

УТВЕРЖДЕНО

RU.НКБГ.70009-01 92 - ЛУ

Клиент криптографического сервера доступа

«DiSec»

Версия 5.0

Руководство пользователя

RU.НКБГ.70009-01 92

Листов 73

Име. № подл. 256	Подпись и дата	Взам. ине. №	Име. № дубл.	Подпись и дата
---------------------	----------------	--------------	--------------	----------------

Содержание

1 Общие сведения.....	4
1.1 Назначение и область применения программы.....	4
1.2 Туннелирование	5
1.2.1 Режим IPSEC-ФАКТОР.....	6
1.2.2 Режим IPSEC-ГОСТ.....	6
1.3 Межсетевое экранирование	6
2 Описание работы ПО DiSec	7
2.1 Взаимодействие компонентов DiSec с компонентами WINDOWS.....	7
2.2 Взаимодействие ПО DiSec с Сервером VPN.....	8
2.2.1 Установление динамического туннеля.....	8
2.2.2 Установление статического туннеля	8
2.2.3 Работа туннеля.....	9
2.3 Организация динамических туннелей с несколькими Серверами VPN.....	9
2.4 Система криптозащиты в DiSec.....	9
2.4.1 Ключевые носители	10
2.4.2 Состав ключевой информации	10
2.4.3 Средства генерации ключей для DiSec	11
3 Условия применения программы.....	12
3.1 Требования к оборудованию.....	12
3.2 Требования к программному окружению.....	12
3.3 Сетевое окружение и подключение к сети Интернет	12
3.4 Настройки на Сервере VPN	13
3.4.1 Настройки на Сервере VPN для организации туннеля в режиме IPSEC-ФАКТОР.....	13
3.4.2 Настройки на Сервере VPN для организации туннеля IPSEC-ГОСТ	13
3.5 Требования к ключевой информации	15
3.6 Подготовка и порядок работы с DiSec	15
3.6.1 Подготовка к работе в режиме IPSEC-ФАКТОР.....	15
3.6.2 Подготовка к работе в режиме IPSEC-ГОСТ	16
3.6.3 Порядок работы с DiSec.....	16
4 Инсталляция DiSec	17
4.1 Комплект поставки DiSec.....	17
4.2 Процедура инсталляции ПО DiSec.....	17
4.3 Проверка контрольных сумм	21
5 Удаление DiSec	22
5.1 Удаление службы DiSecSrv.....	22
5.2 Удаление всех компонентов DiSec	22
6 Режимы работы ПО DiSec	23
6.1 Пользователи ПО DiSec	23
6.2 Работа с оболочкой DiSec	23
6.2.1 Принципы работы	23
6.2.2 Команды оболочки DiSec.....	24
6.3 Работа в режиме службы WINDOWS	25
7 Команда Настройка.....	27
7.1 Вкладка Общие (Настройка ПО DiSec)	27
7.1.1 Режим запуска оболочки.....	28
7.1.2 Журнал событий.....	28
7.1.3 Список интерфейсов	28
7.2 Вкладка Подключения (Настройка ПО DiSec).....	29
7.3 Реквизиты подключения	30
7.3.1 Вкладка Общие (Реквизиты подключения).....	30
7.3.2 Вкладка Параметры (Реквизиты подключения) для режима IPSEC-ФАКТОР.....	31
7.3.3 Вкладка Безопасность (Реквизиты подключения) для режима IPSEC-ФАКТОР.....	31

7.3.4 Вкладка Параметры (Реквизиты подключения) для режима IPSEC-ГОСТ.....	31
7.3.4.1 Настройка политики IKE	32
7.3.4.2 Настройка политики ESP.....	34
7.3.4.3 Настройка Целевых объектов.....	35
7.3.5 Вкладка Безопасность (Реквизиты подключения) для режима IPSEC-ГОСТ.....	36
7.3.5.1 Настройка криптосистемы	37
7.3.5.2 Настройки запроса сертификата Сервера VPN.....	40
7.3.5.3 Защита хранилища Доверенные УЦ.....	41
7.3.5.4 Работа с хранилищами	41
7.3.6 Вкладка Доступ DialUP	45
7.4 Вкладка Драйвер DiSec (Настройка ПО DiSec)	45
7.4.1 Режим запуска и работы драйвера	46
7.4.2 Параметры протоколирования.....	46
7.4.3 Пример протокола.....	48
7.5 Вкладка Драйвер DiSec - Настройка МЭ	48
7.5.1 Алгоритм настройки МЭ DiSec	50
7.5.2 Создание и редактирование правила фильтрации	51
7.6 Вкладка Служба DiSecSrv (Настройка ПО DiSec)	52
7.6.1 Информация об инициализации службы.....	53
7.6.2 Параметры ресурса подключения.....	53
7.6.3 Режим запуска службы DiSecSrv.....	54
7.6.4 Журнал событий службы	55
8 Команды Подключиться/Отключиться	56
8.1 Команда Подключиться	56
8.2 Подключение к IP-сети при использовании DialUP	58
8.3 Команда Отключиться.....	58
9 Команда Состояние	59
9.1 Вкладка Драйвер (Состояние драйвера DiSec).....	59
9.2 Вкладка Интерфейс (Состояние драйвера DiSec).....	60
9.3 Вкладка Туннель (Состояние драйвера DiSec).....	61
9.3.1 Состояние туннеля в режиме IPSEC-ФАКТОР	61
9.3.2 Состояние туннеля в режиме IPSEC-ГОСТ.....	62
10 Команда Тестирование	63
10.1 Вкладка Ping (Тестирование)	63
10.2 Вкладка Маршруты (Тестирование).....	64
10.3 Вкладка ARP-таблица (Тестирование).....	64
10.4 Вкладка Статистика (Тестирование).....	65
10.5 Вкладка Служба DiSecSrv (Тестирование).....	66
11 Информационные команды	69
11.1 Команда Журналы	69
11.2 Команда Диагностика	69
11.3 Команда Протокол сети.....	70
12 Справочная информация	72
13 Команда Выход.....	72

1 Общие сведения

Настоящий документ предназначен для ознакомления с основными принципами функционирования Программного обеспечения «Клиент криптографического сервера доступа «DiSec» RU.НКБГ.70009-01, правилами подготовки к эксплуатации и настройке изделия.

Полное наименование изделия	- «Клиент криптографического сервера доступа «DiSec»
Краткое наименование изделия	- ПО DiSec или DiSec
Обозначение изделия	- RU.НКБГ.70009-01

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 протоколу TCP/IP, и для обеспечения доступа удалённых пользователей к ресурсам сегментов глобальной вычислительной сети, защищённых сетевыми устройствами.

ПО DiSec функционирует под управлением:

- 32-разрядных и 64-разрядных версий операционных систем WINDOWS 2003 Server, WINDOWS Server 2008, WINDOWS Vista, WINDOWS 7;
- 32-разрядных версий операционной системы WINDOWS XP.

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 (криptomаршрутизаторы ДИОНИС): «Многоуровневый криптомаршрутизатор DioNIS TS/FW 16000/KB2», «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» и «Методические рекомендации по использованию комбинированного алгоритма вложений IPSEC ESP на основе ГОСТ 28147-89» - это «ПАК Dionis-NX» и другие криптомаршрутизаторы (KM).

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 абонентами.

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.

На общей схеме IP-доступа к ресурсам защищенных сетей (Рис. 1) представлено взаимодействие мобильных абонентов, 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.

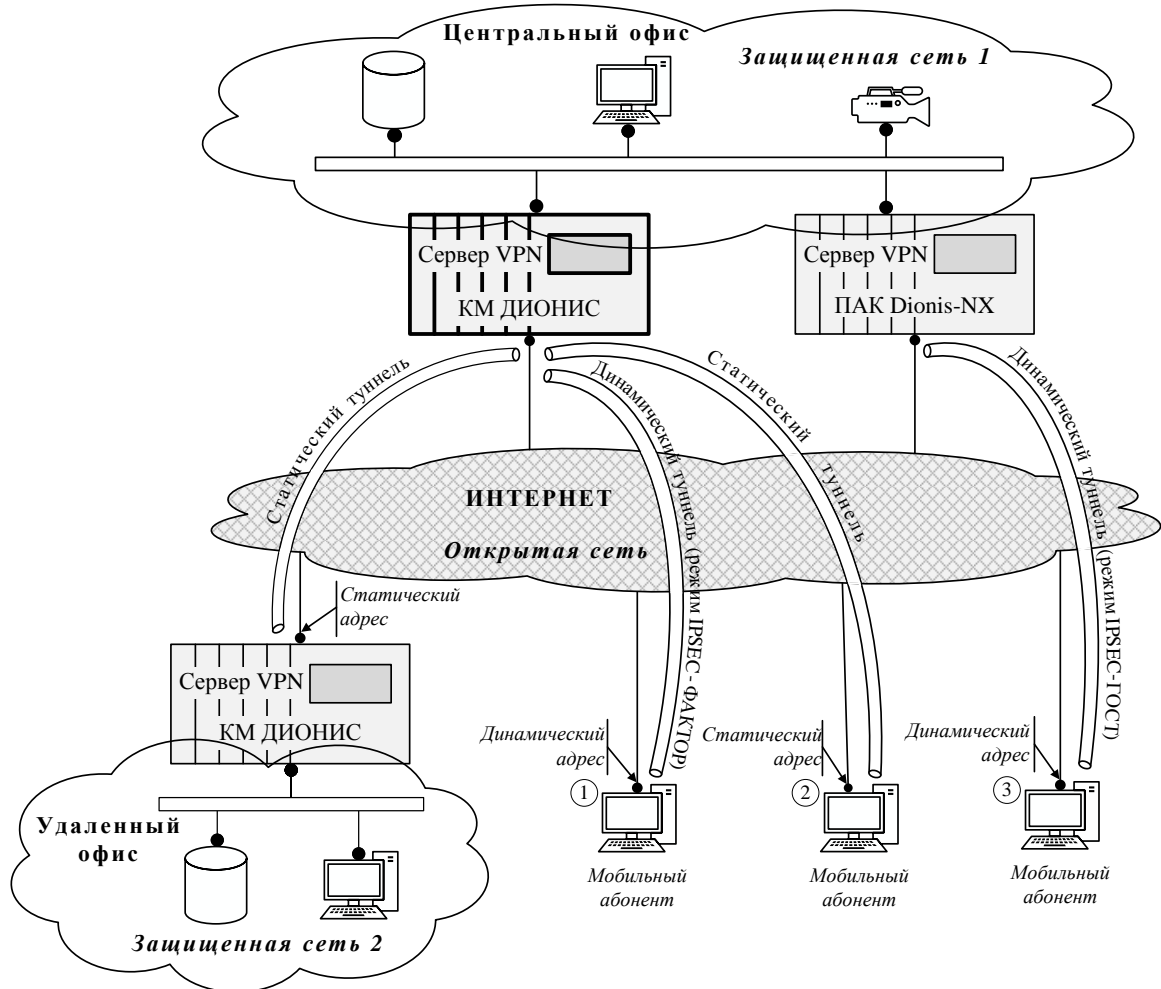


Рис. 1

1.2 Туннелирование

Туннелированием мы называем передачу исходной датаграммы с помощью другой – транспортной. Из всего потока информации, предназначенной для отправки в сеть, выделяется та, которая соответствует правилам отбора в туннель. Исходная датаграмма, соответствующая правилам отбора, подвергается обработке (выполняется шифрование, а также добавляется аутентификационная информация) и размещается в поле данных транспортной датаграммы. Сформированная таким образом транспортная датаграмма отправляется в открытую IP-сеть.

DiSec может работать с туннелями двух типов: 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 специальных алгоритмов. Запускается туннель в момент запуска Сервера VPN и существует до остановки узла.

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.

Значения параметров настройки динамических туннелей согласуются по IP-сети с помощью протокола ISAKMP (Internet Security Association and Key Management Protocol, RFC 2408).

Протокол ISAKMP обеспечивает:

- обмен конфигурационной информацией создаваемого динамического туннеля;
- двустороннюю криптографическую аутентификацию сторон;
- исключение намеренного или случайного вмешательства посторонних лиц в процесс установления динамического туннеля.

DiSec поддерживает два режима организации динамического туннеля: режим IPSEC-ФАКТОР и режим IPSEC-ГОСТ. Выбирается тот или иной режим на этапе настройки реквизитов подключения DiSec к Серверу VPN.

1.2.1 Режим IPSEC-ФАКТОР

Режим организации туннеля IPSEC-ФАКТОР использует симметричную ключевую систему. Распределение ключей шифрования производится заранее доверенным способом.

Туннель, создаваемый DiSec в режиме IPSEC-ФАКТОР, может быть как динамическим (туннель 1 на Рис. 1), так и статическим (туннель 2 на Рис. 1). В случае динамического туннеля используется криптографическая аутентификация по протоколу ISAKMP.

1.2.2 Режим IPSEC-ГОСТ

Режим организации туннеля IPSEC-ГОСТ (туннель 3 на Рис. 1) использует несимметричную ключевую систему на основе инфраструктуры открытых ключей PKI с применением сертификатов взаимодействующих сторон, соответствующих рекомендациям X.509.

Режим IPSEC-ГОСТ используется только для установления динамического туннеля.

При организации туннеля в режиме IPSEC-ГОСТ используются два протокола:

- IKE (Internet Key Exchange) - протокол взаимной аутентификации сторон и выработки ключевого материала для протокола ESP;
- ESP (Encapsulating Security Payload) - протокол шифрования и проверки подлинности IP-пакетов, передаваемых через криптотуннель.

Протоколы IKE (частный случай протокола ISAKMP) и ESP реализованы на основе рекомендаций RFC 2407-2409 и 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» (TK26) (www.tk26.ru).

1.3 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 эквивалентных 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.

МЭ фиксирует все отфильтрованные пакеты в протоколе сети, при этом указывается время прохождения пакета, а также его характеристики.

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. 7); сведения об общих принципах функционирования ПО DiSec и о взаимодействии с Серверами VPN (раздел 2.2, с. 8), а также об основных терминах и принципах системы криптографической защиты информации, используемых в DiSec (раздел 2.4, с. 9).

2.1 Взаимодействие компонентов DiSec с компонентами WINDOWS

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

- на уровне ядра ОС – драйвер DiSec (**DiSec.sys**);
- на уровне приложений - оболочка DiSec (**DiSec.exe**);
- на уровне сервиса операционной системы (службы) – служба DiSecSrv (**DiSecSrv.exe**).

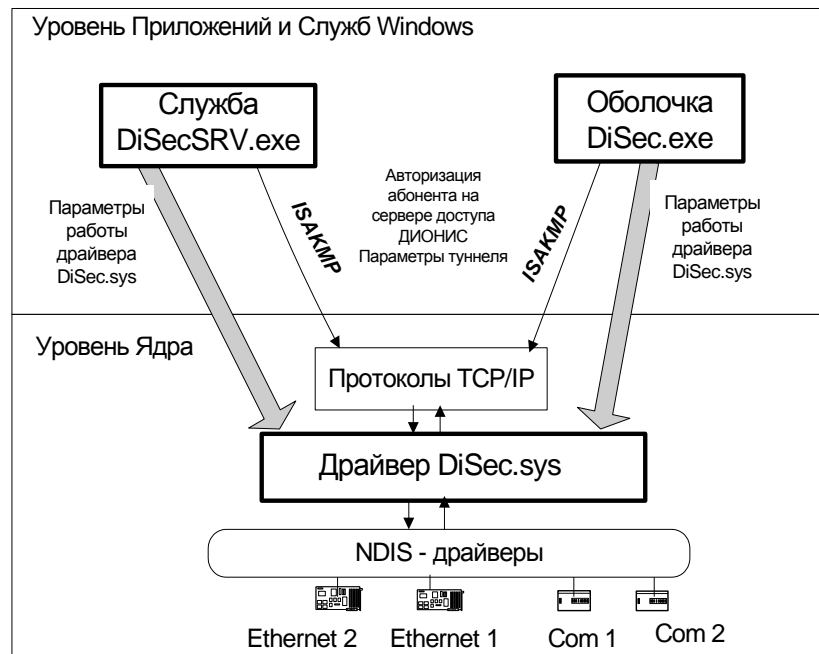


Рис. 2

Драйвер DiSec, подключенный к ядру операционной системы, контролирует IP-потоки между компонентами ядра WINDOWS, реализующими протоколы TCP/IP, и сетевыми интерфейсами WINDOWS, управляемыми драйверами адаптеров локальных сетей, компонентом «Удаленный доступ» (RAS) и т.п.

Драйвер выполняет зашифрование и расшифрование информации, используя в своей работе индивидуальную ключевую информацию пользователя DiSec. Драйвер также выполняет функции межсетевое экрана (МЭ), анализируя пакеты на соответствие правилам фильтрации. Драйвер выполняет контроль информационной части МЭ (фильтров) следующим образом. При передаче сформированного набора правил в систему (привязка фильтра – см. раздел 7.5.1, с. 50) формируется контрольная сумма набора и запоминается. Драйвер при считывании набора правил вычисляет его контрольную сумму и сравнивает с сохраненной. При несовпадении сумм данный фильтр исключается из использования.

Оболочка DiSec взаимодействует с Серверами VPN с целью организации и удаления туннеля, а также управляет работой драйвера DiSec. Кроме того, с помощью оболочки DiSec пользователь может получить информацию о текущем состоянии драйвера DiSec, о текущем состоянии IP-компонентов WINDOWS, а также выполнить различные диагностические функции, в том числе, останавливать, запускать и следить за работой службы DiSecSrv.

Служба DiSecSrv обеспечивает автоматическое подключение к Серверу VPN во время загрузки WINDOWS до входа в систему пользователя WINDOWS. Эта возможность используется при работе в доменной структуре WINDOWS для обеспечения авторизации на доменном контроллере WINDOWS, размещенном в защищенной сети.

2.2 Взаимодействие ПО DiSec с Сервером VPN

Взаимодействие ПО DiSec и Сервера VPN включает в себя два этапа (Рис. 3).

1-й этап – установление туннеля.

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

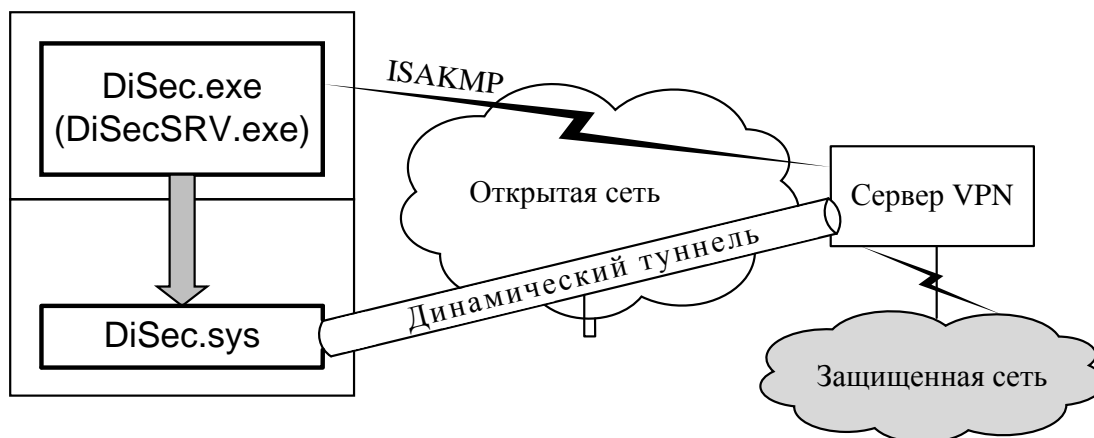


Рис. 3

Выполнение 1-го этапа осуществляется по-разному для статических и динамических туннелей.

2.2.1 Установление динамического туннеля

Для установления динамического туннеля в режиме IPSEC-ФАКТОР пользователь DiSec должен быть зарегистрирован на Сервере VPN - иметь учетную запись, поскольку аутентификация выполняется с использованием этой учетной записи.

Для 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.

Во время 1-го этапа выполняется следующая последовательность действий.

- 1) Пользователь DiSec устанавливает связь с IP-сетью стандартными для WINDOWS средствами и с помощью оболочки DiSec (или посредством службы DiSecSrv) посылает запрос на подключение к Серверу VPN (запрос посылается по протоколу ISAKMP и содержит аутентификационные данные абонента, соответствующие его ключевой информации, необходимые для создания динамического туннеля).
- 2) Сервер доступа VPN выполняет криптографическую аутентификацию и авторизацию абонента, т.е. проверяет, имеет ли данный абонент право на создание личного туннеля.
- 3) В случае успешной аутентификации и авторизации абонента выполняется согласование (по протоколу ISAKMP) параметров динамического туннеля, в том числе проверка ключевой информации пользователя DiSec.
- 4) После этого на клиентской стороне согласованные параметры работы туннеля загружаются в драйвер DiSec, в том числе драйвер получает информацию о том, какие данные необходимо подвергать туннелированию.

