения

Значением поля **Название подключения** является произвольная последовательность букв и цифр, идентифицирующая данный ресурс подключения для конкретной защищенной сети; мы рекомендуем присваивать понятные названия, которые позволят легко отличить данный объект от

других при выборе ресурса из списка во время выполнения команды **Подключиться** (раздел 7.1, с. 84).

Адрес (IP) Сервера VPN

В поле **Адрес (IP) Сервера VPN** следует ввести IP-адрес Сервера VPN или его доменное имя.

Режим соединения

С помощью переключателя надо указать режим организации туннеля – IPSEC-ФАКТОР или IPSEC-ГОСТ.

Имя абонента ДИОНИС

Поле **Имя абонента ДИОНИС** активно только для режима IPSEC-ФАКТОР и динамического туннеля. В поле необходимо ввести имя абонента Сервера VPN (КМ ДИОНИС), для которого при подключении будет создаваться туннель. Имя должно быть заранее получено от администратора КМ ДИОНИС.

Тип туннеля

С помощью переключателя надо указать тип туннеля - ***динамический*** или ***статический***, и для статического туннеля указать его идентификатор – **ID туннеля** (должен быть заранее получен от администратора Сервера VPN).

Отключить Anti-Replay защиту

Флажок Отключить Anti-Replay защиту позволяет отключить эту возможность для настраиваемого подключения, даже если глобально данная проверка включена (п. 6.4.1.2, стр. 70).

6.3.2 Вкладка Параметры для режима IPSEC-ФАКТОР

Содержание вкладки Параметры несколько отличается для динамического (см. 6.3.2.1) и статического туннеля (см. 6.3.2.2).

6.3.2.1 Вкладка Параметры для режима IPSEC-ФАКТОР динамического туннеля

Для режима IPSEC-ФАКТОР на вкладке (Рис. 27) размещены группы доступных для изменения параметров:

- **Проверка входящих пакетов**,
- **Проверка жизнеспособности туннеля (TnlPing)**,
- **Интеграция в защищенную сеть**.

Проверка входящих пакетов

Группа параметров **Проверка входящих пакетов** содержит элементы, позволяющие дополнительно "смягчить" стандартную проверку входящих через туннель пакетов, которая состоит в том, что адрес назначения должен совпадать с адресом интерфейса компьютера пользователя DiSec с учетом подмены адреса в соответствии с параметрами **Интеграция в защищенную сеть.** Это сделано для повышения защищенности от сетевых атак.

Разрешить мультикаст

Флажок **Разрешить мультикаст** используется для пропускания трафика видеоконференций. При установке этого флажка отключается проверка адреса назначения во входящих расшифрованных IP-пакетах для мультикастных пакетов, для которых этот адрес имеет специфические значения.

Отключить проверку

Флажок **Отключить проверку** позволяет отключить в драйвере проверку адреса назначения во входящих расшифрованных IP-пакетах, который должен совпадать с адресом устройства пользователя DiSec. используется ТОЛЬКО в диагностических целях совместно с записью трафика в Протокол сети, в случае необходимости выявления потери пакетов.

Интеграция в защищенную сеть

Группа параметров **Интеграция в защищенную сеть** содержит параметры удаленной сети, с которой устанавливается туннель. Поля на этой вкладке могут не заполняться, однако для более полной интеграции в удаленную сеть, например, для работы с защищенными ресурсами с использованием доменных имен Интернет, можно указать соответствующие значения. Значения должны быть получены от администратора защищенной сети.

В данной группе параметров указываются значения, которые будут присвоены соответствующим параметрам сетевого интерфейса компьютера пользователя DiSec после установления туннеля к защищенной сети. Это позволяет пользователю DiSec работать с ресурсами защищенной сети, используя доменные имена (сервис DNS).

По желанию может быть задан только **DNS сервер** без указания остальных параметров.

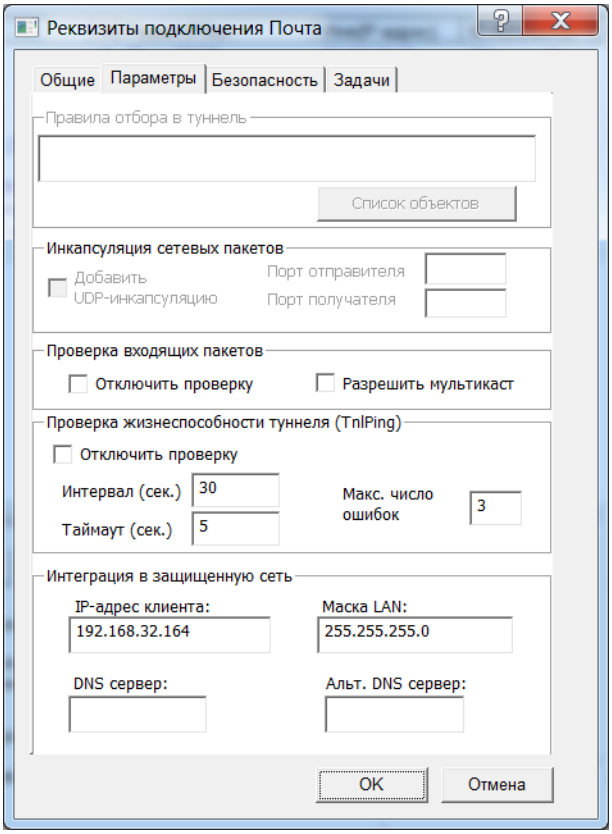


Рис. 27

6.3.2.2 Вкладка Параметры для режима IPSEC-ФАКТОР статического туннеля

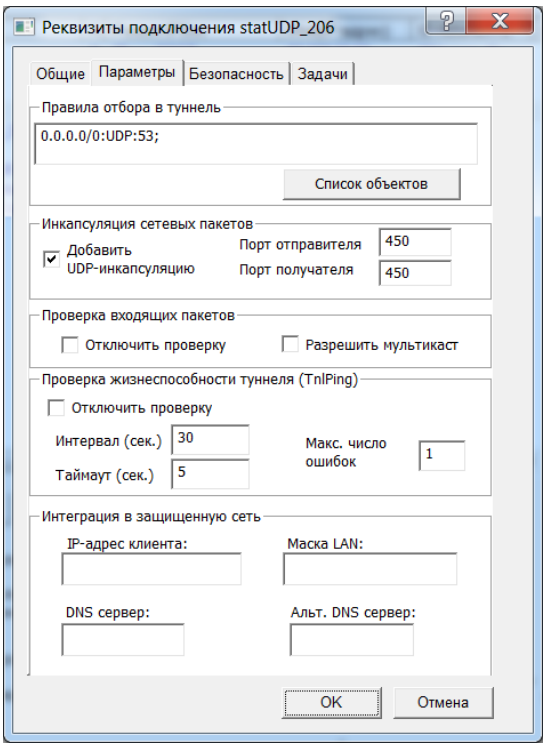


Рис. 28

Вкладка для статического туннеля дополнительно имеет доступные для изменения группы параметров **Правила отбора в туннель** и **Инкапсуляция сетевых пакетов**.

Группа параметров **Инкапсуляция сетевых пакетов** состоит из следующих элементов.

Добавить UDP-инкапсуляцию

Флажок **Добавить UDP-инкапсуляцию** меняет способ туннелирования (инкапсуляции) сетевых пакетов: вместо протокола 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 ***501***. Значения этих полей можно изменить, при этом они должны соответствовать настройкам статического туннеля на Сервере VPN.

Проверка жизнеспособности туннеля (TnlPing)

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

Отключить проверку жизнеспособности туннеля

Флажок **Отключить проверку жизнеспособности туннеля** позволяет выполнить указанное отключение (***не рекомендуется***) и тестовые сообщения проверки жизнеспособности туннеля (Ping-пакеты) не будут посылаться на Сервер VPN.

Интервал(сек.)

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

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.

6.3.3 Вкладка Параметры для режима IPSEC-ГОСТ

Для режима IPSEC-ГОСТ на вкладке **Параметры** (Рис. 29) размещены элементы управления, позволяющие назначать и модифицировать политики согласования криптоалгоритмов и ключевого материала между взаимодействующими сторонами (DiSec и Сервер VPN).

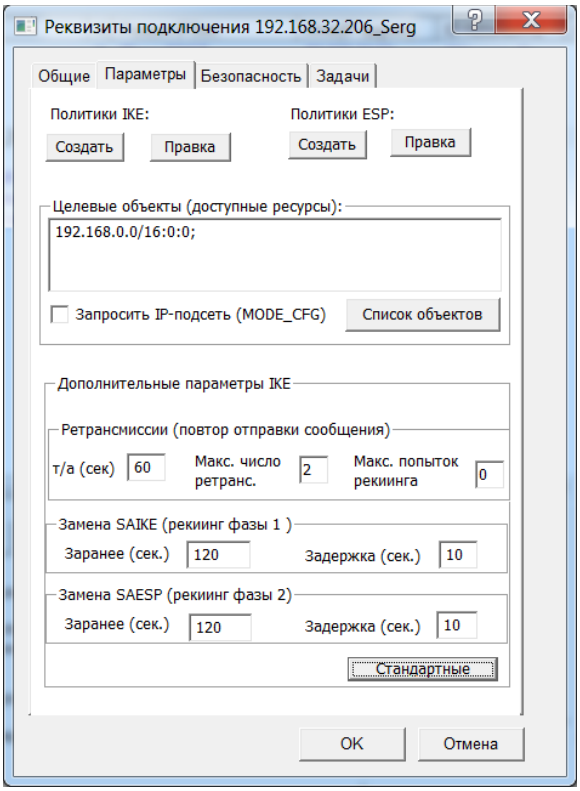


Рис. 29

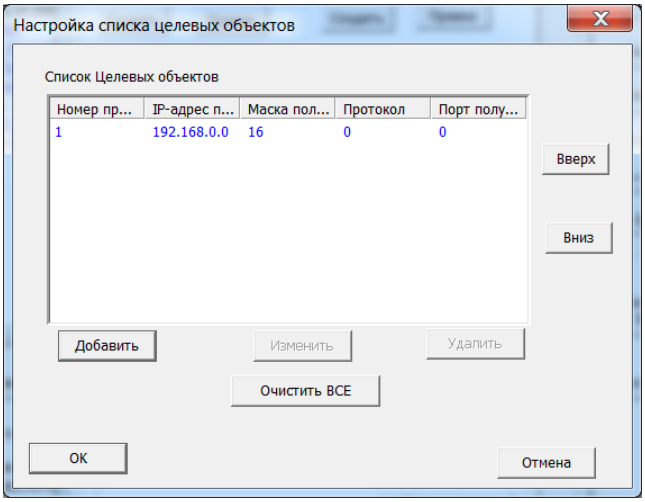


Рис. 30

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 (Рис. 32), и пользователь получает возможность изменять существующую или стандартную политику (создаваемую по клавише **Создать**).

Целевые объекты (доступные ресурсы)

В поле **Целевые объекты (доступные ресурсы)** можно указать ресурсы внутренней сети (защищаемой данным Сервером VPN), к которым получит доступ пользователь DiSec посредством туннеля. При нажатии кнопки **Список объектов** выводится вспомогательное окно для формирования списка элементов и отдельного элемента Целевых объектов (см. п. 6.3.3.3, стр. 48).

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. Данный режим будет работать, только если в настройках политики ESP установлен флажок **Запрос IP-адреса в защищенной сети,** и этот режим соответствует настройкам на сервере VPN.

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. 115). На стороне DiSec одно подключение может содержать весь список объектов.

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 при нажатии кнопки **Стандартные**.

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.

Замена IKE (рекиинг фазы 1)

Подгруппа параметров **Замена IKE (рекиинг фазы 1)** предназначена для указания дополнительных интервалов времени, позволяющих оптимизировать процедуру плановой замены SA IKE в соответствии с параметром **Период смены ключей Ike** (см. 6.3.3.1, стр. 45) Политики IKE.

Заранее Ike(сек.)

Параметр **Заранее (сек.)** определяет более раннее начало процедуры смены ключей фазы 1 (согласования новой SA IKE). На медленном оборудовании согласование SA IKE может занять довольно значительное время, поскольку включает обмен несколькими сообщениями между клиентом DiSec и Сервером VPN. *Стандартное значение* - 120 сек.

Задержка Ike(сек.)

Параметр **Задержка (сек.)** определяет более позднее начало процедуры смены ключей фазы 1 (согласования новой SA IKE). Поскольку обновление SA IKE (фаза 1) и SA ESP (фаза 2) выполняются независимо друг от друга, то бывают моменты, что начало процедуры обновления SA IKE наступает в то время, когда еще не закончена процедура обновления SA ESP. В этом случае процедура обновления SA IKE процедура откладывается на некоторое время, определяемое данным значением. *Стандартное значение* - 10 сек.

Замена ESP (рекиинг фазы 2)

Подгруппа параметров **Замена ESP (рекиинг фазы 2)** предназначена для указания дополнительных интервалов времени, позволяющих оптимизировать процедуру плановой замены SA ESP в соответствии с параметром **Период смены ключей Esp** (см. 6.3.3.2, стр. 47) Политики ESP.

Заранее Esp(сек.)

Параметр **Заранее Esp(сек.)** определяет более раннее начало процедуры смены ключей фазы 2 (согласования новой SA ESP). На медленном оборудовании согласование SA ESP может занять довольно значительное время, поскольку включает обмен несколькими сообщениями между клиентом DiSec и Сервером VPN. *Стандартное значение* - 120 сек.

Задержка Esp(сек.)

Параметр **Задержка Esp(сек.)** определяет более позднее начало процедуры смены ключей фазы 2 (согласования новой SA ESP). Поскольку обновление SA IKE (фаза 1) и SA ESP (фаза 2) выполняются независимо друг от друга, то бывают моменты, что начало процедуры обновления SA ESP наступает в то время, когда еще не закончена процедура обновления SA IKE. В этом случае процедура обновления

SA ESP откладывается на некоторое время, определяемое данным значением. *Стандартное значение* - 10 сек.

6.3.3.1 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. 31).

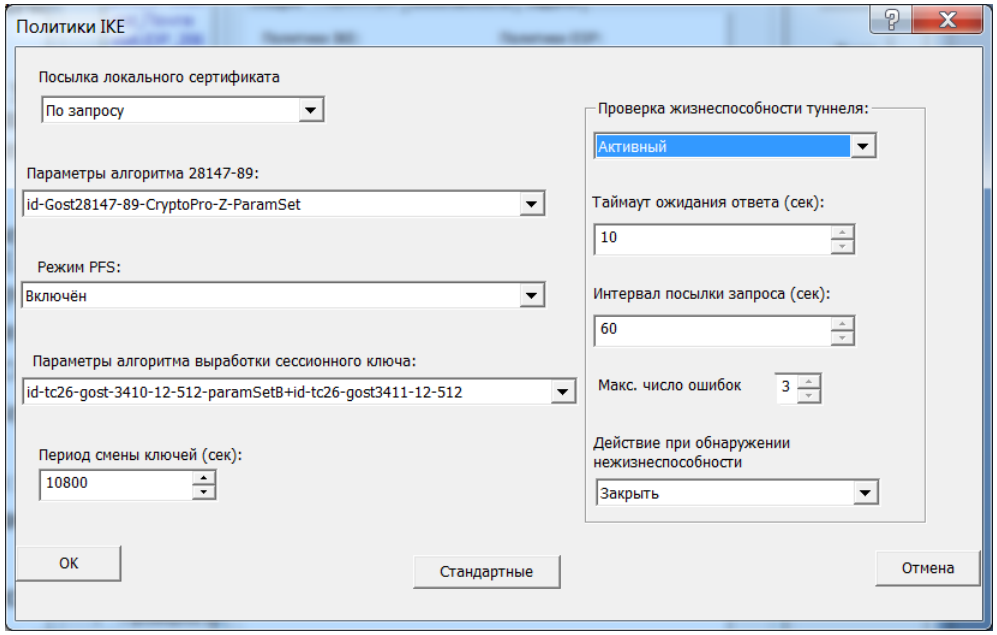


Рис. 31

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*».

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 - *id-Gost28147-89-CryptoPro-Z-ParamSet*. 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

Значение параметра должно соответствовать значению на Сервере VPN (см. раздел 14, п. 19, с. 116).

Примечание. Символ «*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 (см раздел 14, п. 21, с. 116).

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-GostR3410-94
id-GostR3410-2001-CryptoPro-XchB-ParamSet+id-GostR3410-94
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 (см раздел 14, п. 19, с. 116).

Период смены ключей Ike(сек)

Значение параметра определяет *время жизни* установленной фазы 1. По окончании указанного периода (с учетом параметра **Заранее Ike(сек)** в п. 6.3.3) инициируется выполнение фазы 1 протокола IKE для выработки новых ключей шифрования. Стандартное значение для времени жизни 1-ой фазы – *10800 сек*.

Проверка жизнеспособности туннеля

Параметр предназначен для выполнения проверки жизнеспособности туннеля посредством периодической посылки запросов - сообщений протокола IKE специального формата - и контроля поступления ответных сообщений на запрос. Возможные значения параметра:

- *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*.

Действия над туннелем, если собеседник не отвечает

Возможные значения:

- *Закрыть* (значение по умолчанию) – DiSec закрывает туннель, если Сервер VPN не отвечает на запросы.
- *Инициировать заново* – если Сервер VPN не отвечает на запросы, DiSec начинает процедуру установки новой SA IKE.

Интервал посылки запроса (сек)

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

Таймаут ответа Сервера на запрос (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.*

Макс. 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 (значения по умолчанию) параметров протокола IKE.

6.3.3.2 Настройка политики ESP

Политика ESP (Рис. 29) определяет правила формирования ключей шифрования и алгоритмы шифрования сетевых пакетов, передаваемых по туннелю при использовании протокола ESP (Рис. 32).

Режим инкапсуляции трафика

Параметр определяет вариант настройки протокола ESP, возможные значения:

- *Туннель* – стандартное значение;
- *Транспортный*.

Значение параметра должно совпадать с соответствующим значением на Сервере VPN (см раздел 14, п. 8, с. 115).

Преобразование ESP

Поле определяет два параметра, значения которых должны совпадать с соответствующими значениями на Сервере VPN (см раздел 14, п. 20, с 116):

- тип преобразования ESP, стандартное значение - *GOST-4M-IMIT;*
- узел замены для алгоритма ГОСТ 28147-89, стандартное значение - *id-Gost28147-89-CryptoPro-B-ParamSet.*

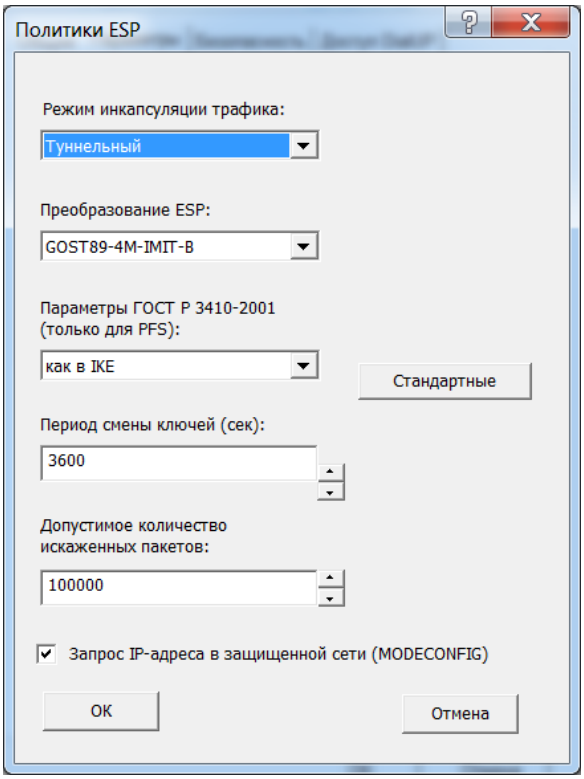


Рис. 32

Параметры ГОСТ Р 3410-2001 (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 6.3.3.1, с. 45). Если потребуется другое значение, его можно выбрать из выпадающего списка. Значение параметра должно совпадать с соответствующим значением на Сервере VPN (см. раздел 14, п. 22, с. 116).

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 совпадать с соответствующим значением на Сервере VPN (см раздел 14, п. 24, с. 116).

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 (см. Рис. 113, Рис. 114).

Для просмотра сообщений об ошибках, выданных драйвером DiSec, можно воспользоваться системными средствами WINDOWS либо воспользоваться командой Протокол сети Главного меню DiSec (см. п. 10.3, стр. 104).

Запрос IP-адреса в защищенной сети (MODECONFIG)

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 виртуальный адрес из диапазона виртуальных адресов защищаемой сети. Если на Сервере VPN указаны адреса внутренних DNS-серверов, то их адреса также будут переданы пользователю DiSec.

В некоторых особых случаях флажок может быть снят.

Напомним, что виртуальный IP-адрес мобильного клиента (или пул адресов) задается в настройках на Сервере VPN (см. раздел 14, с. 115).

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

6.3.3.3 Настройка Целевых объектов

Список целевых объектов (Рис. 29) 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 может быть указан либо в числовом виде, либо в символьном (***tcp***, ***udp***, ***icmp***, ***any***).
- порт протокола TCP или UDP.

Пример списка из двух объектов: ***10.1.1.0/24;10.1.2.10:tcp:80***

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

1. Если поле под заголовком **Целевые объекты (доступные ресурсы)** (Рис. 29) оставить незаполненным, 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*», означающее, что туннель действует для ВСЕХ протоколов и портов.

Кнопка **Список объектов** (Рис. 29) предоставляет более удобный способ задания списка целевых объектов. После ее нажатия открывается окно **Настройка списка целевых объектов (**Рис. 33**)**, которое позволяет создать, изменить, удалить отдельный объект, а также изменить последовательность элементов списка.

При нажатии кнопки **Добавить** (или **Изменить**) открывается окно **Целевой объект** (Рис. 34), которое позволяет задать (отредактировать) все параметры целевого объекта, к которому необходимо получить доступ через туннель, – **IP-адрес**, маску (**Зн.бит**), **Протокол** и **Порт TCP/UDP**.

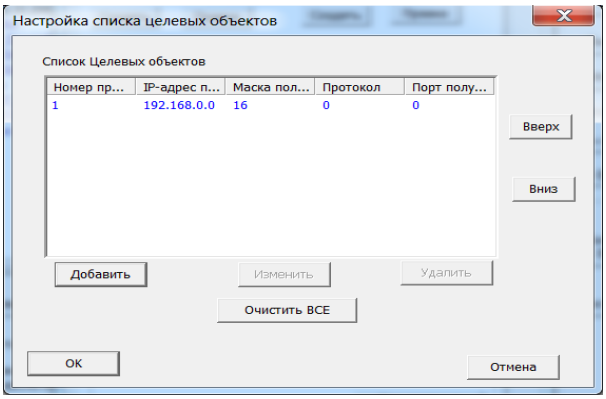


Рис. 33

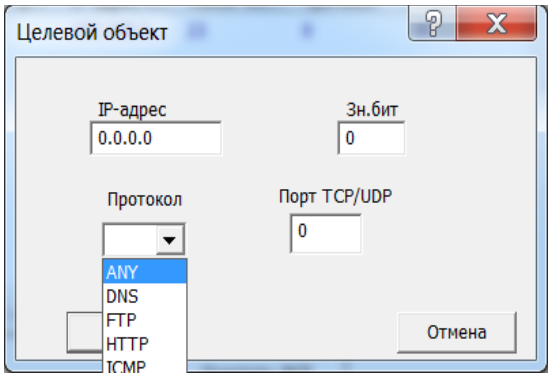


Рис. 34

6.3.4 Вкладка Безопасность для режима IPSEC-ФАКТОР

С помощью переключателя под заголовком **Ключевой носитель** (Рис. 35) следует указать тип ключевого носителя с персональной ключевой информацией пользователя DiSec, необходимой для организации туннеля с Сервером VPN (см. раздел 2.4.1, с. 14).

Параметры ключей

Группа параметров **Параметры ключей** содержит всю необходимую информацию о симметричных ключах, используемых при работе в режиме IPSEC-ФАКТОР.

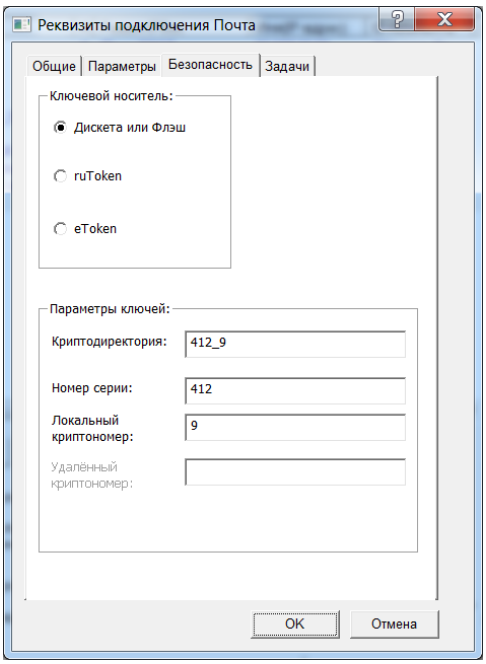


Рис. 35

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 личного туннеля 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 при создании статического туннеля. В поле надо занести криптографический номер ключа удаленного конца туннеля. Значение должно быть получено от администратора Сервера VPN (см. раздел 3.4.1, с. 17).

6.3.5 Вкладка Безопасность для режима IPSEC-ГОСТ

Для режима IPSEC-ГОСТ вкладка **Безопасность** имеет вид, представленный на Рис. 36.

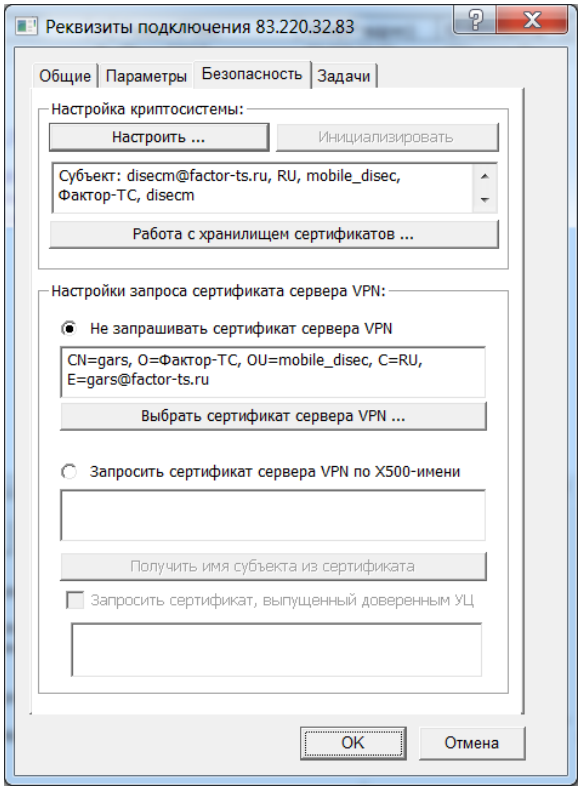


Рис. 36

6.3.5.1 Настройка криптосистемы

Начинать настройку криптосистемы DiSec следует с нажатия кнопки **Настроить** под заголовком **Настройка криптосистемы** (Рис. 36). В дальнейшем с помощью этой кнопки можно внести изменения в параметры настройки.

После нажатия кнопки **Настроить** на экран будет выведено окно **Установки криптосистемы** (Рис. 37).

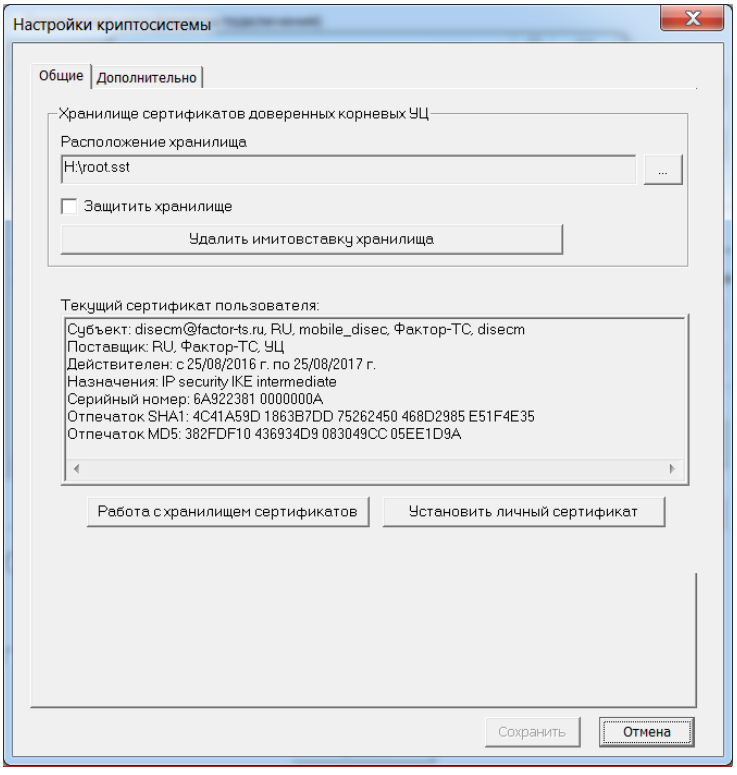


Рис. 37

При начальной настройке в окне заполнено только одно поле под заголовком **Расположение хранилища**. В это поле выводится имя файла (с указанием пути), в котором будет располагаться хранилище **Доверенные УЦ**, предназначенное для хранения сертификатов корневых доверенных удостоверяющих центров. Стандартное значение поля - файл в персональной директории пользователя:

<системный диск>:\Users\<имя пользователя>\AppData\Roaming\Factor-TS\DioNIS Security\RSST\root.sst. Если предполагается разместить файл **root.sst** в другом месте, то надо нажать кнопку **...** (справа от имени), получить окно обзора папок на всех носителях, и выбрать нужную. Имя файла изменить нельзя.