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

- 5) На Сервере VPN активизируется динамический туннель. С этого момента IP-поток между компьютером с DiSec и Сервером VPN становится закрытым (зашифрованным).

Примечание - 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.

2.2.2 Установление 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

2.2.3 Работа туннеля

После установления 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 туннели.

Пока динамический туннель открыт, каждая IP-датаграмма 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 администратор Сервера VPN ограничивает состав ресурсов, обмен данными с которыми будет защищен криптографическими средствами. Параметры туннеля и правила доступа (правила отбора в туннель) можно просмотреть средствами оболочки DiSec (см. раздел 9.3, с. 61).

При работе в режиме IPSEC-ГОСТ настройки правил отбора должны совпадать на стороне DiSec и на стороне Сервера VPN. Если они не совпадают, туннель не будет установлен.

При работе в режиме IPSEC-ФАКТОР правила отбора передаются на клиентский компьютер в процессе согласования параметров динамического туннеля.

Во время работы динамического туннеля его «жизнеспособность» может контролироваться или Сервером VPN, или DiSec, или тем и другим.

Одновременно с защищенными ресурсами пользователь DiSec может работать с открытыми ресурсами при соответствующей настройке (см. раздел 7.4.1, с. 46).

По окончании работы с защищенными ресурсами пользователь DiSec выполняет закрытие туннеля и отсоединение от Сервера VPN (см. раздел 8.3, с. 58).

Закрыть динамический 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. После этого драйвер DiSec продолжает работать в «прозрачном» режиме.

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

2.3 Организация динамических туннелей с несколькими Серверами VPN

Открытая сеть может содержать большое число Серверов VPN, каждый из которых защищает свою закрытую сеть.

Имея на своем компьютере программу «Клиент Криптографического сервера доступа», пользователь может устанавливать защищенное соединение с любым количеством Серверов VPN, но только **поочередно** (в каждый момент времени может быть организован только один туннель).

Для работы с несколькими Серверами VPN пользователь должен выполнить следующие действия:

- подключиться к IP-сети;
- выбрать тот Сервер, который защищает интересующий его ресурс, и организовать с ним туннель;
- закончив работу, отключиться от Сервера (соединение с IP-сетью при этом не разрывается);
- подключиться к следующему Серверу VPN для организации туннеля.

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 и в состав оболочки DiSec

В качестве основного элемента системы криптозащиты используется программный шифратор производства ООО «ФАКТОР-ТС», использующий алгоритмы шифрования ГОСТ 28147-89.

Если DiSec обеспечивает защиту информации по классу КСЗ, то на ПЭВМ должно быть установлено программное обеспечение **DiCheck**, обеспечивающее создание функционально замкнутой среды (см. документ «Программа создания замкнутой среды DiCheck. Руководство по настройке» RU.НКБГ.70011-01 90).

В процессе выполнения подключения к Серверу VPN (в процессе организации туннеля) оболочка DiSec (или служба DiSecSrv) считывает с ключевого носителя ключевую информацию и выполняет инициализацию шифратора.

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.

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 и перезаписываемые (дискета НГМД, съемный USB-носитель и т.п.).

В качестве ключевых носителей также могут использоваться устройства **ruToken** (тип «ruToken» и «ruToken S») или **eToken**. 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 eToken и ruToken, 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.

Для ключевых носителей типа «ruToken S» пользователь должен знать имя директории на данном носителе, в которой сформирована ключевая информация. Данная информация 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.

Закрытый ключ (и необходимая для его использования информация) размещается на съемном ключевом носителе в т.н. «контейнере».

Замечание. DiSec поддерживает два формата «контейнера закрытого ключа»:

- **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;
- **PKCS#15 (PUC)** – 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.

На ключевом носителе может быть размещен 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. Эти сертификаты и списки можно разместить на этом же ключевом носителе, если это не eToken и ruToken.

Если используются ключевые носители eToken или ruToken, то указанные сертификаты и списки отозванных сертификатов размещаются на другом носителе, который ОС WINDOWS может определить как съемный и перезаписываемый.

На ключевой носитель записывается также ссылка на текущий сертификат, создаваемая в процессе настройки криптосистемы (см. раздел 7.3.5.1, с. 37).

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 (например, фельдъегерской службой).

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

- «Автоматизированное рабочее место генерации ключей» (НКБГ.501430.735) – при создании динамических туннелей;
- «Автоматизированное рабочее место генерации ключей АРМ ГК/КВ2» (НКБГ. 467369.865) – при создании статических туннелей.

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

- «Модуль генерации ключей» (НКБГ.501430.772) - создает контейнер в формате **Фактор ТС 1.0**;
- «Модуль генерации ключей» (НКБГ.501430.774) - создает контейнер в двух форматах **Фактор ТС 1.0** и **PKCS#15 (РУС)**

совместно с программно-аппаратными средствами Удостоверяющего центра, поддерживающими формат сертификатов, соответствующий рекомендациям X.509.

В качестве средств генерации ключевой информации и формирования ключевых носителей могут использоваться другие изделия, сертифицированные установленным порядком и поддерживающие необходимые форматы.

В любом случае в ПО DiSec должны использоваться ключи, вырабатываемые криптографическим средством, сертифицированным ФСБ России по классу, не ниже класса криптографической защиты данного ПО.

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.70009-01 90 (далее по тексту ПРАВИЛА) и «СКЗИ Клиент криптографического сервера доступа «DiSec» Формуляр» RU.НКБГ.70009-01 30 (документы входят в комплект поставки DiSec).

Ниже приведены требования:

- к оборудованию компьютера пользователя DiSec (раздел 3.1, с. 12),
- к операционной среде – настройке программных компонентов ОС WINDOWS (раздел 3.2, с. 12) и программных средств, работающих под ее управлением,
- к программно-аппаратным средствам подключения к сети Интернет (раздел 3.3, с. 12),
- к настройкам Сервера VPN (раздел 3.4, с. 13),
- к ключевой информации (раздел 3.5, с. 15).

3.1 Требования к оборудованию

DiSec устанавливается на IBM-совместимом компьютере, функционирующем под управлением 32 и 64-разрядных версий операционных систем Microsoft WINDOWS Server 2008, WINDOWS Vista, WINDOWS 7, WINDOWS 2003 Server и 32-разрядной версии операционной системы WINDOWS XP.

Компьютер должен быть оснащен устройством для считывания ключевых носителей (НГМД, 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.

Системная служба ОС WINDOWS **IPSEC** (IPsec Policy Agent), служба «IKE and AuthIP IPsec Keying Modules», а также другие службы, использующие порт 500 протокола UDP, должны быть отключены или переведены в ручной режим запуска.

3.3 Сетевое окружение и подключение к сети Интернет

Компьютер пользователя DiSec может располагаться внутри локальных сетей любого типа, поддерживающих IP-протокол, 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. При использовании в этой локальной сети фиктивных IP-адресов необходимо, чтобы они отличались от фиктивных адресов защищенной сети.

Коммуникационное оборудование межсетевого экранирования должно пропускать UDP-пакеты с портом 500 (портом источника для входящего трафика и портом назначения для исходящего) и туннелированные пакеты (протокол IP in IP – номер 4), а также протокол ESP (номер 50).

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.

При работе в системе WINDOWS XP: если предполагается использовать **DialUP**-подключение для работы службы DiSecSrv, то необходимо задать автоматический запуск службы **WINDOWS Диспетчер подключений удаленного доступа (RAS)**.

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 криптографическим и технологическим параметрам туннелей, и т.п.).

Ниже (раздел 3.4.1, с. 13) приведена типовая настройка Сервера VPN для организации туннеля в режиме IPSEC-ФАКТОР. Так могут быть настроены все перечисленные в разделе 1.1 (с. 4) криптомаршрутизаторы.

В разделе 3.4.2, с. 13 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 датаграмм (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 датаграмм, обеспечивающие контроль функционирования туннеля - протокола ISAKMP и Ping-пакетов (см. раздел 9.3, с. 61). При отборе датаграмм в туннель и при извлечении их из туннеля правила просматриваются по порядку, начиная с первого, и просмотр заканчивается, как только будет обнаружено соответствие параметров датаграммы (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. Должен быть организован статический туннель для IP-адреса компьютера пользователя DiSec.
2. Должна быть проинициализирована подсистема **Криптозащита** и введена ключевая информация.
3. Статический туннель должен быть настроен на загруженные ключи шифрования.
4. Пользователю DiSec должен быть передан идентификатор статического туннеля и номер ключа удаленного конца туннеля..

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 следующее (в качестве примера приведена настройка на узле «ПАК Dionis-NX» - описана минимальная, не исчерпывающая настройка).

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**»).
5. Загрузить в систему сертификат для данного узла, соответствующий загруженному закрытому ключу (команда «**crypto pki import cert**»).
6. 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 OCSP).
7. Войти в режим настройки IPSEC-соединения (команда «**crypto ike conn**»).
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 внутреннюю (защищаемую, корпоративную) подсеть вида «**A.B.C.D/M**» (команда «**local subnet**»).
11. Указать имя сертификата данного узла (команда «**local cert**»).
12. Задать опцию «**remote ip ***», что означает: принимать соединения от клиентов с любых Интернет IP-адресов.
13. 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.
14. 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**»).

Замечание. Эти адреса не должны пересекаться с адресами внутренней (защищаемой) подсети – см. выше п. 10.

15. Если мобильному клиенту требуется сообщить IP-адреса внутренних (корпоративных) серверов DNS, то необходимо указать опцию «**modeconfig dns**».
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 по номеру локального и 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; action close**»).
18. Рекомендуется указать настройки «**no rekey**» и «**keying tries 1**», чтобы ПАК Dionis-NX не брал на себя инициативу продления туннеля.
19. Если необходимо, изменить криптопараметры IKE, согласуемые на фазе 1 (команда «**ph1 transforms**»):
 - узел замены для алгоритма ГОСТ 28147-89, используемый для шифрования протокола IKE, значение по умолчанию - *id-Gost28147-89-CryptoPro-B-ParamSet*;
 - параметры алгоритма ГОСТ Р 3410-2001, используемые для выработки сессионного ключа, значение по умолчанию - *id-GostR3410-2001-CryptoPro-XchB-ParamSet+id-GostR3410-94*.
20. Если необходимо, изменить криптопараметры ESP, согласуемые на фазе 2 (команда «**ph2 transforms**»):
 - преобразование ESP, значение по умолчанию - *ESP_GOST-4M-IMIT*;

- узел замены для алгоритма ГОСТ 28147-89, используемый для шифрования данных в протоколе ESP, значение по умолчанию - *id-Gost28147-89-CryptoPro-B-ParamSet*.
- 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**»). По умолчанию устанавливается значение, совпадающее со значением параметров алгоритма ГОСТ Р 3410-2001, используемых для выработки сессионного ключа (см. выше п. 19) - *id-GostR3410-2001-CryptoPro-XchB-ParamSet+id-GostR3410-94*.
- 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*.
- 25. Включить службу IKE. (Команда «**crypto ike enable**»).
- 26. Активировать настроенное IPSEC-соединение (команда «**crypto ike enable conn**»).

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.

3.5 Требования к ключевой информации

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

- 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 «**Extended 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*.

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. 13) 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 (см. ниже).

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);
- данные о криптографических ключах Сервера (**номер** и **серия ключа**).

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 надо предварительно выполнить следующее.

- 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).

- 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.

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 закрытый ключ, свой сертификат, всю цепочку сертификатов доверенных УЦ вплоть до корневого и действующий список отозванных сертификатов.
- Получить от администратора Сервера VPN следующие данные:
 - IP-адрес (или доменное имя) Сервера VPN, с которого будет устанавливаться туннель;
 - IP-адрес внутренней (защищаемой, корпоративной) подсети.
- Получить от службы безопасности организации или от ответственного лица:
 - сертификаты всех Серверов VPN, с которыми предполагается устанавливать туннели, выпущенные определенными доверенными УЦ;
 - 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 (работа с хранилищами описана в разделе 7.3.5.4, с. 41).

Замечание - 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 (п. 19, с. 14);
- параметры алгоритма ГОСТ Р 3410-2001, используемые для выработки сессионного ключа фазы 1 протокола IKE (п. 19, с. 14)
- параметры алгоритма ГОСТ Р 3410-2001, используемые для выработки общего секрета фазы 2 протокола IKE в режиме PFS (п. 22, с. 15);
- узел замены (алгоритм ГОСТ 28147-89), используемый для шифрования данных в протоколе ESP (п. 20, с. 14);
- преобразование ESP (п. 20, с. 14);
- режим Perfect Forward Secrecy (PFS) (п. 21, с. 15);
- 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. 17).
2. Запустить оболочку DiSec (раздел 6.2, с. 23), либо обеспечить ее автоматический запуск при запуске ОС WINDOWS (раздел 7.1, с. 27).
3. Сообщить DiSec все необходимые данные, для чего выполнить команду **Настройка** из Главного меню оболочки (Рис. 11) и заполнить список **Защищенные сети (ресурсы подключения)** (раздел 7.2, с. 29).
4. 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.
5. Дать команду **Подключиться** из Главного меню оболочки (Рис. 11) и, выбрав необходимый ресурс из списка, отправить ему запрос для организации динамического туннеля (см. раздел 8.1, с. 56).

4 Инсталляция DiSec

Инсталляция состоит из двух этапов: инсталляция основного ПО – инсталляция собственно DiSec (раздел 4.2, с. 17) 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 5, с. 22).

Инсталляция выполняется запуском программы **DiSec-Setup.exe** с дистрибутивного носителя.

Начинается установка с предупреждающего сообщения (Рис. 4).

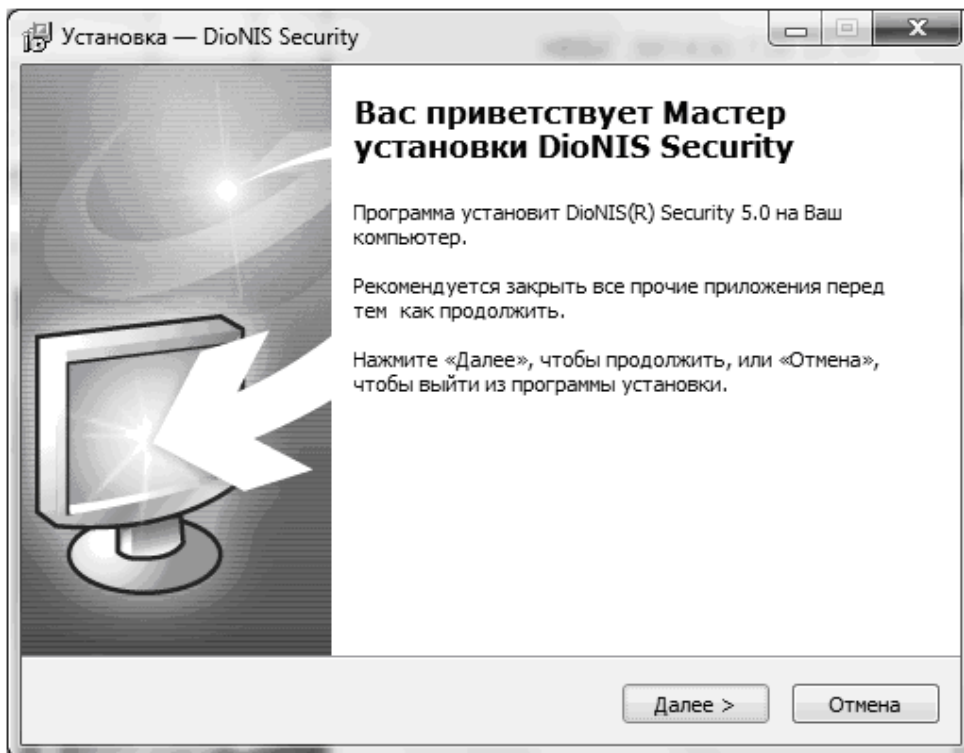


Рис. 4

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

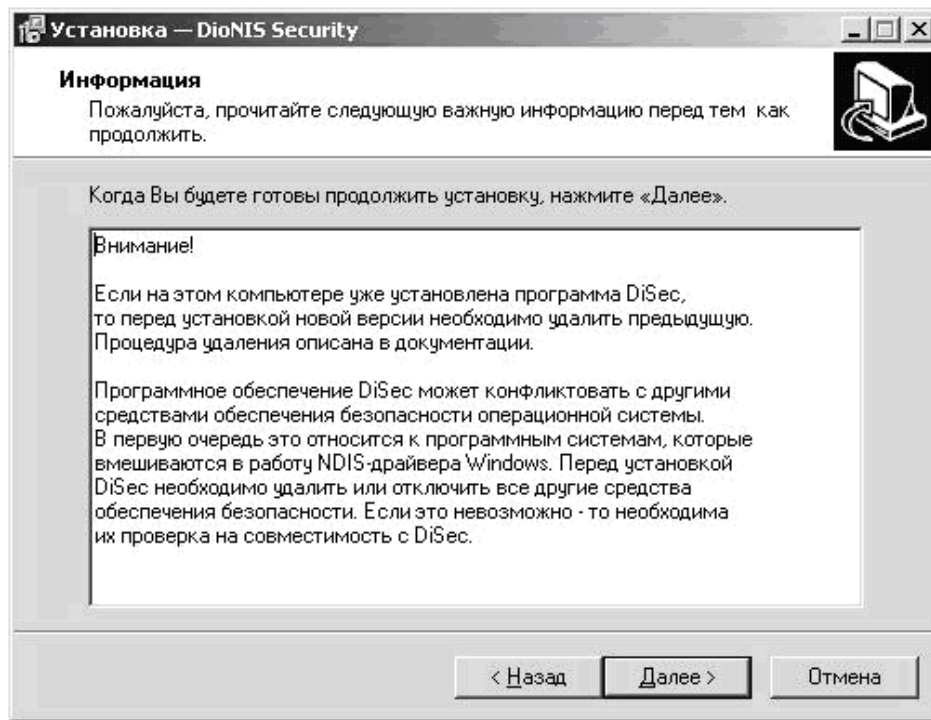


Рис. 5

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.

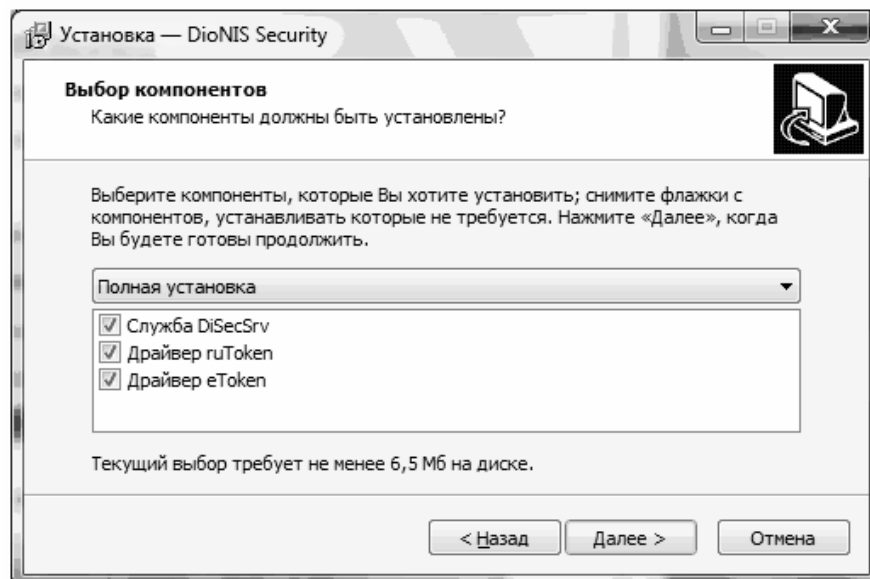


Рис. 6

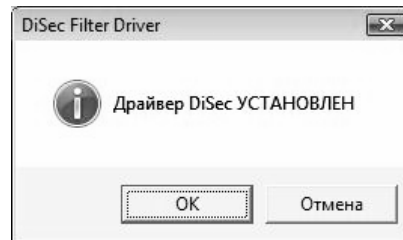
Далее программа установки выведет на экран окно с полученной от пользователя информацией для установки и после нажатия кнопки **Установить** выполнит разархивацию и копирование файлов с дистрибутивного носителя в указанную папку.

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:



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

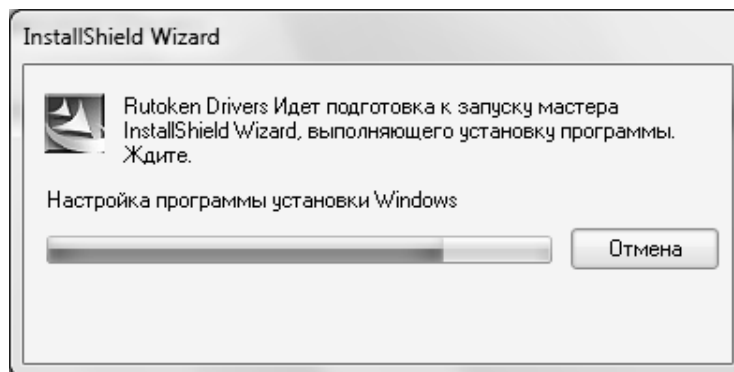


Рис. 8

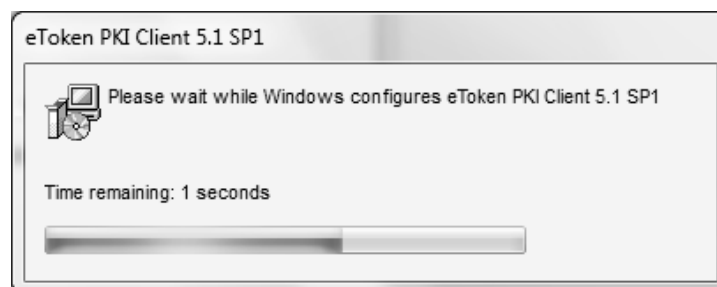


Рис. 9

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

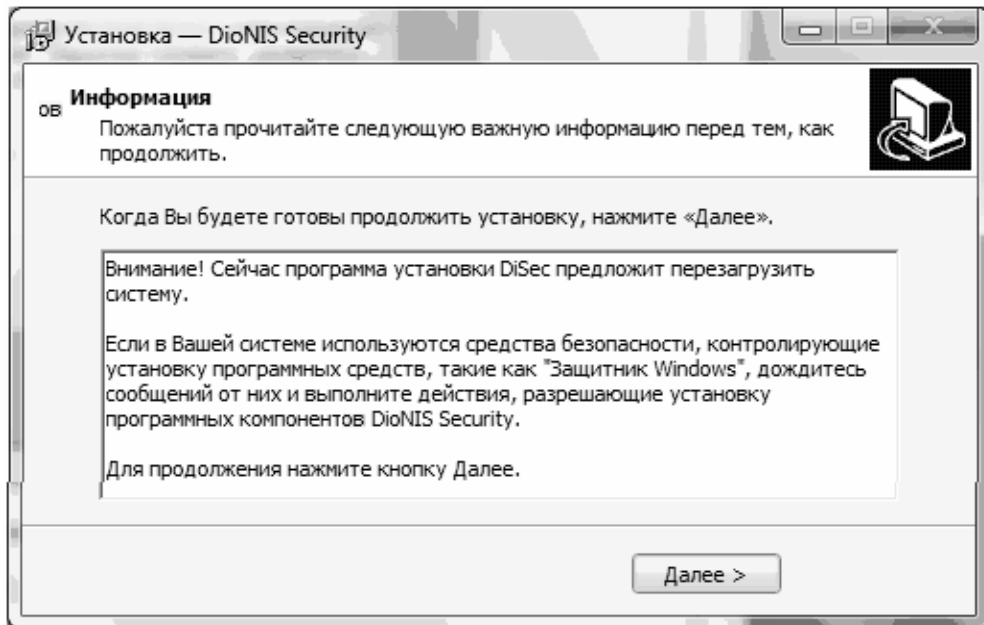


Рис. 10

По окончании установки будет предложено перезагрузить компьютер.

Перезагрузку выполнить необходимо, поскольку в процессе перезагрузки выполняются действия по регистрации (формированию 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 оболочки DiSec.

В стартовых системных меню всех пользователей компьютера появится программная папка **FACTOR Applications\DioNIS Security**, в которой помещен ярлык для запуска оболочки DiSec, ярлык программы деинсталляции DiSec и ярлык служебной программы проверки контрольных сумм **Контрольные суммы (Checkwin)**.

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 (установка, настройка и деинсталляция);
- папка **Ключи**, содержащая команды установки драйверов ключевых носителей ruToken и eToken;
- папка **Документация**.

Примечание - Если в процессе установки 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 (Checkwin)** и список файлов программного обеспечения, подлежащих проверке. При установке DiSec программа **Контрольные суммы** размещается 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.70009-01 90 (комплектации 1.1, 1.2, 1.3) или RU.НКБГ.70009-01 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.

Примечание - при первом включении DiSec пользователь должен визуально убедиться в идентичности значений контрольных сумм, выведенных на экран, и контрольных сумм, содержащихся в Правилах пользования).

Если суммы совпадут, то программа выдаст сообщение, что контрольные суммы проверены успешно.

Если будет обнаружено несоответствие, то программа укажет файл, для которого имеет место ошибка контрольной суммы. В этом случае необходимо удалить установленное программное обеспечение (раздел 5, с. 22).

В дальнейшем следует периодически при запуске DiSec проводить контроль целостности ПО. Периодичность проверки зависит от условий эксплуатации и определяется политикой безопасности эксплуатирующей организации. Периодический контроль можно выполнять так же, как и при первом включении.

В составе ПО DiSec, обеспечивающего защиту по классам КС2 и КС3, используется средство доверенной загрузки (АПМДЗ), в таких изделиях контроль целостности ПО выполняется этим средством (при соответствующей настройке) автоматически при каждом включении ПЭВМ, на которой функционирует DiSec.

В составе ПО DiSec, обеспечивающего защиту по классу КС3, используется средство для создания функционально замкнутой среды (Программа «DiCheck»). При первом включении такого изделия пользователь должен выполнить проверку целостности ПО «DiCheck». Порядок проверки рассмотрен в документе «Программа создания замкнутой среды «DiCheck» RU.НКБГ.70011-01 90». Все контролируемые файлы ПО «DiCheck» должны быть включены в список проверяемых файлов АПМДЗ.

5 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.

5.1 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 10.5, с. 66).

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

5.2 Удаление всех компонентов DiSec

При необходимости перед удалением 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»), а также сохранить файл настроек службы DiSecSrv - файл **disecsrv.ini**, помещенный в эту же директорию.

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

- запустить оболочку DiSec (если она не запущена);
- активизировать в **Главном меню** оболочки (Рис. 11) команду **Настройка**, получить окно **Настройка**, открытое на вкладке **Общие** (раздел 7.1, с. 27) и снять флажок **Автоматически запускать оболочку DiSec при загрузке ОС**;
- на вкладке **Драйвер DiSec** окна **Настройка** снять флажок **Разрешить запись протокола**;
- из **Главного меню** оболочки DiSec выполнить команду **Выход** (выйти из оболочки).

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, оболочки 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 XP имя персональной директории имеет следующий вид:

<системный диск>:\Documents and Settings\<<имя пользователя>\Application Data\Factor-TS\DionIS Security.

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

6 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 6.1, с. 23);
- возможность использования ПО различными пользователями ОС WINDOWS компьютера независимо друг от друга в режиме работы с оболочкой DiSec (раздел 6.2, с. 23);
- работа в режиме службы WINDOWS (раздел 6.3, с. 25).

6.1 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 (**Administrations**), 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 оболочки DiSec, хранятся в системной локальной области каждого пользователя (в персональной директории пользователя) в файле настроек (**INI**-файле) 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 активизации этих кнопок выдается запрос на ввод данных пользователя с административными правами.


Запуск службы DiSecSrv выполняется либо от имени одного «выделенного» пользователя, имеющего соответствующие права (право входа в систему в качестве службы), либо от имени системной учетной записи LOCAL SYSTEM.

6.2 Работа с оболочкой DiSec

Оболочка (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.

6.2.1 Принципы работы

После установки ПО DiSec и перезагрузки компьютера (как это требуется в процедуре инсталляции) на рабочем столе каждого пользователя WINDOWS появляется ярлык программы для запуска оболочки DiSec.

При запуске оболочки DiSec с помощью ярлыка программы или посредством команды стартового системного меню: **Пуск** ⇒ **Программы** ⇒ **DioNIS Security** ⇒ **DiSec** на панели задач рабочего стола пользователя в области уведомлений (SYSTEM TRAY) появится значок программы , который служит признаком того, что оболочка активна. 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. 6.3, стр. 25).

Отсутствие значка означает, что оболочка не запущена, и ее необходимо запустить.


При постоянном использовании DiSec рекомендуется установить режим автоматического вызова оболочки при старте операционной системы, в противном случае флажок автоматического запуска следует снять (см. раздел 7.1, с. 27).

При постоянной работе с каким-либо одним ресурсом (защищенной сетью) рекомендуется выполнить настройку автоматического установления соединения при запуске оболочки (см. раздел 7.1, с. 27). В этом случае после входа в систему пользователь сразу сможет работать с защищенными ресурсами.

В процессе работы оболочки DiSec и выполнения ее команд ведется журнал событий, таких как запуск и останов оболочки, при этом фиксируется имя текущего пользователя; в журнал заносятся 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 оболочки 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.

6.2.2 Команды оболочки DiSec

Работа с оболочкой DiSec выполняется посредством команд Главного меню оболочки (Рис. 11). Для вывода на экран Главного меню оболочки необходимо кликнуть правой кнопкой «мыши» на значке программы , расположенном на панели задач рабочего стола в области уведомлений (SYSTEM TRAY).

Команды Главного меню оболочки (Рис. 11) служат для выполнения следующих действий:

- настройка всех компонентов DiSec;
- подключение (и отключение) к одной из защищенных сетей 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.

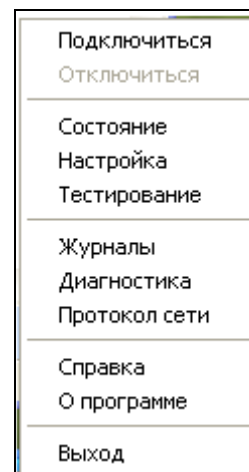


Рис. 11. Главное меню оболочки DiSec

По команде **Подключиться** выполняется процедура организации туннеля с одним из Серверов VPN для работы с сетевыми ресурсами соответствующей защищенной сети. Действия, выполняемые при этом DiSec, зависят от типа туннеля и режима его организации (см. разделы 8.1, с. 56 и 8.2, с. 58).

По команде **Отключиться** выполняется разъединение с соответствующим Сервером VPN. Команда доступна только при наличии связи с Сервером VPN. Действия DiSec, выполняемые при активизации команды, зависят от типа туннеля и режима его организации (см. раздел 8.3, с. 58).

Команда **Состояние** позволяет просмотреть текущее состояние параметров работы драйвера DiSec, в том числе информацию об установленном туннеле и статистические данные по сетевым интерфейсам (раздел 9, с. 59).

Команда **Настройка** обеспечивает выполнение следующих функций (раздел 7, с. 27):

- установка основных параметров всех составляющих системы - драйвера DiSec, оболочки DiSec и службы DiSecSrv;
- настройка реквизитов подключения к защищенным сетям для оболочки и службы;
- задание параметров ведения журналов работы ПО DiSec;
- задание параметров ведения протокола сети.

Команда **Тестирование** предназначена для проверки состояния IP-компонента WINDOWS, а также для тестирования доступности сетевых ресурсов (раздел 10, с. 63). 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 оболочки DiSec и журнал работы службы DiSecSrv (раздел 11, с. 69).

Команда **Диагностика** служит для просмотра накопленных во время сеанса работы DiSec диагностических сообщений, которые выдают компоненты (оболочка и драйвер) DiSec при подключении к Серверу VPN (раздел 11.2, с. 69). 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 случаев неработоспособности.

Команда **Протокол сети** позволяет просмотреть на экране файл, содержащий протокол работы сети (раздел 11.3, с. 70) – заданную при настройке информацию о проходящих через драйвер DiSec сетевых пакетах.

Команда **Справка** позволяет получить полную справочную информацию по работе с DiSec (раздел 12, с. 72).

Команда **Выход** позволяет завершить работу с оболочкой DiSec. Данная команда используется при удалении ПО DiSec с компьютера (см. раздел 5, с. 22), а также при работе в режиме ручного запуска оболочки (раздел 13, с. 72). 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.

6.3 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 (см. Рис. 15, с. 30), с которым будет работать служба DiSecSrv, и назначить его для использования службой (см. раздел 7.6, с. 52).

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. 17). 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. 12).

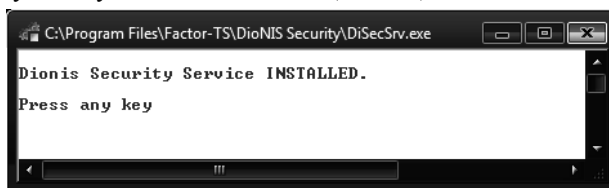


Рис. 12

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 7.6, с. 52), 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 **Dionis Security Service**, и в окне свойств на вкладке **Вход в систему** выбрать пользователя.

Рекомендуется проверить работу службы в окне **Тестирование** (см. раздел 10.5, с. 66).

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.

Примечание - При работе в режиме IPSEC-ГОСТ необходимо обеспечить защиту хранилища сертификатов, иначе служба будет пытаться выдать сообщение.

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.

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.

Примечание - Одновременная организация туннеля службой DiSecSrv и оболочкой DiSec невозможна. При необходимости работы с оболочкой следует остановить работу службы DiSecSrv.

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. 10.5, с. 66).

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. 10.5, с. 66).

Для диагностирования проблем с запуском службы следует просмотреть журнал событий **DiSecSrv.log** при помощи соответствующий команды Главного меню оболочки ПО DiSec (раздел 11, с. 69).

7 Команда Настройка

Команда Главного меню оболочки (Рис. 11) **Настройка** позволяет установить параметры работы для всех компонентов DiSec - драйвера, службы и оболочки. Команда позволяет:

- задать список ресурсов подключений (защищенных сетей) и указать необходимые для подключения реквизиты;
- задать режимы работы драйвера, в частности задать режим протоколирования сетевой активности (доступно только пользователю, обладающему административными правами в операционной системе WINDOWS);
- задать режим запуска оболочки и параметры ведения журнала событий;
- 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.

7.1 Вкладка Общие (Настройка ПО DiSec)

После активизации команды **Настройка** на экран будет выведено окно **Настройка ПО DiSec**, открытое на вкладке **Общие** (Рис. 13).

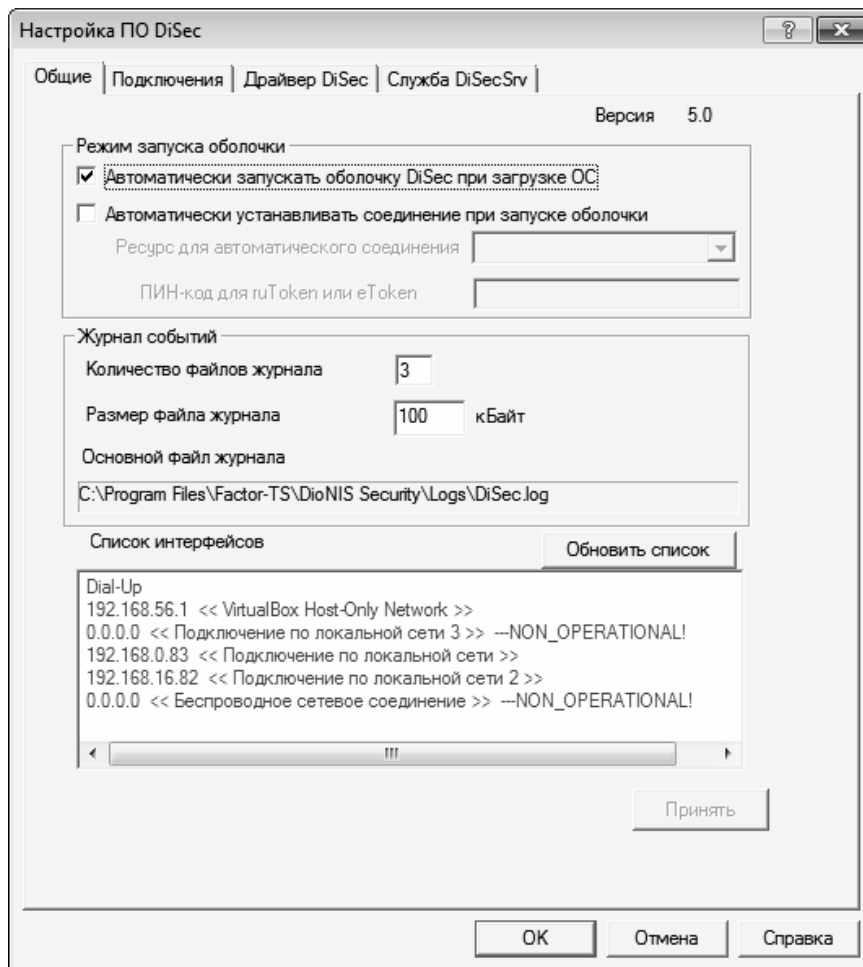



Рис. 13

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

7.1.1 Режим запуска оболочки

Два флажка под заголовком **Режим запуска оболочки**.

1. **Автоматически запускать оболочку DiSec при загрузке ОС** - установленный флажок обеспечивает автоматический запуск оболочки DiSec при старте операционной системы. При этом в области уведомлений SYSTEM TRAY рабочего стола пользователя появляется значок программы . При снятом флажке автоматический запуск оболочки 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.

2. **Автоматически устанавливать соединение при запуске оболочки** - установленный флажок обеспечивает автоматическое подключение к указанному ресурсу после запуска оболочки DiSec.

При снятом флажке попытка автоматического подключения не выполняется, и пользователь должен подключиться к защищенной сети вручную посредством команды **Подключиться** из Главного меню оболочки DiSec (см. раздел 8.1, с. 56).

Если флажок установлен, становится активным элемент **Ресурс для автоматического соединения** для выбора ресурса автоматического соединения из списка ресурсов данного пользователя (см. раздел 7.2, стр. 29). При успешном подключении в области уведомления SYSTEM TRAY рабочего стола появляется значок программы зеленого цвета.

Если флажок установлен и для работы с ресурсом подключения указано использование ключевого носителя типа **ruToken** или **eToken**, то становится активным элемент **ПИН-код для ruToken или eToken** для ввода пароля ключевого носителя, соответствующего ресурсу автоматического соединения (см. раздел 7.3, с. 30).

7.1.2 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.

7.1.3 Список интерфейсов

В секции под заголовком **Список интерфейсов** отображаются активные сетевые интерфейсы TCP/IP (интерфейсы, соответствующие платам Ethernet, беспроводным соединениям, 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 не успешна, например, после инсталляции не была выполнена перезагрузка ОС.

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

При отсутствии какого-либо интерфейса в списке необходимо проверить настройку ОС (наличие драйверов плат локальной сети, 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.

7.2 Вкладка Подключения (Настройка ПО DiSec)

Вкладка **Подключения** (Рис. 14) 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.

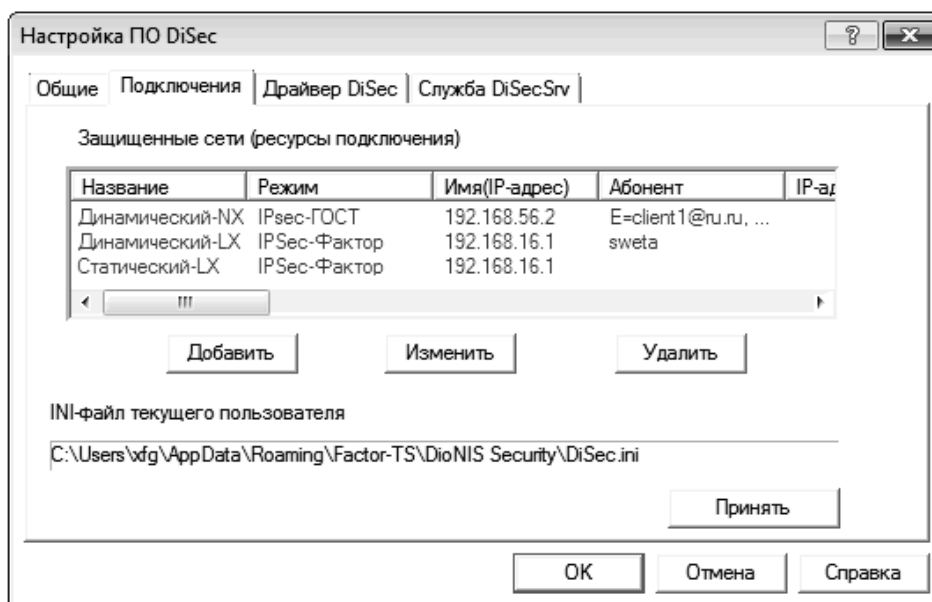


Рис. 14

Под заголовком **Защищенные сети (ресурсы подключения)** выводится список ресурсов подключения к соответствующим защищенным сетям 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 7.3, с. 30.

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

- кнопка **Добавить** позволяет внести в список новый ресурс; после ее нажатия открывается окно **Реквизиты подключения** (Рис. 15), 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**; при ее нажатии открывается то же окно **Реквизиты подключения** (Рис. 15) с установленными ранее значениями реквизитов, и пользователю предоставляется возможность изменить данные;
- нажатие кнопки **Удалить** без дополнительного запроса удаляет выделенный курсором ресурс.