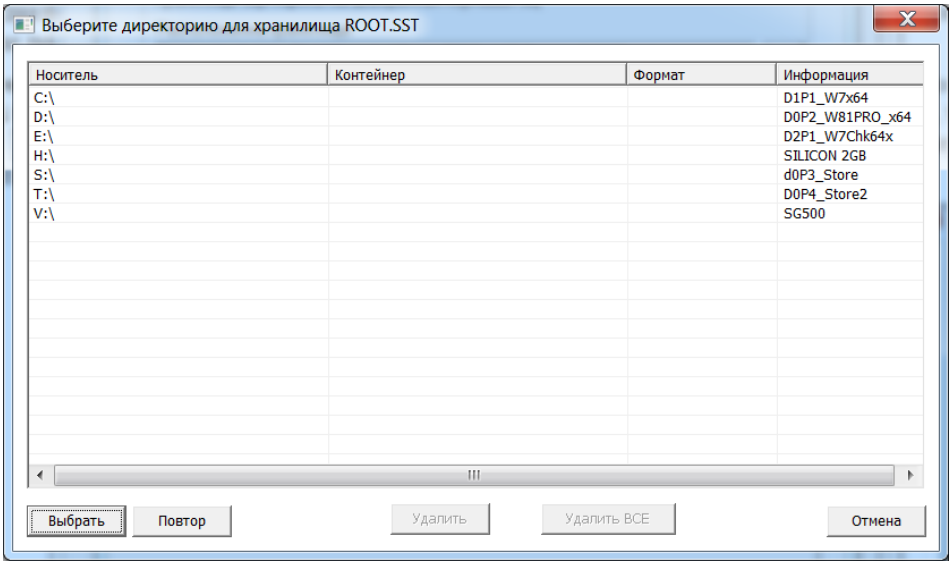


Рис. 38

Можно перейти в поддиректорию на любом диске и нажать кнопку **Выбрать**.

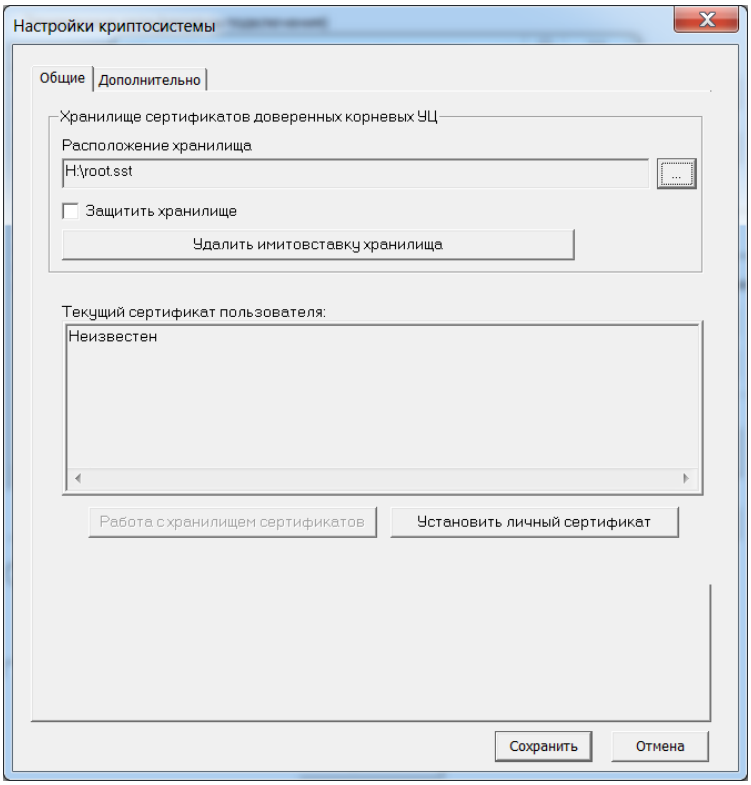


Рис. 39

Настройка криптосистемы обеспечивает ввод в систему закрытого ключа пользователя, создание необходимых хранилищ, занесение личного сертификата пользователя в локальное хранилище сертификатов пользователя

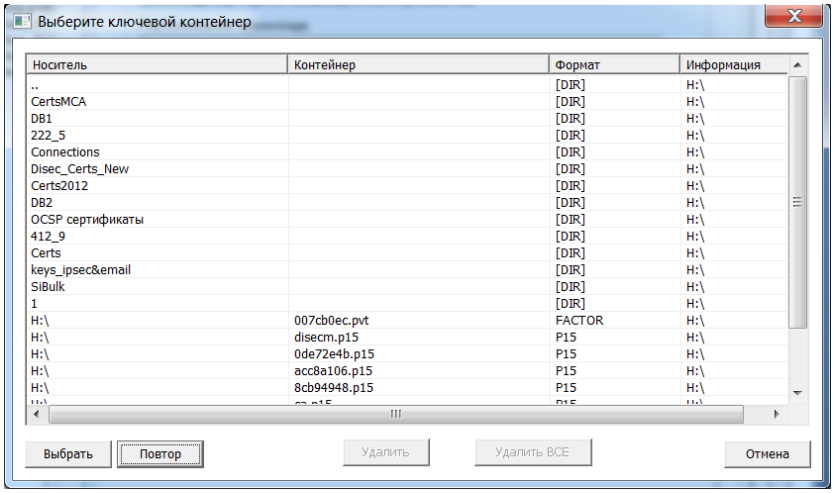
DiSec и назначение этого сертификата текущим, а также занесение в соответствующие хранилища всех необходимых сертификатов УЦ и списков отозванных сертификатов (СОС).

Начальная настройка криптосистемы выполняется следующей последовательностью действий.

> *Примечание*. Пока не будет выполнена инициализация криптосистемы, при переходах от одной операции к другой DiSec будет выводить на экран окно с сообщением-предупреждением о том, что **Не удалось инициализировать криптосистему**; в некоторых случаях будет изложена причина. Окно надо закрывать и продолжать настройку.

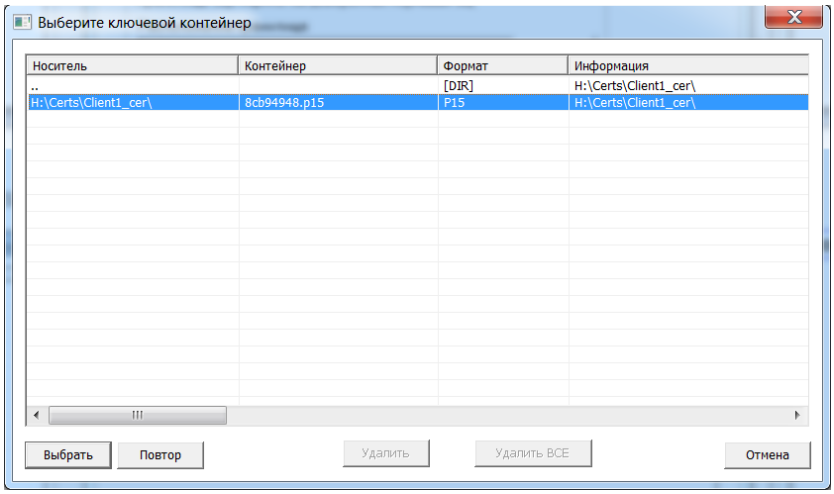
1. Вставить ключевой носитель в считывающее устройство или в порт **USB** и в окне **Установки криптосистемы** (Рис. 37) нажать кнопку **Установить личный сертификат**.

   На экран будет выведено окно **Выберите ключевой контейнер** (Рис. 41), содержащее список съемных носителей, а для PKCS11-токенов список контейнеров.



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

Рис. 40



Продолжая переходы по поддиректориям, следует выбрать нужный контейнер.

Рис. 41

Если считывающее устройство окажется не готовым или формат носителя будет некорректным, то в списке не окажется нужного контейнера. В этом случае надо исправить ошибку и нажать кнопку **Повтор**.

В списке носителей надо выделить строчку с нужным контейнером (т.е. с тем контейнером, который содержит закрытый ключ пользователя DiSec) и нажать кнопку **Выбрать**. Если информация на носителе закрыта паролем, система потребует ввести этот пароль.

2. Программа DiSec проверит наличие хранилища доверенных корневых УЦ в указанном месте (см. выше – расположение файла **root.sst**). Если хранилища не окажется, система предложит его создать:

   Затем система приступит к созданию ссылки на личный сертификат. Будет выдано сообщение:

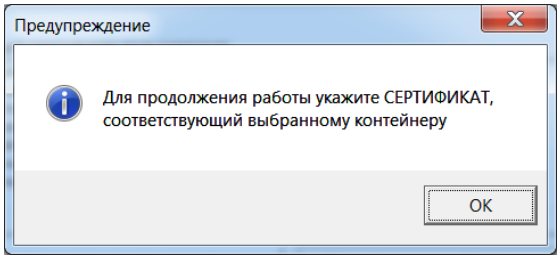


Рис. 42

После нажатия кнопки **OK,** если в директории контейнера найден один или несколько сертификатов на экран будет выведено сообщение:

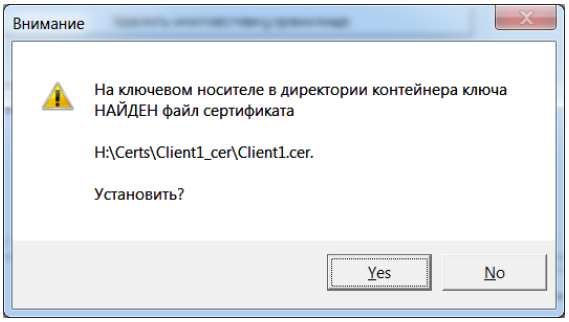


Рис. 43

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

При отрицательном ответе будут последовательно предложены для рассмотрения все сертификаты из текущей директории, а затем предложен выбор самостоятельного поиска сертификата.

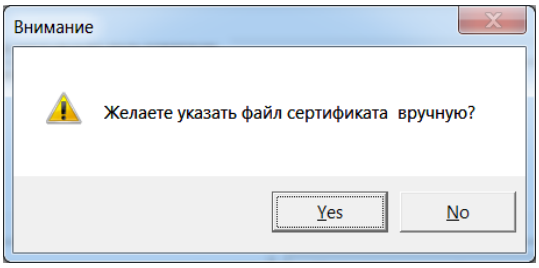


Рис. 44

При положительном ответе на данный запрос будет выведено окно **Выберите сертификат**, позволяющее выбрать файл с нужным сертификатом (имена файлов с расширением **cer**).

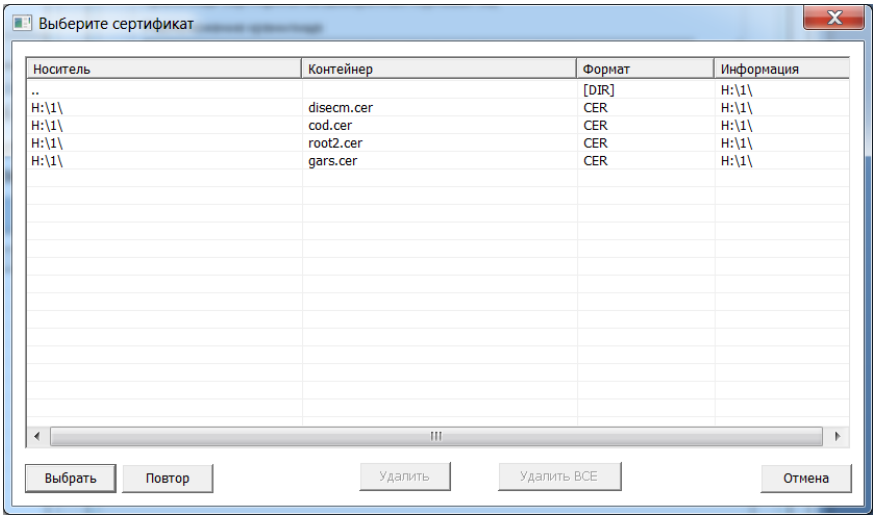


Рис. 45

В этом окне надо выбрать файл, содержащий нужный сертификат, и нажать кнопку **Выбрать**.

Система выведет на экран информацию из выбранного сертификата, которая позволит пользователю идентифицировать сертификат (Рис. 46), и предложит назначить его текущим.

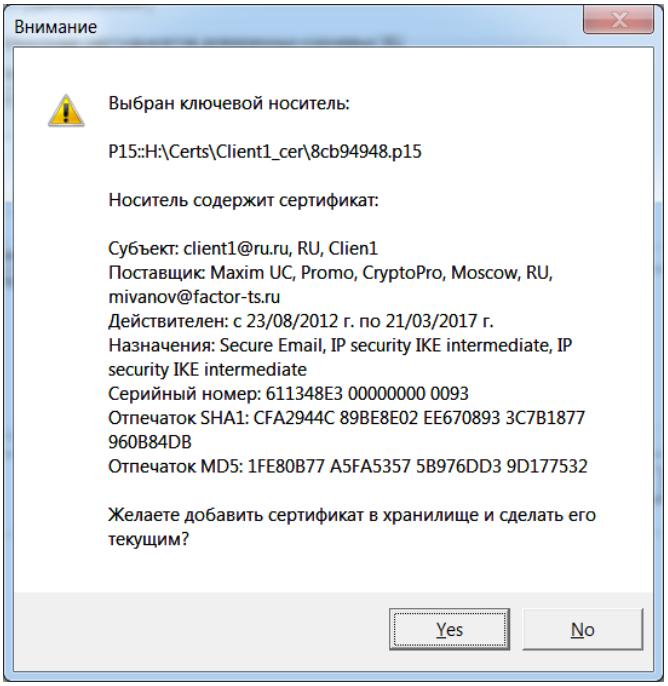


Рис. 46

По нажатию кнопки **ДА** будет сформирована необходимая ссылка, личный сертификат пользователя будет добавлен в локальное хранилище сертификатов пользователя DiSec и назначен текущим (нажатием кнопки **НЕТ** операцию добавления личного сертификата в хранилище можно прервать). Его можно будет увидеть при работе с локальным хранилищем на вкладке **Сертификаты.**

Созданная ссылка записывается в файл, который помещается на ключевой носитель:

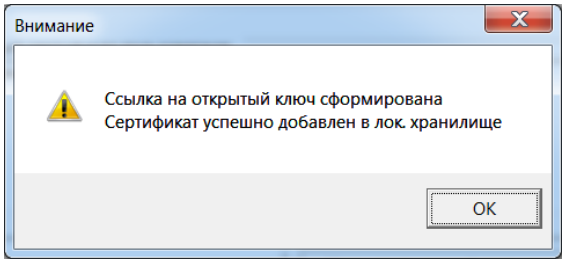


Рис. 47

3. DiSec проверит наличие файла с сертификатом доверенного корневого УЦ (и цепочкой сертификатов доверенных УЦ) на ключевом носителе и предложит добавить цепочку в хранилище:

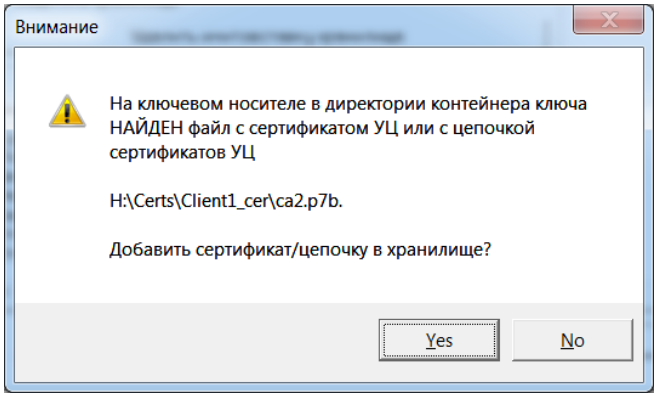


Рис. 48

Процедура выбора сертификата УЦ и\или файла с цепочкой сертификатов УЦ аналогична выбору сертификата пользователя, т.е. поочередно будут предложены все элементы с расширением “**p7b**” и “**cer**” из текущей директории ключевого контейнера, а при отказе предложен выбор вручную.

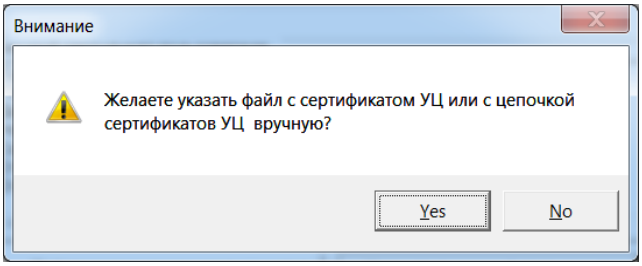


Рис. 49

При положительном ответе будет предложен поиск по съемным носителям.

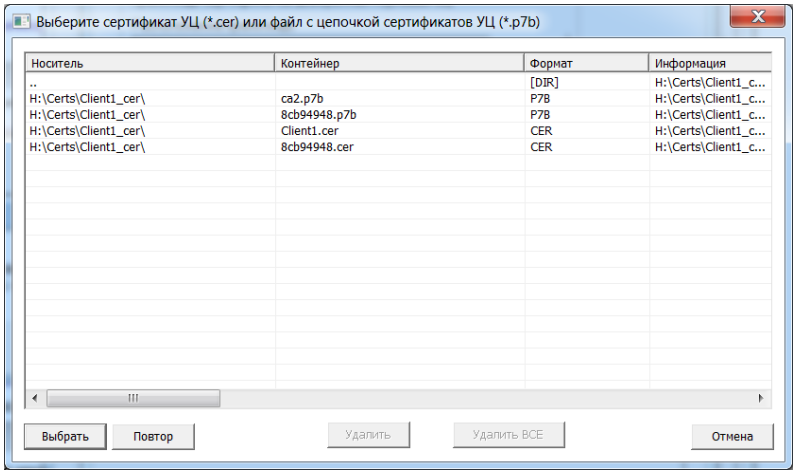


Рис. 50

Пользователь может выбрать либо отдельный сертификат УЦ (файл с расширением "**cer**", либо контейнер с цепочкой сертификатов УЦ (файл с расширением "**p7b**").

После выбора элемента выводится предупреждение:

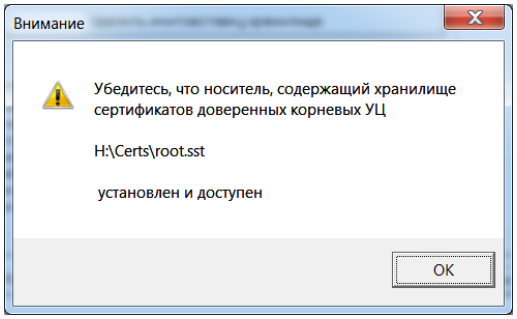


Рис. 51

После этого система выведет на экран информацию из корневого сертификата, которая позволит пользователю идентифицировать сертификат (Рис. 52), и предложит добавить его в хранилище (или заменить, если сертификат уже находится в хранилище).

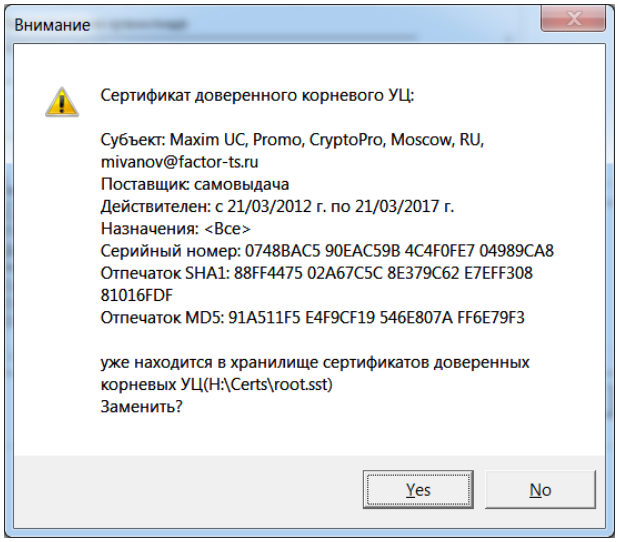


Рис. 52

По нажатию кнопки **Да** сертификат будет добавлен в локальное хранилище пользователя и в корневое хранилище доверенных сертификатов. Его можно будет увидеть при работе с локальным хранилищем на вкладке **Сертификаты** и **Доверенные УЦ.**

Если был выбран контейнер с цепочкой сертификатов УЦ, то в этом контейнере может находиться один или несколько файлов со списками отзыва. В этом случае будет выдан запрос на добавление их в хранилище.

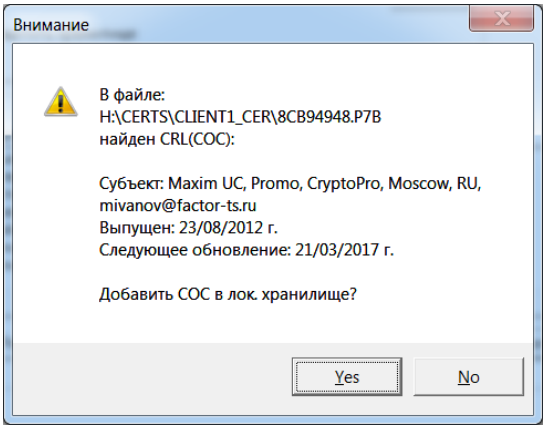


Рис. 53

4. DiSec проверит наличие файла со списком отозванных сертификатов (COC) на ключевом носителе (файл с расширением **crl**) в директории ключевого контейнера и предложит добавить его в хранилище:

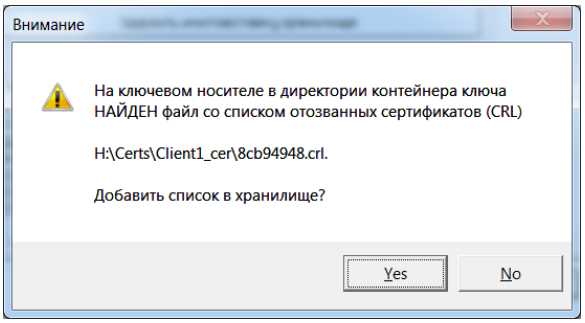


Рис. 54

После нажатия кнопки **Да** файл будет добавлен локальное хранилище пользователя DiSec. Его можно будет увидеть при работе с локальным хранилищем на вкладке **Списки отзыва**.

5. После этого будет выведено информационное сообщение

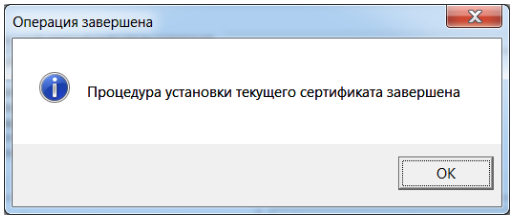


Рис. 55

6. После того как будут выполнены все настройки, надо в окне **Установки криптосистемы** (Рис. 37) нажать кнопку **Сохранить**. Система выдаст предупреждение (Рис. 56):

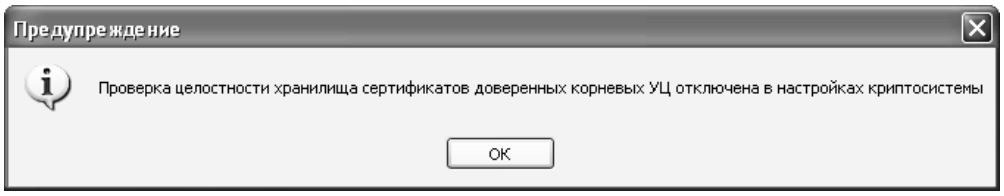


Рис. 56

После нажатия кнопки ОК DiSec выполнит инициализацию криптосистемы и вернется на вкладку **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**.

7. После успешной инициализации рекомендуется снова зайти в настройку криптосистемы и выполнить защиту хранилища сертификатов доверенных корневых УЦ.

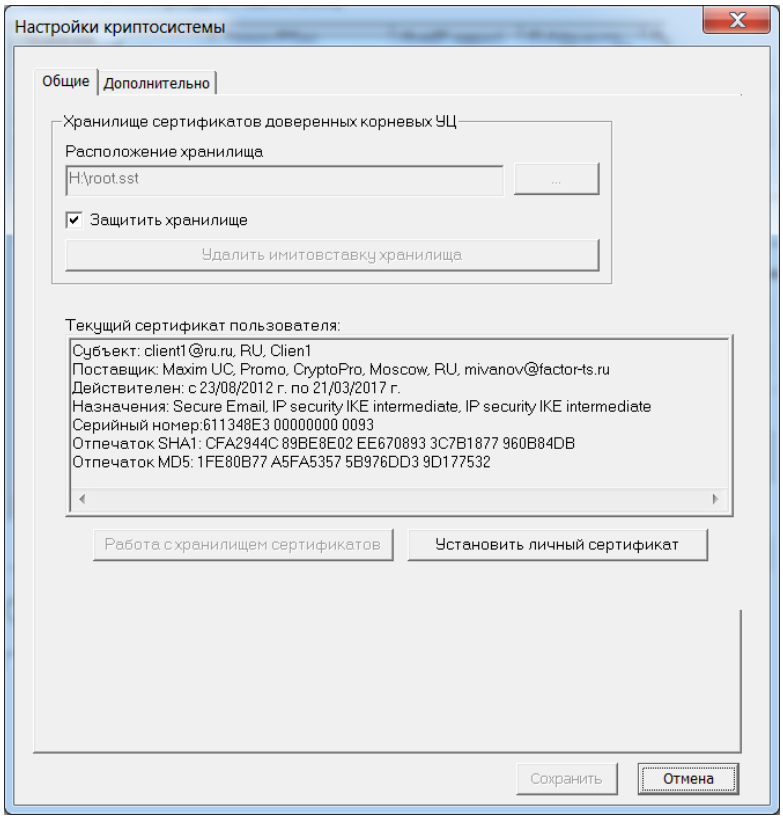


Рис. 57

Установить флажок **Защитить хранилище** и сохранить настройки.

> *Примечание*. Необходимо иметь в виду, что в соответствии с требованиями безопасности при выборе расположения для корневого хранилища на несъемном носителе оно ОБЯЗАТЕЛЬНО должно быть защищено имитовставкой.

6.3.5.2 Настройка дополнительных параметров контроля сертификата

В окне **Настройки криптосистемы** имеется возможность настраивания параметров автоматического обновления списка отзыва (**CRL**) локального сертификата пользователя DiSec, используемого в данном Подключении, либо его проверки по протоколу **OCSP (Online Certificate Status Protocol**).

Автоматическое обновление **CRL** и\или проверка по протоколу **OCSP** будет выполняться каждый раз при инициализации криптосистемы для данного пользователя (сертификата), а также при принудительной команде проверки текущего сертификата. настройка выполняется на вкладке **CRL и OCSP.**

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

Протокол OCSP работает следующим образом: DiSec посылает запрос серверу, адрес (URL) которого указан в настройках для получения информации о X.509-сертификате. В ответ он получает OCSP ответ, один из следующих вариантов:

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 подтвердить (или поставить под сомнение) возможность использования данного сертификата.

Протокол OCSP стремительно ускорил процесс получения информации о X.509-сертификатах и таким образом стал предпочтительным инструментом проверки их статуса в режиме реального времени.

Вкладка CRL и OCSP

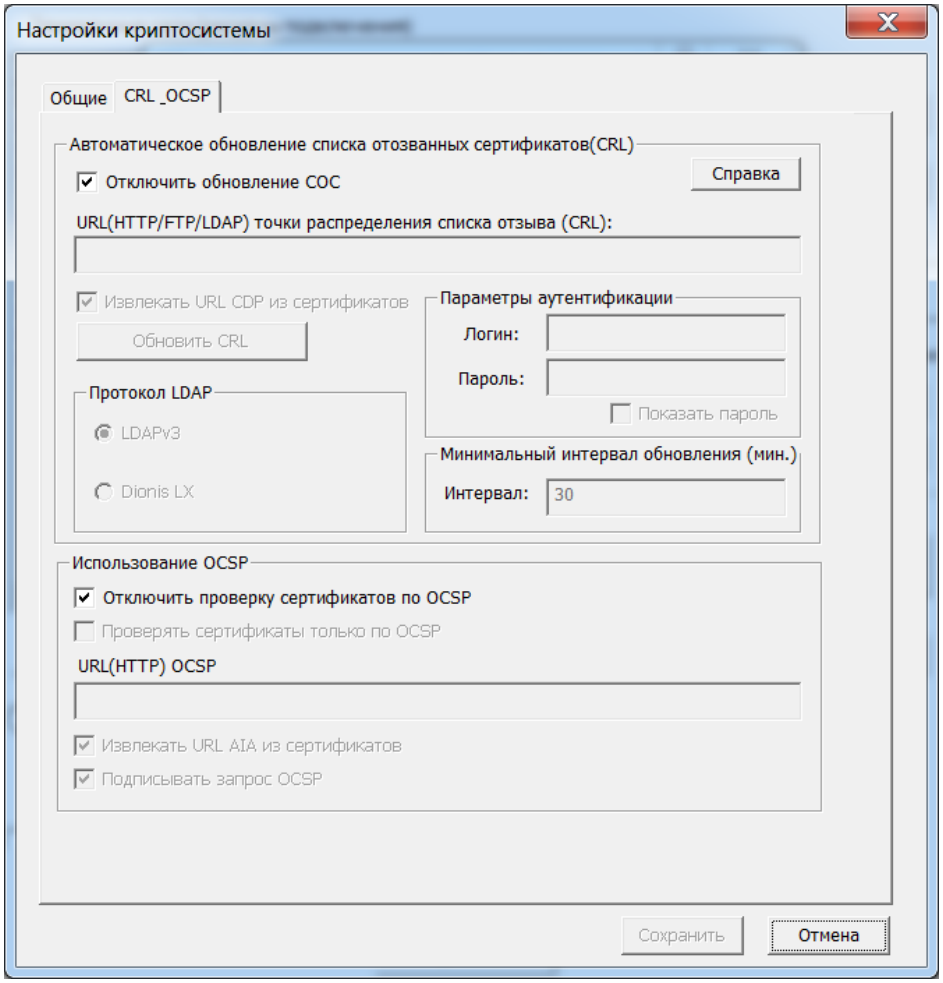


Рис. 58

На вкладке **CRL и OCSP** можно настроить автоматическое обновление списка отзыва и проверку статусов сертификатов по протоколу OCSP.