В нижней части экрана в поле под заголовком **INI-файл текущего пользователя** выводится имя файла с индивидуальными параметрами абонента DiSec (см раздел 6.1, с. 23).

7.3 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.

Открывается окно на вкладке **Общие** (Рис. 15).

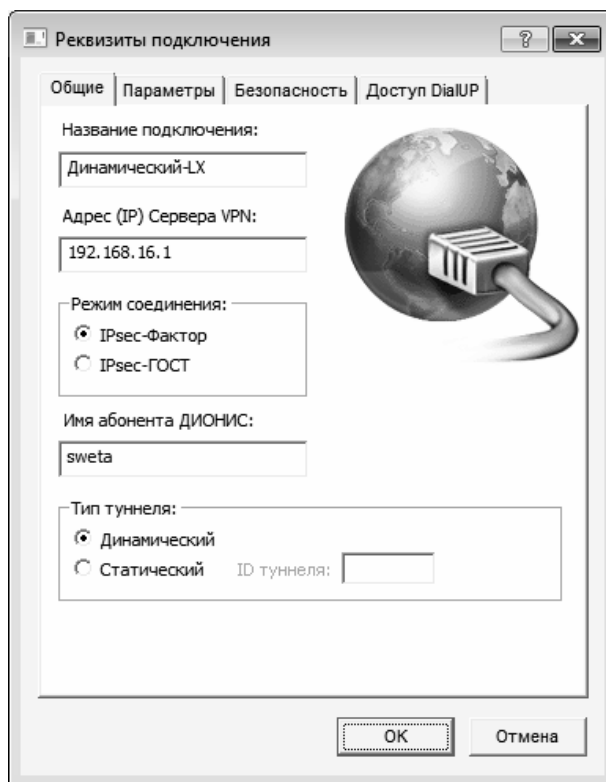


Рис. 15

7.3.1 Вкладка Общие (Реквизиты подключения)

На вкладке **Общие** (Рис. 15) назначаются основные параметры, которые определяют содержание остальных вкладок.

Название подключения – 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 8, с. 56). Длина названия не должна превышать 32 символов, название может содержать символы латинского алфавита и кириллицы, а также другие знаки, кроме знаков «=» и «,».

Адрес (IP) Сервера VPN - в поле следует ввести IP-адрес Сервера VPN или его доменное имя (адрес того интерфейса Сервера VPN, к которому осуществляется подключение).

Режим соединения. С помощью переключателя надо указать режим организации туннеля – IPsec-Фактор или IPsec-ГОСТ.

Имя абонента ДИОНИС – данное поле 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 КМ ДИОНИС).

7.3.2 Вкладка Параметры (Реквизиты подключения) для режима IPSEC-ФАКТОР

Для режима IPSEC-ФАКТОР на вкладке (Рис. 16) размещены 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).

Если указан **IP-адрес клиента**, то необходимо указать также параметры: **Маска LAN**, **Шлюз LAN** и **Метрика**.

Может быть задан только **DNS сервер** (и его **Индекс**) без указания остальных параметров.

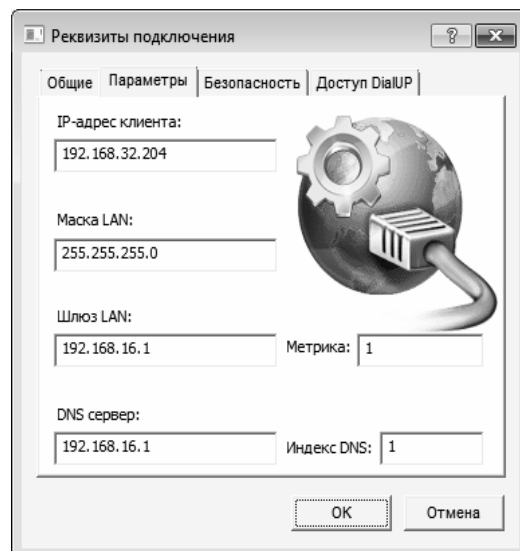


Рис. 16

Выполнив настройки на вкладке **Параметры** окна **Реквизиты подключения**, надо открыть вкладку **Безопасность** и выполнить настройку криптосистемы (см. раздел 7.3.3, с. 31).

7.3.3 Вкладка Безопасность (Реквизиты подключения) для режима IPSEC-ФАКТОР

Вкладка представлена на Рис. 17. С помощью переключателя под заголовком **Ключевой носитель** надо указать ключевой носитель с персональной ключевой информацией пользователя DiSec, необходимой для организации туннеля с Сервером VPN (см. раздел 2.4.1, с. 10).

Поля под заголовком **Параметры ключей**

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

Значения полей **Номер серии** и **Локальный** 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. Поле 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. 13).



Рис. 17

7.3.4 Вкладка Параметры (Реквизиты подключения) для режима IPSEC-ГОСТ

Для режима IPSEC-ГОСТ на вкладке **Параметры** (Рис. 18) размещены элементы управления, позволяющие назначать и модифицировать политики согласования криптоалгоритмов и ключевого материала между взаимодействующими сторонами (DiSec и Сервер VPN).

Элемент управления **Политики IKE** позволяет выбрать из выпадающего списка политику IKE для данного туннеля. Политика IKE содержит параметры, используемые на 1-ой фазе протокола IKE.

Элемент управления **Политики ESP** позволяет выбрать из выпадающего списка политику ESP для данного туннеля. Политика ESP содержит параметры, используемые на 2-ой фазе протокола IKE, и параметры протокола ESP.

Нажатие той или иной кнопки под элементами **Политики IKE** и **Политики ESP** приводит к выводу на экран соответствующего окна (Рис. 19, Рис. 20), и пользователь получает возможность создавать новые политики, изменять и удалять выбранные ранее (см. ниже разделы 7.3.4.1 и 7.3.4.2).

Целевые объекты (хост или сеть) - в поле под этим заголовком надо указать ресурсы внутренней сети (защищаемой данным Сервером VPN), к которым получит доступ пользователь DiSec посредством туннеля.

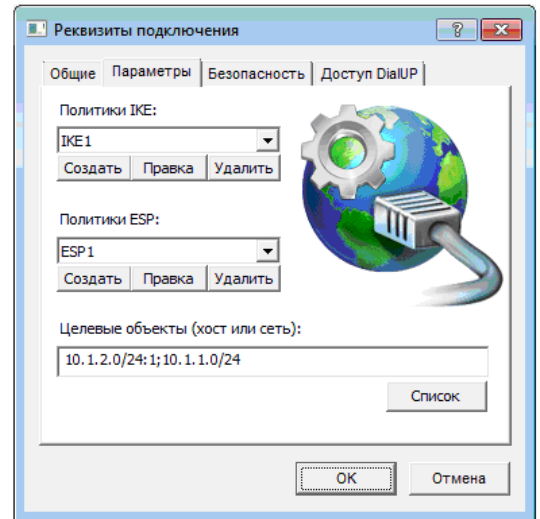


Рис. 18

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 3.4.2, п. 10, с. 14).

Выполнив настройки на вкладке **Параметры** окна **Реквизиты подключения**, надо в этом окне открыть вкладку **Безопасность** и выполнить настройку криптосистемы (см. ниже раздел 7.3.4.3, с. 35).

Замечание. Если криптосистема настроена и не требует никаких изменений, то надо нажать кнопку **OK** и вернуться на вкладку **Подключения** окна **Настройка ПО DiSec** (Рис. 14).

7.3.4.1 Настройка политики IKE

Политика IKE (Рис. 18) 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. 19).

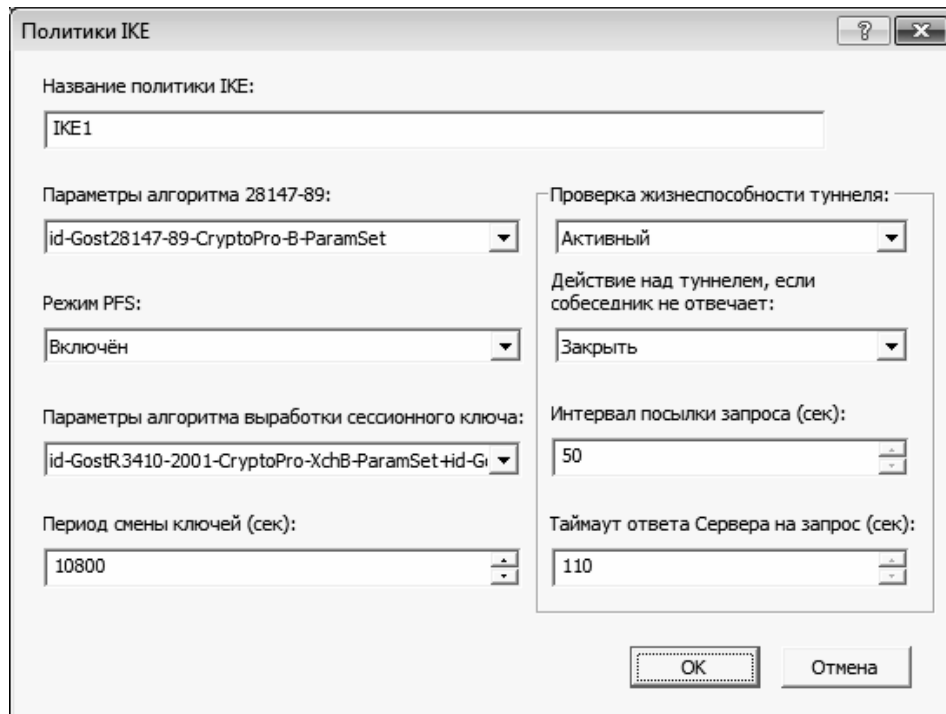


Рис. 19

Название политики IKE

В поле под этим заголовком надо ввести произвольную последовательность символов, за исключением знаков запятой и двоеточия. Длина последовательности не должна превышать 32 символа.

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-B-ParamSet*. Если потребуется другое значение, его можно выбрать из выпадающего списка.

Значение параметра должно совпадать с соответствующим значением на Сервере VPN (см. раздел 3.4.2, п. 19, с. 14).

Замечание. Символ «B» 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 *Выключен* (значение по умолчанию), *Включен*.

Значение параметра должно быть согласовано со значением на Сервере VPN (см раздел 3.4.2, п. 21, с. 15).

Замечание. 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. Значение по умолчанию - *id-GostR3410-2001-CryptoPro-XchB-ParamSet+id-GostR3410-94*. Если потребуется другое значение, его можно выбрать из выпадающего списка.

Значение параметра должно совпадать с соответствующим значением на Сервере VPN (см раздел 3.4.2, п. 19, с. 14).

Период смены ключей (сек)

Значение параметра определяет *время жизни* установленной фазы 1. По окончании указанного периода инициируется выполнение фазы 1 протокола IKE для выработки новых ключей шифрования. По умолчанию время жизни 1-ой фазы – *10800 сек*.

Значение параметра должно совпадать с соответствующим значением на Сервере VPN (см раздел 3.4.2, п. 24, с. 15).

Проверка жизнеспособности туннеля

Параметр предназначен для выполнения проверки жизнеспособности туннеля посредством периодической отправки 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 (значение по умолчанию) отвечает на запросы Сервера VPN;
- *Активный* – DiSec посылает запросы на Сервер VPN и контролирует ответы.

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 не отвечает на запросы
- *Инициировать заново* – если Сервер не отвечает на запросы, DiSec закрывает туннель и пытается установить его еще раз.

Интервал отправки запроса (сек)

В поле под этим заголовком надо задать целое число – интервал отправки запросов в секундах. Значение по умолчанию – *50*.

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. Значение по умолчанию – *110*.

7.3.4.2 Настройка политики ESP

Политика ESP (Рис. 18) определяет правила формирования ключей шифрования и алгоритмы шифрования сетевых пакетов, передаваемых по туннелю при использовании протокола ESP (Рис. 20).

Название политики ESP

В поле под этим заголовком надо ввести произвольную последовательность символов, за исключением знаков запятой и двоеточия. Длина последовательности не должна превышать 32 символа.

Режим инкапсуляции трафика

Параметр определяет вариант настройки протокола ESP, возможные значения:

- *Туннель* – значение по умолчанию;
- *Транспортный*.

Значение параметра должно совпадать с соответствующим значением на Сервере VPN (см раздел 3.4.2, п. 8, с. 14).

Преобразование ESP

Значение по умолчанию в поле - *GOST-4M-IMIT-B*.

Замечание - Поле определяет два параметра, значения которых должны совпадать с соответствующими значениями на Сервере VPN (см раздел 3.4.2, п. 20, с. 14):

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

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 7.3.4.1, с. 32 «**Параметры алгоритма выработки сессионного ключа**»). Если потребуется другое значение, его можно выбрать из выпадающего списка. Значение параметра должно совпадать с соответствующим значением на Сервере VPN (см раздел 3.4.2, п. 22, с. 15).

Период смены ключей (сек) :

Значение параметра определяет *время жизни* установленной фазы 2. По окончании указанного периода инициируется выполнение фазы 2 протокола IKE для выработки новых ключей шифрования. По умолчанию время жизни 2-ой фазы – *3600 сек*. Значение параметра должно совпадать с соответствующим значением на Сервере VPN (см раздел 3.4.2, п. 24, с. 15).

Допустимое количество искаженных пакетов

Если число искаженных пакетов превысит заданное параметром значение, туннель будет закрыт (наличие искажений фиксируется при проверке имитовставки пакета). Значение по умолчанию параметра – *100000*.

При этом в системном журнале **EventLog** будет зафиксирована ошибка (см. Рис. 21, Рис. 22).

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 3.4.2, п. 14, с. 14).

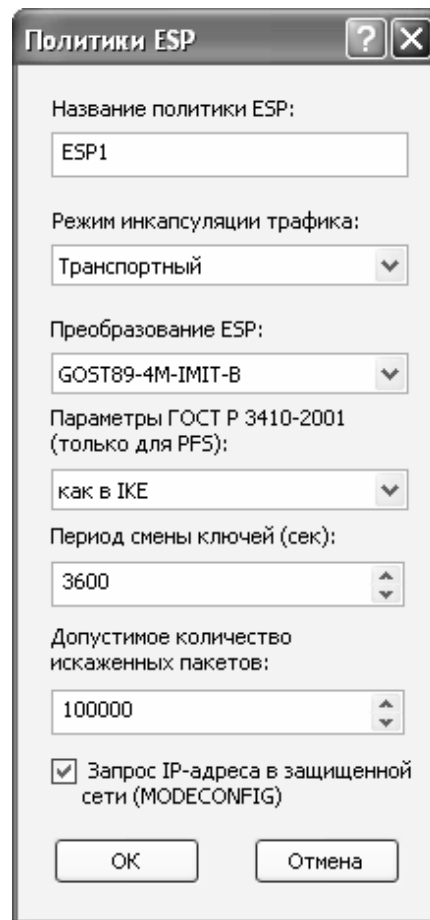


Рис. 20

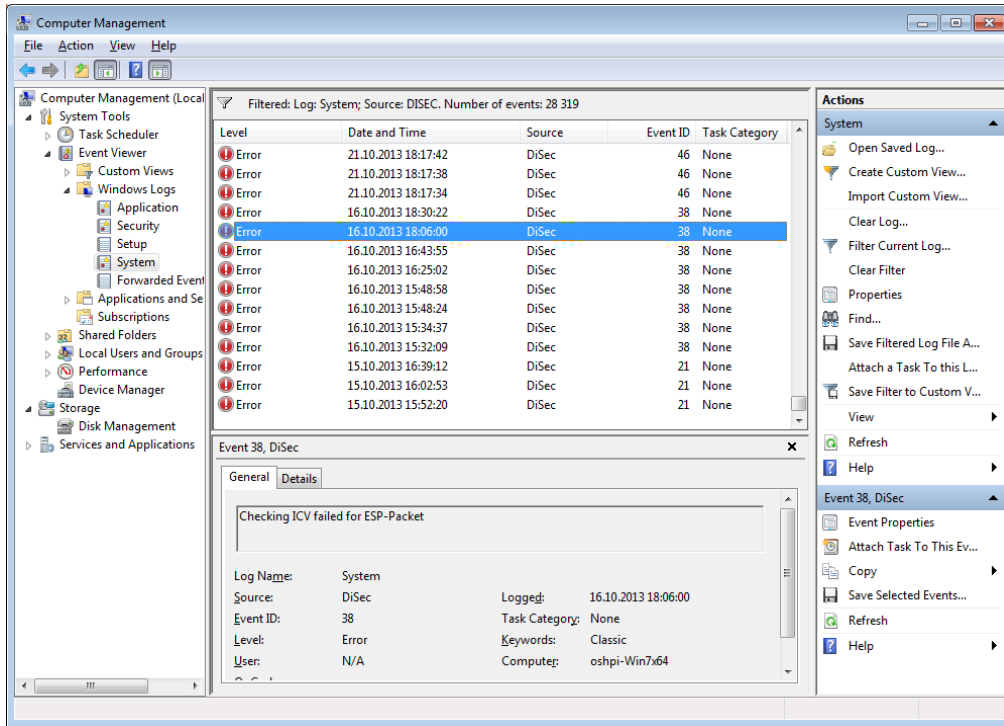


Рис. 21

Более подробная информация имеет вид:

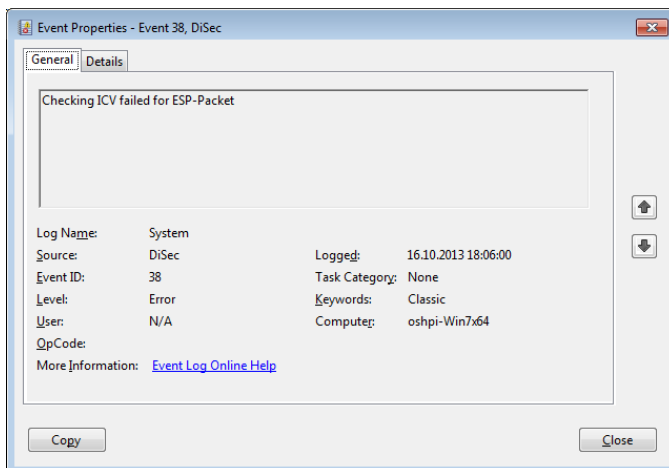


Рис. 22

7.3.4.3 Настройка Целевых объектов

Список целевых объектов (Рис. 18) 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 (хост или сеть)** (Рис. 18) оставить незаполненным, то клиент DiSec получит доступ только к самому Серверу VPN. Значение параметра должно быть согласовано с соответствующей настройкой на Сервере VPN (см раздел 3.4.2, п. 10, с. 14).
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** (Рис. 18) предоставляет более удобный способ задания списка целевых объектов. После ее нажатия открывается окно **Настройка списка целевых объектов** (Рис. 23), которое позволяет создать, изменить, удалить отдельный объект, а также изменить последовательность элементов списка.

При нажатии кнопки **Добавить** (или **Изменить**) открывается окно **Целевой объект** (Рис. 24), которое позволяет задать (отредактировать) все параметры целевого объекта, к которому необходимо получить доступ через туннель, – IP-адрес, маску (**Зн. бит**), протокол и порт.

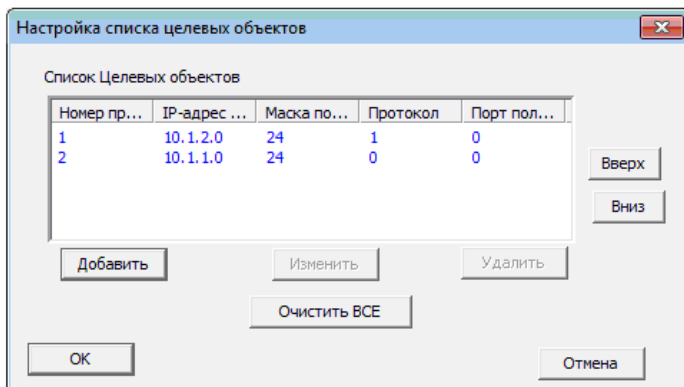


Рис. 23

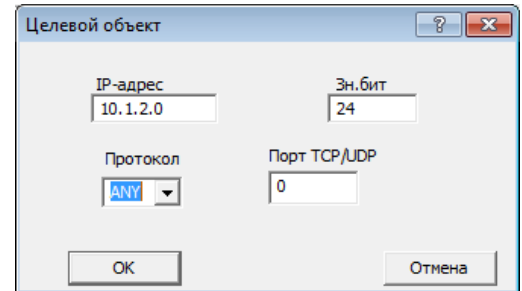


Рис. 24

7.3.5 Вкладка Безопасность (Реквизиты подключения) для режима IPSEC-ГОСТ

Для режима IPSEC-ГОСТ вкладка **Безопасность** имеет вид, представленный на Рис. 25.