Обе возможности позволяют повысить эффективность проверки статуса сертификатов, обеспечивая использование во время проверки сертификата (построения Цепочки Доверия) актуального СОС (CRL), получаемого с соответствующего сервера. Адреса для обоих вариантов задаются при помощи **URL**-адресов (***Uniform Resource Locator*** - унифицированный указатель информационного ресурса).

Автоматическое обновление списков отзыва позволяет загрузить с сервера LDAP и поместить в локальное хранилище сертификатов пользователя имеющийся СОС (CRL).

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

Опции могут быть включены одновременно, при этом последовательность проверки статуса сертификатов следующая:

1) проверка по OCSP протоколу,

2) проверка по списку отзыва (если сервер OCSP недоступен, и не установлена опция **Проверять сертификаты только по OCSP**).

Автоматическое обновление списка отозванных сертификатов (CRL)

Группа параметров **Автоматическое обновление списка отозванных сертификатов (CRL)** содержит параметры, относящиеся к обращению к серверам (точкам распределения списка отзыва), на которых централизовано хранятся Списки отзыва сертификатов.

Отключить обновление СОС

Опция **Отключить обновление СОС** 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 СОС** становятся доступными элементы управления в данной секции.

URL (http/ftp/ldap) точки распределения списка отзыва (CRL):

Поле **URL (http/ftp/ldap) точки распределения списка отзыва (CRL)** задает адрес ресурса, с которого будет выполняться обновления списка отзыва. Формат URL соответствует синтаксису адресов протоколов http, ftp, ldap и имеет вид:

FTP/HTTP/HTTPS:<Протокол>://<адрес сервера>/<путь к файлу>

Например:

ftp://192.168.1.1/some.crl

http://somesite/some/some.crl

Формат URL для LDAP:

LDAP://<адрес сервера>:<порт>/<имя DN элемента>?<attributes>?<scope>?<filter>?<extensions>

Извлекать URL CDP из сертификатов

При установке флажка **Извлекать URL CDP из сертификатов** вместо адреса в поле **URL (http/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, в этом случае будет использоваться адрес из поля "**URL (http/ftp/ldap) точки распределения списка отзыва(CRL):**".

Обновить CRL

Кнопка **Обновить CRL** позволяет обновить список отзыва вручную с соответствующего сервера, указанного в поле "**URL (http/ftp/ldap) точки распределения списка отзыва (CRL):**".

Подгруппа параметров **Протокол LDAP** – позволяет выбрать один из версий протокола LDAP.

- протокол **LDAPV3** используется по умолчанию, поскольку он совместим со всеми серверами LDAP.

- **Dionis LX** – это протокол, необходимый только для совместимости с реализацией LDAP-сервера на серверах Dionis LX.

Группа **Параметры аутентификация** позволяют задать логин и пароль необходимый для аутентификации на сервере LDAP. Поля могут оставаться пустыми, если сервер не требует аутентификации.

Минимальный интервал

Поле **Минимальный интервал обновления** задает минимальный интервал между обращениями к серверам для обновления списка отзыва. При проверках статусов сертификатов список отзыва не будет обновляться, если он уже был обновлен меньше чем N минут назад, где N - заданное минимальное время обновления. Этот параметр минимизирует количество обращений в серверу.

Использование OCSP

Группа параметров **Использование OCSP** позволяет включить и настроить параметры контроля локального сертификата пользователя для данного подключения по протоколу OCSP (.

Настройка параметров OCSP протокола

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.

При снятии флажка **Отключить проверку сертификатов по OCSP** становятся доступными элементы управления в данной секции:

Опция **Проверять сертификаты только по OCSP протоколу** задать строгую проверку сертификата только по OCSP протоколу. Если данная опция отключена, то после выполнения проверки по OCSP, будет выполнена проверка статуса сертификата по списку отзыва, но только в том случае, если сервер OCSP не даст точный ответ, что проверяемый сертификат не действителен. Например, если сервер будет недоступен или вернет ответ, что на нем произошла внутренняя ошибка.

Поле **URL(HTTP) OCSP** – это адрес OCSP сервера, по которому будет происходить проверка статусов 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 "**URL(HTTP) OCSP**" (если задан).

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

6.3.5.3 Работа с локальным хранилищем сертификатов пользователя DiSEC

Если у пользователя DiSec имеется сертификат Сервера VPN, с которым предполагается взаимодействие, то его рекомендуется поместить в локальное хранилище сертификатов пользователя DiSec. В противном случае необходимо настроить запрос сертификата в процессе переговоров по протоколу IKE.

Для выполнения размещения сертификата на вкладке **Безопасность** имеется кнопка **Работа с хранилищем сертификатов**.

Примечание. Рекомендуется заранее получить сертификат Сервера VPN для уменьшения накладных расходов по пересылке его по сети.

После ее нажатия открывается окно **Работа с хранилищем сертификатов**.

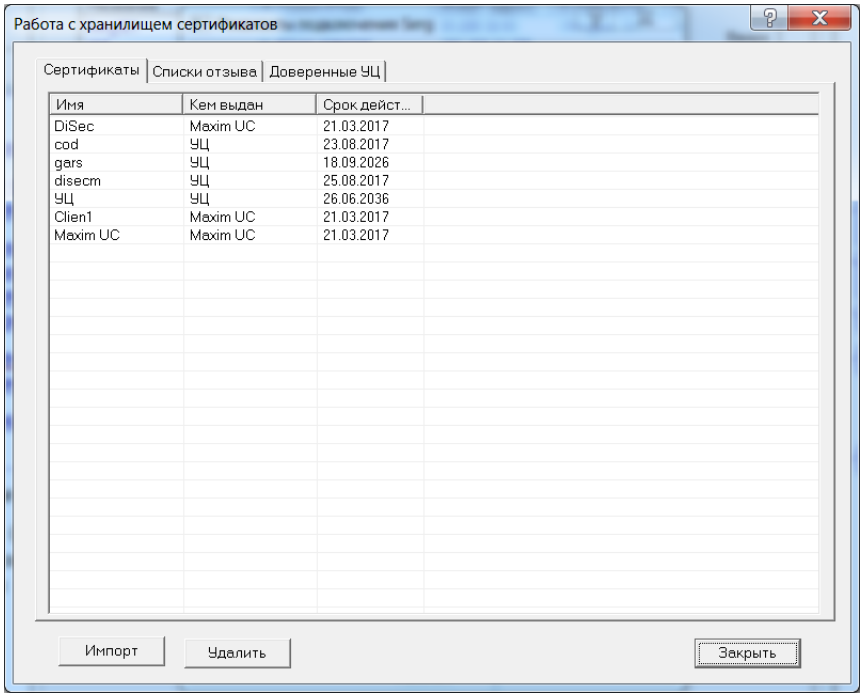


Рис. 59

На вкладке **Сертификаты** необходимо нажать кнопку **Импорт** и в открывшемся списке выбрать нужный сертификат. При необходимости следует выполнить поиск на нужном съемном носителе в нужной поддиректории и выбрать сертификат.

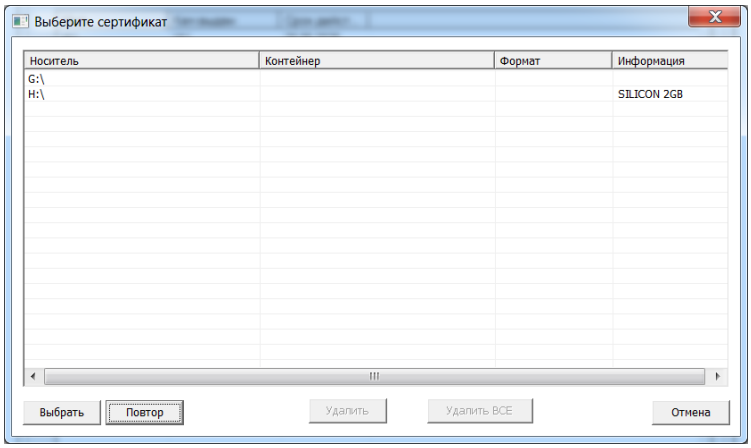


Рис. 60

6.3.5.4 Настройки запроса сертификата Сервера VPN

Вкладка **Безопасность** (Рис. 36). Настройки под заголовком **Настройки запроса сертификата сервера VPN** служат для того, чтобы указать сертификат того Сервера VPN, с которым предполагается устанавливать туннель, и определить, будет ли DiSec запрашивать у Сервера VPN его сертификат для сравнения с имеющимся у пользователя DiSec сертификатом.

> *Напомним* – сертификаты всех Серверов VPN, с которыми предполагается создавать туннели, предварительно должны быть помещены в локальное хранилище пользователя DiSec (см. раздел 3.6.2, с. 19).

При установленном переключателе **Не запрашивать сертификат сервера VPN** становится активной кнопка **Выбрать сертификат сервера VPN**. После ее нажатия на экран будет выведено содержимое хранилища пользователя DiSec (Рис. 61). В списке надо выделить требуемый сертификат (предварительно сертификат можно просмотреть) и нажать кнопку **ОК** - информация о сертификате Сервера VPN (**X500-имя**) будет занесена в поле под переключателем на вкладке **Безопасность** (Рис. 36)..

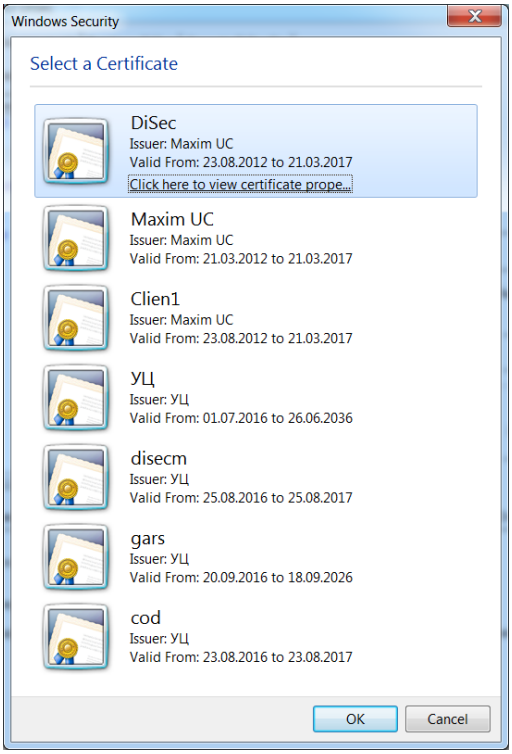


Рис. 61

При такой настройке DiSec будет использовать указанный сертификат для организации туннеля, не запрашивая у Сервера VPN его сертификат.

При установленном переключателе **Запросить сертификат сервера VPN** надо нажать кнопку **Получить имя Сервера VPN**. На экран будет выведено сертификаты из локального хранилища пользователя (Рис. 61). В списке надо выделить требуемый сертификат и нажать кнопку **ОК** - ***X500-имя*** из сертификата Сервера VPN будет занесено в поле под переключателем.

При такой настройке DiSec в процессе согласования SA IKE, запросит у Сервера VPN его сертификат. Если ***X500-имя*** из полученного сертификата совпадет с указанным при настройке, то DiSec будет использовать его для организации туннеля.

Если необходимо, чтобы сертификат Сервера VPN был выпущен конкретным УЦ, то следует запросить у Сервера VPN предоставить сертификат, подписанный требуемым Удостоверяющим Центром.

Для этого надо на вкладке **Безопасность** (Рис. 36):

- установить флажок **Запросить сертификат, выпущенный доверенным УЦ.** На экран будет выведено сообщение «Выберите сертификат УЦ для запроса сертификата сервера VPN» и после нажатия кнопки OK на экране появится список сертификатов, находящихся в личном хранилище пользователя DiSec. В списке надо выделить сертификат требуемого УЦ. ***X500-имя*** из сертификата выбранного доверенного УЦ будет занесено в поле под флажком.

При наличии такого запроса Сервер VPN должен будет прислать по запросу DiSec требуемый сертификат, подписанный тем УЦ, который указан в запросе. Если ***X500-имя*** из полученного сертификата совпадет с указанным при настройке, то DiSec будет использовать его для организации туннеля.

> *Примечание.* В личном хранилище пользователя DiSec может находиться несколько сертификатов одного Сервера VPN с одним и тем же ***X500-именем***, но выпущенных разными УЦ. DiSec не контролирует наличие сертификата с заданным при настройке ***X500-именем***, выпущенным заданным при настройке доверенным УЦ.

6.3.5.5 Защита хранилища Доверенные УЦ

Если файл **root.sst**, содержащий хранилище доверенных корневых УЦ размещен на незащищенном носителе или на жестком диске, то 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** (Рис. 37) – система сформирует имитовставку хранилища

root.sst на текущем закрытом ключе пользователя. Имитовставка будет проверяться каждый раз при инициализации криптосистемы.

> *Примечание*. Если у данного пользователя DiSec имеется несколько подключений IPSEC-ГОСТ для разных локальных сертификатов (и соответственно для различных ключей), и имеется необходимость защитить хранилище имитовставкой, то необходимо иметь различные хранилища доверенных корневых УЦ для этих подключений.

Защиту хранилища можно отменить (снять флажок **Защитить хранилище**); после этого станет активной кнопка **Удалить имитовставку**, нажатие которой имитовставку удаляет.

6.3.5.6 Работа с хранилищами

Для хранения сертификатов, необходимых пользователю DiSec, используется локальное хранилище, размещенное в персональной директории пользователя. Локальное хранилище пользователя DiSec содержит два типа объектов:

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** - действующие списки отозванных сертификатов всех УЦ, необходимые для построения цепочки доверия.

После того как будет выполнена инициализация криптосистемы, в окне **Установки криптосистемы** (Рис. 37), а также на вкладке **Безопасность** (рис.25) становится активной кнопка **Работа с хранилищем сертификатов**. После нажатия этой кнопки на экран будет выведено окно **Работа с хранилищем сертификатов**, открытое на вкладке **Сертификаты** (Рис. 62).

Вкладка Сертификаты

В таблице на Рис. 62 каждый сертификат занимает одну строку. В первой графе таблицы выводится имя владельца сертификата, во второй - имя удостоверяющего центра, выдавшего сертификат, в третьей - срок действия сертификата.

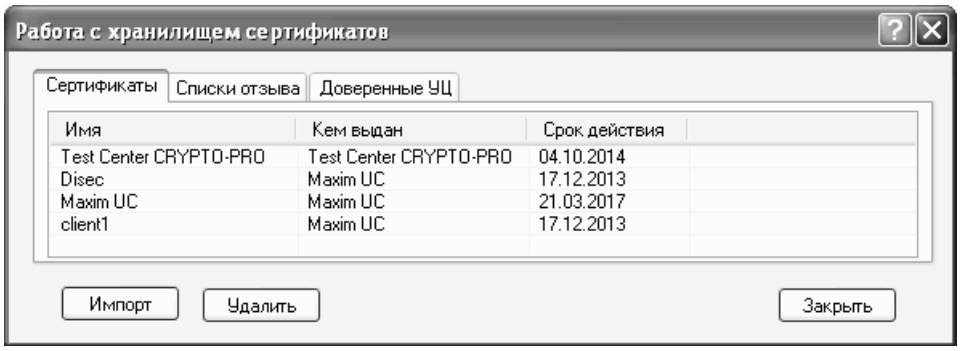


Рис. 62

Пользователь может добавить в хранилище новый сертификат, удалить имеющийся, а также получить более подробную информацию о сертификате. Для этого надо перевести курсор на строчку в таблице и щелкнуть правой кнопкой мыши – на экран будет выведено меню:

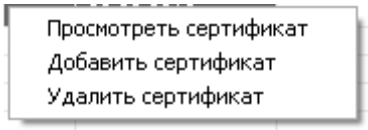


Рис. 63

Кнопка **Импорт** в нижней части экрана также служит для добавления сертификата в хранилище; кнопка **Удалить** - для удаления.

При *добавлении* сертификата на экран выводится стандартное окно (Рис. 64), позволяющее выбрать файл с нужным сертификатом. При вызове окна оно содержит список файлов с сертификатами Серверов VPN (имена файлов, как правило, имеют расширение **cer**), в столбце **Формат** отображается "CER".

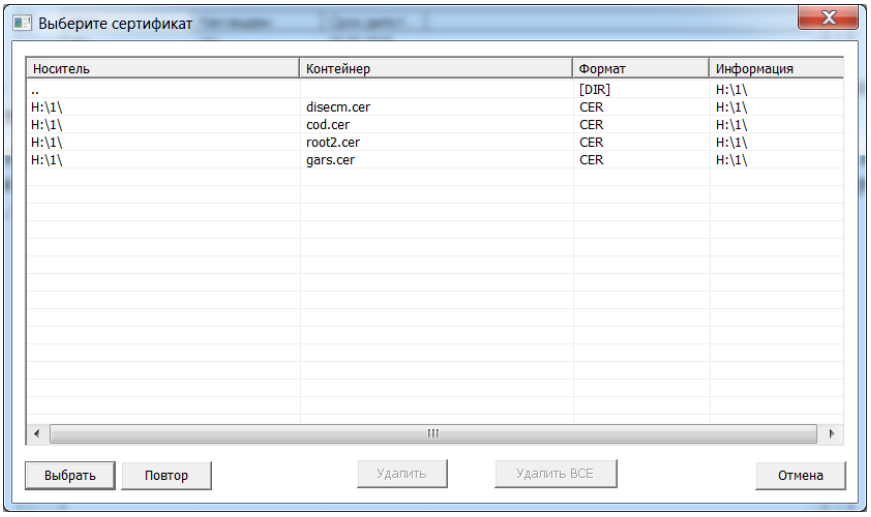


Рис. 64

Если требуется добавить сертификат УЦ, то необходимо перейти на вкладку **Доверенные УЦ** и выполнить команду добавления или **Импорт**. В результате появится окно для поиска сертификатов УЦ или контейнеров с цепочками сертификатов доверенных УЦ (файлы с расширением **p7b**).

В списке надо перевести курсор на требуемый файл и, либо при помощи двойного щелчка мышью, либо кнопкой **Выбрать** указать сертификат, который будет добавлен в локальное хранилище.

При *удалении* сертификата из хранилища система выдает дополнительный запрос и после подтверждения удаляет сертификат.

Чтобы *просмотреть* сертификат ключа, надо выделить соответствующую строчку в таблице (Рис. 62) и дважды щелкнуть левой кнопкой мыши. Или в меню на Рис. 63 выбрать альтернативу **Просмотреть сертификат**. На экран будет выведено окно **Сертификат**, содержащее две вкладки и открытое на вкладке **Общие**. На этой вкладке содержатся общие сведения о сертификате: имя владельца сертификата, имя УЦ, выдавшего сертификат и время действия сертификата.

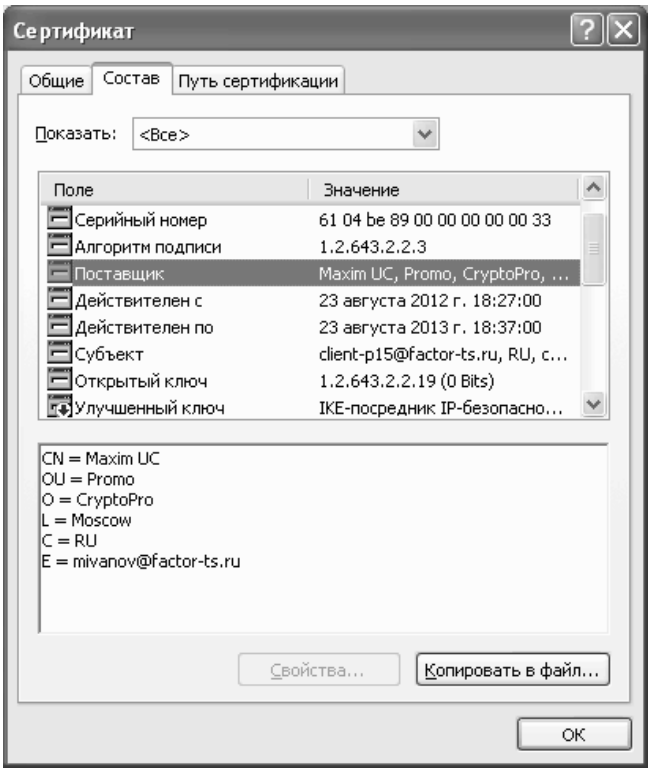


Рис. 65

На вкладке **Состав** (Рис. 65) 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.

Вкладка Списки отзыва

Вкладка **Списки отзыва** окна **Работа с хранилищем сертификатов** представлена на Рис. 66.

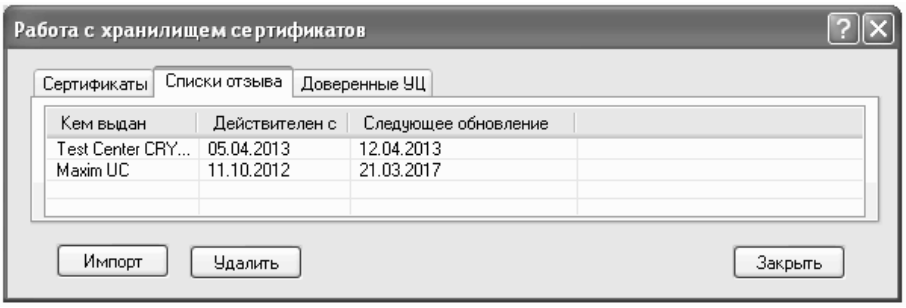


Рис. 66

В таблице каждый список занимает одну строку. В первой графе таблицы выводится имя удостоверяющего центра, выпустившего список, в третьей – дата выпуска списка, в третьей – срок действия списка.

Пользователь DiSec может добавить в хранилище новый список и удалить имеющийся, а также получить более подробную информацию о списке.

Добавление, *удаление* и *просмотр* списков выполняется так же, как рассмотренные выше операции с добавлением сертификатов.

При *просмотре* списка на экран выводится окно **Список отзыва сертификатов**, содержащее две вкладки и открытое на вкладке **Общие**. На этой вкладке (Рис. 67) 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.

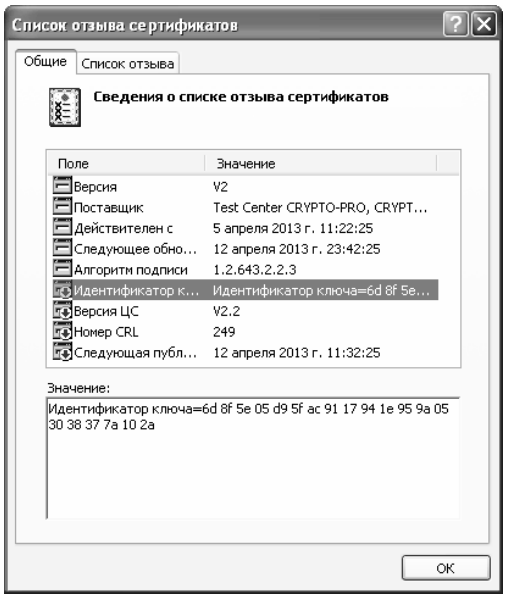


Рис. 67

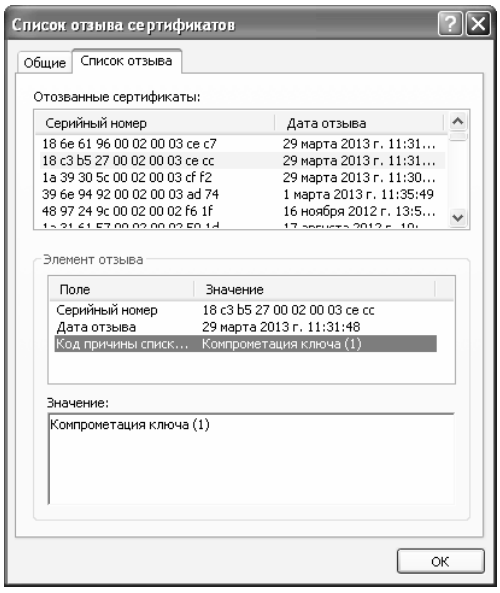


Рис. 68

На вкладке **Список отзыва** (Рис. 68) 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 Доверенные УЦ

Вкладка **Доверенные УЦ** содержит сертификаты корневых удостоверяющих центров (напомним, что они продублированы на вкладке **Сертификаты**).

В таблице на Рис. 69 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**.

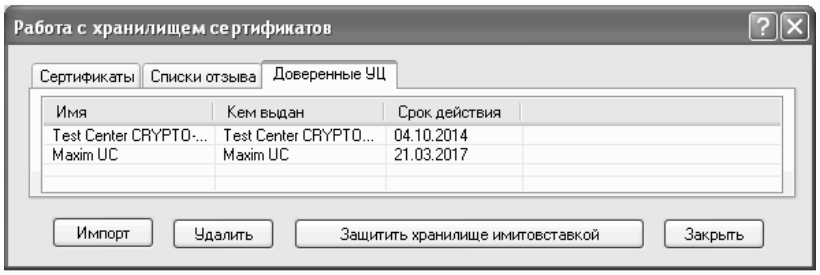


Рис. 69

На вкладке **Доверенные УЦ** пользователь может сформировать имитовставку, нажав на кнопку **Защитить хранилище имитовставкой**. Имитовставка будет сформирована на текущем закрытом ключе пользователя. Формируя имитовставку таким способом, пользователь получает возможность контролировать состав сертификатов корневых УЦ, защищаемых имитовставкой.

6.3.6 Вкладка Задачи (Реквизиты подключения)

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

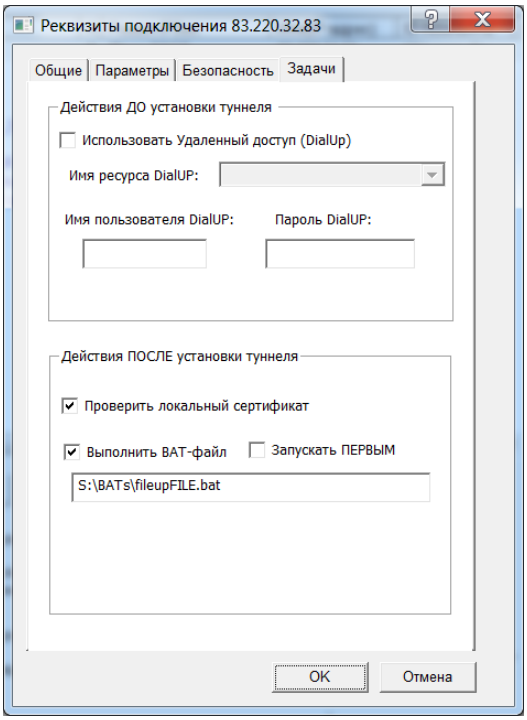


Рис. 70

Действия ДО установки туннеля

Группа параметров **Действия ДО установки туннеля** в настоящее время содержит только одну задачу - выполнить подключение к Интернет по модемному каналу (***DialUP***).

Использовать Удаленный доступ

Установка флажка **Использовать Удаленный доступ** позволяет выбрать из списка заранее созданный ресурс удаленного доступа WINDOWS (RAS), используемый для подключения к IP-сети (сеть Интернет). После установки флажка становятся активными и другие элементы управления этой группы. При снятии флажка подключение к Интернет по модемному каналу выполняться не будет. Остальные элементы становятся не активными, хотя их значение сохраняется.

Имя ресурса DialUP

Поле **Имя ресурса DialUP** позволяет выбирать имя из раскрывающегося списка ресурсов удаленного доступа WINDOWS (RAS), каждый из которых настроен на использование модема, подключенного к данному компьютеру, хранит номер телефона для дозвона на модемные входы **сервера удаленного доступа** и обеспечивает подключение к IP-сети по протоколу PPP или аналогичному.

Имя пользователя DialUP

Поле **Имя пользователя DialUP** - позволяет задать имя пользователя; имя служит для аутентификации на **сервере удаленного доступа**, в частном случае оно может совпадать с именем абонента Сервера VPN (если последний служит также и **сервером удаленного доступа**). Если имя не указано, то используется имя, заданное при создании ресурса RAS средствами Windows.

Пароль DialUP

Поле **Пароль DialUP** предназначено для ввода пароля пользователя, соответствующего введенному имени; пароль также служит для авторизации на **сервере удаленного доступа**. Если пароль не указан, то используется пароль, заданный при создании ресурса RAS средствами Windows.

Действия ПОСЛЕ установки туннеля

Группа параметров **Действия ПОСЛЕ установки туннеля** в настоящее время содержит две задачи, которые выполняются в заданном порядке практически одновременно, т.е. вторая задача запускается как только запущена первая, не дожидаясь ее завершения.

Проверить локальный сертификат

Флажок **Проверить локальный сертификат** запускает проверку локального сертификата в условиях установленного туннеля. При этом выполняются действия, заданные на вкладке **CRL и OCSP** настройки криптосистемы, а именно при соответствующих настройках проверяется наличие новых Списков отозванных сертификатов на указанных серверах (точках распределения списков отзыва) и\или проверка сертификата по протоколу OCSP. Рекомендуется подключать данную задачу, например, при недоступности серверов в отсутствие туннеля, т.е. когда серверы находятся в защищенной зоне, доступной только при наличии данного туннеля.

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 (Рис. 71) и предоставляется возможность выбора командного файла в любой директории.