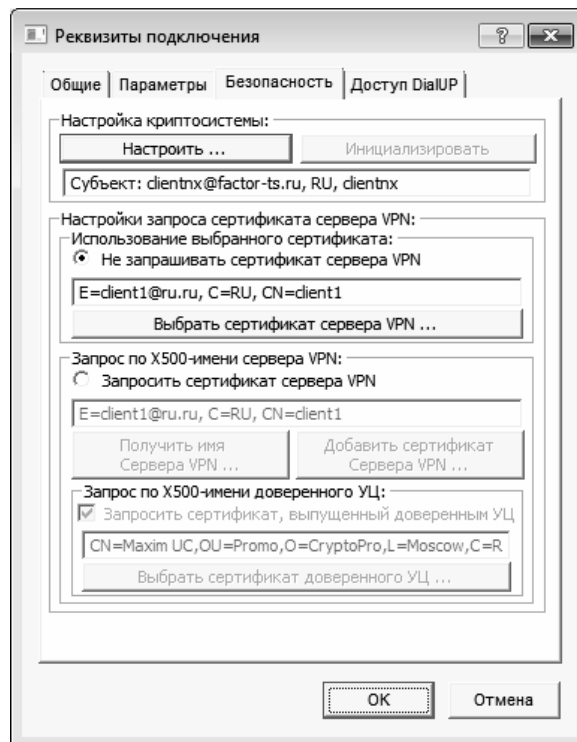


Рис. 25

7.3.5.1 Настройка криптосистемы

Начинать настройку криптосистемы DiSec надо с нажатия кнопки **Настроить** под заголовком **Настройка криптосистемы** (Рис. 25). В дальнейшем с помощью этой кнопки можно внести изменения в параметры настройки.

После нажатия кнопки **Настроить** на экран будет выведено окно **Установки криптосистемы** (Рис. 26).

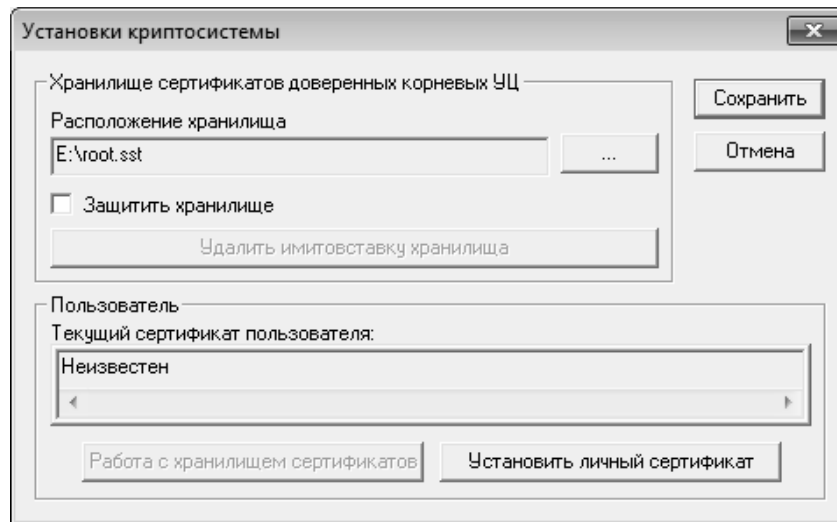


Рис. 26

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. По умолчанию значение поля - **a:\root.sst**. Если предполагается разместить файл **root.sst** в другом месте, то надо нажать кнопку **...** (справа от имени), получить стандартное окно WINDOWS обзора папок и выбрать нужную. Имя файла изменить нельзя.

Настройка криптосистемы обеспечивает ввод в систему закрытого ключа пользователя, создание необходимых хранилищ, занесение личного сертификата пользователя в хранилище **Сертификаты** и назначение его текущим, а также занесение в соответствующие хранилища всех необходимых сертификатов УЦ и списков отозванных сертификатов.

Замечание - Для хранения сертификатов в DiSec используется набор из трех хранилищ: **Сертификаты**, **Списки отзыва** и **Доверенные УЦ**. Подробно работа с хранилищами описана ниже в разделе 7.3.5.4, с. 41.

Начальная настройка криптосистемы выполняется следующей последовательностью действий.

Замечание - 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. 26) нажать кнопку **Установить личный сертификат**.

На экран будет выведено окно **Выберите носитель** (Рис. 27), содержащее список имен контейнеров (с указанием системного имени считывающего устройства) на этом ключевом носителе, а также и на других носителях, если они вставлены в другие считывающие устройства.

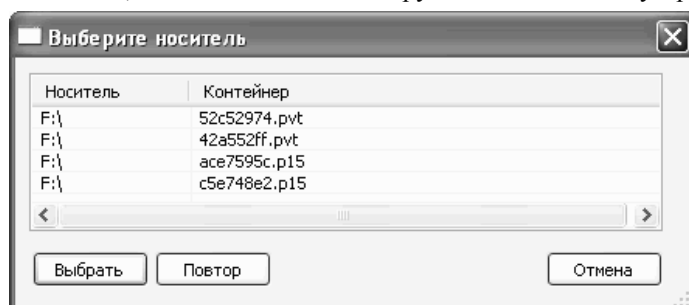


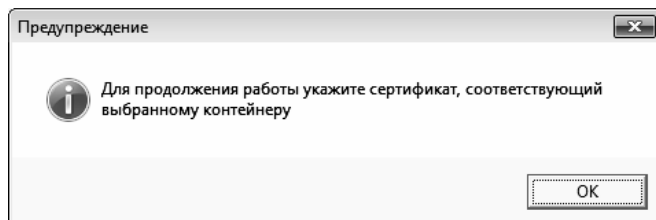
Рис. 27

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:



После нажатия кнопки **OK** на экран будет выведено стандартное окно WINDOWS, позволяющее выбрать файл с нужным сертификатом (имена файлов с расширением **cer**).

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

Система выведет на экран информацию из выбранного сертификата, которая позволит пользователю идентифицировать сертификат (Рис. 28), и предложит назначить его текущим.

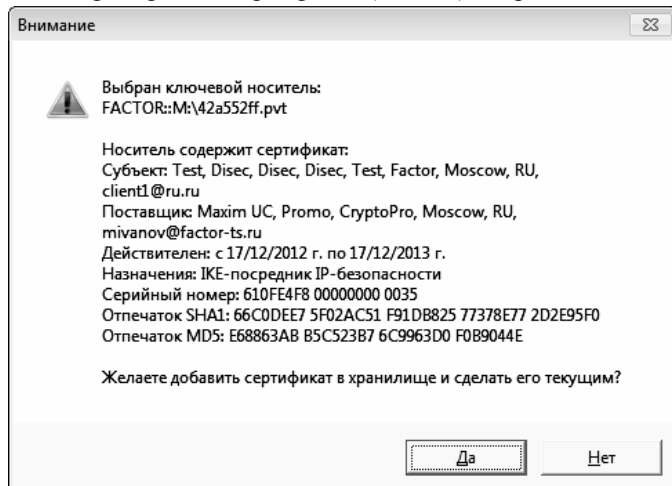
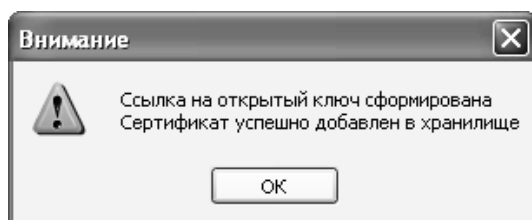


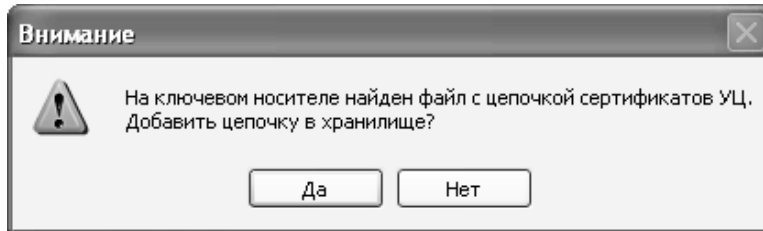
Рис. 28

По нажатию кнопки **ДА** будет сформирована необходимая ссылка, личный сертификат пользователя будет добавлен в хранилище **Сертификаты** и назначен текущим (нажатием кнопки **НЕТ** операцию добавления личного сертификата в хранилище можно прервать).

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

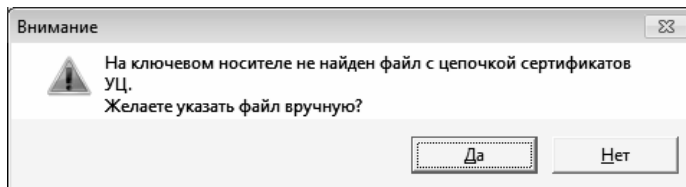


3. DiSec проверит наличие файла с сертификатом доверенного корневого УЦ (и цепочкой сертификатов доверенных УЦ) на ключевом носителе и предложит добавить цепочку в хранилище:

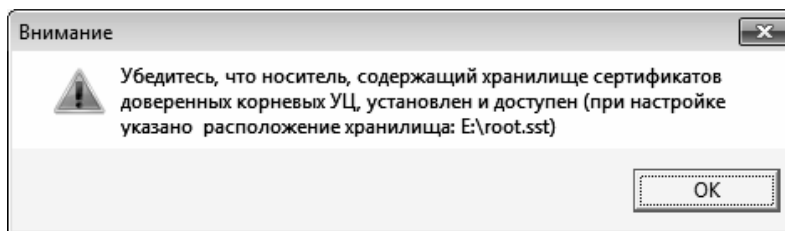


По умолчанию имя файла - **cacer.p7b**; основную часть имени можно изменить соответствующей записью в файле **crypt.ini**, расширение имени менять не разрешается.

Если файла не окажется, то будет выдано предупреждение-запрос и предоставлена возможность указать файл вручную:



После нажатия кнопки **Да** выводится предупреждение:



И затем на экран будет выведено стандартное окно WINDOWS, позволяющее выбрать файл. Имена файлов с сертификатами доверенных УЦ имеют расширение **p7b**.

После того как файл будет найден, система выведет на экран информацию из корневого сертификата, которая позволит пользователю идентифицировать сертификат (Рис. 29), и предложит добавить его в хранилище (или заменить, если сертификат уже находится в хранилище).

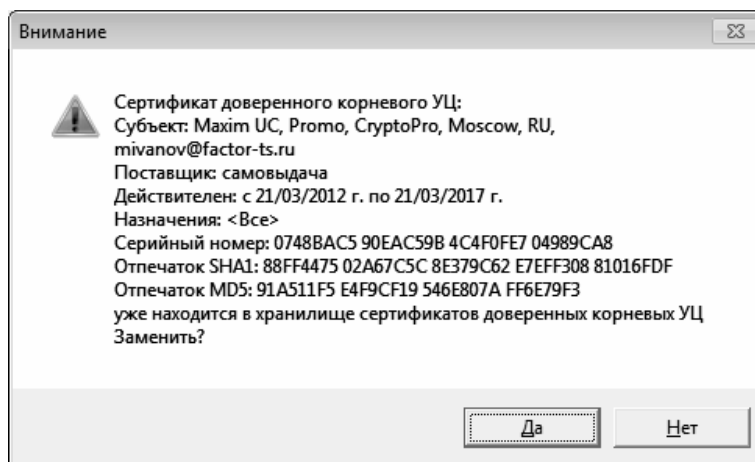


Рис. 29

По нажатию кнопки **Да** сертификат будет добавлен в два хранилища **Сертификаты** и **Доверенные УЦ**.

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

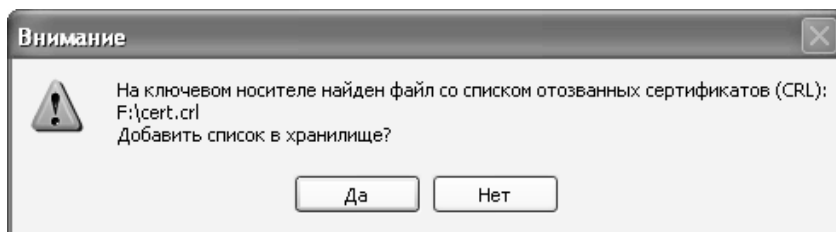


Рис. 30

После нажатия кнопки **Да** файл будет добавлен в хранилище **Списки отзыва**.

- После того как будут выполнены все настройки, надо в окне **Установки криптосистемы** (Рис. 26) нажать кнопку **Сохранить**. Система выдаст предупреждение (Рис. 31):

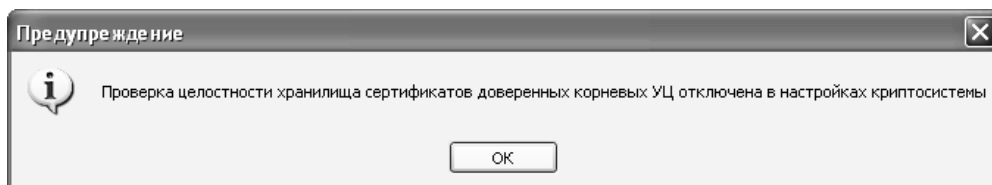


Рис. 31

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**.

7.3.5.2 Настройки запроса сертификата Сервера VPN

Вкладка **Безопасность** (Рис. 25). 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 (контроля идентификации) сравнения с тем сертификатом, который имеется у пользователя DiSec (запрос посылается после того как с Сервером будет установлена связь на 1 фазе работы протокола IKE).

Напомним – сертификаты всех Серверов VPN, с которыми предполагается создавать туннели, предварительно помещаются в хранилище **Сертификаты** (см. раздел 3.6.2, с. 16).

----- Использование выбранного сертификата -----

При установленном переключателе **Не запрашивать сертификат сервера VPN** становится активной кнопка **Выбрать сертификат сервера VPN**. После ее нажатия на экран будет выведено содержимое хранилища **Сертификаты** (Рис. 32). 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. 25)..

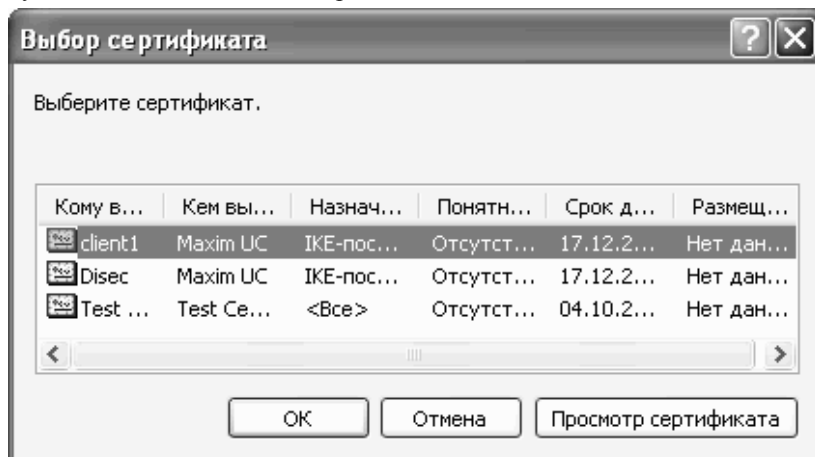


Рис. 32

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

----- Запрос по X500-имени сервера VPN -----

При установленном переключателе **Запросить сертификат сервера VPN** надо нажать кнопку **Получить имя Сервера VPN**. На экран будет выведено содержимое хранилища **Сертификаты** (Рис. 32). В списке надо выделить требуемый сертификат и нажать кнопку **ОК - X500-имя** из сертификата Сервера VPN будет занесено в поле под переключателем.

Если в хранилище не окажется нужного сертификата, то надо нажать кнопку **Добавить сертификат Сервера VPN**. На экран будет выведено стандартное окно WINDOWS поиска файлов со списком сертификатов на ключевом носителе (файлы с именами, имеющими расширение **cer**). В этом окне надо найти нужный сертификат (на ключевом носителе или в другом месте) и нажать кнопку **Открыть**. Выбранный сертификат будет добавлен в хранилище **Сертификаты**.

При такой настройке DiSec после того, как будет установлена связь, запросит у Сервера VPN его сертификат. Если **X500-имя** из полученного сертификата совпадет с указанным при настройке, то DiSec будет использовать указанный сертификат для организации туннеля.

----- Запрос по X500-имени доверенного УЦ -----

Если сертификат Сервера VPN выпущен не тем УЦ, который рекомендован службой безопасности эксплуатирующей организации, то можно запросить у Сервера VPN предоставить сертификат, подписанный требуемым Удостоверяющим Центром.

Для этого надо на вкладке **Безопасность** (Рис. 25):

- установить переключатель **Запросить сертификат Сервера VPN** и занести в поле **X500-имя** из сертификата Сервера VPN, как описано выше;
- установить флажок **Запросить сертификат, выпущенный доверенным УЦ** и нажать кнопку **Выбрать сертификат доверенного УЦ ...** На экран будет выведен список сертификатов доверенных УЦ, находящихся в хранилище **Доверенные УЦ**. 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 пришлет 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 указанный сертификат для организации туннеля.

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

7.3.5.3 Защита хранилища Доверенные УЦ

Если файл **root.sst**, содержащий хранилище доверенных 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 хранилища **Доверенные УЦ**.

Чтобы установить требуемый режим, надо на вкладке **Безопасность** нажать кнопку **Настроить** и установить флажок **Защитить хранилище** (Рис. 26) – система сформирует имитовставку хранилища **Доверенные УЦ** на текущем закрытом ключе пользователя. Имитовставка будет проверяться каждый раз при инициализации криптосистемы.

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

7.3.5.4 Работа с хранилищами

Как было сказано выше, для хранения сертификатов в DiSec используется набор из трех хранилищ:

1. Хранилище **Сертификаты** - предназначено для хранения личного сертификата ключа пользователя DiSec, сертификатов всех Серверов VPN, с которыми предполагается устанавливать туннели, и сертификатов доверенных удостоверяющих центров, включая корневые.
2. Хранилище **Списки отзыва** - предназначено для хранения действующих списков отозванных сертификатов всех УЦ, необходимых для построения цепочки доверия.
3. Хранилище **Доверенные УЦ** - предназначено для хранения сертификатов корневых УЦ (эти сертификаты продублированы в первом хранилище).

После того как будет выполнена инициализация криптосистемы, в окне **Установки криптосистемы** (Рис. 26) 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. 33).

Хранилище Сертификаты

В таблице на Рис. 33 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.

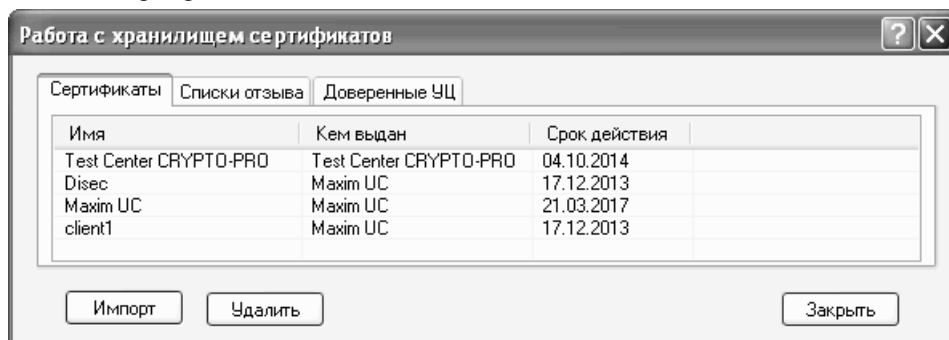


Рис. 33

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

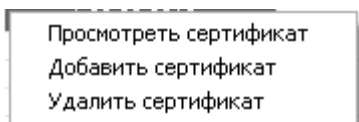


Рис. 34

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

При *добавлении* сертификата на экран выводится окно (Рис. 35), 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 поле **Тип файлов:** автоматически установлено **Сертификат (*.cer)**.

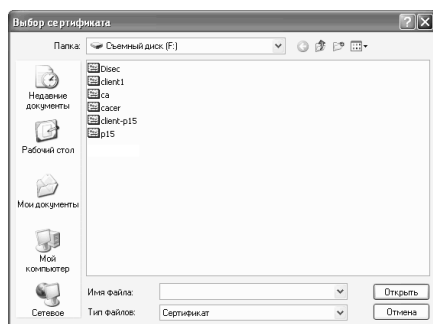


Рис. 35

Если надо добавить сертификат УЦ, то необходимо в поле **Тип файлов** выбрать значение **Хранилище сертификатов (*.p7b)** (имена файлов, содержащих сертификаты Удостоверяющих центров, имеют, как правило, расширение **p7b**), после чего список сертификатов УЦ появится в окне.

В списке надо перевести курсор на требуемый файл и нажать кнопку **Открыть** – выбранный сертификат будет добавлен в хранилище **Сертификаты**.

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

Чтобы *просмотреть* сертификат ключа, надо выделить соответствующую строку в таблице (Рис. 33) и дважды щелкнуть левой кнопкой мыши. Или в меню на Рис. 34 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.