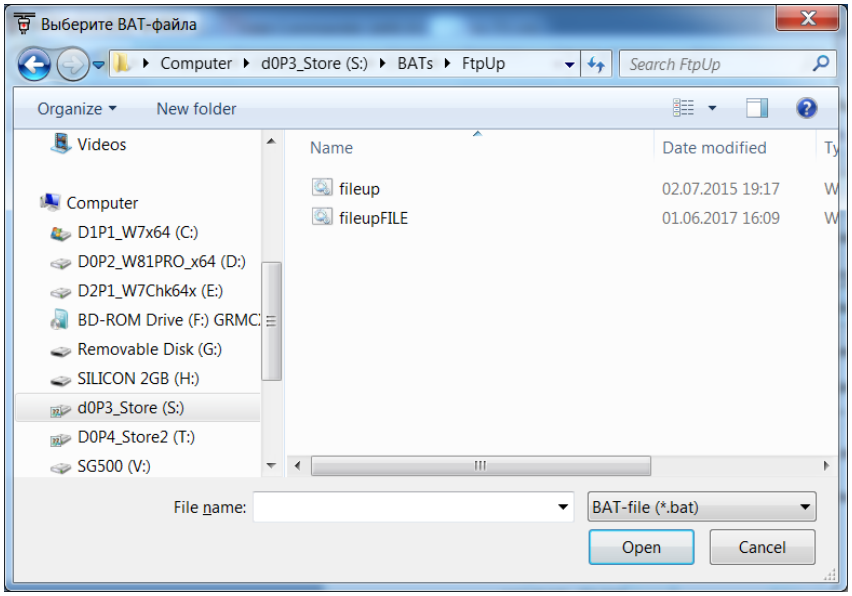


Рис. 71

Запускать первым

Флажок **Запускать первым** позволяет изменить порядок выполнения задач. При его установке первой будет запускаться задача командного файла, а затем (не дожидаясь ее окончания) задача проверки локального сертификата.

6.4 Вкладка Драйвер DiSec (Настройка ПО DiSec)

На вкладке **Драйвер DiSec** окна **Настройка ПО DiSec** выполняются настройки режима работы драйвера и устанавливаются параметры протоколирования сети. Драйвер выполняет функции межсетевого экрана (МЭ) при соответствующей настройке (см. раздел 6.4.1.5, с. 74).

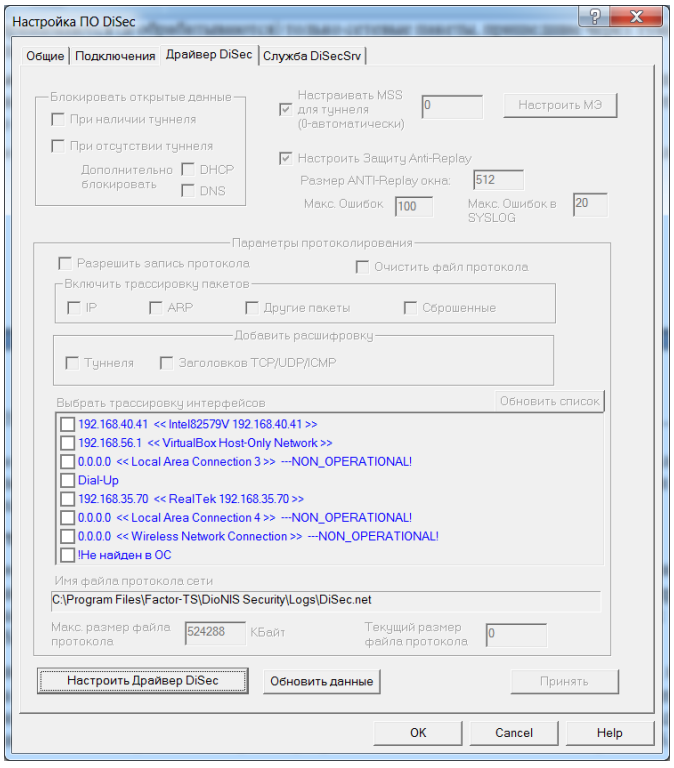


Рис. 72

Поскольку для выполнения настройки драйвера необходимы повышенные административные права, в нижней части вкладки **Драйвер DiSec** имеется кнопка **Настроить драйвер DiSec** (Рис. 73) при нажатии которой на экран будет выведено системное окно с запросом на ввод авторизационных данных (вид окна

зависит от версии ОС WINDOWS). При успешном вводе данных открывается такое же окно **Настройка Драйвера DiSec** (Рис. 73), в котором доступны все элементы и отсутствует кнопка **Настроить драйвер DiSec**.

По окончании выполнения настроек параметров драйвера (после нажатия кнопки **OK** или **Отмена**) в основном окне появляется кнопка **Обновить данные**, которую следует нажать для отображения на экране измененных параметров драйвера. 6.3.3.1

6.4.1 Настройка драйвера DiSec

В окне **Настройка Драйвера DiSec** (Рис. 73) размещены опции, которые действуют для всех подключений как правило во время работающего туннеля, а также в отсутствие установленных туннелей.

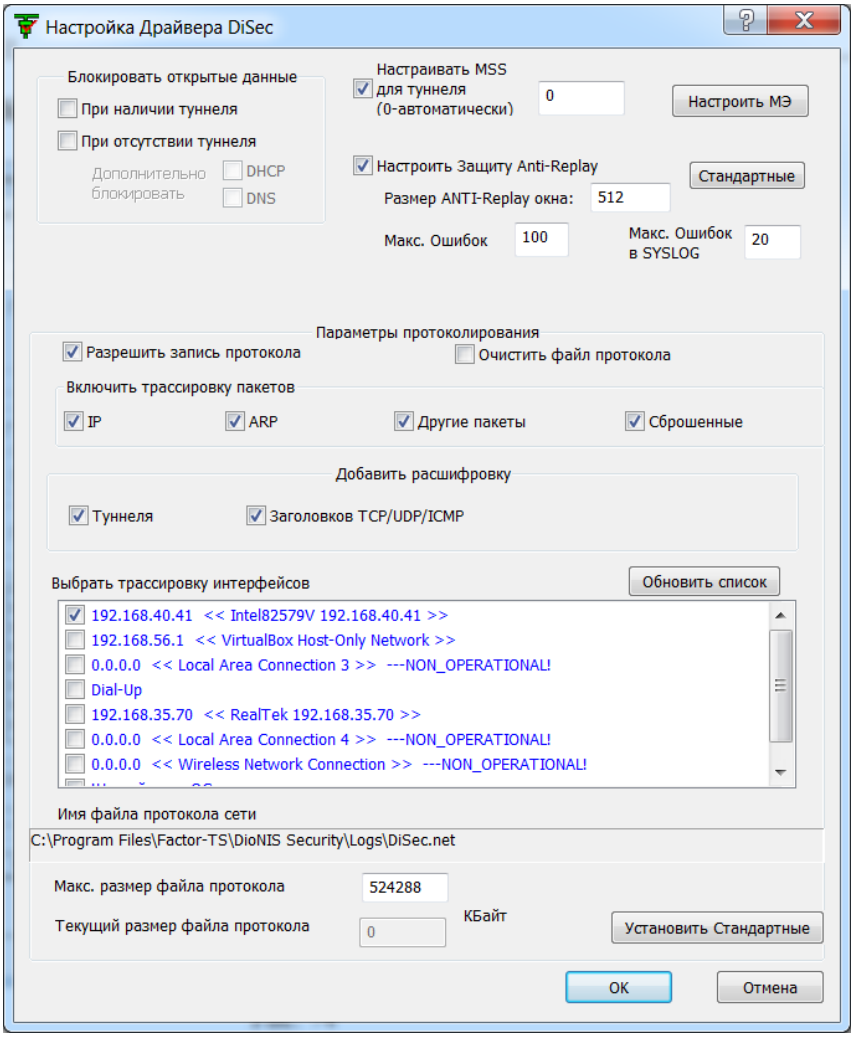


Рис. 73

6.4.1.1 Режим блокировки открытых данных

Блокировать открытые данные

Группа параметров **Блокировать открытые данные** (Рис. 73) определяют действия, которые будет выполнять драйвер с не туннелированными 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 7.1, с. 84) 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 динамический 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 динамическому 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 (см. раздел 6.3.1, с. 39).

Настроить МЭ

Настройка межсетевого экрана рассмотрена ниже (п. 6.4.1.5, с. 74).

6.4.1.2 Параметры сетевых пакетов

При передаче сетевых пакетов по туннелю драйвер Disec не только зашифровывает их содержимое, но выполняет некоторую модификацию, например, изменяет их характеристики для оптимального прохождения через сетевые устройства (маршрутизаторы, коммутаторы и т.п.). При получении сетевых пакетов по туннелю, выполняется дополнительный контроль с целью защиты от различного рода сетевых атак.

Настроить MSS

Параметр **Настроить MSS** служит для гибкой настройки в целях обеспечения прохождения сетевого трафика через сетевые устройства с ограничениями по размеру сетевых пакетов. При нулевом значении приложение (служба) DiSec автоматически вычислит размер пакета с учетом максимально возможного для данной линии связи и способа туннелирования. При необходимости будет выполнено фрагментирование исходного пакета. Пользователь DiSec может попытаться самостоятельно назначить это значение и протестировать прохождение трафика до пункта назначения.

Настроить Защиту Anti-Replay

Группа параметров **Настроить Защиту Anti-Replay** 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*.

6.4.1.3 Параметры протоколирования

Драйвер DiSec имеет возможность записывать информацию о проходящих через него пакетах данных в текстовый файл, т.е. вести протокол работы сети, при этом запись выполняется как при наличии активного туннеля, так и при его отсутствии. Файл протокола всегда размещается в директории установки ПО DiSec в поддиректории **Logs** и имеет имя **DiSec.net** (изменить имя файла нельзя).

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**, а затем и флажки под заголовком **Добавить расшифровку**). 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.

---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**.

Флажок IP

Флажок определяет запись в протокол (трассировку) информации обо всех IP-пакетах, проходящих через выбранные для трассировки интерфейсы, при этом для каждого фиксируемого пакета всегда выполняется расшифровка заголовка IP-пакета. Расшифровка заголовка в протоколе начинается с префикса «IP:».

Флажок ARP

Флажок включает протоколирование всех 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:».

Флажок Другие пакеты

При установке флажка в протокол сети будет добавлено фиксирование пакетов, имеющих любой транспортный тип (отличный от ARP и IPv4), например, пакеты пртокола IPv6, при этом расшифровка заголовков не выполняется.

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-заголовков.

---Добавить расшифровку---

Флажки в группе **Добавить расшифровку** под этим заголовком определяют количество и вид информации, которая будет заноситься в протокол сети.

Туннеля

При установке флажка в протокол сети будет добавлена информация о туннелированных пакетах, проходящих через выбранные для трассировки интерфейсы. Выводимая информация содержит данные о туннелированном пакете (протокол 4) и об исходном пакете, инкапсулированном в туннелированный пакет. Флажок активен только при установленном флажке **IP.**

Заголовков TCP/UDP/ICMP

При установке флажка в протокол сети будет добавлена расшифровка заголовков пакетов прикладных протоколов TCP, UDP и ICMP. Флажок активен только при установленном флажке **IP.**

Выбрать трассировку интерфейсов

Секция 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 закрытия окна **Настройка**. Использование данной кнопки рекомендуется, если во время работы с окном **Настройка** 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.

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).

6.4.1.4 Пример протокола

При фиксировании информации о передаваемом по сети пакете (трассировке) в соответствии с настройками в протокол заносится следующая информация о каждом пакете:

- дата и время прохождения пакета;
- номер интерфейса - порядковый номер интерфейса, присвоенный драйвером DiSec в процессе регистрации интерфейсов;

- направление передачи, например: «`IFC_1 <- recv:`» - означает, что фиксируется пакет, полученный по 1-му интерфейсу;
- параметры пакета, полученные драйвером от Windows, отражающие его тип;
- расшифровка Ethernet-фрейма, если он имеется. Для пакетов получаемых и направляемых адаптерам широкополосных мобильных сетей этот уровень отсутствует;
- расшифровка заголовков заданного типа (ARP, IP, заголовков протокола прикладного уровня – TCP, UDP или ICMP), при этом выделяются отдельные поля заголовков и выводятся в протокол в мнемоническом виде, например:

```
07-06-2017 18:43:14,690  IFC_0 (MediaType=0) <- recv:
 --- PacketType=00000001(RCV+, TNL-, UDP-, MCFG-, REJ-, REJFW-, ERR-); RejOpen=0, RejAll=00000000
(DNS-, DHCP-)
   Ethernet: MacRcv=ff:ff:ff:ff:ff:ff MacSnd=bc:5f:f4:48:1b:ee Type=0608
   ARP: Ethernet REQUEST
   192.168.40.42 [bc:5f:f4:48:1b:ee] -> 192.168.40.44 [00:00:00:00:00:00]

07-06-2017 18:43:14,955  IFC_0 (MediaType=0) <- recv:
 --- PacketType=00000001(RCV+, TNL-, UDP-, MCFG-, REJ-, REJFW-, ERR-); RejOpen=0, RejAll=00000000
(DNS-, DHCP-)
   Ethernet: MacRcv=ff:ff:ff:ff:ff:ff MacSnd=08:00:27:b3:47:26 Type=0608
   ARP: Ethernet REQUEST
   192.168.40.11 [08:00:27:b3:47:26] -> 192.168.40.6 [00:00:00:00:00:00]

07-06-2017 18:43:15,265  IFC_0 (MediaType=0) <- recv:
 --- PacketType=00000001(RCV+, TNL-, UDP-, MCFG-, REJ-, REJFW-, ERR-); RejOpen=0, RejAll=00000000
(DNS-, DHCP-)
   Ethernet: MacRcv=c8:60:00:c6:67:b5 MacSnd=00:1b:21:d6:fe:23 Type=0008
   IP: 83.220.32.83->192.168.40.41 len 176 ihl 20 ttl 63 prot 17 id 11126 offs 0 DF ~MF CkSum=0xc6b2
   UDP: 4500->4500 len 156 CkSum=0xeb6b

07-06-2017 18:43:15,266  IFC_0 (MediaType=0) -> sent:
 --- PacketType=02000000(RCV-, TNL-, UDP-, MCFG-, REJ-, REJFW-, ERR-); RejOpen=0, RejAll=00000000
(DNS-, DHCP-)
   Ethernet: MacRcv=00:1b:21:d6:fe:23 MacSnd=c8:60:00:c6:67:b5 Type=0008
   IP: 192.168.40.41->83.220.32.83 len 176 ihl 20 ttl 128 prot 17 id 14763 offs 0 ~DF ~MF
CkSum=0x91a3
   UDP: 4500->4500 len 156 CkSum=0xbaa0

07-06-2017 18:43:15,433  IFC_0 (MediaType=0) <- recv:
 --- PacketType=00000001(RCV+, TNL-, UDP-, MCFG-, REJ-, REJFW-, ERR-); RejOpen=0, RejAll=00000000
(DNS-, DHCP-)
   Ethernet: MacRcv=01:00:5e:7f:ff:fa MacSnd=bc:5f:f4:48:1b:ee Type=0008
   IP: 192.168.40.42->239.255.255.250 len 202 ihl 20 ttl 1 prot 17 id 5802 offs 0 ~DF ~MF
CkSum=0xacc9
   UDP: 50933->1900 len 182 CkSum=0xa657
```

- для туннелированных пакетов добавляется строка, в которой указывается признак туннелированного (инкапсулированного) пакета, идентификатор туннеля (см. раздел 8.3, с. 91), а также добавляются строки с расшифровкой заданных заголовков в исходном ORIGINAL(Incapsulated): и результирующем пакете (INCAPSULATING Packet:), например:

```
07-06-2017 18:51:23,116  IFC_0 (MediaType=0) -> sent:
 --- PacketType=02001000(RCV-, TNL+, UDP-, MCFG+, REJ-, REJFW-, ERR-); RejOpen=0, RejAll=00000000
(DNS-, DHCP-)
 ORIGINAL(Incapsulated) data:
   Ethernet: MacRcv=00:1b:21:d6:fe:23 MacSnd=c8:60:00:c6:67:b5 Type=0008
   IP: 192.168.40.41->192.168.0.3 len 1028 ihl 20 ttl 255 prot 1 id 15038 offs 0 ~DF ~MF
CkSum=0xbdd3
   ICMP: Echo Request code 0
 INCAPSULATING Packet:
   TnlID 32769(0x00008001). MODE_CFG=192.168.32.164(0xC0A820A4)
   Ethernet: MacRcv=00:1b:21:d6:fe:23 MacSnd=c8:60:00:c6:67:b5 Type=0008
   IP: 192.168.40.41->192.168.0.3 len 1076 ihl 20 ttl 255 prot 4 id 4 offs 0 ~DF ~MF CkSum=0x450e
   IP2IP: ID=8001, SeqNUM=4, Length=1028, KeyLen=12

07-06-2017 18:51:23,116  IFC_0 (MediaType=0) <- recv:
 --- PacketType=00001001(RCV+, TNL+, UDP-, MCFG+, REJ-, REJFW-, ERR-); RejOpen=0, RejAll=00000000
(DNS-, DHCP-)
 ORIGINAL(Incapsulated) data:
   Ethernet: MacRcv=c8:60:00:c6:67:b5 MacSnd=00:1b:21:d6:fe:23 Type=0008
   IP: 192.168.0.3->192.168.40.41 len 1028 ihl 20 ttl 63 prot 1 id 16904 offs 0 ~DF ~MF CkSum=0x748c
   ICMP: Echo Reply code 0
 INCAPSULATING Packet:
   TnlID 32769(0x00008001). MODE_CFG=192.168.32.164(0xC0A820A4)
```

```
   Ethernet: MacRcv=c8:60:00:c6:67:b5 MacSnd=00:1b:21:d6:fe:23 Type=0008
   IP: 192.168.0.3->192.168.40.41 len 1076 ihl 20 ttl 62 prot 4 id 3 offs 0 ~DF ~MF CkSum=0x46cf
   IP2IP: ID=8001, SeqNUM=4, Length=1028, KeyLen=12
```

- для отброшенных пакетов добавляется информация об этом (REJECTED Packet!)

```
 07-06-2017 18:55:05,181  IFC_0 (MediaType=0) <- recv:
 --- PacketType=00000101(RCV+, TNL-, UDP-, MCFG-, REJ+, REJFW-, ERR-); RejOpen=1, RejAll=00000000
(DNS-, DHCP-)
   REJECTED Packet!
   Ethernet: MacRcv=33:33:ff:5e:8a:3b MacSnd=bc:5f:f4:48:1b:ee Type=DD86
   IPv6:

07-06-2017 18:55:06,180  IFC_0 (MediaType=0) <- recv:
 --- PacketType=00000101(RCV+, TNL-, UDP-, MCFG-, REJ+, REJFW-, ERR-); RejOpen=1, RejAll=00000000
(DNS-, DHCP-)
   REJECTED Packet!
   Ethernet: MacRcv=33:33:ff:5e:8a:3b MacSnd=bc:5f:f4:48:1b:ee Type=DD86
   IPv6:
```

6.4.1.5 Настройка МЭ

Как было сказано выше, драйвер DiSec имеет элементы межсетевого экрана (МЭ), а именно: драйвер обеспечивает контроль проходящего потока информации и выполняет отсеивание нежелательных IP-пакетов. Контроль выполняется с помощью фильтров. Фильтр представляет собой набор правил проверки IP-пакетов.

Настройка МЭ заключается в следующем:

- формирование фильтров (создание наборов правил фильтрации);
- привязка фильтра к интерфейсу/интерфейсам; фильтры могут быть предназначены как для конкретного интерфейса, так и для всех интерфейсов одновременно;
- привязке фильтра к направлению обмена данными; фильтр может контролировать входящий, исходящий или оба потока информации.

После нажатия кнопки **Настроить МЭ** в окне на Рис. 73 (с. 69) открывается окно **Настройка правил МЭ** (Рис. 74), содержащее данные о текущих настройках МЭ и позволяющее изменить его конфигурацию.

Рис. 74

В верхней части окна информация, отображающая текущее состояние тех фильтров, которые являются общими для всех интерфейсов:

- если установлен переключатель **Для всех интерфейсов**, то все рассмотренные ниже настройки будут относиться сразу ко всем интерфейсам;
- в строке **Фильтры FW:Вх.+|Исх+|Оба-|** указаны три направления обмена данными: знак «плюс» после названия означает наличие фильтра (фильтров) для указанного направления, знак «минус» - отсутствие.

Список интерфейсов

- В таблице под этим заголовком в левом столбце (под заголовком **Интерфейсы**) выведен список всех имеющихся в данный момент на компьютере пользователя IP-интерфейсов: указано имя интерфейса и его параметры (IP-адрес, статус).

В правом столбце (под заголовком **Фильтры FW**) указано наличие действующих фильтров и контролируемые направления для соответствующего интерфейса:

- при наличии хотя бы одного подключенного фильтра первые символы - **Вкл.**, в противном случае - **Выкл.**;
- далее перечислены три направления, после каждого из них может быть знак «плюс», что означает наличие фильтра для указанного направления, или знак «минус» - фильтр отсутствует.

Направление

Группа переключателей определяет привязку фильтра к направлению потока информации.

Текущие правила

По нажатию кнопки в поле под заголовком **Правила фильтрации** выводится список правил (фильтр), созданный для выделенного курсором в верхнем списке интерфейса и указанного направления.

Установить привязку

По нажатию кнопки список правил (фильтр), выведенный на экран в секции под заголовком **Правила фильтрации**, «привязывается» к интерфейсу (выделенному курсором в верхнем списке).

> *Внимание!* Работа по новым правилам начнет выполняться только после выхода из окна **Настройка правил МЭ** по кнопке **ОК**.

Правила фильтрации

В секции под этим заголовком отображается список правил. Для работы с правилами фильтрации используются кнопки, расположенные справа от секции и ниже секции.

Добавить, Изменить

По нажатию этих кнопок открывается окно **Правило фильтрации МЭ** (см. Рис. 75, с. 77), подробно рассмотренное ниже в п. 6.4.1.7, с. 76.

Удалить

По нажатию кнопки без дополнительного запроса удаляется правило, на котором установлен курсор

Очистить ВСЕ

По нажатию кнопки без дополнительного запроса стираются все правила в секции **Правила фильтрации**, а также в поле **Хранилище правил**.

Сохранить в файл

По нажатию кнопки на экран выводится стандартное окно для указания местоположения и имени файла в директориях компьютера; список правил, отображенный на экране, заносится в файл; имя файла указывается в поле **Хранилище правил**.

Загрузить из файла

По нажатию кнопки на экран выводится стандартное окно поиска файла в директориях компьютера, из указанного файла список правил копируется на экран, его имя указывается в поле **Хранилище правил**.

Фильтр рекомендуется сохранить в файле, если предполагается его многократное использование. Возможно формирование фильтра из нескольких файлов.

Вверх

По нажатию кнопки выделенное правило в списке перемещается на строку вверх, если оно не первое в списке.

Вниз

По нажатию кнопки выделенное правило в списке перемещается на строку вниз, если оно не последнее в списке.

Дубль

По нажатию кнопки выделенное правило в списке дублируется и помещается под выделенным.

Реверс

По нажатию кнопки выделенное правило в списке дублируется, помещается под выделенным, в нем меняются местами адреса получателя и отправителя.

6.4.1.6 Последовательность настройки МЭ DiSec

Для того чтобы настроить межсетевой экран драйвера DiSec, надо выполнить следующую последовательность действий:

1. Выбрать область действия фильтра: либо установить флажок **Для всех интерфейсов**, либо в **Списке интерфейсов** выбрать (выделить курсором) нужную строку.
2. С помощью переключателя под заголовком **Направление** установить направление фильтруемого потока информации.
3. В секции под заголовком **Правила фильтрации** нажать кнопку **Добавить** и создать список правил (см. п. 6.4.1.7, стр.76). При этом в поле **Хранилище правил** будет выведено **REGISTRY.**
4. После того как список правил (фильтр) будет создан, надо выполнить его привязку к направлению и интерфейсу. Для этого надо нажать кнопку **Установить привязку**.

Содержание фильтра можно просмотреть (вывести его на экран в секцию **Правила фильтрации**). Для того надо:

- в **Списке интерфейсов** выбрать (выделить курсором) нужную строчку, либо установить флажок **Для всех интерфейсов**;
- с помощью переключателя под заголовком **Направление** выбрать направление фильтра;
- нажать кнопку **Текущие правила**.

Чтобы отключить фильтр от интерфейса, надо вывести содержимое фильтра на экран, удалить все правила (можно использовать кнопку **Очистить ВСЕ**) и выполнить привязку ПУСТОГО фильтра.

6.4.1.7 Создание и редактирование правила фильтрации

Для создания (редактирования) каждого правила фильтра надо в окне **Настройка правил МЭ** (Рис. 74, с. 75) нажать кнопку **Добавить** (**Изменить**) . На экран будет выведено окно **Правило фильтрации МЭ** (Рис. 75).

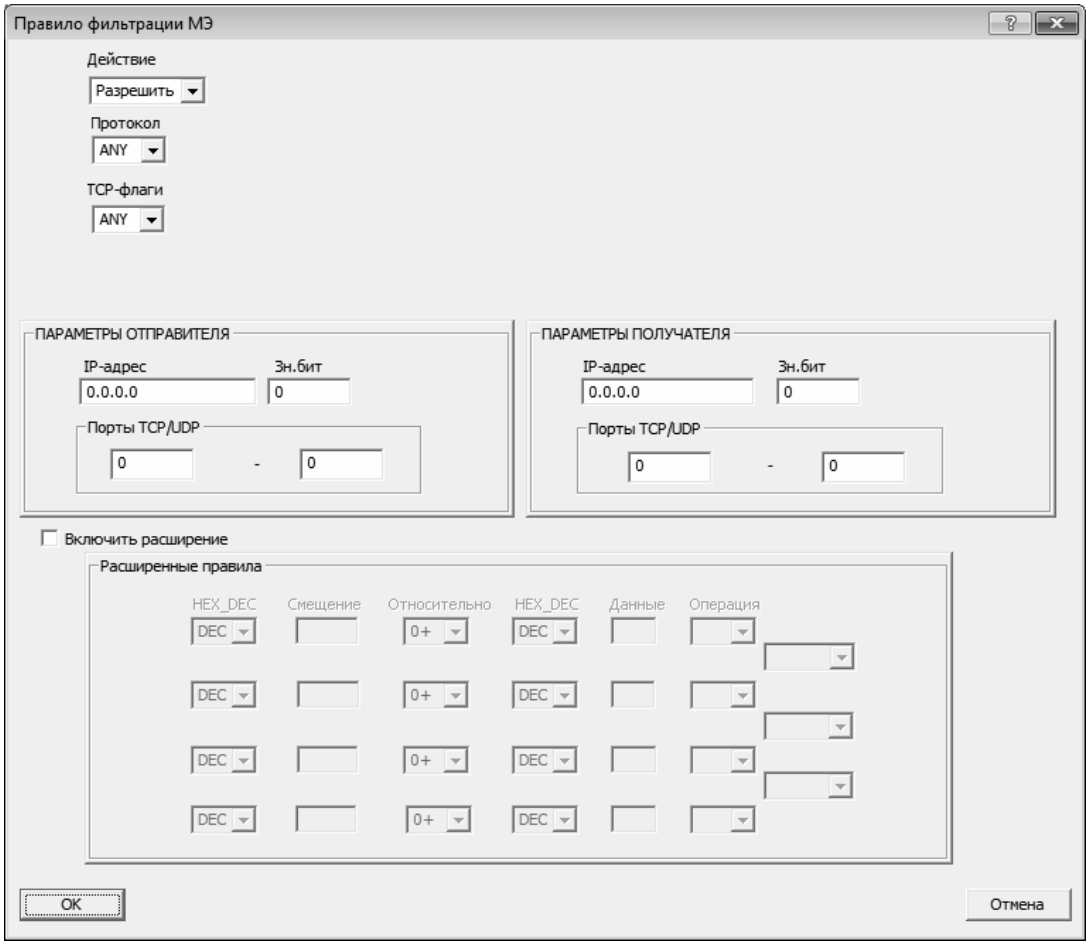


Рис. 75

Правило содержит набор параметров; одна часть параметров составляет базовый (обязательный) набор, вторая часть - расширенный.

Верхняя часть окна **Правило фильтрации МЭ** содержит базовый набор параметров.

Действие

Параметр определяет действие, которое будет применено к контролируемому сетевому пакетуе в случае совпадения параметров пакета с соответствующими значениями всех остальных параметров правила (базовой и расширенной части). Выпадающий список состоит из двух значений: *Разрешить* и *Запретить*.

Протокол

Параметр задает проверку значения поля «протокол» в заголовке IP-пакета. Выпадающий список состоит из значений:

- *ANY* – поле «протокол» в заголовке пакета может иметь любое значение;
- *ICMP* – поле «протокол» в заголовке пакета должно иметь значение *1* (ICMP);
- *TCP* – поле «протокол» в заголовке пакета должно иметь значение *6* (TCP);
- *UDP* – поле «протокол» в заголовке пакета должно иметь значение *17* (UDP - протокол может использоваться для передачи туннелированных пакета).;

TCP-флаги

Параметр задает проверку поля «флаги» TCP-пакета. Выпадающий список состоит из значений:

- *ANY* - проверка не производится;
- *SYN* - требуется, чтобы в TCP-пакете был установлен флаг **SYN** и сброшен флаг **ACK**;
- *ACK*, *URG*, *PSH*, *RST*, *FIN* - требуется, чтобы в TCP-пакете был установлен флаг, указанный параметром, остальные флаги могут быть любыми.

Параметры отправителя \ Параметры получателя

Параметры под этими заголовками задают проверку соответствующих полей в заголовке IP- пакета.

IP-адрес

В поле указывается либо конкретный адрес отдельного компьютера, либо начальный адрес подсети.

Зн. бит

В поле указывается маска сети в числовом выражении. Для одиночного IP-адреса необходимо указать значение **32**, для «стандартной» подсети из 255 IP-адресов – значение *24*.

Порты TCP/UDP

Параметры задают **диапазон** проверяемых значений. Если необходимо указать всего один порт, то указываются два одинаковых значения.

Включить расширение

Установленный флажок активизирует параметры для создания расширенного правила.

В расширенное правило добавлена возможность анализа до четырех полей, расположенных в любом месте сетевого пакета.

Первые два параметра **Смещение** и **Относительно** задают местоположение контролируемого поля сетевого пакета:

Смещение – числовое значение смещения контролируемого поля сетевого пакета от начальной точки отсчета;

Относительно – параметр определяет точки отсчета смещения контролируемого поля; может принимать следующие значения:

0+ – смещение отсчитывается от начала сетевого пакета;

IP+ – смещение отсчитывается от начала поля данных сетевого пакета.

Значение указанного поля сетевого пакета сравнивается с эталонным значением (параметр **Данные**), при этом используется заданная операция сравнения:

- **Данные** – параметр задает эталонное значение контролируемого поля;
- **Операция** – параметр задает операцию сравнения контролируемого поля с эталонным значением; возможные значения операции: == (равно), *!* = (не равно), > (больше), >= (больше, равно), < (меньше), <= (меньше, равно).

Полученные результаты анализа каждого из четырех полей комбинируются в соответствии со значениями последних трех параметров (**AND/OR**).

Числовые значения параметров могут быть указаны как в десятичной (**DEC**), так и в шестнадцатеричной (**HEX**) системе исчисления.

Каждое правило фильтра описывает одну операцию проверки IP-пакета и работает следующим образом: выполняется проверка полученного (передаваемого) сетевого пакета последовательно по всем установленным в правиле параметрам. Сначала выполняется проверка на совпадение по параметрам базового набора, затем по параметрам расширенного набора и при совпадении ВСЕХ параметров применяется действие, указанное в поле **Действие** (*Разрешить*/*Запретить*) окна **Правило фильтрации МЭ**.

6.5 Вкладка Служба DiSecSrv (Настройка ПО DiSec)

Вкладка **Служба DiSecSrv** окна **Настройка ПО DiSec** (Рис. 76) предназначена для изменения настроек службы DiSecSrv. Заданные параметры работы службы вносятся в базу данных служб WINDOWS и в раздел системного реестра для службы DiSecSrv.

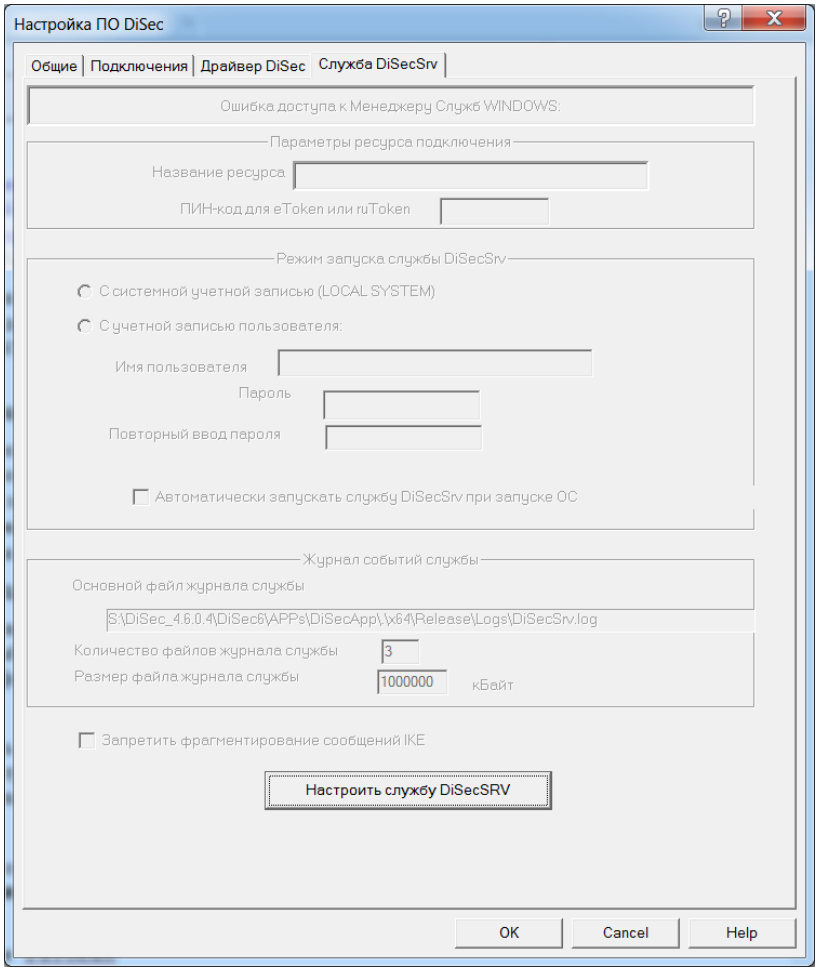


Рис. 76

Поскольку для настройки параметров требуются повышенные административные права, выводится сообщение об отсутствии прав доступа к службам WINDOWS, и текущие настройки группы параметров не отображаются.

Все элементы управления на вкладке неактивны, кроме кнопки **Настроить службу DiSecSrv**. После нажатия кнопки на экран будет выведено системное окно с запросом на ввод авторизационных данных (вид окна зависит от версии ОС WINDOWS). При успешном вводе данных открывается окно **Настройка службы DiSecSrv** (Рис. 77).

Выполнив все настройки, надо выйти из окна **Настройка службы DiSecSrv** (Рис. 77) нажатием кнопки **OK**. Система вернется на вкладку **Служба DiSecSrv** (Рис. 76), в нижней части которой появится кнопка **Обновить данные**, которую можно нажать для отображения на экране измененных параметров службы.

6.5.1 Настройка службы DiSecSRV

В окне **Настройка службы DiSecSRV** размещены опции и параметры, влияющие на режим запуска и работу службы DiSecSRV.

6.5.1.1 Информация об инициализации службы

В верхней части окна настройки службы выводится информация об инициализации службы. Если служба DiSecSrv была инициализирована, то выводится сообщение: *Служба DiSecSrv ИНИЦИАЛИЗИРОВАНА*, и элементы управления данной вкладки доступны для использования. В противном случае выводится сообщение: *Служба DiSecSrv НЕ инициализирована*, и элементы управления неактивны. В этом случае следует инициализировать службу, как это описано в разделе 5.3, с. 31.

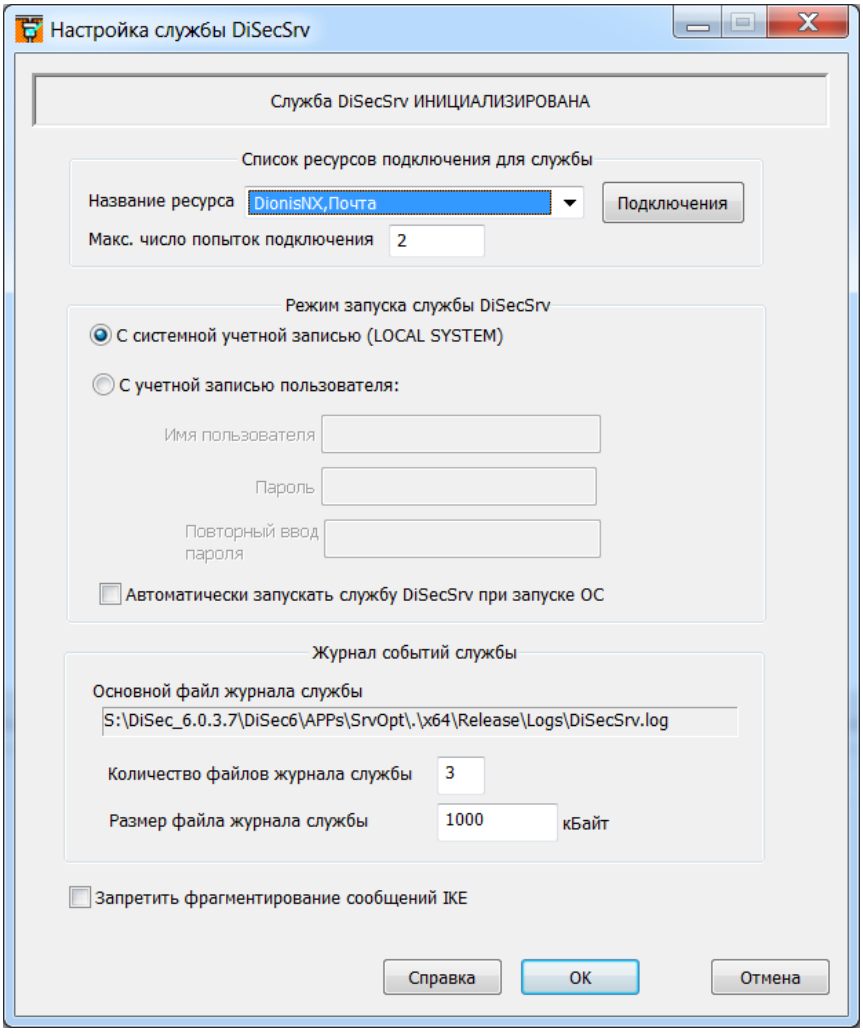


Рис. 77

6.5.1.2 Список ресурсов подключений для службы

Группа параметров **Список ресурсов подключения для службы** (Рис. 77) позволяют создать (настроить) один или несколько ресурсов подключения для службы и выбрать один из них или несколько в качестве текущего списка, а также настроить параметры цикла. Цикл для службы выполняется бесконечно до вмешательства пользователя, который может прервать его командой отключения службы (см. 5.3, стр. 31).

Список

Параметр позволяет выбрать из списка ресурсов подключений (защищенных сетей) тот, 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**.

Макс. число попыток подключения

Данный параметр определяет количество попыток подключения, после которых в случае разрыва туннеля выполняется переход к следующему в списке.

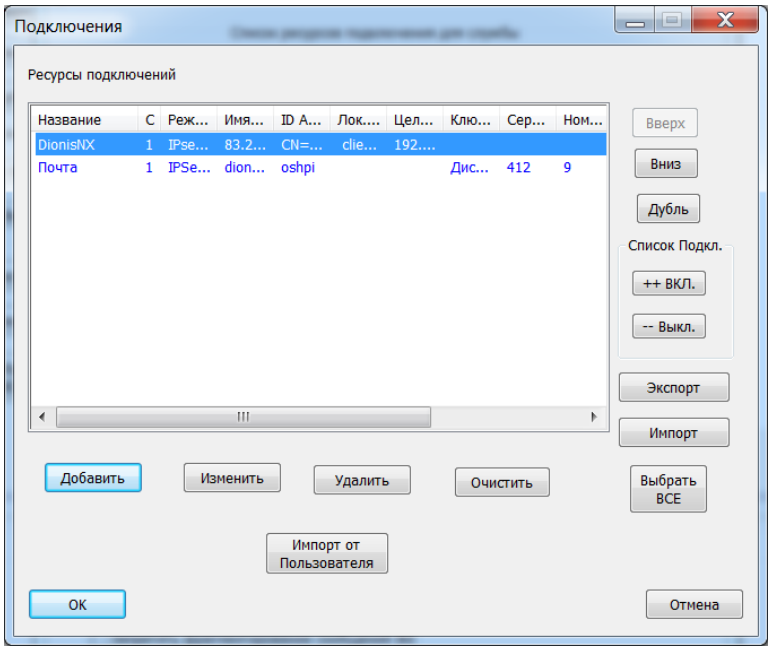


Рис. 78

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. При этом для режима IPSEC-ГОСТ все необходимые сертификаты и списки отзыва переносятся в личное хранилище сертификатов для службы.

По данной кнопке на экран выводится список подключений текущего пользователя

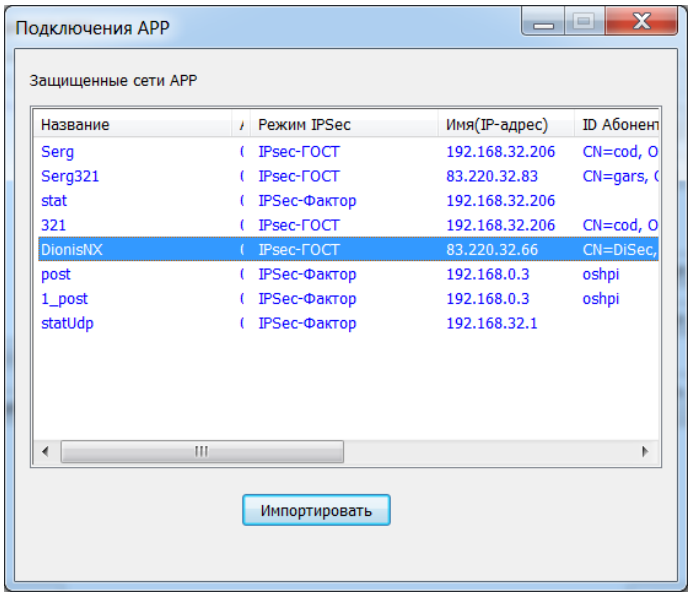


Рис. 79

Необходимо выделить нужный ресурс и нажать кнопку **Импортировать** или выполнить двойной щелчок мышью.

В списке подключений службы появится выбранный ресурс.

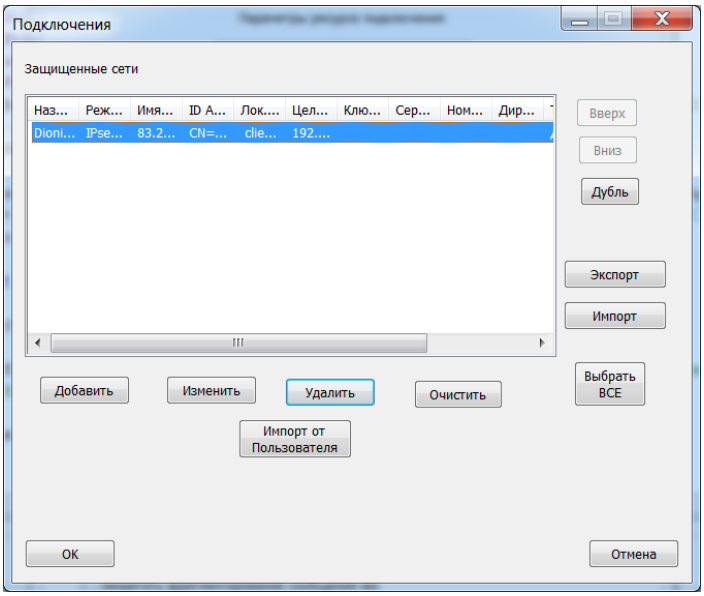


Рис. 80

Остальные кнопки аналогичны кнопкам окна списка подключений для приложения (см. 6.2, стр. 35).

6.5.1.3 *Режим запуска службы DiSecSrv*

Группа параметров под этим заголовком (Рис. 77) 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.

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: **`.\.`**

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 в окне **Тестирование** (раздел 9.5, с. 98).

6.5.1.4 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.

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.

6.5.1.5 Запретить фрагментирование для сообщений IKE

Флажок **Запретить фрагментирование для сообщений IKE** устанавливается в крайнем случае по требованию службы безопасности, поскольку считается, что в этом случае меньше вероятность нарушения работоспособности Сервера VPN. Однако, это может привести к тому, что сертификаты большого размера не смогут быть переданы при согласовании туннеля в режиме IPSEC-ГОСТ (SA IKE). Значение этого флажка влияет не только на работу службы, но и на работу приложения и распространяется на все подключения в режиме IPSEC-ГОСТ.

7 Команды Подключиться/Отключиться

Команда **Подключиться** Главного меню приложения DiSec (Рис. 14) служит для установки туннеля с конкретной защищенной сетью, после ее выбора на экран выводится окно (Рис. 82) в котором выбирается ресурс и инициируется процедура подключения.

Команда **Отключиться** Главного меню приложения DiSec (Рис. 14) служит для снятия ранее установленного средствами приложения DiSec туннеля. Подробнее ниже.

7.1 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 (Рис. 81), содержащее элементы управления, необходимые для выбора одного подключения или нескольких подключений; кнопки для запуска и прерывания процедуры подключения, а также информационную секцию для вывода сообщений о прохождении процедуры.

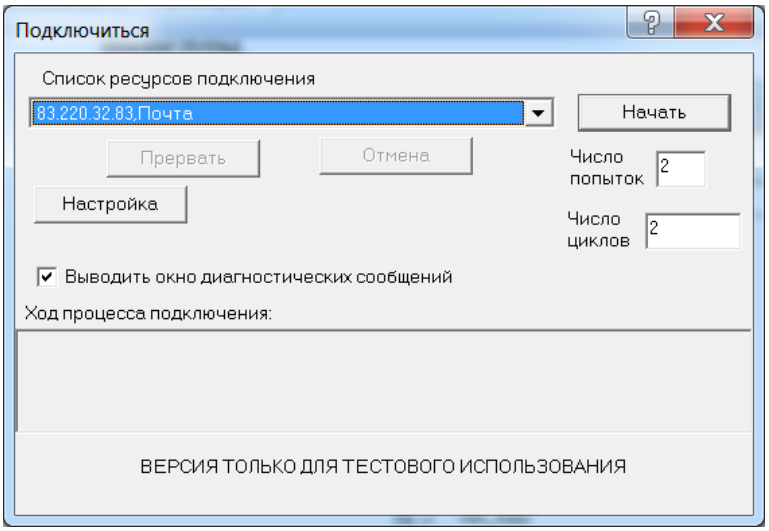


Рис. 81

Список ресурсов подключения

В текстовом поле элемента **Список ресурсов подключения** выводится название одного или нескольких ресурсов, к которым будет последовательно выполняться подключение.

Примечание. Переход к подключению к следующему ресурсу будет выполняться ТОЛЬКО в случае разрыва соединения по инициативе Сервера VPN (или по таймауту процедуры проверки жизнеспособности туннеля), либо в случае невозможности установить соединение.

Список ресурс можно выбрать (изменить), посредством установки или снятия флажков соответствующих ресурсов с раскрывающемся списке. Перечень ресурсов в выпадающем по нажатию значка стрелки списке содержит все созданные заранее на этапе настройки системы ресурсы (раздел 6.3, 38).

Выполнение процедуры (окончание цикла) может быть прервано пользователем. В этом случае перехода к следующему ресурсу в списке, а также к следующей попытке подключения к текущему ресурсу не выполняется.

Число попыток

Числовое значение в поле **Число попыток** определяет число попыток подключения к КАЖДОМУ ресурсу в списке до перехода к следующему. Стандартное значение - 2.

Число циклов

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

выдачей диагностического сообщения об этом факте (в окно **Диагностика DiSEC** и журнал **DiSec.log**. Стандартное значение - 0, означает "бесконечный" цикл.

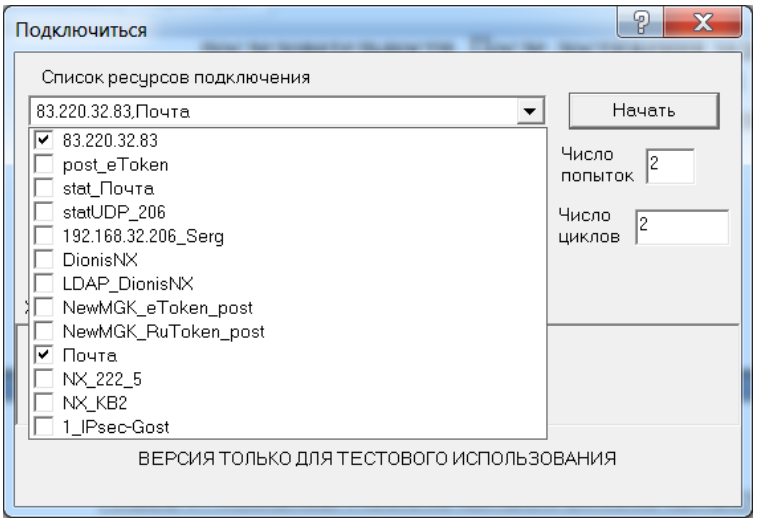


Рис. 82

Начать

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

Прервать

Кнопка **Прервать** становится доступной после того, как начнется процесс подключения, и позволяет процесс подключения прервать.

Настройка

Кнопка **Настройка** предназначена для проверки и, при необходимости, изменения списка ресурсов подключения и их реквизитов. По нажатию этой кнопки вызывается окно **Настройка** на вкладке **Общие** (Рис. 16, с. 33), т.е. действие кнопки аналогично вызову одноименной команды Главного меню приложения DiSec. По окончании работы с окном **Настройка** управление возвращается к окну **Подключиться** (Рис. 82), при этом выполняется коррекция параметров в соответствии со сделанными изменениями.

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.

Ход процесса подключения:

В секции под этим заголовком отображается процесс выполнения процедуры установления туннеля и результаты отдельных операций, из которых состоит эта процедура.

7.1.1 Выполнение процедуры подключения

Выполнение процедуры подключения необходимо начать с формирования списка ресурсов подключений из выпадающего списка **Список ресурсов подключения**, настроить параметры цикла (установить значения **Число попыток** и **Число циклов**) после чего нажать кнопку **Начать**. Дальнейшие действия пользователя и системы зависят от реквизитов выбранного ресурса.

В режиме соединения IPSEC-ФАКТОР после нажатия кнопки **Подключение** в окне **Начать** (Рис. 82) будет выдан запрос на установку ключевого носителя. В зависимости от указанного в реквизитах подключения типа ключевого носителя появится одно из сообщений, приведенных ниже.

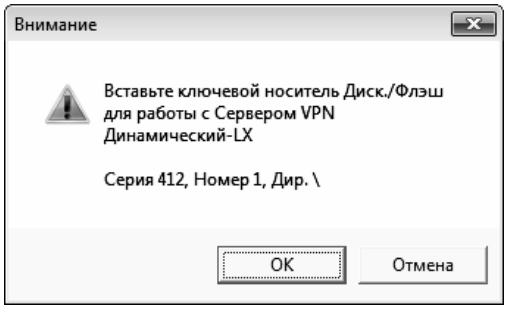


Рис. 83

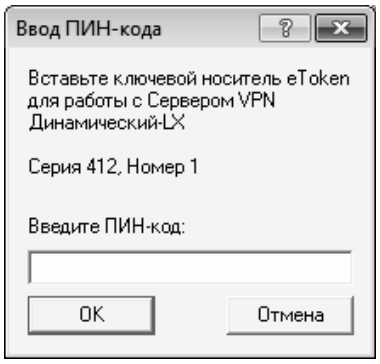


Рис. 84

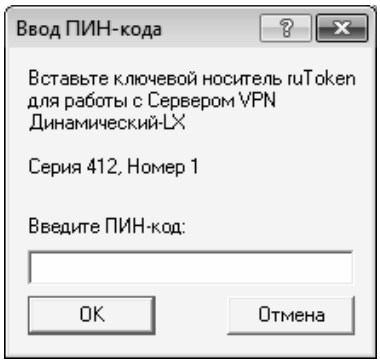


Рис. 85

В случае работы с ключевыми носителями ***eToken*** (Рис. 84) или ***ruToken*** (Рис. 85) необходимо ввести секретный код (ПИН-код). ПИН-код устанавливается во время формирования ключевого носителя и предоставляет дополнительную защиту от несанкционированного использования ключевых носителей.

> *Примечание.* Серия и номер ключей могут отсутствовать в данных сообщениях, если соответствующие данные не введены на этапе настройки реквизитов подключения (см. 6.3.4, с. 49).

Статический туннель. После ввода ключевой информации 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, в режиме соединения IPSEC-ФАКТОР DiSec получает от Сервера правила отбора). Согласованные параметры работы туннеля загружаются в драйвер DiSec. Обмен данными между Сервером VPN и DiSec выполняется по протоколу ISAKMP.

Процесс выполнения процедуры подключения в виде последовательных сообщений отражается в информационном окошке (нижняя части окна Рис. 82), там же будет выведено сообщение об ошибке, если она произойдет при выполнении соединения. Дополнительную информацию можно получить в окне **Диагностика** DiSec.

> *Примечание.* Диагностические сообщения сохраняются в оперативной памяти компьютера, их можно просмотреть и позднее до окончания сеанса работы с приложением DiSec с помощью команды Главного меню приложения DiSec **Диагностика** (раздел 10.1, с. 102).

После того как начнется процесс соединения, в окне **Подключиться** (Рис. 82) становится доступной кнопка **Прервать**. Она позволяет прервать процесс установления соединения, если он, например, сильно затянется из-за каких-то неполадок в сети.

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.

7.2 Подключение к IP-сети при использовании DialUP

Если в реквизитах подключения задано использование WINDOWS-ресурса удаленного доступа (**DialUP**), то перед установкой туннеля автоматически выполняется процедура дозвона и подключения к соответствующему серверу удаленного доступа.

> *Примечание. С*ервер удаленного доступа и Сервер VPN в общем случае не совпадают. Следовательно, имена (IP-адреса серверов) и имена пользователей (абонентов – в случае использования Сервера VPN в качестве сервера доступа) могут не совпадать.

Процедура дозвона и подключения к серверу удаленного доступа выполняется в соответствии с параметрами, указанными при настройке реквизитов подключения к защищенной сети (см. раздел 6.3, с. 38), а именно: выбирается указанный системный ресурс Удаленного подключения (Сетевые подключения) и выполняется его запуск с указанными именем и паролем пользователя. Если в процессе удаленного подключения произошла ошибка, то вся процедура заканчивается, а причины ее завершения отображаются в окне **Подключиться** и в окне **Диагностика** DiSec. В случае работы службы причины отказа можно увидеть в Журнале событий службы.

Если удаленное подключение, указанное в настройках, уже функционирует, то DiSec выполняет процедуру установки туннеля.

7.3 Команда Отключиться

Команда Главного меню приложения DiSec (Рис. 14) **Отключиться** становится доступной после того, как будет выполнено соединение хотя бы с одним Сервером VPN.

По команде **Отключиться** выполняется отсоединение от соответствующего Сервера VPN:

- выполняется процедура закрытия туннеля;
- драйвер DiSec возвращается в исходное состояние;
- связь с Сервером VPN корректно разрывается, подключение к IP-сети сохраняется.

Статический туннель на стороне Сервера VPN остается в рабочем состоянии.

8 Команда Состояние

Команда Главного меню приложения DiSec (Рис. 14) **Состояние** 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. 86).

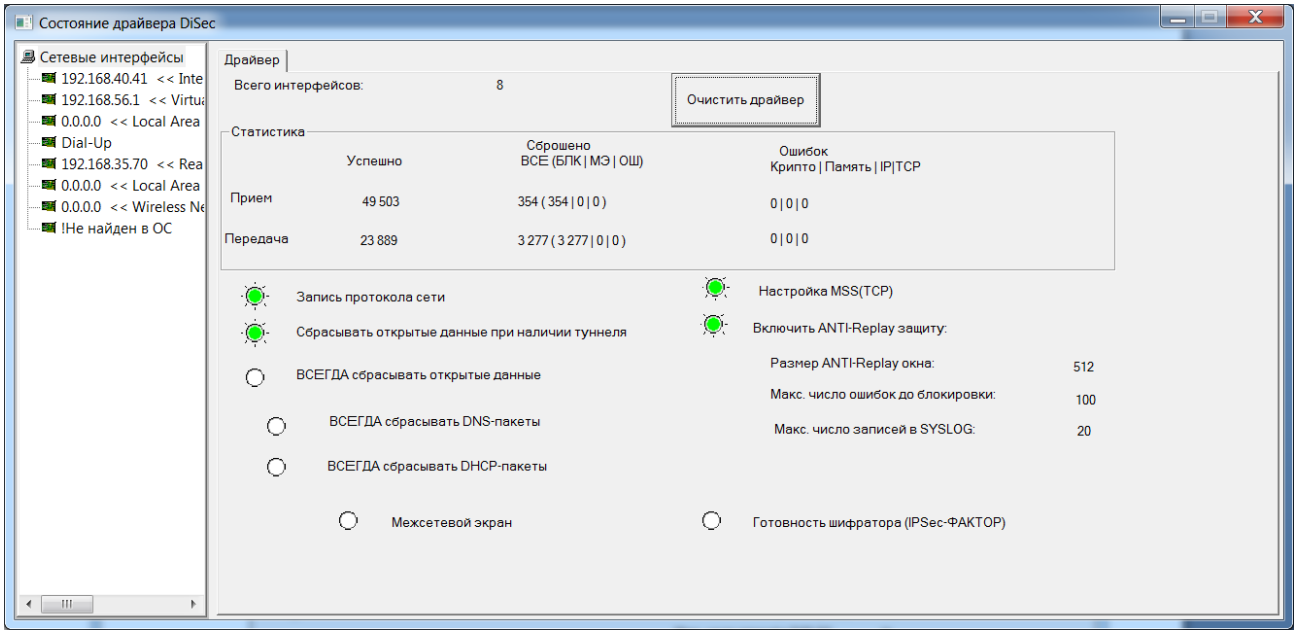


Рис. 86

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. Для интерфейсов локальной сети (Ethernet, WiFi) выводятся IP-адреса, для интерфейса службы Удаленного доступа WINDOWS (RAS) - название **Dial-UP**.

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** (Рис. 86).

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**.

Очистить драйвер

Кнопка **Очистить драйвер** может быть использована в случае аварийного завершения работы с туннелем, когда он не был закрыт средствами DiSec посредством команды **Отключиться**. В этом случае может оказаться, что в драйвере сохранились предыдущие настройки туннеля и новое соединение не устанавливается, и выдается сообщение о "пересечении" правил отбора, например, как показано на рисунке:

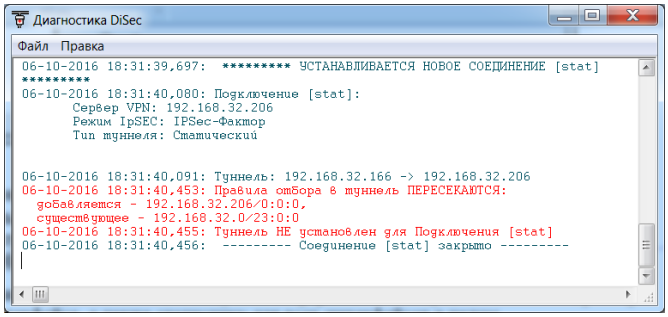


Рис. 87

Если пользователю точно известно, что другого туннеля не существует, он может воспользоваться кнопкой **Очистить драйвер**.