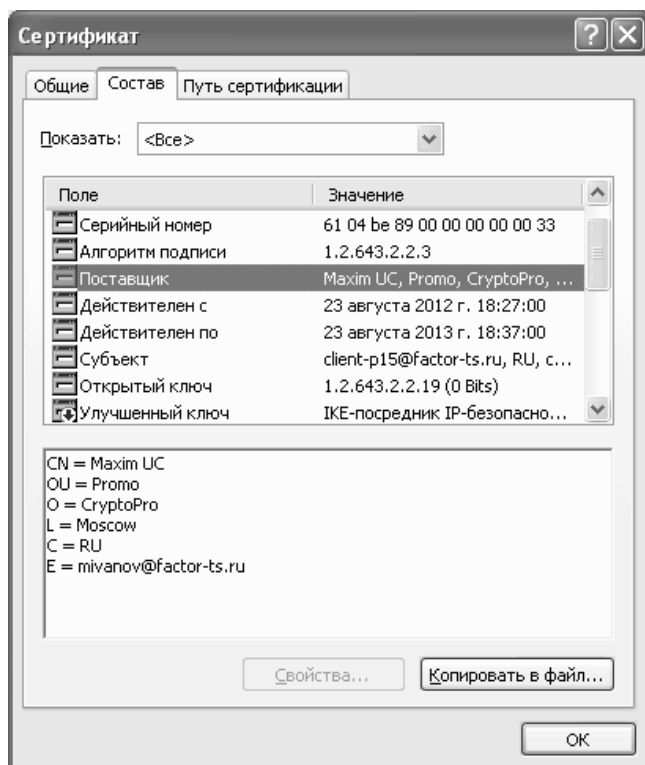


Рис. 36

На вкладке **Состав** (Рис. 36) 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.

Хранилище Списки отзыва

Вкладка **Списки отзыва** окна **Работа с хранилищем сертификатов** представлена на Рис. 37.

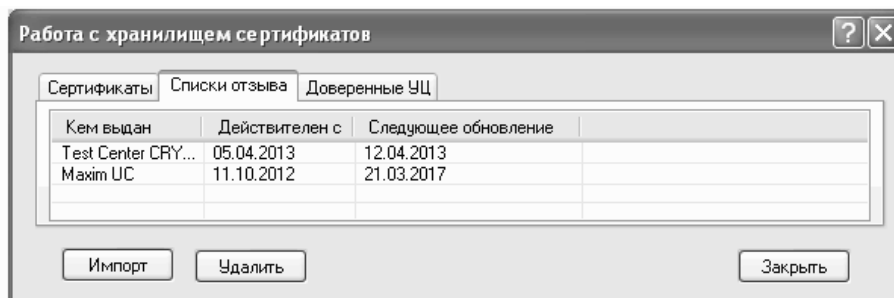


Рис. 37

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 сертификатами в хранилище **Сертификаты**.

При *просмотре* списка на экран выводится окно **Список отзыва сертификатов**, содержащее две вкладки и открытое на вкладке **Общие**. На этой вкладке (Рис. 38) 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.

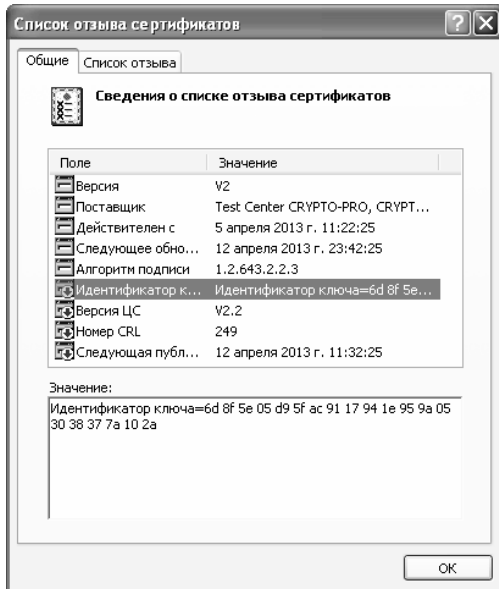


Рис. 38

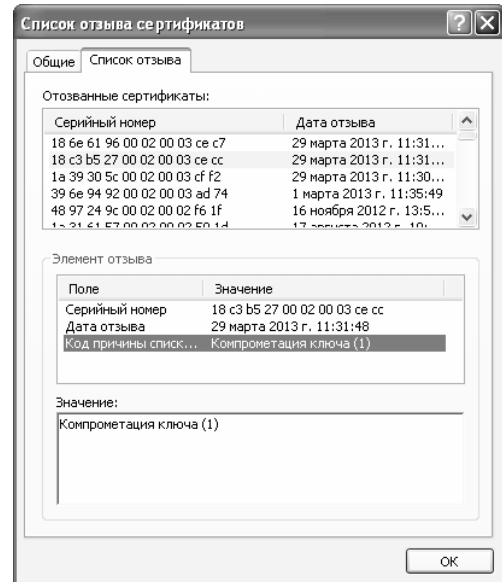


Рис. 39

На вкладке **Список отзыва** (Рис. 39) 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.

Хранилище **Доверенные УЦ**

Хранилище **Доверенные УЦ** содержит сертификаты корневых удостоверяющих центров (напомним, что они продублированы в хранилище **Сертификаты**).

В таблице на Рис. 40 каждый сертификат занимает одну строку. Формат записей полностью совпадает с рассмотренным выше форматом записей для хранилища **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 хранилища **Сертификаты**.

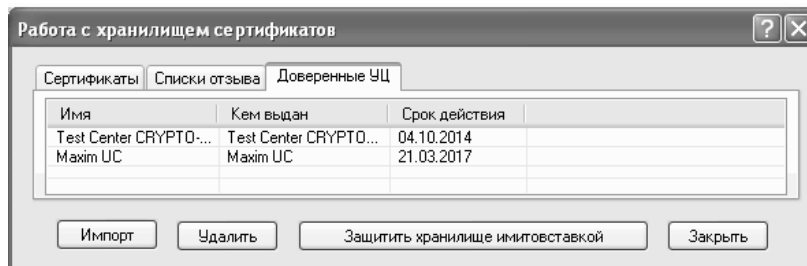


Рис. 40

Для хранилища **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.

7.3.6 Вкладка Доступ DialUP

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.

Имя ресурса DialUP - выбирается 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 предназначено для ввода имени пользователя; имя служит для авторизации на **сервере удаленного доступа**, в частном случае оно может совпадать с именем абонента Сервера VPN (если последний служит также и **сервером удаленного доступа**).

Пароль DialUP - поле предназначено для ввода пароля пользователя, соответствующего введенному имени; пароль также служит для авторизации на **сервере удаленного доступа**. Длина пароля не должна превышать 256 символов.

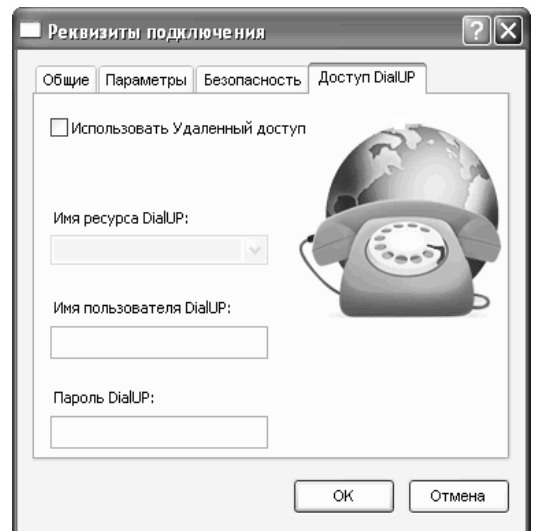


Рис. 41

7.4 Вкладка Драйвер DiSec (Настройка ПО DiSec)

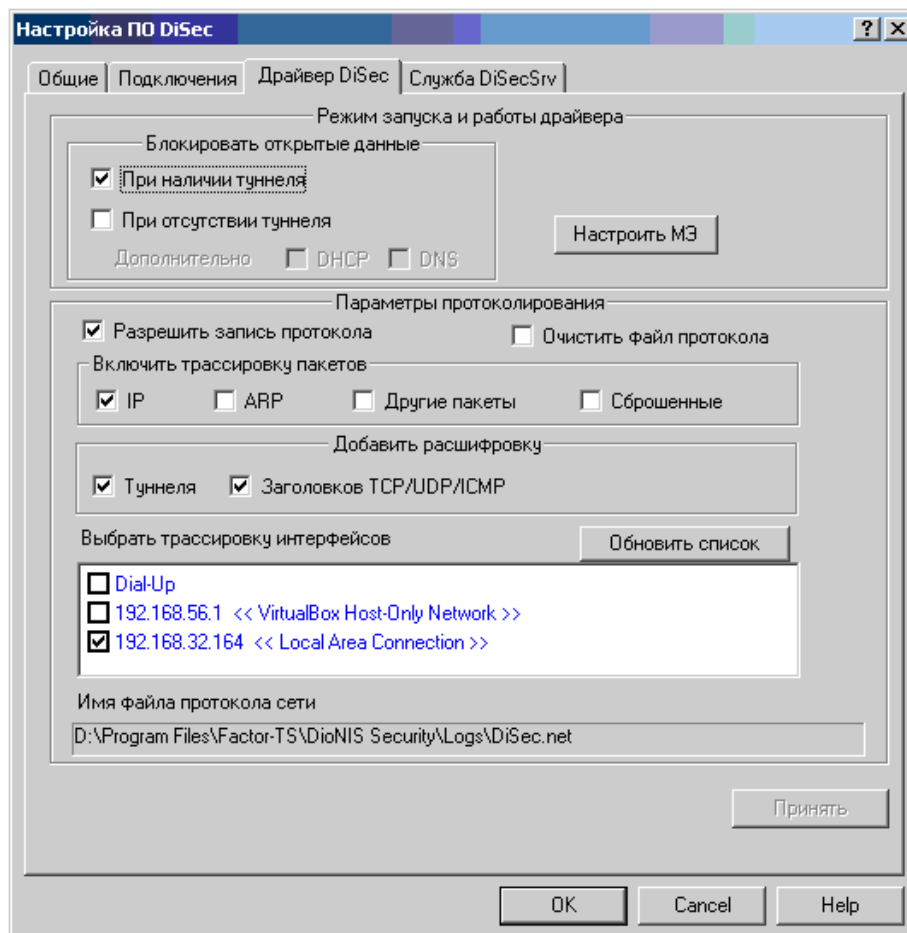


Рис. 42

На вкладке **Драйвер DiSec** окна **Настройка ПО DiSec** выполняются настройки режима работы драйвера и устанавливаются параметры протоколирования сети. Драйвер имеет элементы межсетевого экрана (МЭ); настройка МЭ выполняется на этой же вкладке (см. раздел 7.5, с. 48).

Если пользователь, запустивший оболочку DiSec и вызвавший окно **Настройка ПО DiSec**, обладает административными правами в WINDOWS XP/WINDOWS 2003 Server, то ему доступны все элементы вкладки **Драйвер DiSec**, и он может сразу приступить к настройке драйвера.

Если пользователь не обладает административными правами в WINDOWS XP/WINDOWS 2003 Server, а также при работе в WINDOWS VISTA и более поздних версиях операционной системы элементы этой вкладки ему не доступны, а в нижней части вкладки **Драйвер DiSec** появляется кнопка **Настроить драйвер DiSec** (Рис. 42). 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 такое же окно, как и на Рис. 42, в котором доступны все элементы и отсутствует кнопка **Настроить драйвер DiSec**.

Примечание - Если DiSec функционирует под управлением WINDOWS VISTA и более поздних версий ОС, то по окончании выполнения настроек параметров драйвера (после нажатия кнопки **ОК** или **Отмена**) в основном окне появляется кнопка **Обновить данные**, которую следует нажать для отображения на экране измененных параметров драйвера.

7.4.1 Режим запуска и работы драйвера

Два флажка под заголовком **Блокировать открытые данные** (Рис. 42) определяют действия, которые будет выполнять драйвер с нетуннелированными пакетами («открытыми данными»).

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

При наличии туннеля

Установленный флажок указывает драйверу DiSec, что после подключения к защищенной сети и установки динамического туннеля (см. раздел 8.1, с. 56) необходимо блокировать весь открытый трафик, т.е. отбрасывать датаграммы, 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 датаграмм** - принимаются (и обрабатываются) только датаграммы, пришедшие через туннель; все остальные датаграммы отбрасываются;
- **отправка датаграмм** - датаграммы будут отправляться только через туннель; те датаграммы, которым не разрешено прохождение через туннель (не соответствуют правилам отбора в туннель), отбрасываются (в том числе, по интерфейсам, по которым туннелирование не выполняется).

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

При отсутствии туннеля

Установленный флажок 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.

Одновременно с флажком 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 7.3.1, с. 30).

Настроить МЭ

Настройка межсетевого экрана рассмотрена ниже (раздел 7.5, с. 48).

7.4.2 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---** – см. ниже). 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 под этим заголовком 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 трассировку 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 IP), при этом всегда выполняется расшифровка всего пакета (HEX-дамп), а расшифровка заголовков не выполняется.

Флажок Сброшенные

Флажок задает трассировку всех пакетов, сброшенных (заблокированных) в соответствии с настройками блокировки открытых данных. При этом в протокол выводится расшифровка IP- и TCP/UDP/ICMP-заголовков. Дополнительно можно настроить запись в протокол содержимого всего пакета (установить флажок **HEX-Дамп пакета**).

--- Добавить расшифровку ---

Флажки в группе 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 выводится полное имя файла протокола сети. Пользователь не может изменить данное значение.

7.4.3 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;
- расшифровка заголовков заданного типа (ARP, IP, заголовок протокола прикладного уровня – TCP, UDP или ICMP), при этом выделяются отдельные поля заголовков и выводятся в протокол в мнемоническом виде, например:

```
29-08-2012 15:21:55,812 IFC_1 <- recv:
IP: 81.176.67.171->192.168.32.39 len 1500 ihl 20 ttl 56 prot 6 id 46026 offs 0 DF
MF CkSum=0xadf8
TCP: 80->1095 Seq x6111fb50 Ack x7d18c941 ACK Wnd 8576
```

- для туннелированных пакетов добавляется строка, в которой указывается признак туннелированного пакета (tunneled), идентификатор туннеля (см. раздел 9.3, с. 61), а также добавляются строки с расшифровкой заданных заголовков в исходном и результирующем пакете (tunneled datagram:), например:

```
29-08-2012 15:21:55,812 IFC_1 -> sent:
tunneled, TnlID 32768, original data was:
IP: 192.168.32.39->192.168.32.1 len 64 ihl 20 ttl 128 prot 1 CkSum=0x1dfb
ICMP: Echo Request code 0
tunneled datagram:
IP: 192.168.32.39->192.168.32.1 len 112 ihl 20 ttl 128 prot 4
```

- расшифровка в шестнадцатеричном виде всего Ethernet-кадра, включая расшифровку заголовков всех уровней и самих данных (HEX-дамп).

7.5 Вкладка Драйвер DiSec - 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-датаграмм. Контроль выполняется с помощью фильтров. Фильтр представляет собой набор правил проверки IP-датаграмм.

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. 42 (с. 45) открывается окно **Настройка правил МЭ** (Рис. 43), содержащее данные о текущих настройках МЭ и позволяющее изменить его конфигурацию.

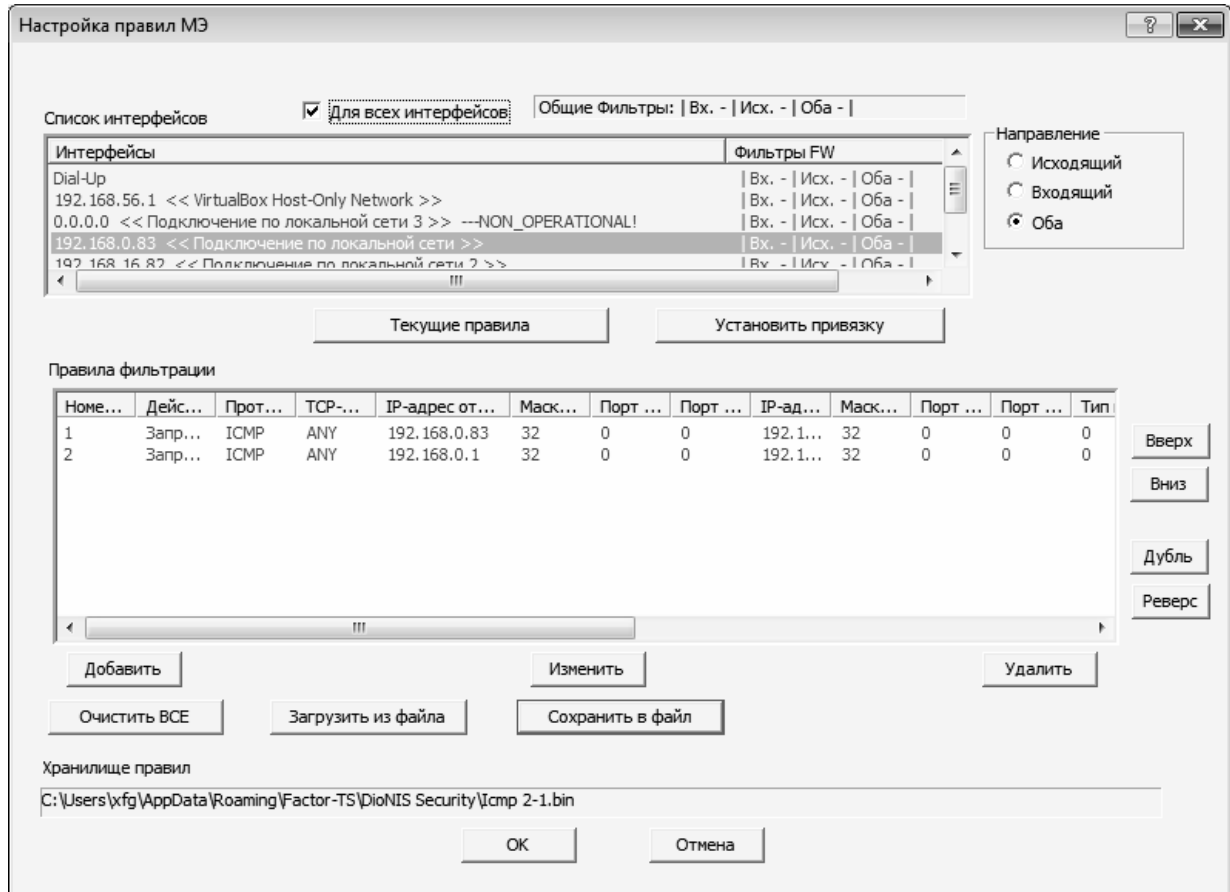


Рис. 43

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** (Рис. 44, с. 51), подробно рассмотренное ниже в разделе 7.5.2, с. 51.

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.

7.5.1 Алгоритм 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. ниже - раздел 7.5.2). 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.

7.5.2 Создание и редактирование правила фильтрации

Для создания (редактирования) каждого правила фильтра надо в окне **Настройка правил МЭ** (Рис. 43, с. 49) нажать кнопку **Добавить (Изменить)**. На экран будет выведено окно **Правило фильтрации МЭ** (Рис. 44).

Рис. 44

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 контролируемой датаграмме в случае совпадения параметров датаграммы 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-датаграммы. Выпадающий список состоит из значений:

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

ТСР-флаги

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

- *ANY* - проверка не производится;
- *SYN* - требуется, чтобы в ТСР-пакете был установлен флаг **SYN** и сброшен флаг **ACK**;
- *ACK, URG, PSH, RST, FIN* - требуется, чтобы в ТСР-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-датаграммы.

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 ТСР/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 датаграммы.

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

- **Смещение** – числовое значение смещения контролируемого поля датаграммы от начальной точки отсчета;
- **Относительно** – параметр определяет точки отсчета смещения контролируемого поля; может принимать следующие значения:

0+ – смещение отсчитывается от начала датаграммы;

IP+ – смещение отсчитывается от начала поля данных датаграммы.

Значение указанного поля датаграммы 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-датаграммы 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**.

7.6 Вкладка Служба DiSecSrv (Настройка ПО DiSec)

Вкладка **Служба DiSecSrv** окна **Настройка ПО DiSec** (Рис. 45) предназначена для изменения настроек службы DiSecSrv. Заданные параметры работы службы вносятся в базу данных служб WINDOWS и в файл настроек (**INI-файл**) службы.

Для пользователя, обладающего административными правами в WINDOWS XP/WINDOWS 2003 Server, на вкладке отображаются текущие настройки службы, и в верхней секции вкладки выводится сообщение: «Служба DiSecSrv ИНИЦИАЛИЗИРОВАНА». Пользователь может сразу приступить к настройке службы, нажав кнопку **Настроить службу DiSecSrv**. Ему будут выведены настройки службы (Рис. 46).

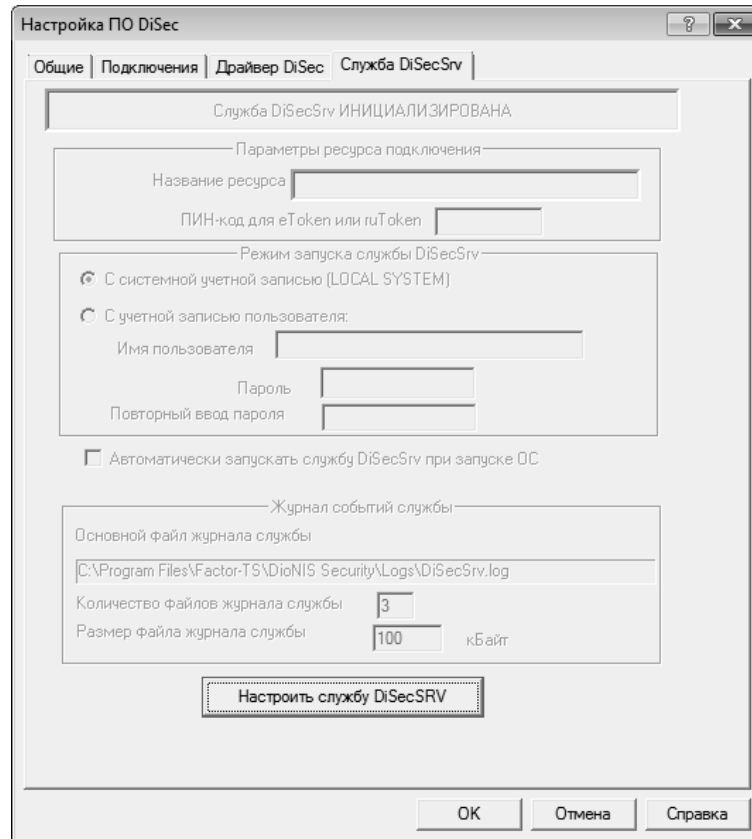


Рис. 45

Если пользователь не обладает административными правами в WINDOWS XP/WINDOWS 2003 Server, а также при работе в WINDOWS VISTA и более поздних версиях операционной системы 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. 46).

7.6.1 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 6.3, с. 25.

7.6.2 Параметры ресурса подключения

Параметры под этим заголовком (Рис. 46) позволяют создать (настроить) один или несколько ресурсов подключения для службы и выбрать один из них в качестве текущего, а также при необходимости задать пароль для считывания ключевой информации пользователя с ключевого носителя.

Название ресурса

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

Подключения

Кнопка предназначена для создания или модификации списка подключений для службы, после ее нажатия откроется окно **Подключения** аналогичное окну настроек списка подключений для оболочки (раздел 7.2, с. 29; Рис. 14).

ПИН-код для eToken или ruToken

Элемент управления под этим заголовком позволяет ввести код защиты ключевых носителей eToken и ruToken. Данный элемент активен (т.е. предоставляет возможность ввода значения) только в том случае, если в реквизитах выбранного подключения указано использование ключевых носителей данного типа.

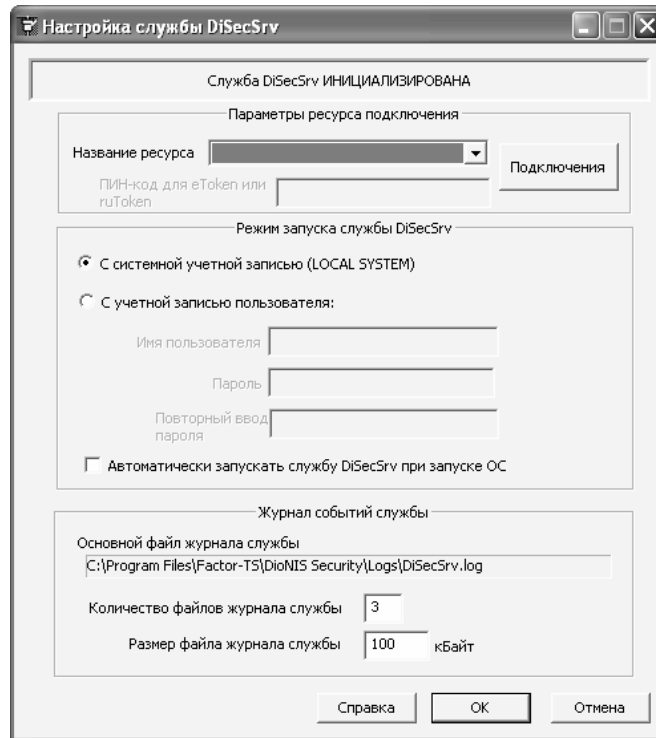


Рис. 46

7.6.3 Режим запуска службы DiSecSrv

Группа параметров под этим заголовком (Рис. 46) 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 10.5, с. 66).

7.6.4 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.

Выполнив все настройки, надо выйти из окна **Настройка службы DiSecSrv** (Рис. 46) нажатием кнопки **ОК**. Система вернется на вкладку **Служба DiSecSrv** (Рис. 45), в нижней части которой появится кнопка **Обновить данные**, которую следует нажать для отображения на экране измененных параметров службы.

8 Команды Подключиться/Отключиться

Команда **Подключиться** Главного меню оболочки DiSec (Рис. 11) служит для установки туннеля с конкретной защищенной сетью, после ее выбора на экран выводится окно (Рис. 47) в котором выбирается ресурс и инициируется процедура подключения.

Команда **Отключиться** Главного меню оболочки DiSec (Рис. 11) служит для снятия ранее установленного средствами оболочки DiSec туннеля. Подробнее ниже.

8.1 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. 47), содержащее элементы управления, необходимые для выбора параметров подключения, и информационную секцию для вывода сообщений о прохождении процедуры.

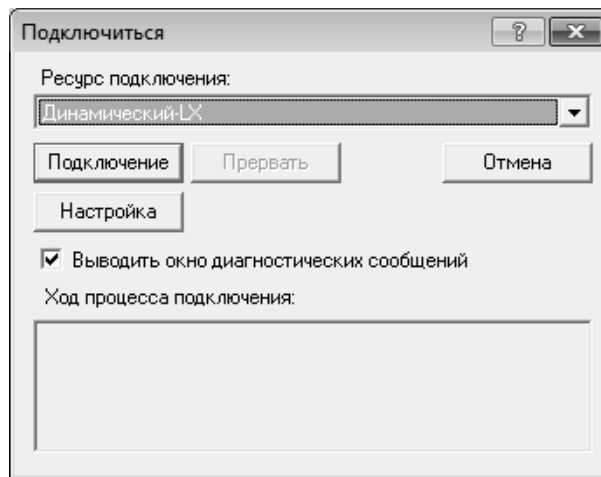


Рис. 47

Ресурс подключения :

В поле под этим заголовком выводится название ресурса, к которому будет выполняться подключение. Ресурс можно изменить, выбрав его из раскрывающегося списка. Список должен быть создан заранее на этапе настройки системы (раздел 7.3, 30).

Подключение

Кнопка инициирует процесс подключения к выбранному ресурсу и установку туннеля с Сервером VPN.

Прервать

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

Настройка

Кнопка предназначена для проверки и, при необходимости, изменения списка ресурсов подключения и их реквизитов. По нажатию этой кнопки вызывается окно **Настройка** на вкладке **Общие** (Рис. 13, с. 27), т.е. действие кнопки аналогично вызову одноименной команды Главного меню оболочки DiSec. По окончании работы с окном **Настройка** управление возвращается к окну **Подключиться** (Рис. 47), 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 оболочки DiSec.

Ход процесса подключения :

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

Выполнение команды **Подключиться** необходимо начать с выбора ресурса подключения из списка, после чего нажать кнопку **Подключение** в окне **Подключиться** (Рис. 47). Дальнейшие действия пользователя и системы зависят от реквизитов выбранного ресурса.

В режиме соединения IPSEC-ФАКТОР после нажатия кнопки **Подключение** в окне **Подключиться** (Рис. 47) будет выдан запрос на установку ключевого носителя. В зависимости от указанного в реквизитах подключения типа ключевого носителя появится одно из сообщений, приведенных ниже.

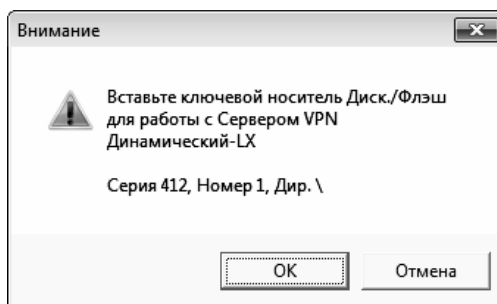


Рис. 48

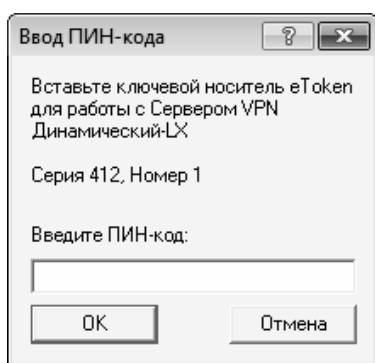


Рис. 49

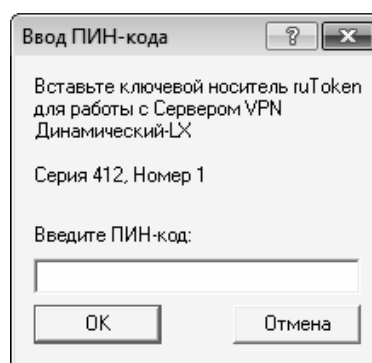


Рис. 50

В случае работы с ключевыми носителями eToken (Рис. 49) или guToken (Рис. 50) необходимо ввести секретный код (ПИН-код) для работы с ключевым носителем типа eToken или guToken. 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. 7.3.3, с. 31).

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 часть окна Рис. 47), 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 оболочкой DiSec с помощью команды Главного меню оболочки DiSec **Диагностика** (раздел 11.2, с. 69).

После того как начнется процесс соединения, в окне **Подключиться** (Рис. 47) 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 оболочки 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.

8.2 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.

Обратите внимание, что сервер 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 7.3, с. 30), 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.

8.3 Команда Отключиться

Команда Главного меню оболочки DiSec (Рис. 11) **Отключиться** становится доступной после того, как будет выполнено соединение с Сервером VPN.

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

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

Статический туннель остается в рабочем состоянии.

9 Команда Состояние

Команда Главного меню оболочки DiSec (Рис. 11) **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 **Состояние драйвера DiSec** (Рис. 51).

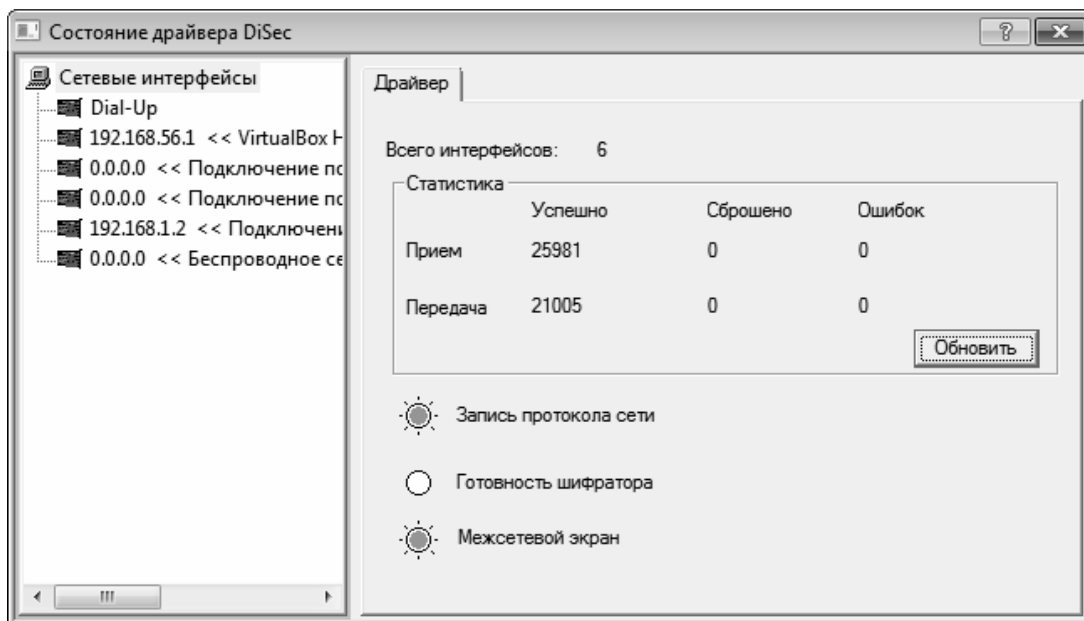


Рис. 51

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) 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. 51).

Если в левой части окна курсором выделена строка с названием одного из интерфейсов, то в правой части окна появляется набор из трех вкладок **Драйвер**, **Интерфейс** и **Туннель**.

9.1 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.

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

Количество пакетов, не соответствующих правилам отбора в туннель и сброшенных драйвером DiSec в соответствии с настройкой блокировки открытых данных (раздел 7.4.1, с. 46).

Ошибок

Количество пакетов, сброшенных драйвером DiSec или из-за ошибок в самих пакетах, или из-за возникновения ситуации нехватки ресурсов в драйвере DiSec для передачи пакета.

В нижней части экрана размещены три индикатора, информирующие о настройках режима протоколирования и состоянии программного (встроенного в ПО DiSec) шифратора.

Запись протокола сети

Индикатор имеет зеленый цвет, если при настройке ПО DiSec установлено ведение протокола сети (раздел 7.4.2, с. 46).

Готовность шифратора

Индикатор имеет зеленый цвет, если шифратор, входящий в состав ПО DiSec и используемый драйвером DiSec для шифрования данных, проинициализирован.

Межсетевой экран

Индикатор имеет зеленый цвет, если хотя бы для одного интерфейса сформирован хотя бы один фильтр (набор правил) (7.5, с. 48).

9.2 Вкладка Интерфейс (Состояние драйвера DiSec)

Вкладка **Интерфейс** (Рис. 52) содержит параметры и информацию о текущем состоянии конкретного интерфейса.

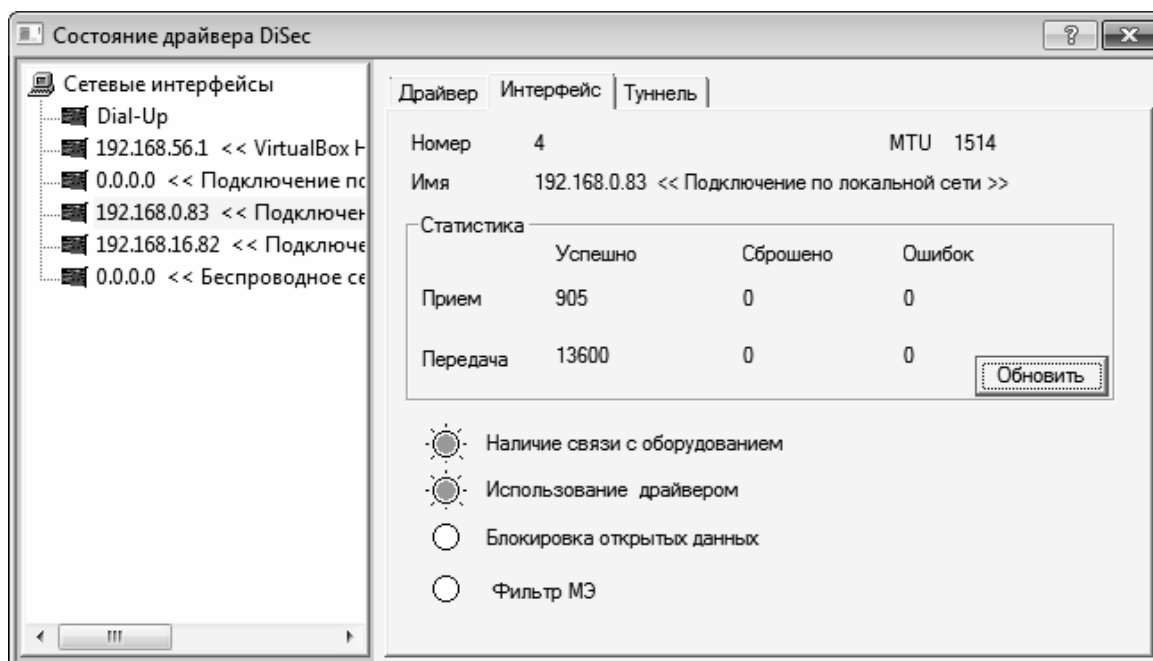


Рис. 52

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 7.4.2, с. 46).

Блокировка открытых данных

Индикатор имеет зеленый цвет, если прохождение открытых данных заблокировано соответствующей настройкой (см. раздел 7.4.1, с. 46).

Фильтр МЭ

Индикатор имеет зеленый цвет, если для данного интерфейса сформирован хотя бы один фильтр (набор правил) (7.5, с. 48).

9.3 Вкладка Туннель (Состояние драйвера DiSec)

Вкладка **Туннель** (Рис. 53, Рис. 54) позволяет просмотреть текущее состояние параметров динамического туннеля, установленного через данный интерфейс. Если динамический туннель отсутствует, то значения параметров на вкладке отсутствуют.

9.3.1 Состояние туннеля в режиме IPSEC-ФАКТОР

При установленном туннеле в режиме IPSEC-ФАКТОР вкладка имеет вид (Рис. 53):

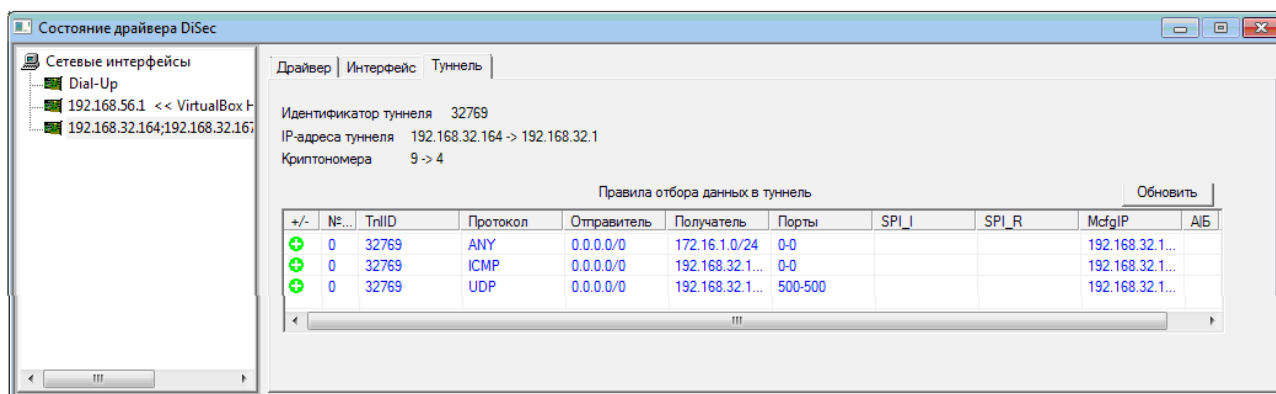


Рис. 53

Идентификатор туннеля

Идентификатор - целое число, присвоенное туннелю во время его создания и согласования параметров туннеля по протоколу ISAKMP. Идентификатор туннеля (с предшествующими символами «TnIID») присутствует в протоколах сети, если в настройках протоколирования был установлен соответствующий флажок (см. 7.4.2, с. 46 и 7.4.3, с. 48).

IP-адреса туннеля

Значение поля - пара адресов, из которых первый адрес - IP-адрес локального конца туннеля (этот адрес будет подставлен в качестве адреса отправителя в дополнительный IP-заголовок при упаковке датаграммы в туннель); второй адрес - IP-адрес удаленного конца туннеля (этот адрес будет подставлен в качестве адреса назначения в дополнительный IP-заголовок при упаковке датаграммы в туннель).

Криптономера

Значение поля - пара чисел; числа присваиваются двум взаимодействующим сторонам в криптографической сети при организации туннеля в режиме IPSEC-ФАКТОР: первое число - криптономер данного пользователя (абонента Сервера VPN); второе число - криптономер Сервера VPN, с которым организован туннель.

--- Правила отбора данных в туннель ---

Таблица под этим заголовком содержит список правил отбора, определяющих характеристики пакетов, подлежащих туннелированию. Правила отбора ограничивают состав ресурсов, обмен данными с которыми будет защищен криптографическими средствами. Правила создаются индивидуально для каждого пользователя DiSec.

Для успешного функционирования туннеля необходимо наличие правил, разрешающих прохождение пакетов, обеспечивающих контроль функционирования туннеля, то есть разрешающие правила для датаграмм протокола ISAKMP (протокол UDP, порт 500) и для датаграмм протокола ICMP (прохождение Ping-пакетов).