8.1 Вкладка Драйвер (Состояние драйвера DiSec)

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

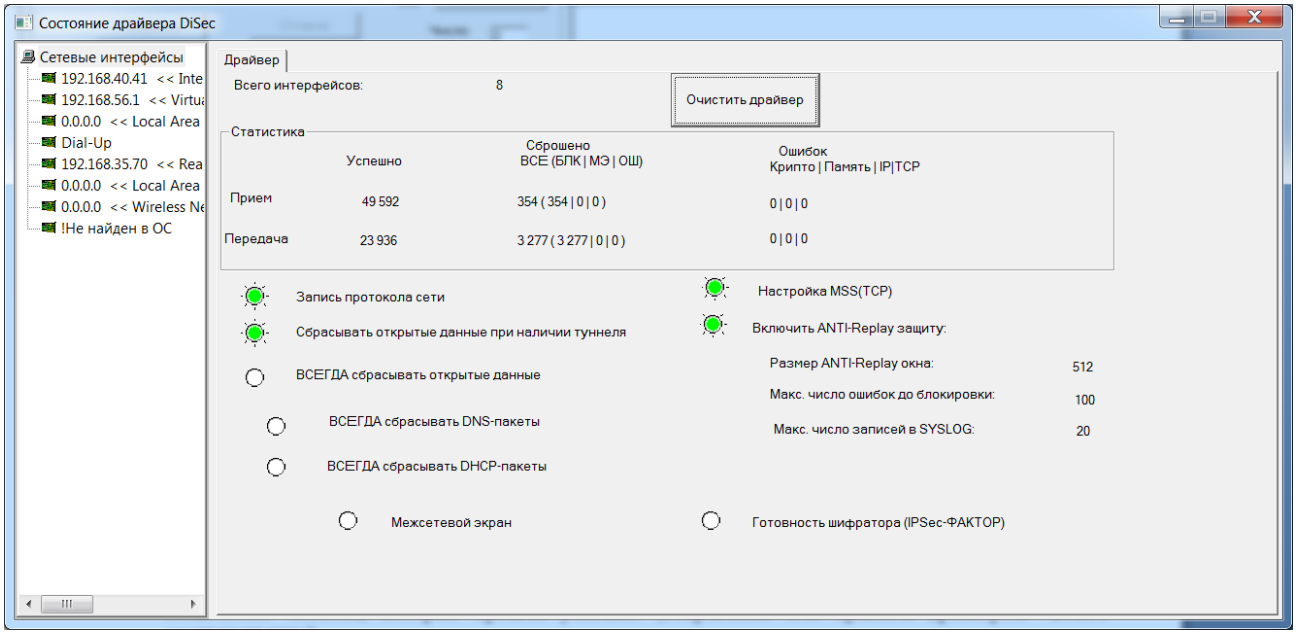


Рис. 88

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|МЭ|ОШ)

Количество пакетов, отвергнутых драйвером:

БЛК - не соответствующих правилам отбора в туннель и сброшенных драйвером DiSec в соответствии с настройкой блокировки открытых данных (см. п. 6.4.1.1, с. 69).

МЭ - отфильтрованных Межсетевым экраном

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-за 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.

8.2 Вкладка Интерфейс (Состояние драйвера DiSec)

Вкладка **Интерфейс** (Рис. 89) содержит параметры и информацию о текущем состоянии конкретного интерфейса.

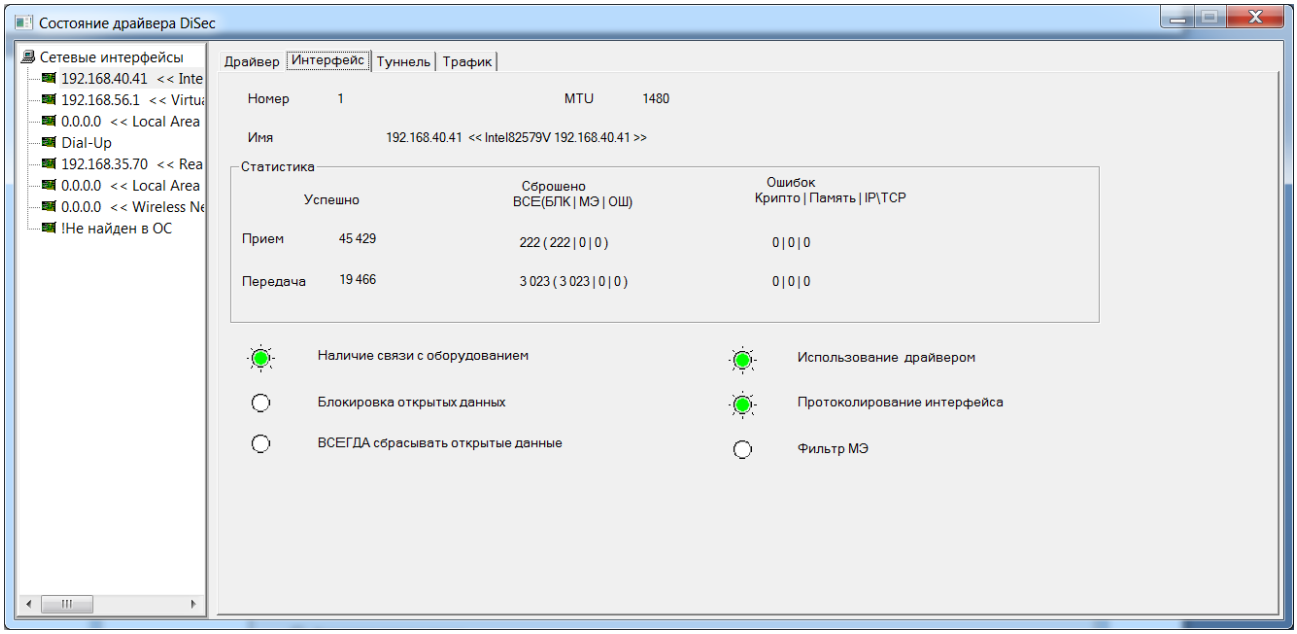


Рис. 89

Номер

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

Имя

Имя интерфейса, присвоенного драйвером DiSec в процессе регистрации интерфейсов (IP-адрес и имя для интерфейсов локальной сети и **DialUP** – для интерфейса удаленного доступа).

MTU

Значение **MTU** (Maximum-Transmission-Unit) совпадает с максимальным размером пакета (в байтах), который может быть передан через данный интерфейс. Для интерфейсов типа Ethernet оно обычно принимается равным 1514 байт.

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 четыре индикатора, отображающие режимы работы драйвера.

Наличие связи с оборудованием

Индикатор показывает состояние регистрации данного интерфейса в ОС WINDOWS и не относится к наличию или отсутствию физической связи компьютера с оборудованием передачи данных (например, подсоединение кабеля локальной сети). При наличии регистрации в ОС WINDOWS индикатор имеет зеленый цвет.

Использование драйвером

Зеленый цвет индикатора означает, что драйвером DiSec организован туннель по данному интерфейсу и/или задано протоколирование пакетов для данного интерфейса (см. раздел 6.4.1.2, с. 70).

Блокировка открытых данных

Индикатор имеет зеленый цвет, если прохождение открытых данных заблокировано соответствующей настройкой (см. п. 6.4.1.1, с. 69).

Протоколирование интерфейса

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

Фильтр МЭ

Индикатор имеет зеленый цвет, если для данного интерфейса сформирован хотя бы один фильтр (набор правил) (п. 6.4.1.5, с. 74).

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

8.3 Вкладка Туннель (Состояние драйвера DiSec)

Вкладка **Туннель** (Рис. 90) позволяет просмотреть текущее состояние параметров туннелей, установленных для данного интерфейса.

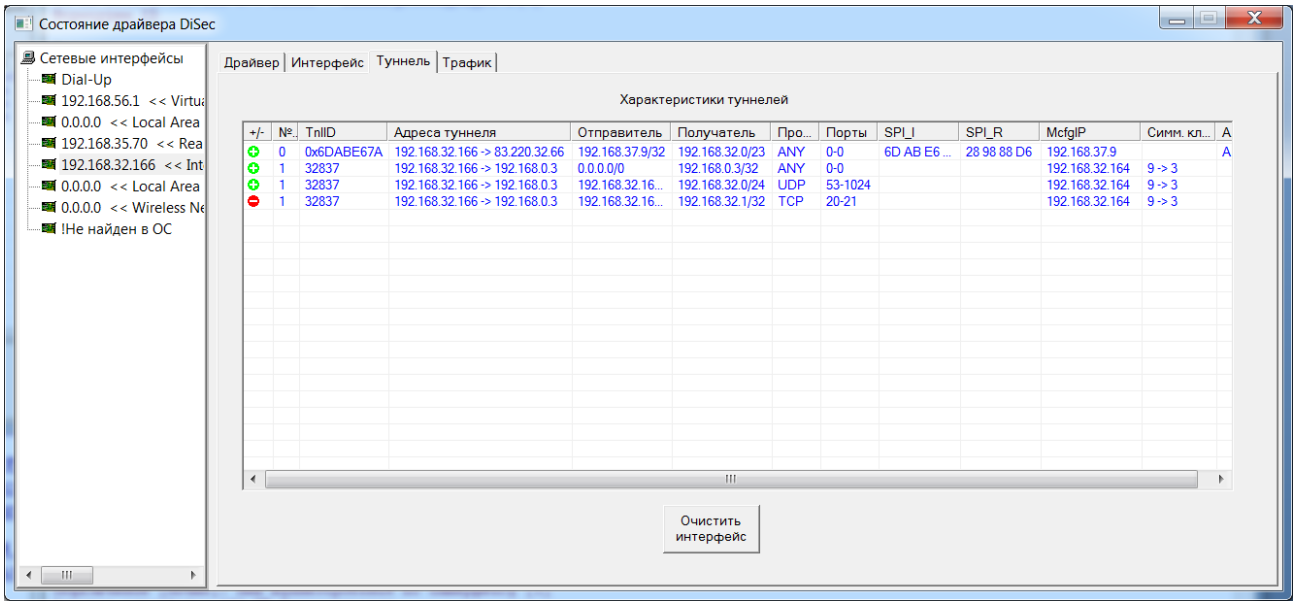


Рис. 90

В таблице **Характеристики туннеля** отображаются все активные в данный момент туннели, 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 **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 режима IPSEC-ГОСТ, или IP-адрес клиента при интеграции в удаленную сеть для режима IPSEC-ФАКТОР). При этом в самом 1-м столбце отображается признак разрешающего или запрещающего правила (для режима IPSEC-ГОСТ правила всегда разрешающие, поскольку соответствуют доступным защищенным ресурсам).

Столбцы **SPI_I** и **SPI_R** относятся только к режиму IPSEC-ГОСТ и идентифицируют активные 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.

Столбец **McfgIP** отображает "новый" подставляемый в сетевые пакеты IP-адрес (MODE_CFG для режима IPSEC-ГОСТ, или IP-адрес клиента при Интеграции в удаленную сеть для режима IPSEC-ФАКТОР).

Столбец **Симм. ключи** относится к режиму IPSEC-ФАКТОР, как к динамическим, так и к статическим туннелям. Первое значение соответствует локальному ключу, 2-е - ключу Сервера VPN. Для динамического

туннеля значение ключа Сервера VPN определяется в результате согласование туннеля по протоколу ISAKMP, а в случае статического туннеля - задается в настройках.

Последний столбец **A** - отображает состояние активности туннеля в режиме IPSEC-ГОСТ: активен или заблокирован в результате контроля целостности пакетов - превышено заданное при настройке политики ESP допустимое число искаженных, т.е. имеющих неверную имитовставку, туннелированных сетевых пакетов (Integrity Fail).

Под таблицей находится кнопка **Очистить интерфейс.** Применение этой кнопки аналогично применению кнопке **Очистить драйвер**. Отличие состоит в том, что в настоящем случае удаляются настройки только текущего интерфейса.

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

8.4 Вкладка Трафик (Состояние драйвера DiSec)

На данной вкладке приведены дополнительные параметры и статистические данные туннеля, такие как тип инкапсуляции, режим ESP и время жизни SA ESP (для режима IPSEC-ГОСТ). В первых двух столбцах дублируются номер подключения и идентификатор туннеля.

В столбце **Инкапсуляция** отображается протокол туннелирования и номера используемых портов для UDP-инкапсуляции.

В столбце **ESP-режим** отображается либо слово "*Транспортный*", либо "*Туннельный*".

В столбце **MSS-TCP** отображается текущее значение MSS для TCP протокола. Данное значение либо настраивается пользователем, либо вычисляется приложением (службой) DiSec.

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 IPSEC-ФАКТОР значение отсутствует).

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

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.

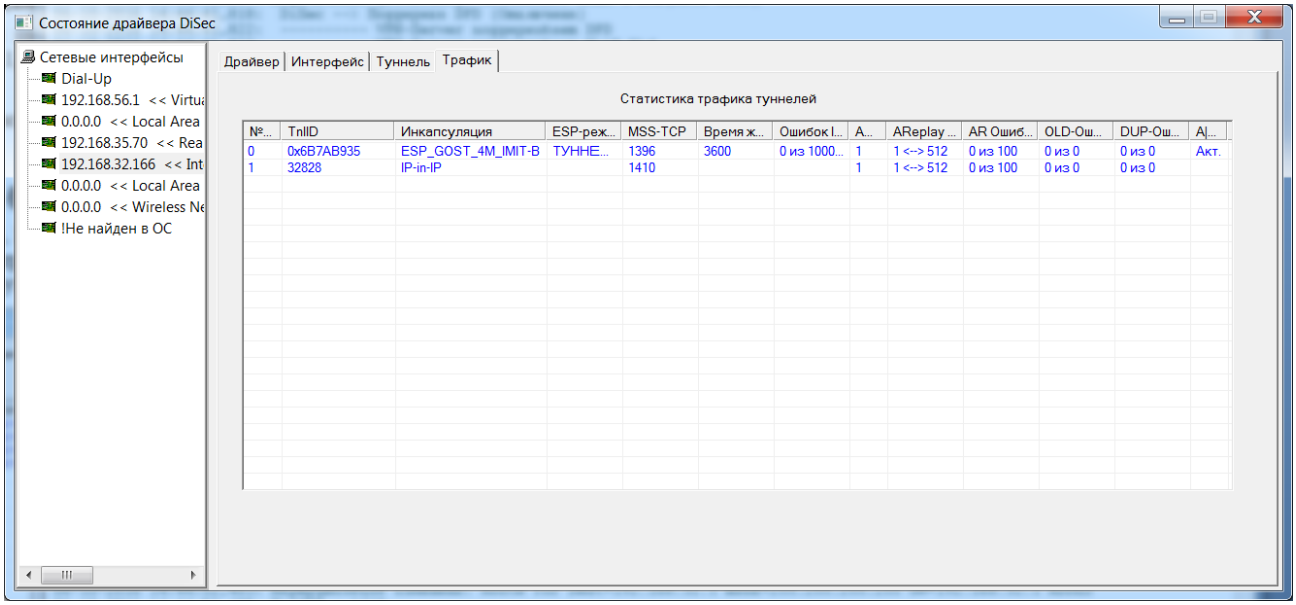


Рис. 91

Для статического туннеля с UDP-инкапсуляцией с портами *450* окно имеет вид:

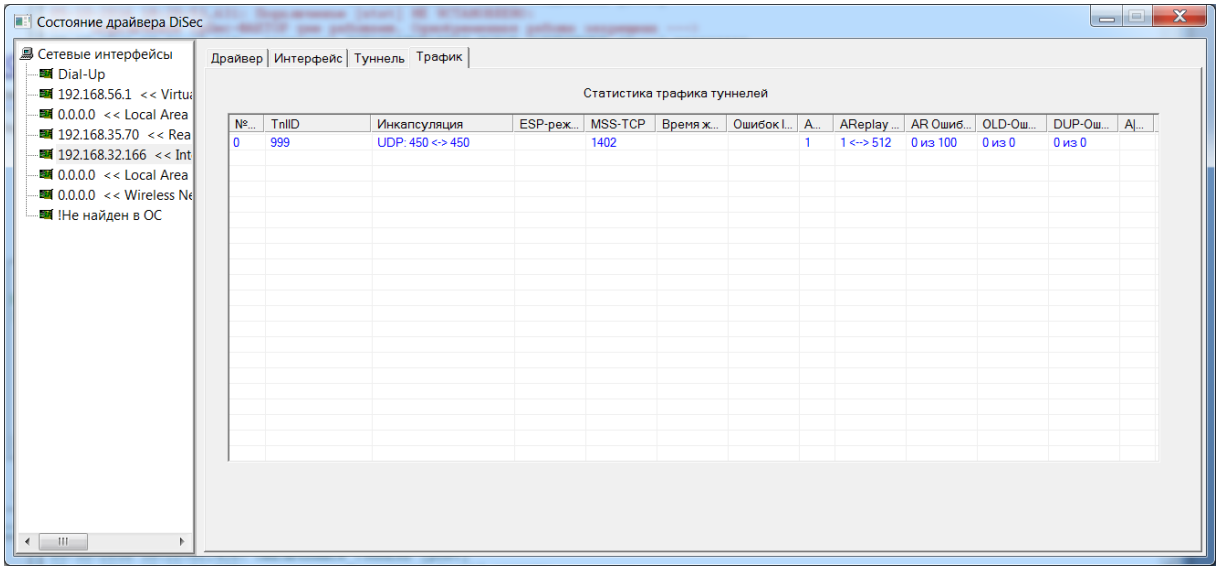


Рис. 92

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

9 Команда Тестирование

Команда Главного меню приложения DiSec (Рис. 14) **Тестирование** предназначена для проверки функционирования динамического туннеля, а также анализа состояния IP-компонента WINDOWS. Команда позволяет проверить правильность настройки и функционирования службы DiSecSrv.

Окно **Тестирование** состоит из нескольких вкладок, позволяющих выполнить и наглядно представить результаты проверок отдельных компонентов и функций.

9.1 Вкладка Ping (Тестирование)

Вкладка **Ping** (Рис. 93) предоставляет возможность выполнить стандартную тестовую процедуру **Ping**, которая позволяет проверить доступность с данного компьютера любых сетевых устройств IP-сети при помощи пакетов сетевого протокола ICMP. При этом проверяется настройка IP-компонента WINDOWS, драйвера DiSec, а также работа динамического туннеля, если он установлен между клиентской станцией и Сервером VPN.

Тестовая процедура **Ping** выполняется в соответствии с параметрами, введенными в верхней части вкладки. Результат тестирования отражается в окне в нижней части вкладки. Сначала выводится строка с IP-адресом проверяемого узла, а затем отчет о полученных ответных пакетах от тестируемого узла - по одной строке на каждый ответ. В случае возникновения ошибок выводятся диагностические сообщения.

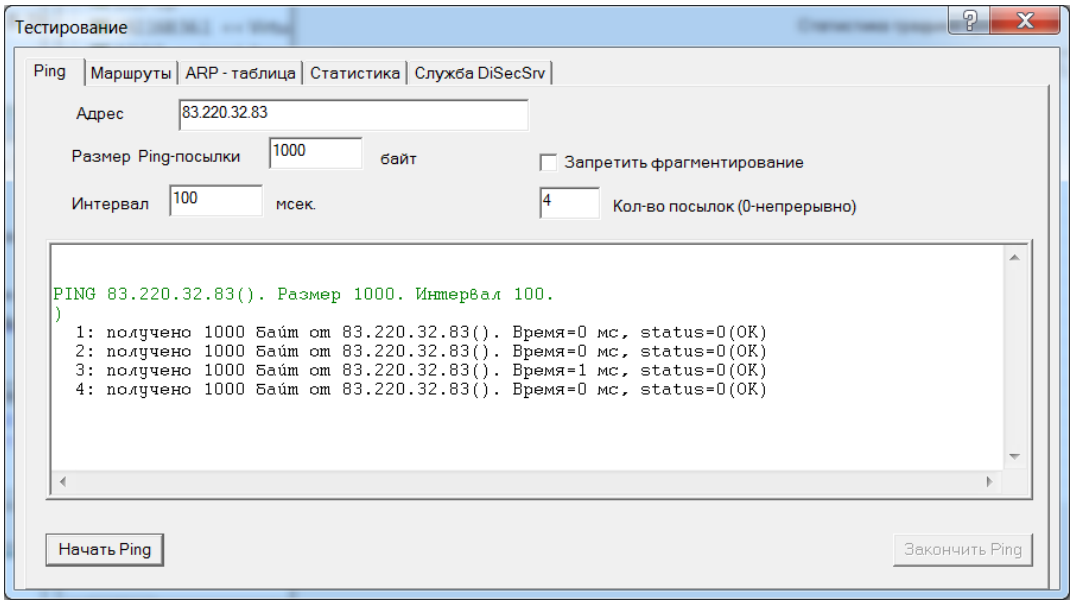


Рис. 93

Адрес

В поле следует задать IP-адрес или доменное имя проверяемого узла в сети Интернет.

Размер Ping-посылки

Параметр позволяет установить нестандартный размер тестовой посылки **Ping** (больше 32 байт), если требуется проверить прохождение длинных пакетов.

Интервал

В поле можно указать интервал следования посылок пакетов **Ping** в миллисекундах. По умолчанию установлено значение 1000, т.е. посылки будут следовать с интервалом одна секунда.

Кол-во посылок(0-Непрерывно)

В поле можно указать количество посылок пакетов **Ping**, если не указано будет отправлено пять посылок; если указан 0 - посылка будет выполняться до тех пор, пока не будет нажата кнопка **Закончить Ping**.

Запретить фрагментирование

Флажок используется для определения максимального размера пакета, проходящего данный маршрут, на пути которого могут использоваться "нестандартные" сетевые устройства, имеющие ограничения на

размер пакетов. Результаты этого тестирования могут быть использованы при настройках драйвера для таких нестандартных устройств (см. п. 6.4.1.2, стр. 70).

Две кнопки под окном с результатами тестирования:

Начать Ping - нажатие кнопки запускает процедуру отправки Ping-пакетов в соответствии с установленными параметрами;

Закончить Ping - нажатие кнопки останавливает процедуру отправки Ping-пакетов.

9.2 Вкладка Маршруты (Тестирование)

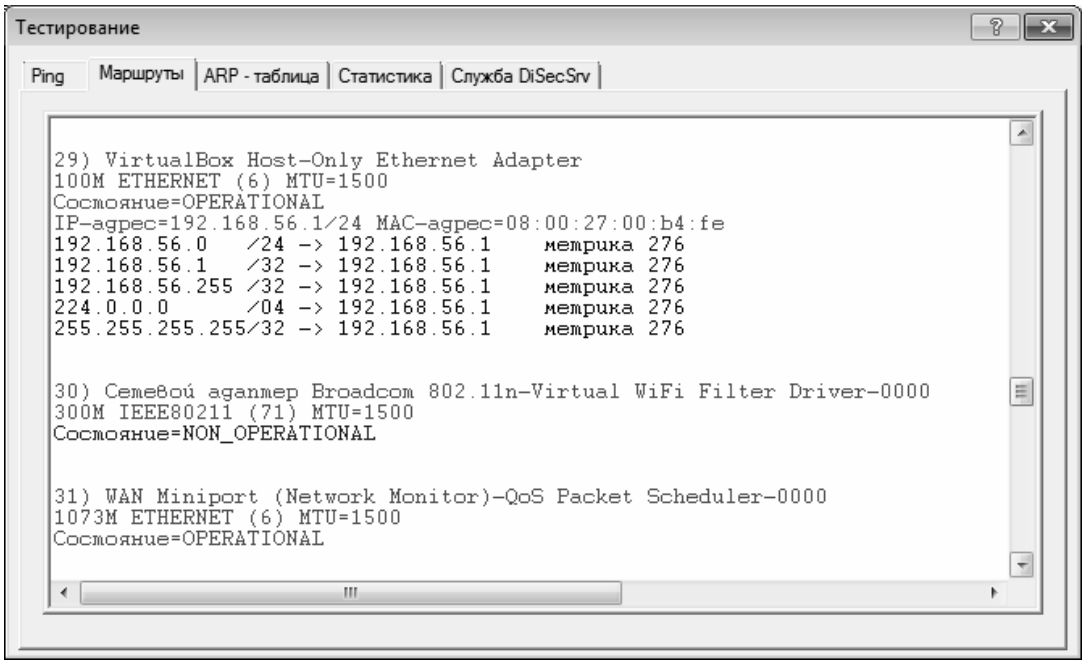


Рис. 94

С помощью вкладки **Маршруты** (Рис. 94) пользователь может просмотреть текущее состояние интерфейсов и маршрутных таблиц IP-компонента WINDOWS.

Список текущих аппаратно-программных интерфейсов устройства пользователя и текущих маршрутных таблиц выводится на экран в следующем формате:

- зеленым цветом - наименование интерфейса;
- синим цветом - дополнительная информация об интерфейсе, IP-адрес и MAC-адрес (если он есть);
- черным цветом - маршрутные таблицы.

9.3 Вкладка ARP-таблица (Тестирование)

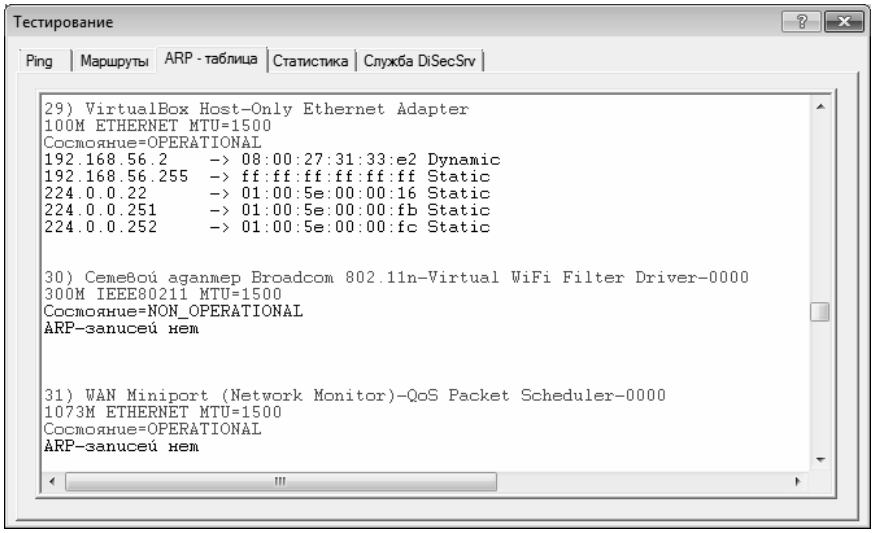


Рис. 95

С помощью вкладки **ARP-таблица** (Рис. 95) пользователь может просмотреть текущее состояние интерфейсов и ARP-таблиц IP-компонента WINDOWS (соответствие IP и MAC-адресов сетевых интерфейсов).

Список аппаратно-программных интерфейсов устройства пользователя и текущих ARP-таблиц выводится на экран в следующем формате:

- зеленым цветом - наименование интерфейса;
- синим цветом - дополнительная информация об интерфейсе и IP-адрес;
- черным цветом - ARP-таблицы.

9.4 Вкладка Статистика (Тестирование)

Вкладка **Статистика** позволяет просмотреть данные статистики раздельно по протоколам TCP (Рис. 97), UDP (Рис. 99), IP (Рис. 100) и ICMP (Рис. 101).

Нажатие кнопки с названием протокола приводит к выводу на экран соответствующей выбранному протоколу информации. Информация, выводимая для разных протоколов, различна. Для протокола, кроме данных статистики, выводится список всех текущих соединений по этому протоколу.

По таблице о UDP-сокетах можно определить наличие активности по портам, используемым DiSec (*500* и *4500*).

Повторное нажатие кнопки вызывает обновление статистики по данному протоколу.

Информация о TCP-соединениях

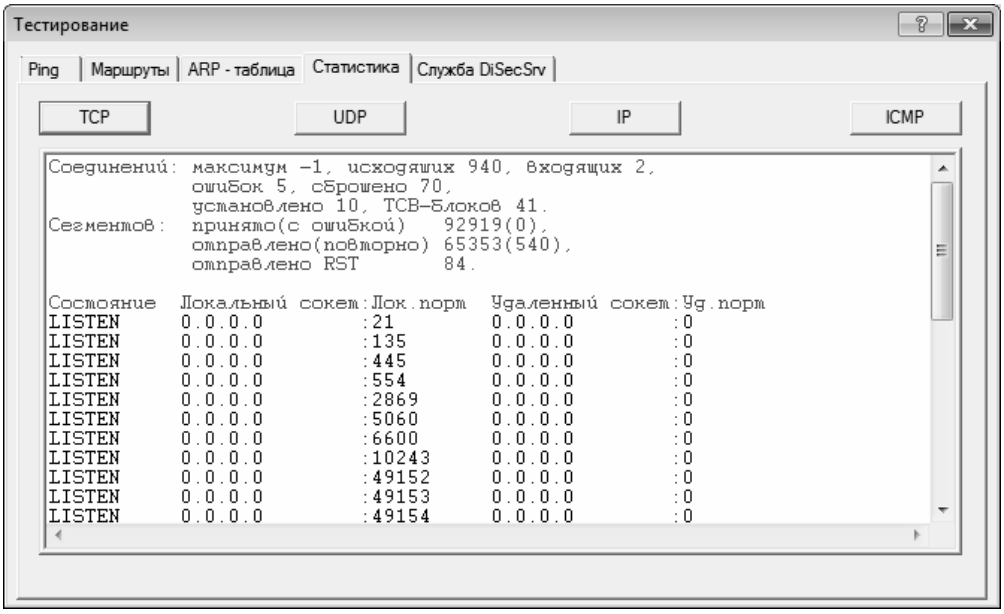


Рис. 96

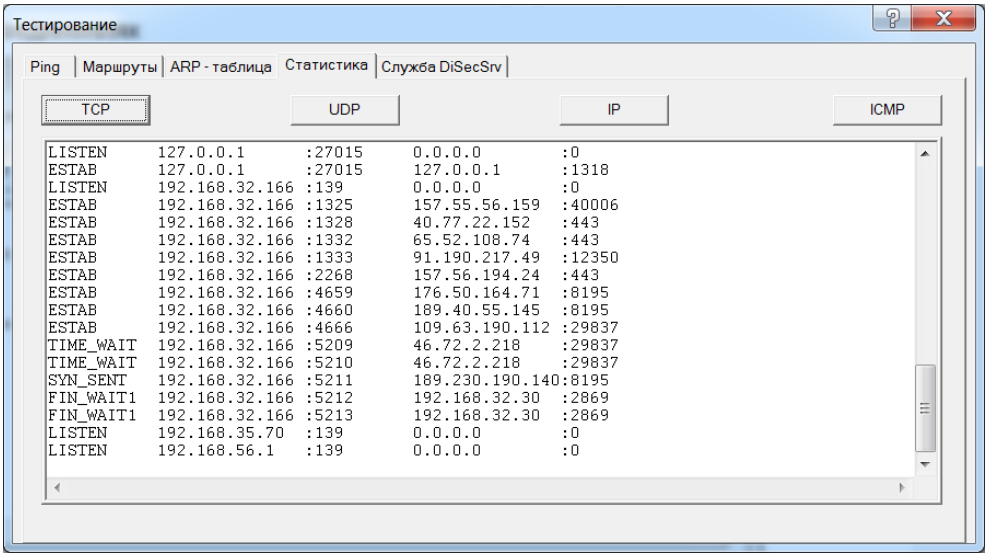


Рис. 97

Информация о UDP-сокетах

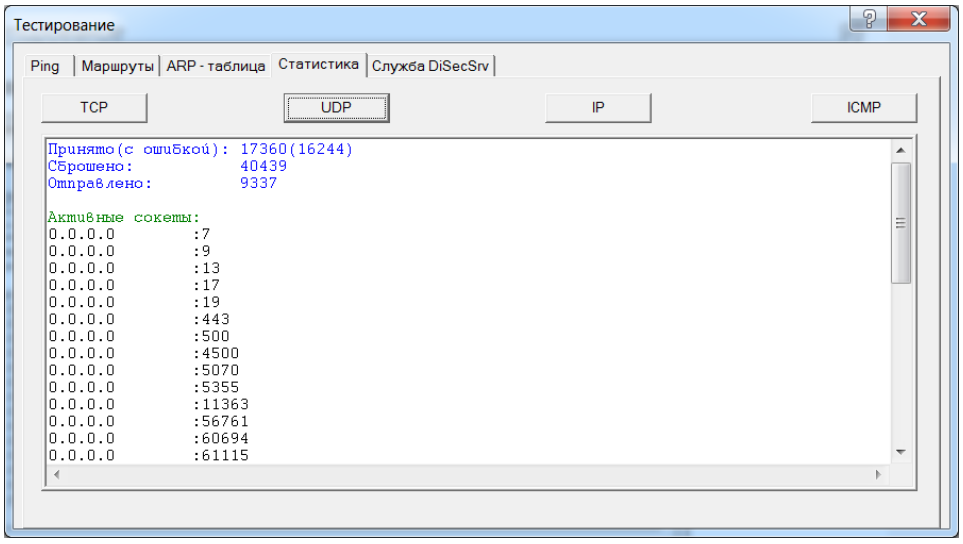


Рис. 98

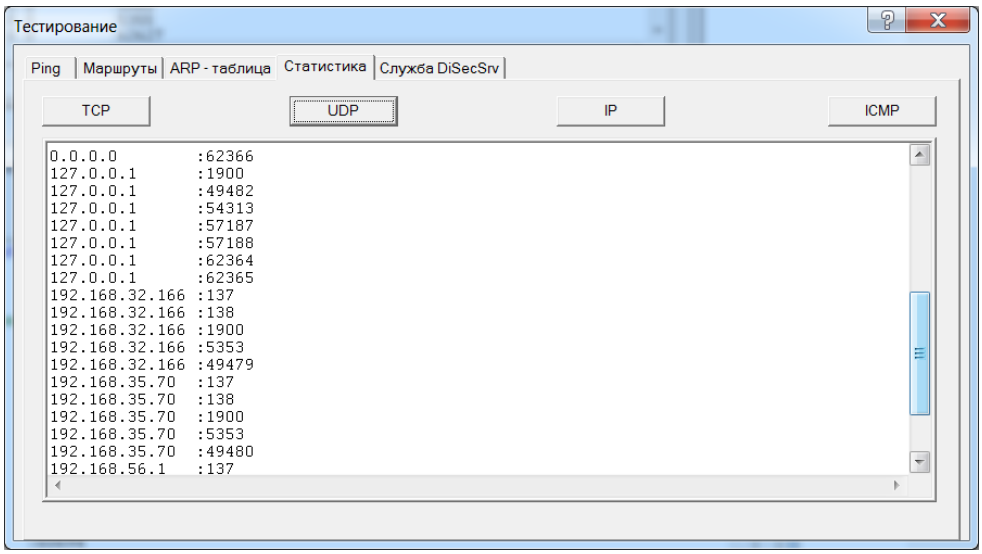


Рис. 99

Информация об IP-соединениях

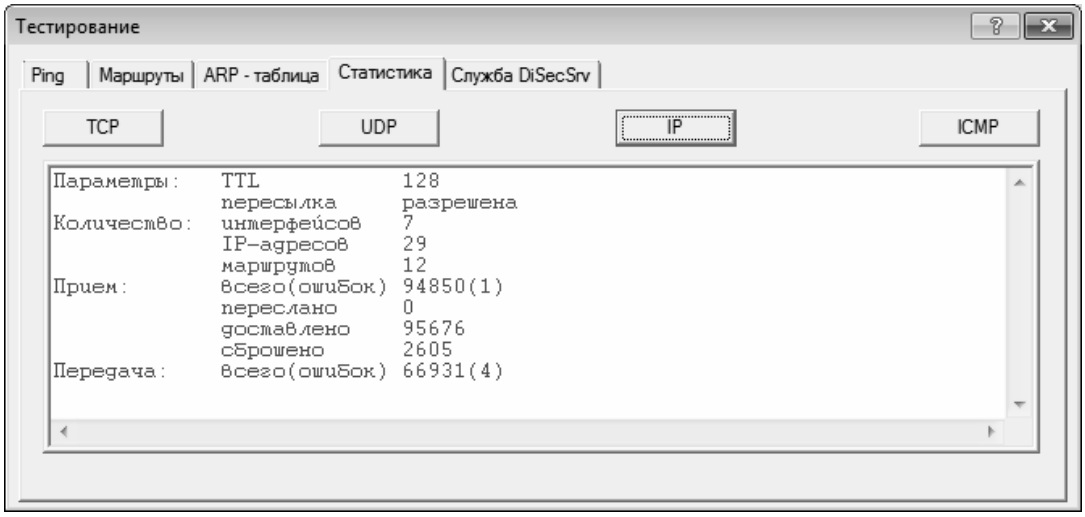


Рис. 100

Информация об ICMP-сообщениях

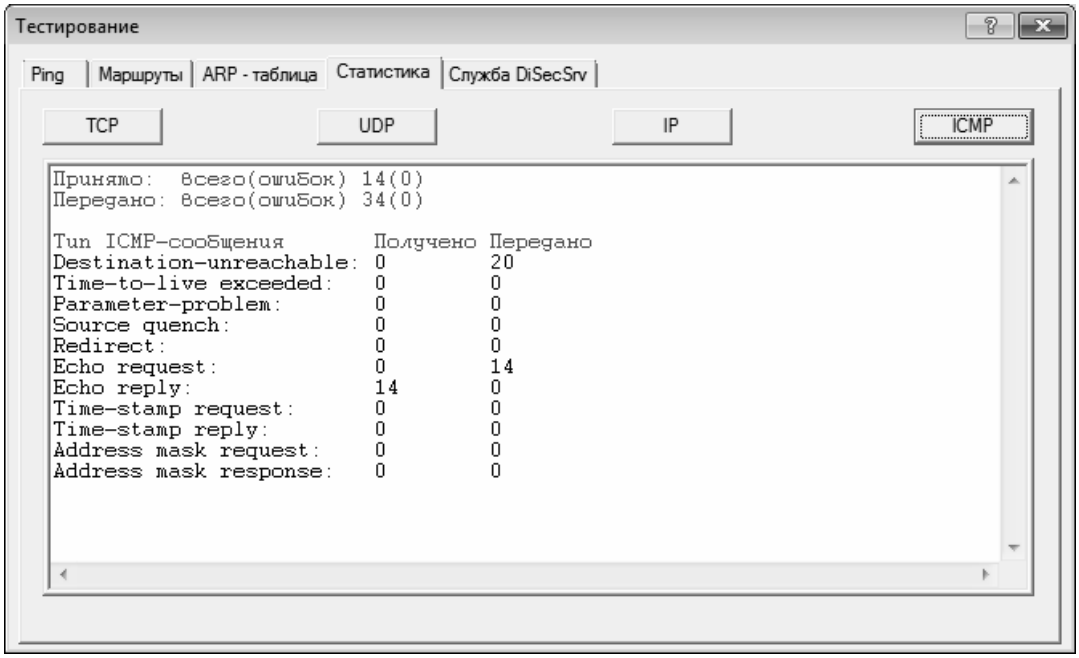


Рис. 101

9.5 Вкладка Служба DiSecSrv (Тестирование)

Вкладка **`Служба DiSecSrv`** предназначена для тестирования настроек и функционирования службы и позволяет определить, в каком состоянии находится служба DiSecSrv, а также получить информацию о ее текущих настройках (Рис. 102, **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**).

На вкладке расположены кнопки для запуска (**`Старт`**), останова (**`Стоп`**) и получения информации о состоянии и параметрах настройки (**`Состояние`**) службы.

Диагностические сообщения, выдаваемые в процессе запуска и останова службы, также записываются в журнал событий службы **`DiSecSrv.log`**, который можно просмотреть с помощью команды **`Журналы`** Главного меню приложения DiSec (см. раздел 10, с. 102).

> *Примечание.* Тестирование службы DiSecSrv может быть выполнено только пользователем, обладающим правами администратора WINDOWS. При попытке пользователя, не

обладающего правами администратора, выполнить какие-либо действия на этой вкладке будет выдано сообщение об отсутствии прав доступа.

При выходе из окна **Тестирование** во время работы службы DiSecSrv выполняется ее автоматический останов.

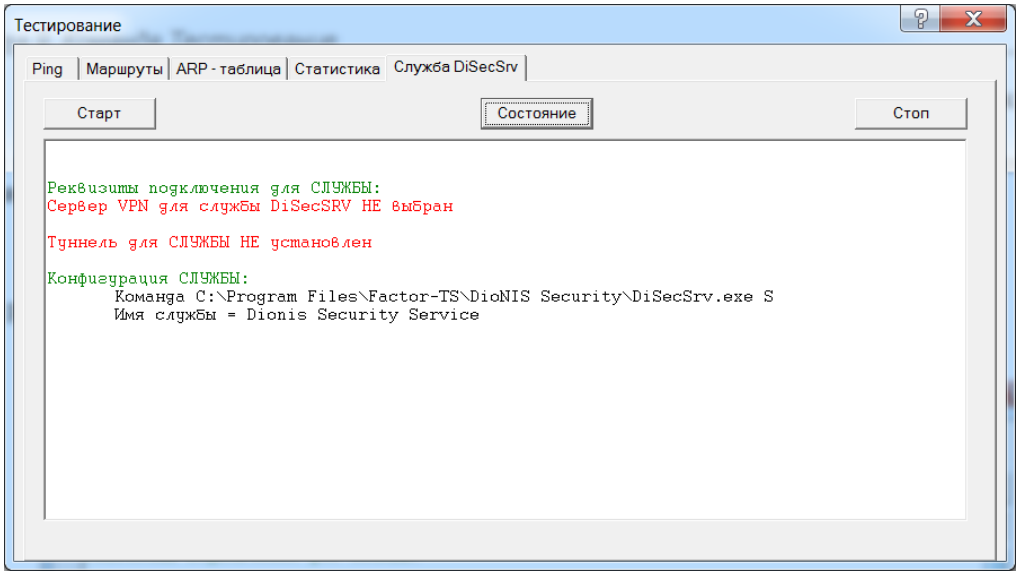


Рис. 102

Для режима IPSEC-ФАКТОР состояние службы отображается следующим образом (Рис. 103).

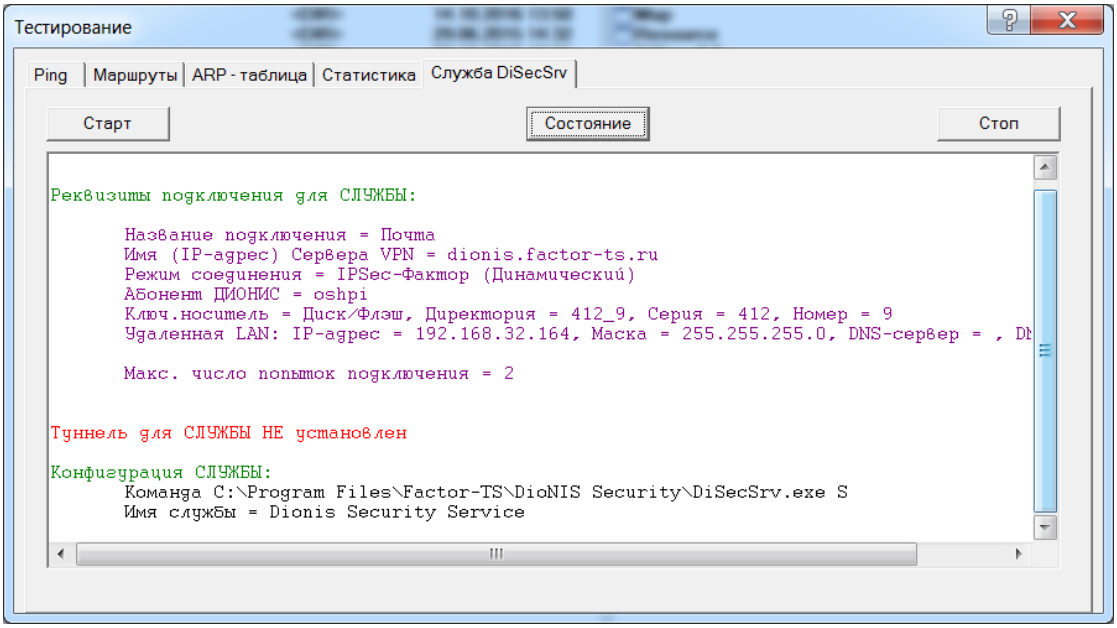


Рис. 103

Для режима IPSEC-ГОСТ состояние службы отображается следующим образом (Рис. 104).

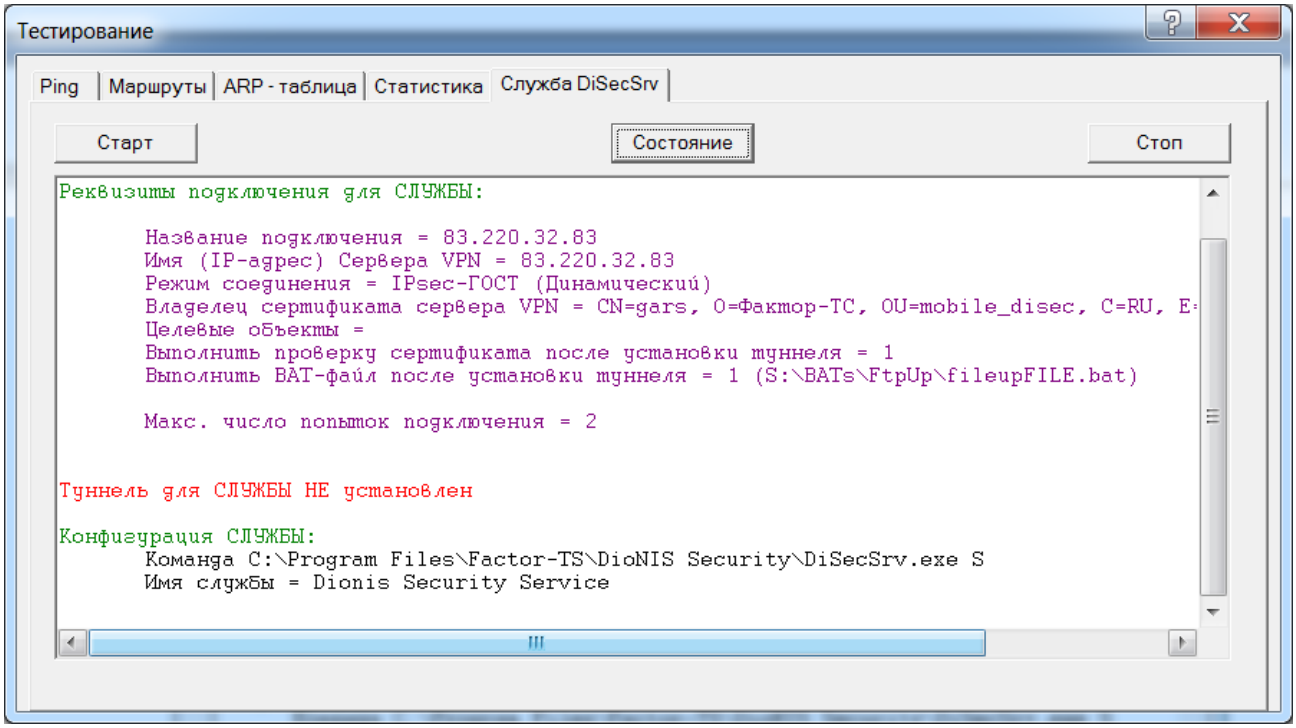


Рис. 104

Для работы службы могут быть выбраны несколько подключений (цикл), при этом переход к установке следующего подключения выполняется в случае неудачи предыдущего. Состояние настройки службы в этом случае выглядит, как показано на Рис. 105.

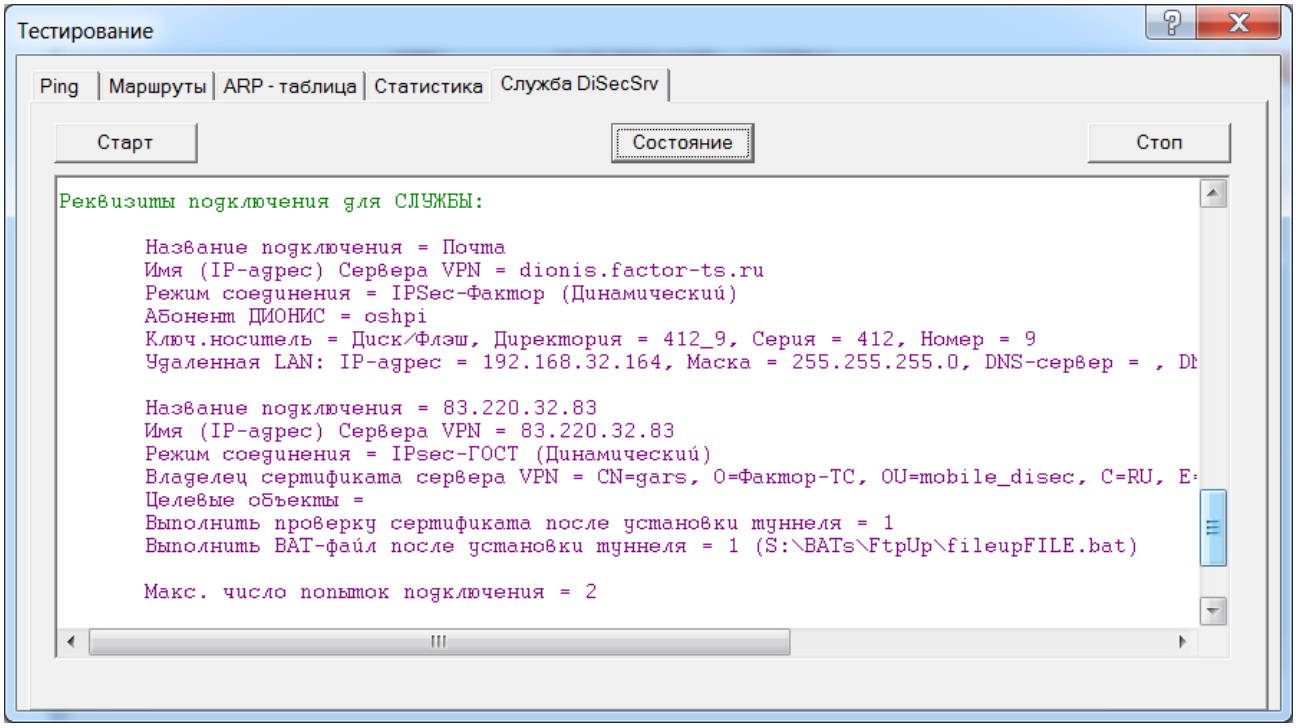


Рис. 105

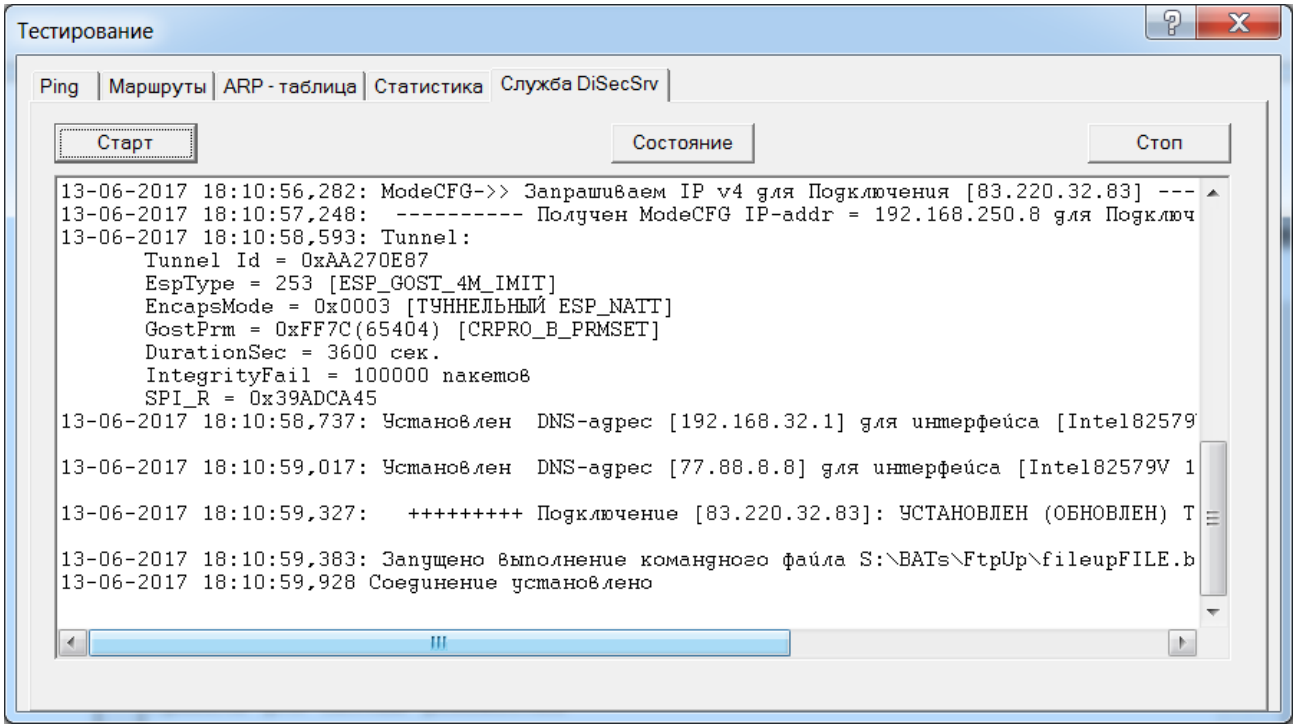

Тестирование
Ping
Маршруты
ARP - таблица
Статистика
Служба DiSecSrv
Старт
Состояние
Стоп
13-06-2017 18:10:56,282: ModeCFG->> Запрашиваем IP v4 для Подключения [83.220.32.83] ---
13-06-2017 18:10:57,248: ---------- Получен ModeCFG IP-addr = 192.168.250.8 для Подключ
13-06-2017 18:10:58,593: Tunnel:
Tunnel Id = 0xAA270E87
EspType = 253 [ESP_GOST_4M_IMIT]
EncapsMode = 0x0003 [ТУННЕЛЬНЫЙ ESP_NATT]
GostPrm = 0xFF7C(65404) [CRPRO_B_PRMSET]
DurationSec = 3600 сек.
IntegrityFail = 100000 пакетов
SPI_R = 0x39ADCA45
13-06-2017 18:10:58,737: Установлен DNS-адрес [192.168.32.1] для интерфейса [Intel82579
13-06-2017 18:10:59,017: Установлен DNS-адрес [77.88.8.8] для интерфейса [Intel82579V 1
13-06-2017 18:10:59,327: +++++++++ Подключение [83.220.32.83]: УСТАНОВЛЕН (ОБНОВЛЕН) Т
13-06-2017 18:10:59,383: Запущено выполнение командного файла S:\BATs\FtpUp\fileupFILE.b
13-06-2017 18:10:59,928 Соединение установлено

Рис. 106

10 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** (раздел 10.1, с. 102) и **Протокол Сети** (раздел 10.3, с. 104), либо при нарушении регламента безопасности в Журнале работы DiSec (раздел 10.1, с. 102).

10.1 Команда Диагностика

Активизация команды Главного меню приложения DiSec (Рис. 14) **Диагностика** 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 (Рис. 107).

> *Примечание* - Такое же окно выводится на экран при организации динамического туннеля при установке флажка **Выводить окно диагностических сообщений** в окне **Подключиться** (см. раздел 7.1, с. 84).

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 **Diagnostika**;
- команды меню **Правка** позволяют найти нужный фрагмент текста, выделить его и скопировать в другое приложение, например, в стандартный редактор текстовых файлов NotePad.

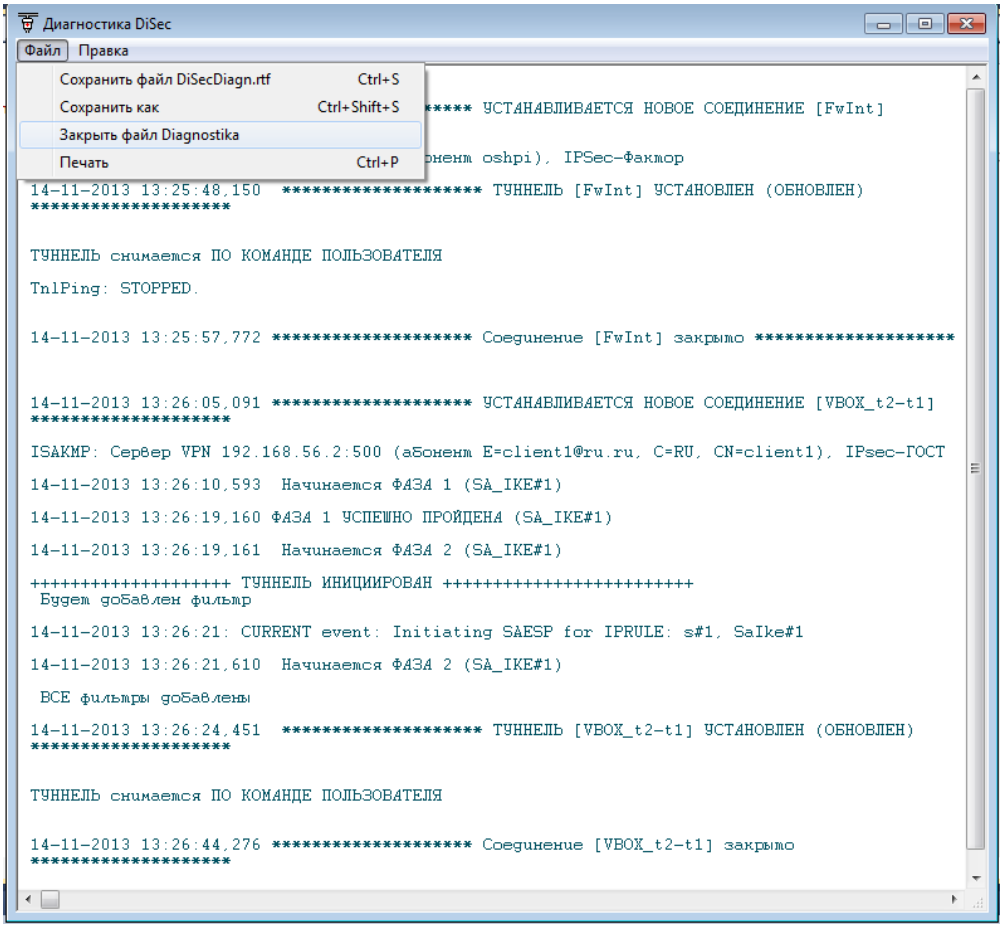


Рис. 107

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.

10.2 Команда Журналы

Команда Главного меню приложения DiSec (Рис. 14) **Журналы** позволяет просмотреть на экране журнал работы приложения DiSec , журнал работы службы DiSecSrv и журнал вспомогательной службы DiSecIsm.

В журналы записываются основные события, происходящие в процессе работы, в том числе изменение настроек межсетевого экрана.

Журналы представляют собой текстовые файлы и хранятся на диске в директории установки программы в одном или нескольких файлах в зависимости от настройки (см. п. 6.1.2, с. 34).

Вид журнала на экране может быть, например, таким (Рис. 108):

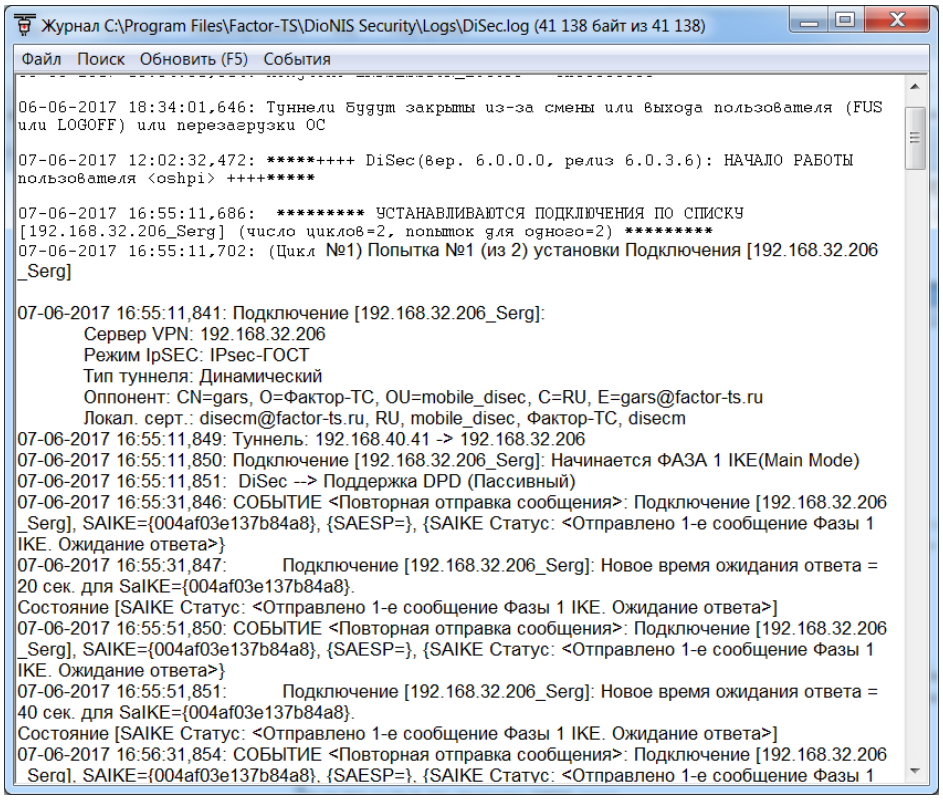


Рис. 108

Журнал службы DiSecIsm содержит информацию, которая может понадобиться разработчикам ПО DiSec для выяснения причин неработоспособности.

В командной строке окна находятся команды навигации по журналам.

Файл

Команда **Файл** служит для переключения между файлами, содержащими журналы работы приложения DiSec, службы DiSecSrv и службы DiSecIsm. 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 (см. Рис. 109).

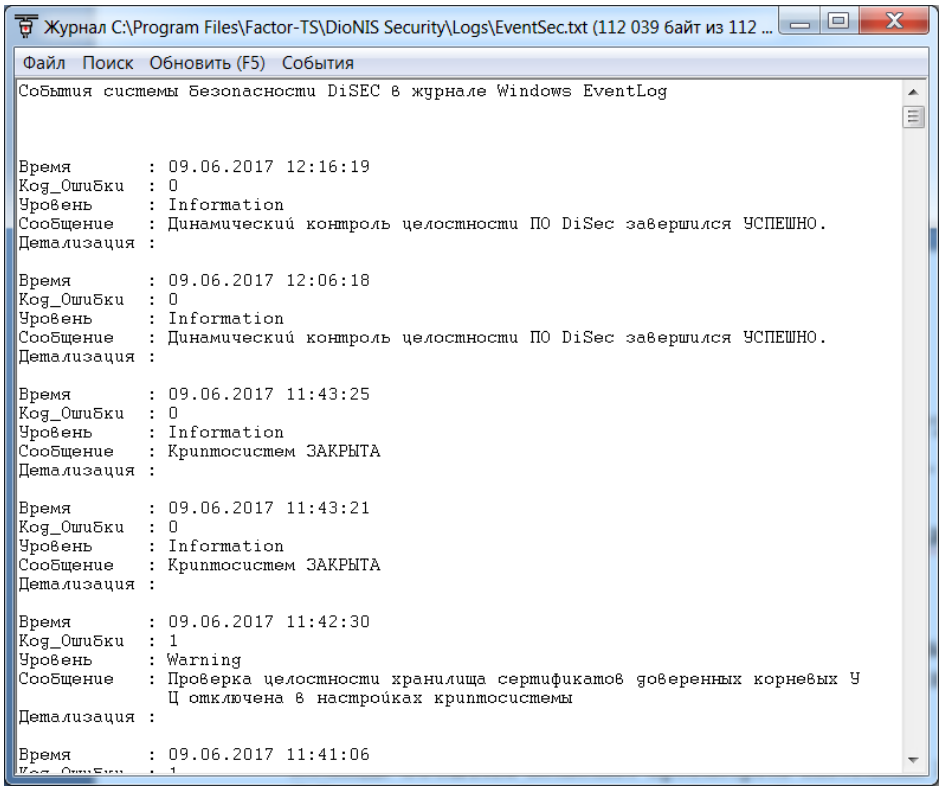


Рис. 109

10.3 Команда Протокол сети

Команда Главного меню приложения DiSec (Рис. 14) **Протокол сети** позволяет просмотреть на экране файл, содержащий протокол сетевой активности.

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 6.4.1.2, с. 70).

В верхней строке после названия окна (Рис. 110) 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**.

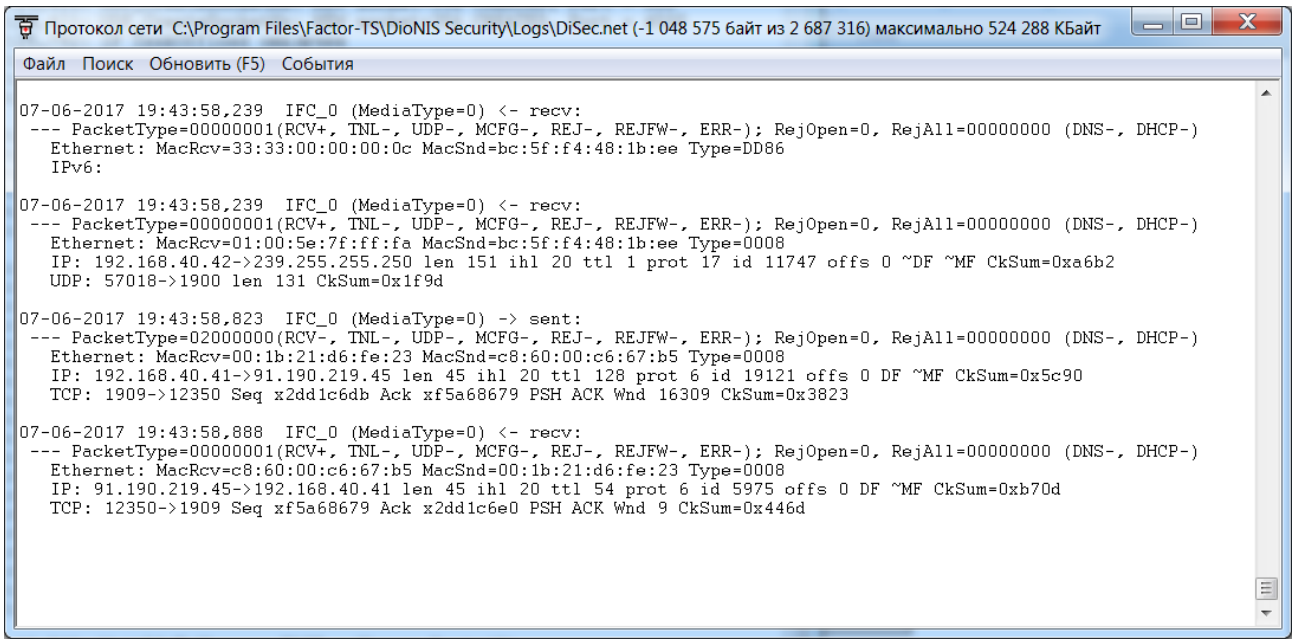


Рис. 110

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 (см. Рис. 111).

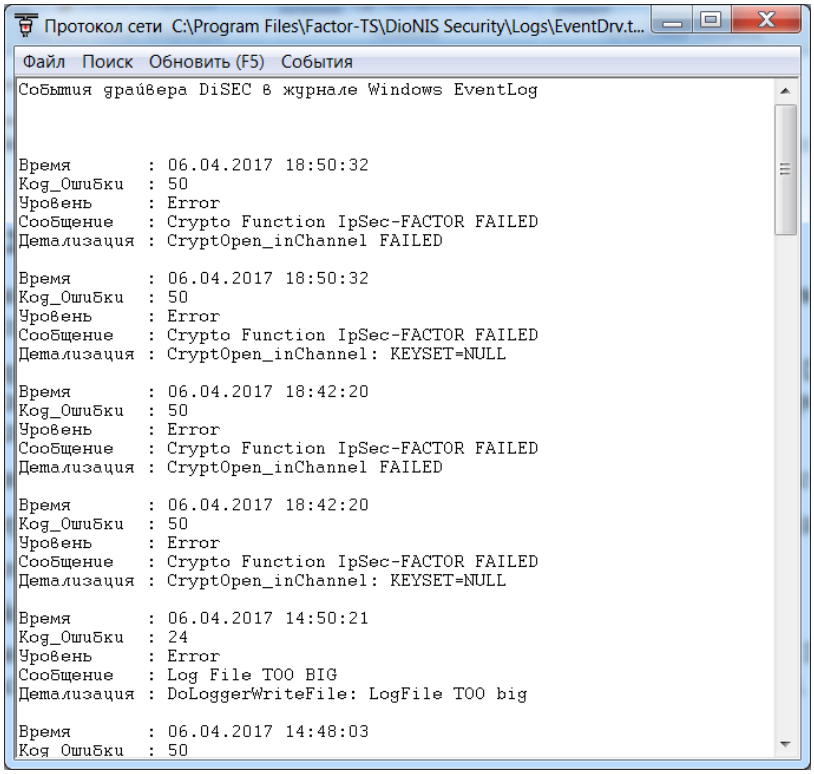


Рис. 111

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".

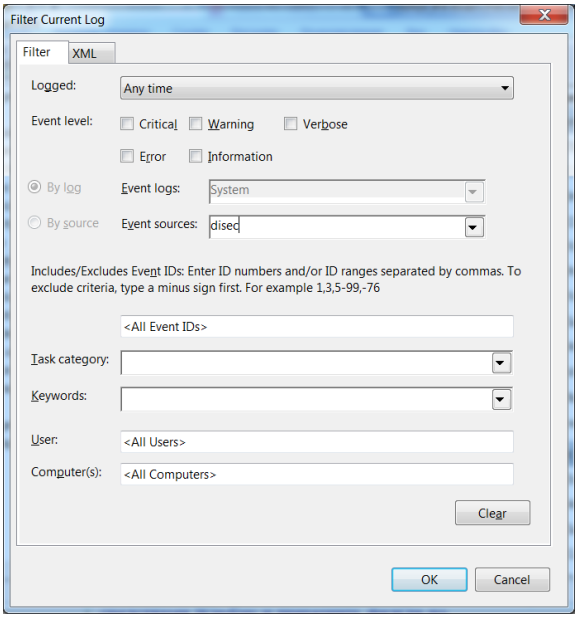


Рис. 112

На экране останутся сообщения драйвера DiSec, например, как показано на Рис. 113.

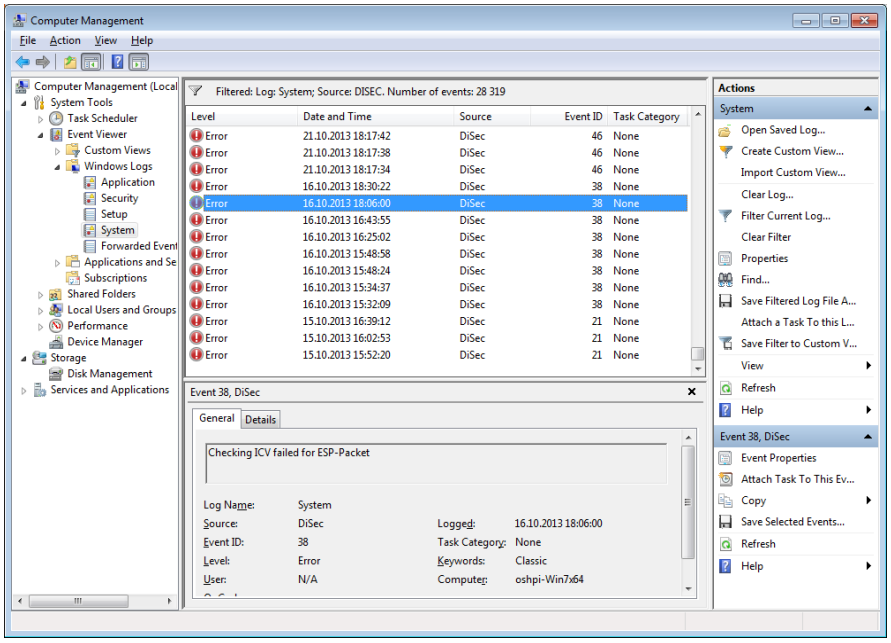


Рис. 113

Более подробная информация имеет вид:

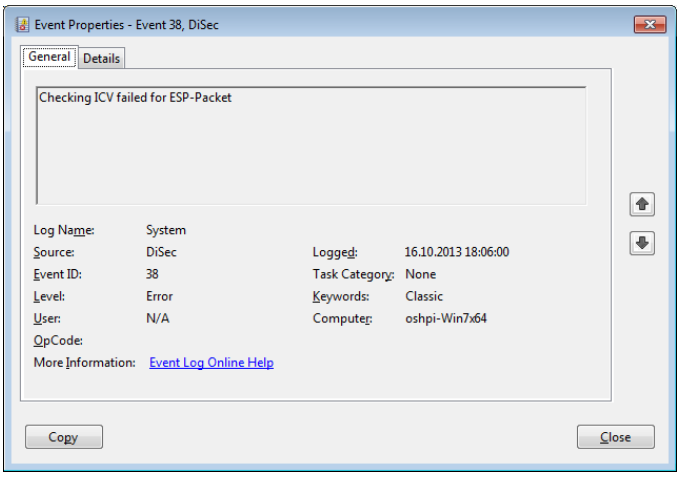


Рис. 114

11 Справочная информация

11.1 Справка

Приложение DiSec снабжено стандартной для программ под управлением WINDOWS справочной подсистемой, вызываемой по команде Главного меню приложения DiSec (Рис. 14) **Справка**. 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**.

11.2 О программе

По команде Главного меню приложения DiSec (Рис. 14) **О программе** на экран выводится краткая информация о версии и компонентах ПО DiSec, а также о фирме-разработчике.

12 Команда Выход

По команде Главного меню приложения DiSec (Рис. 14) **Выход** выполняются следующие действия:

- разрывается подключение к защищенной сети, если оно было установлено из приложения;
- 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.

13 Приложение 1. Функциональные возможности DiSec версии 6.0

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	- криптомаршрутизатор **DioNIS TS/FW**, **DioNIS-LXM** - 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 WiFi (статический и динамический IP-адрес), мобильные широкополосные модемы GSM
Режимы реализации IPSec	- IPSec-Фактор (ISAKMP) - IPSec-ГОСТ (IKE v1)
Количество виртуальных каналов (подключений)	**IPSec-Фактор:** один **IPSec-ГОСТ:** один
Тип туннеля (по методу организации)	**IPSec-Фактор:** динамический, статический (с настройками правил отбора и выбором типа инкапсуляции). **IPSec-ГОСТ:** динамический.
Количество туннелей в виртуальном канале (каждый туннель предоставляет доступ к одному целевому объекту из списка в настройках подключения или соответствует одному правилу отбора)	**IPSec-Фактор:** задается на сервере - не ограничено на стороне DiSec **IPSec-ГОСТ** не ограничено на стороне DiSec
Настройка доступа к защищенным ресурсам	**IPSec-Фактор:** **Динамический туннель -** правила задаются на сервере. **Статический туннель** - правила НЕ согласовываются автоматически, задаются в настройках подключения. **IPSec-ГОСТ:** правила НЕ согласовываются автоматически, задаются в настройках подключения. Несколько правил в одном подключении соответствуют нескольким IPSEC-соединениям (***Connection)*** на стороне сервера VPN. Возможна настройка на получение правил от сервера.
Режимы взаимной аутентификации клиента и сервера	**IPSec-Фактор:** симметричные ключи шифрования **IPSec-ГОСТ:** инфраструктура PKI (асимметричные ключи шифрования). Режим "Preshared key" - не реализован
Интегрированный межсетевой экран (МЭ)	Фильтрация пакетов на сетевом и транспортном уровне (TCP\IP).Функционирование и при наличии туннеля.
Контроль целостности	Статический. Динамический - периодический в процессе работы приложения,

	корректное отключение туннеля при нарушении целостности ПО.
Состав ПО	Приложение Windows - DiSec.exe Службы Windows - DiSecSRV.exe, DiSecIsm.exe. Драйвер Kernel Mode - DiSec.sys Дополнительные программы и службы: настройка, запуск и останов служб, Сбор информации о системе, Лицензирование).
Лицензирование	Защита ключом регистрации - разрешена одна установка на одном компьютере.
Программная операционная среда	
Поддерживаемые операционные системы: Microsoft Windows (x32, x64)	Microsoft Windows 10 Microsoft Windows 8.1 Microsoft Windows Server 2012 Microsoft Windows 7 Microsoft Windows Vista Microsoft Windows Server 2008
Совместимость со средствами защиты	- Функционирует при наличии установленного антивирусного ПО - функционирует при наличии драйверов, разработанных в соответствии с требованиями NDIS 6.30
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	Несколько подключений (виртуальных каналов) 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; - настройка МЭ. 2. Защита паролем процедуры выполнения настроек.
Сетевые конфигурации	
Сетевые интерфейсы	Ethernet WiFi Модем телефонной линии Mobile Broadband modem
Стек TCP\IP	IPv4 IPv6 - **не поддерживается**

	Динамическая настройка размера TCP\IP пакета (MSS)
Поддержка нескольких сетевых интерфейсов	- Автоматическое определение сетевого интерфейса для виртуального туннеля и маршрутизация трафика
	- возможность блокирования "открытого" трафика при наличии\отсутствии туннеля
Работа через NAT (NAT Traversal)	**IPSec-ГОСТ**: NAT Traversal **IPSec-Фактор**: статический туннель (UDP-инкапсуляция)
Интеграция в существующую сетевую инфраструктуру	**IPSec-ГОСТ**: ModeCfg - динамическое получение адреса из пула IP-адресов защищенной сети, а также адреса DNS и адрес IP-подсети в качестве целевого объекта. **IPSec-Фактор**: RLAN - назначение статического заранее согласованного IP-адреса, а также адреса DNS (Аналог ModeCfg).
Свойства Ethernet-адаптеров	- Поддержка свойств TaskOffload (автоматическое отключение при инсталляции ПО DISEC).
	- поддержка Jumbo-фреймов
Изменение сетевой конфигурации компьютера	Отслеживает отключение и подключение сетевых адаптеров - автоматически отключает туннель.

Особенности реализации

Шифрование и контроль целостности передаваемого трафика	**IPSec-Фактор**: Протоколы IPsec: "IP Encapsulation within IP" (RFC 2003), с использованием (только) ***российских*** криптографических алгоритмов. **IPSec-ГОСТ**: Протоколы IPsec ESP (RFC2401-2412), с использованием (только) ***российских*** криптографических алгоритмов.
Аутентификация взаимодействующих сторон	**IPSec-Фактор**: по протоколу ISAKMP (Internet Security Association and Key Management Protocol, RFC 2408) с использованием симметричных ключей. **IPSec-ГОСТ**: по протоколу IKE (RFC 2407-2409 и RFC 4303) с использованием сертификатов X509 (RFC 5280).
Режимы туннелирования	**IPSec-Фактор**: - туннельный режим "IP-in-IP" - UDP-инкапсуляция пакет (поверх IP-in-IP) для статических туннелей **IPSec-ГОСТ**: - транспортный и туннельный режимы ESP-инкапсуляции.
Режимы инкапсуляции	**IPSec-ГОСТ**: -ESP_GOST-4M-IMIT, -ESP_GOST-1K-IMIT - UDP\ESP-инкапсуляция (NAT-Traversal)
Информационные обмены протокола IKE	**IPSec-ГОСТ**: IKEv1 - Main mode - Quick mode

	- Informational Exchanges - Transaction Exchanges (MODECFG) IKEv2 - **не реализован**
Алгоритмы выработки сессионных ключей	**IPSec-Фактор**: VKO ГОСТ Р 34.10-2001 **IPSec-ГОСТ**: - VKO ГОСТ Р 34.10-2001 - VKO_GOSTR3410_2012_256
Режимы аутентификации в протоколе IKE	- ГОСТ Р 34.10-2001 - ГОСТ Р 34.10-2012
Алгоритмы шифрования	- ГОСТ28147-89 DES, AES - **не реализованы**
Алгоритмы контроля целостности	**IPSec-Фактор**: ГОСТ Р 34.11-94 **IPSec-ГОСТ**: ГОСТ Р 34.11-94 ГОСТ Р 34.11-2012 ESP_GOST-4M-IMIT, ESP_GOST-1K-IMIT MD5, SHA1- **не реализованы**
Алгоритмы электронной цифровой подписи (ЭЦП)	**IPSec-ГОСТ**: - ГОСТ Р 34.10-2001 - ГОСТ Р 34.10-2012 DSA, RSA - **не реализованы**
Мониторинг доступности удаленного узла (жизнеспособности туннеля)	**IPSec-ГОСТ**: Dead Peer Detection (DPD) протокол (RFC 3706)
	IPSec-Фактор: пингование клиентом сервера (с возможностью отключения), сообщения Notification от сервера к клиенту
Обновление сессионных ключей (rekeying)	**IPSec-Фактор**: нет **IPSec-ГОСТ**: Разрешен только со стороны клиента
Обработка искаженных пакетов (Integrity Fail)	**IPSec-ГОСТ**: реализована в соответствии с ГОСТ
Защита от Replay-атак	**IPSec-ГОСТ, IPSec-Фактор**: реализовано с использованием алгоритма сдвига окна (bit-shifting)
Журналирование и протоколирование	
Журнал действий оператора	- начало\окончание сеанса пользователя с указанием имени пользователя - основные этапы установки подключения, возникшие ошибки - смена пользователя Windows - действия по настройке МЭ
Протоколирование сетевого трафика	Опционально при включении данной опции администратором. Возможность фиксировать отброшенный МЭ трафик.
Системный журнал (Event Log, System	Фиксируются ошибки функционирования виртуального канала

Log)	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, МЭ, ошибки); - количество ошибочных пакетов с разбивкой по типу ошибок (крипто, нехватка памяти, искаженные IP\TCP-пакеты)
Статистика Туннелей	**IPSec-ГОСТ:** - число пакетов с искаженной контр. суммой (Integrity Fail); - статистика повторяющихся пакетов (Replay атаки). **IPSec-Фактор:** - повторяющихся пакетов (Replay атаки).
Криптография	
Криптографические библиотеки	Встроенные библиотеки разработки ООО "Фактор-ТС"
Формат сертификатов публичных ключей	X.509 v.3 (ГОСТ) X.509 v.3 (RSA, DSA) не реализовано
Поддержка списка отозванных сертификатов	Обработка Certificate Revocation List (CRL). Поддерживается CRL v.2. Способ получения CRL – протокол LDAP v.3
Контроль валидности сертификатов по протоколу OCSP.	Опционально.
Ключевые носители	- Дискеты (НГМД) - 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	Фактор ТС 1.0 PKCS#15 PKCS#11 PKCS11-токены - не поддерживаются.

14 Приложение 2. Пример настройки на узле «ПАК Dionis-NX» для работы с ПО DISEC

1. Инициализировать криптосистему узла ПАК «Dionis-NX» (если это ещё не сделано) с использованием ключевого носителя, сгенерировать ключ доступа (КД) и сохранить его на внешнем носителе или в памяти LCD-индикатора (команды «**crypto access key init/store/load/replace**»).
2. Загрузить в криптосистему сертификат(ы) корневого(ых) УЦ (команда «**crypto pki import root ca cert**»).
3. Если требуется, загрузить в криптосистему сертификаты всех необходимых подчинённых УЦ (команда «**crypto pki import ca cert**»).
4. Загрузить в систему закрытый ключ для данного узла (команда «**crypto pki import key**»). Загрузить в систему сертификат для данного узла, соответствующий загруженному закрытому ключу (команда «**crypto pki import cert**»).
5. В соответствии с требованиями политики безопасности организации может потребоваться проверка, не является ли сертификат отозванным, в этом случае может потребоваться загрузить действующий(е) список(ки) отозванных сертификатов (команда «**crypto pki import crl**»), включить опцию «**crl policy strict**» в глобальных настройках службы IKE (команда «**crypto ike config**»), а также настроить динамическую проверку отозванных сертификатов (команды «**crl fetch interval**», «**crl cache**», «**crypto ike cainfo**», команды настройки протокола OCSP).
6. Рекомендуется загрузить в систему сертификат клиента. Если с некоторым IPSEC-соединением предполагается работа нескольких клиентов с различными сертификатами или сертификат клиента отсутствует, необходимо задать режим запроса сертификата «…»
7. Войти в режим настройки IPSEC-соединения (команда «**crypto ike conn XXX**»). Здесь XXX – имя IPSEC-соединения.
8. Если необходимо, изменить режим инкапсуляции трафика (команда «**type tunnel**»). По умолчанию - *TUNNEL*.
9. Указать локальный IP-адрес (адрес, с которого будет устанавливаться туннель) ПАК Dionis-NX (команда «**local ip**»).
10. Указать имя сертификата данного узла (команда «**local cert**»).
11. Задать опцию «**remote ip ***», что означает: принимать соединения от клиентов с любых Интернет IP-адресов.
12. Задать X500-имя субъекта сертификата клиента (либо сам сертификат) (команда «**remote id**»). Если требуется принимать соединения от нескольких клиентов, то необходимо задать шаблон X500-имени.
13. Задать виртуальный (назначаемый) IP-адрес мобильного клиента (команда «**remote source ip**»). Если мобильных клиентов несколько, то необходимо задать пул IP-адресов в виде подсети с маской («**A.B.C.D/M**»).
14. Если мобильному клиенту требуется сообщить IP-адреса внутренних (корпоративных) серверов DNS, то необходимо указать опцию «**modeconfig dns**». Если мобильному клиенту требуется сообщить IP-адреса внутренних подсетей, то необходимо указать опцию "**local subnet from pool**"
15. Указать доступные по туннелю ресурсы - внутреннюю (защищаемую, корпоративную) подсеть вида «**A.B.C.D/M**» (команда «**local subnet**»). В частном случае, это может представлять собой единственный ресурс, в этом случае «**A.B.C.D**» - IP-адрес этого ресурса, а «**M**» равно «32».
16. Если требуется направлять в туннель не весь трафик, то необходимо задать правила отбора трафика по номеру протокола; для протоколов TCP/UDP можно задать правила отбора могут включать номер локального и\или удалённого порта (команды «**local protoport**», «**remote protoport**»).
17. Рекомендуется включить режим «**Dead Peer Detection**» («Проверка жизнеспособности туннеля») для быстрого закрытия IPSEC-соединения, если мобильный клиент аварийно отключился (команда «**dpd**»). Рекомендуется задавать значения параметров DPD - интервал посылок и время ожидания - с учетом возможных задержек на медленных линиях связи и для медленных устройств во избежание "ложного" срабатывания.

18. Необходимо указать настройки «**no rekey**» и «**keying tries 1**», чтобы ПАК Dionis-NX не брал на себя инициативу продления туннеля (DiSec не поддерживает "входящий" рекиинг).
19. Если необходимо, изменить криптопараметры IKE, согласуемые на фазе 1 (команда «**ph1 transforms**»): рекомендуется значение "*no strict*" – политика, разрешающая клиенту выбирать любые параметры шифрования.
20. Если необходимо, изменить криптопараметры ESP, согласуемые на фазе 2 (команда «**ph2 transforms**»): рекомендуется значение "*no strict*" – политика, разрешающая клиенту выбирать любые параметры шифрования.
21. Если необходимо, изменить режим Perfect Forward Secrecy (команда «**pfs mode**»). Значение по умолчанию – *propose*.
22. Если необходимо, изменить параметры алгоритма ГОСТ Р 3410-2001, используемые для выработки общего секрета фазы 2 протокола IKE в режиме PFS (команда «**pfs group**»).
23. Если необходимо, изменить значение максимального количества фаз 2, порождаемых из одной фазы 1 (команда «**ph2 max**»). Значение по умолчанию - *16384*. (при значении режима Perfect Forward – *propose*, см. выше п. 21).
24. Если необходимо, изменить настройки таймеров жизни туннелей (команды «**ph1 life time**», «**ph2 life time**», «**ph margin time**», «**ph margin fuzz**»). По умолчанию время жизни 1-ой фазы – *10800 сек*, 2-ой фазы – *3600 сек*. Рекомендуется указывать максимально возможные значения для параметров "**life time**" и нулевые значения для "**margin**" и "**fuzz**", поскольку инициирование процесса обновления ключей (рекиинг) выполняется со стороны DiSec (см. п. 18).
25. Включить службу IKE. (Команда «**crypto ike enable**»).
26. Активировать настроенное IPSEC-соединение (команда «**crypto ike enable conn XXX**»).

Если необходимо обеспечить доступ к нескольким защищенным ресурсам, либо к одному ресурсу (IP-адресу), но разным протоколам и\или портам, то необходимо создать соответствующее число IPSEC-соединений, в каждом указывая единственный объект, т.е. IPSEC-соединения будут отличаться значениями в пп. 15) и 16).

С этого момента соединение будет переведено в «слушающее» состояние («**offline**»), и ПАК Dionis-NX будет готов принять начальное сообщение об установлении туннеля от клиента DiSec.

Лист регистрации изменений

Номер изменения	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводительного документа	Подпись	Дата
	изменен-ных	заменен-ных	новых	аннули-рованных					