В режиме IPSEC-ФАКТОР при отсутствии правил отбора, сформированных на Сервере VPN, на стороне DiSec автоматически формируется правило, обеспечивающее туннелирование всех данных.

В режиме IPSEC-ГОСТ реализована проверка только по «адресу получателя» (см. раздел 7.3.4, с. 31).

При отборе датаграмм в туннель, а также при их извлечении из туннеля правила просматриваются по порядку, начиная с первого, и просмотр заканчивается, как только будет обнаружено соответствие параметров датаграммы (пакета) с параметрами правила, поэтому список правил формируется таким образом, чтобы правила с меньшим диапазоном действия предшествовали правилам с большим диапазоном.

9.3.2 Состояние туннеля в режиме IPSEC- ГОСТ

При установленном туннеле в режиме IPSEC-ГОСТ вкладка имеет вид (Рис. 54)

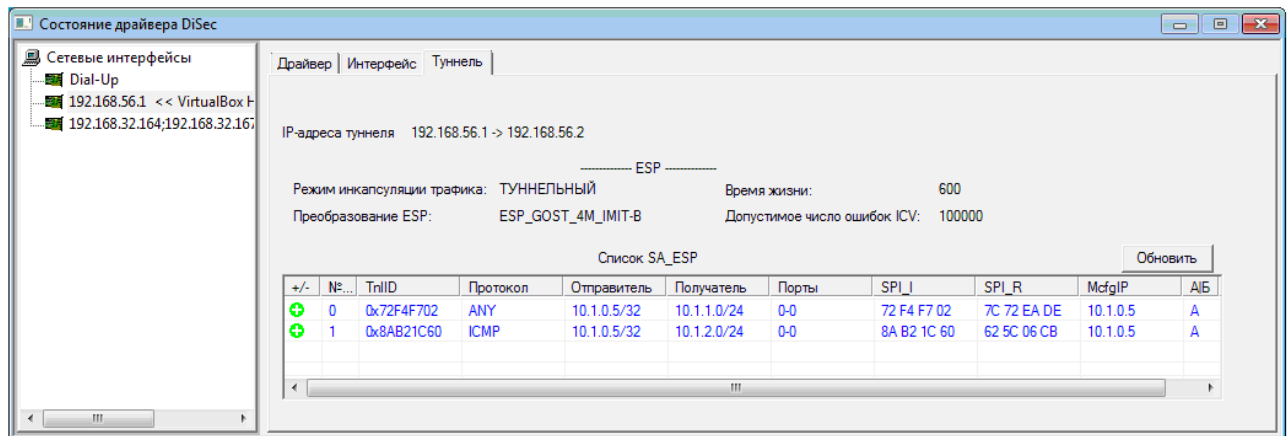


Рис. 54

IP-адреса туннеля

Значение поля - пара адресов, из которых первый адрес - IP-адрес локального конца туннеля (этот адрес будет подставлен в качестве адреса отправителя в дополнительный IP-заголовок при упаковке датаграммы в туннель); второй адрес - IP-адрес удаленного конца туннеля (этот адрес будет подставлен в качестве адреса назначения в дополнительный IP-заголовок при упаковке датаграммы в туннель).

----- ESP -----

Под этим заголовком приведены согласованные параметры инкапсуляции IP-пакетов по протоколу ESP. Значения этих параметров задаются при настройке подключения в политике ESP (см. 7.3.4.2), однако результирующие значения могут отличаться от задаваемых при настройке, поскольку принимаются во внимание ответы от Сервера VPN. Таким образом, значение параметра **Время жизни** принимает меньшее из значений (указанное в настройке и предлагаемое Сервером VPN).

--- Список SA ESP ---

В таблице приведен список всех установленных SA (Security Association – Ассоциация безопасности), каждая из которых представляет собой туннель для отдельного целевого объекта (см. раздел 7.3.4.3. с. 35). Каждый туннель имеет свой идентификатор и ключи шифрования.

Помимо идентификатора туннеля (**TnIID**) каждый элемент списка содержит:

- порядковый номер туннеля, фактически соответствующий порядку элементов в списке целевых объектов;
- правило отбора в туннель, соответствующее значению Целевого объекта;
- параметры **SA ESP (SPI_I и SPI_R)**, идентифицирующие данную SA;
- IP-адрес, присвоенный компьютеру пользователя DiSec, если в настройках политики ESP было задано выполнение запроса IP-адреса в защищенной сети – **MODECONFIG** (см. раздел 7.3.4.2, с. 34);
- активность или блокировка туннеля. Блокировка выполняется в случае превышения максимально допустимого количества искаженных пакетов (см. 7.3.4.2, с. 34).

10 Команда Тестирование

Команда Главного меню оболочки DiSec (Рис. 11) **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.

10.1 Вкладка Ping (Тестирование)

Вкладка **Ping** (Рис. 55) 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.

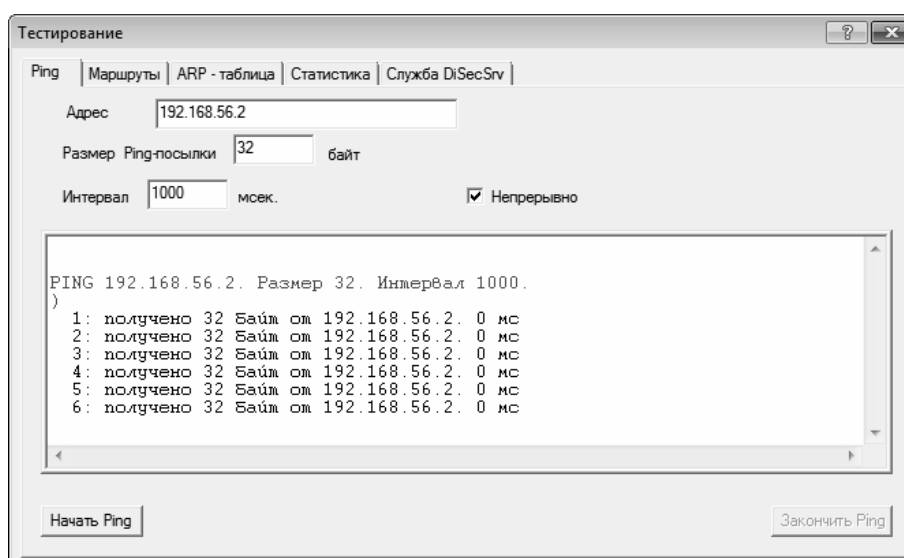


Рис. 55

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.

Непрерывно

Флажок устанавливает соответствующий режим посылки пакетов **Ping** - посылка будет выполняться до тех пор, пока не будет нажата кнопка **Закончить Ping**; если флажок не установлен (состояние флажка по умолчанию), то будет выполнено три посылки.

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.

10.2 Вкладка Маршруты (Тестирование)

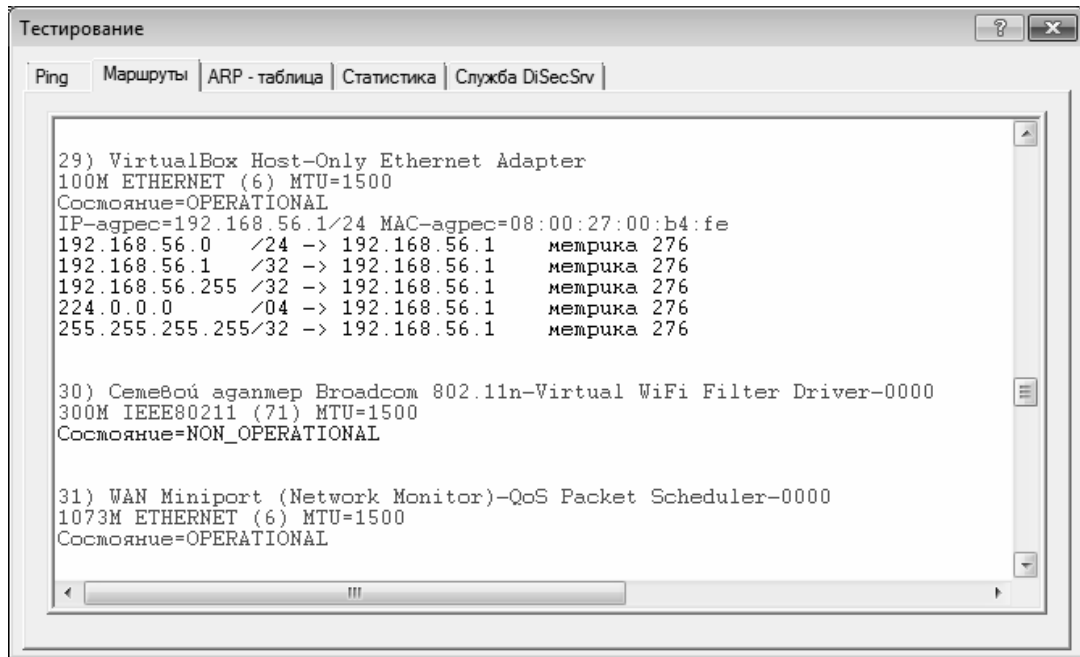


Рис. 56

С помощью вкладки **Маршруты** (Рис. 56) пользователь может просмотреть текущее состояние интерфейсов и маршрутных таблиц IP-компонента WINDOWS.

Список текущих интерфейсов WINDOWS 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.

10.3 Вкладка ARP-таблица (Тестирование)

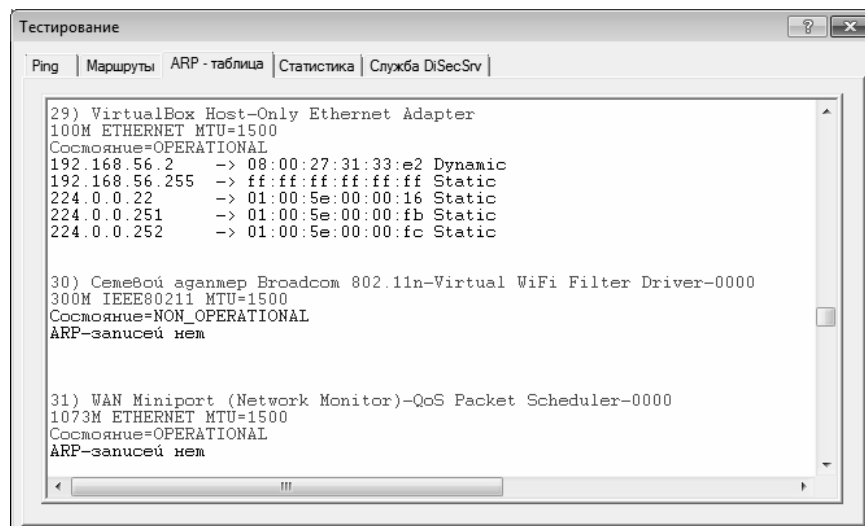


Рис. 57

С помощью вкладки **ARP-таблица** (Рис. 57) пользователь может просмотреть текущее состояние интерфейсов и ARP-таблиц IP-компонента WINDOWS (соответствие IP и MAC-адресов сетевых интерфейсов).

Список сетевых интерфейсов WINDOWS 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.

10.4 Вкладка Статистика (Тестирование)

Вкладка **Статистика** позволяет просмотреть данные статистики отдельно по протоколам TCP (Рис. 58), UDP (Рис. 59), IP (Рис. 60) и ICMP (Рис. 61).

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

Повторное нажатие кнопки вызывает обновление статистики по данному протоколу.

Информация о TCP-соединениях

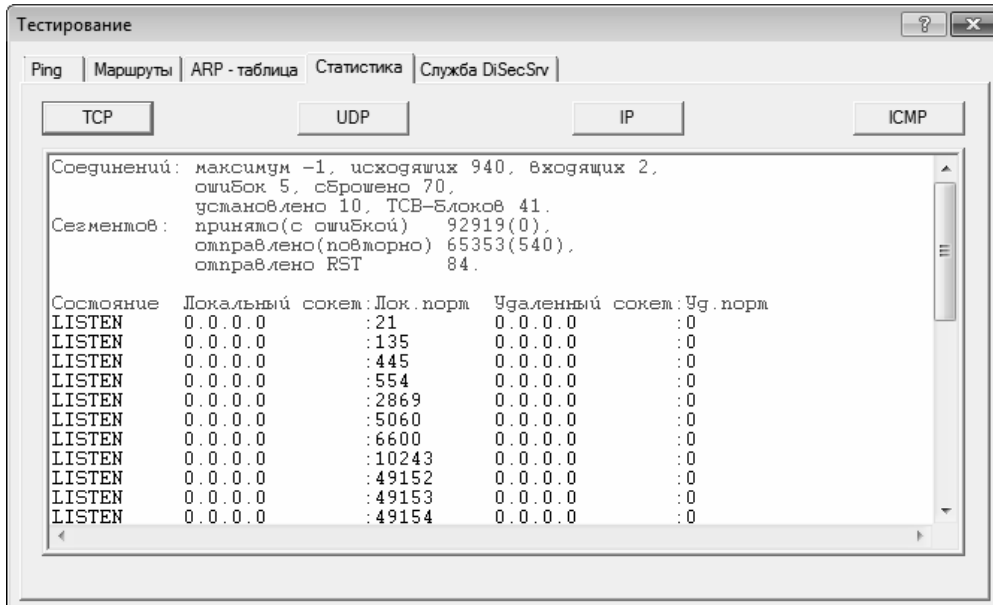


Рис. 58 TCP - статистика

Информация о UDP-соединениях

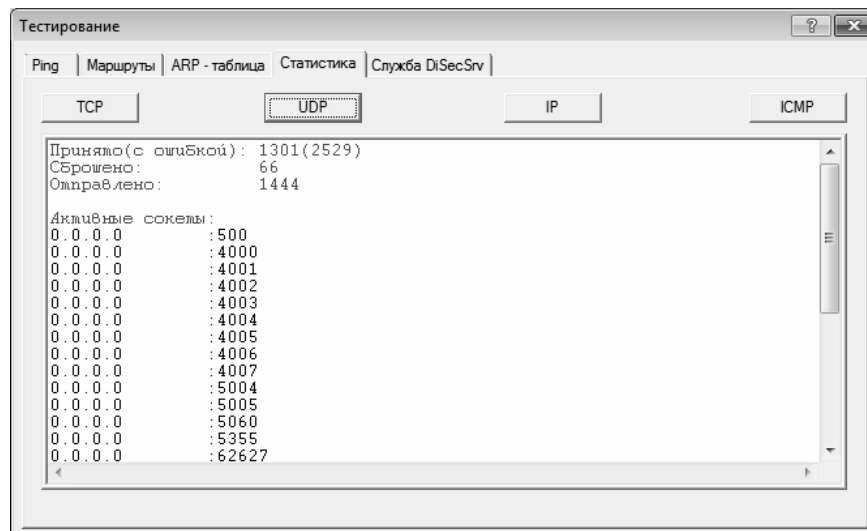


Рис. 59 UDP статистика

Информация об IP-соединениях

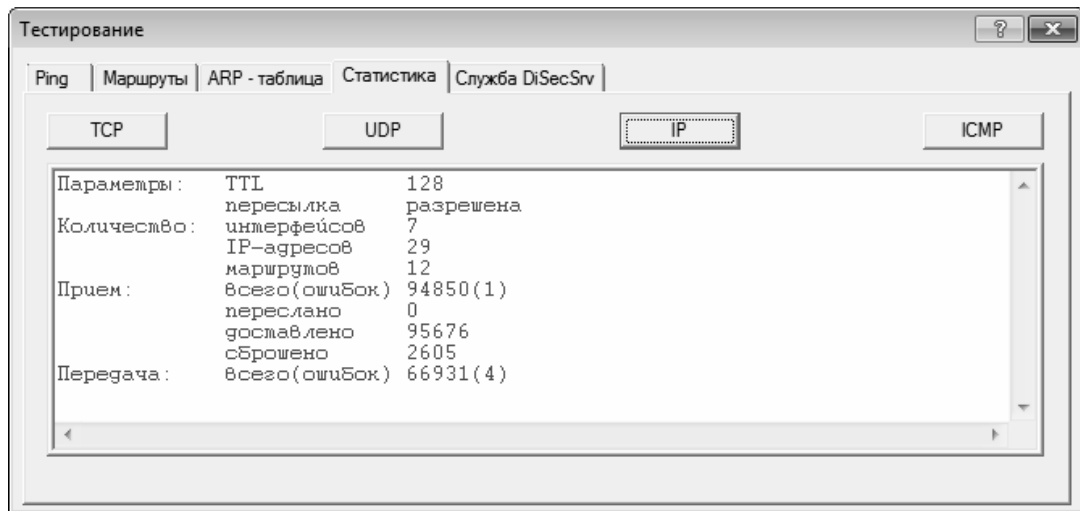


Рис. 60 IP статистика

Информация об ICMP-сообщениях

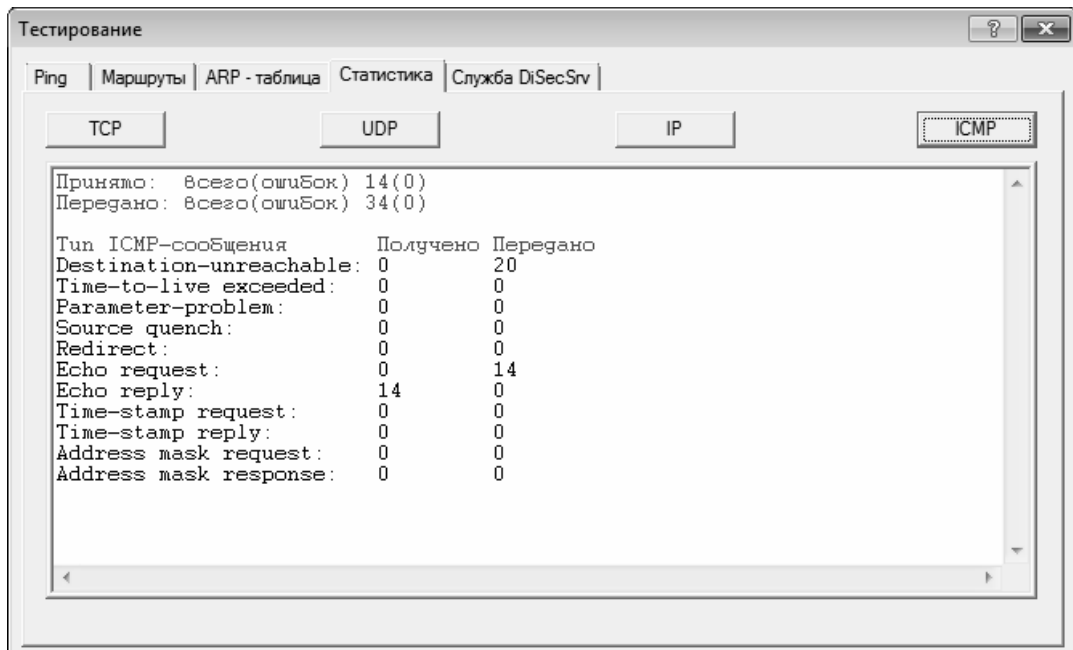


Рис. 61 ICMP статистика

10.5 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. 62, Рис. 63, Рис. 65).

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 оболочки DiSec (см. раздел 11, с. 69).

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.

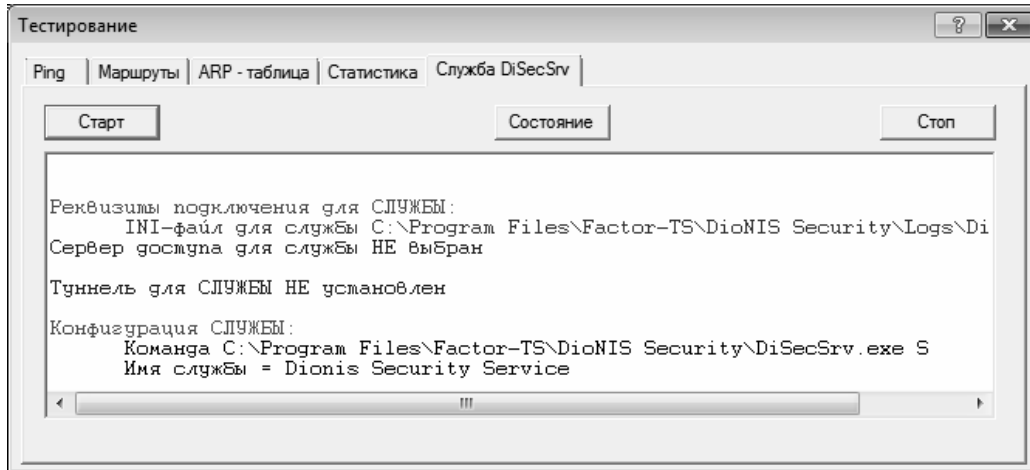


Рис. 62 Служба не настроена

Для режима IPSEC-ФАКТОР состояние службы отображается следующим образом (Рис. 63)

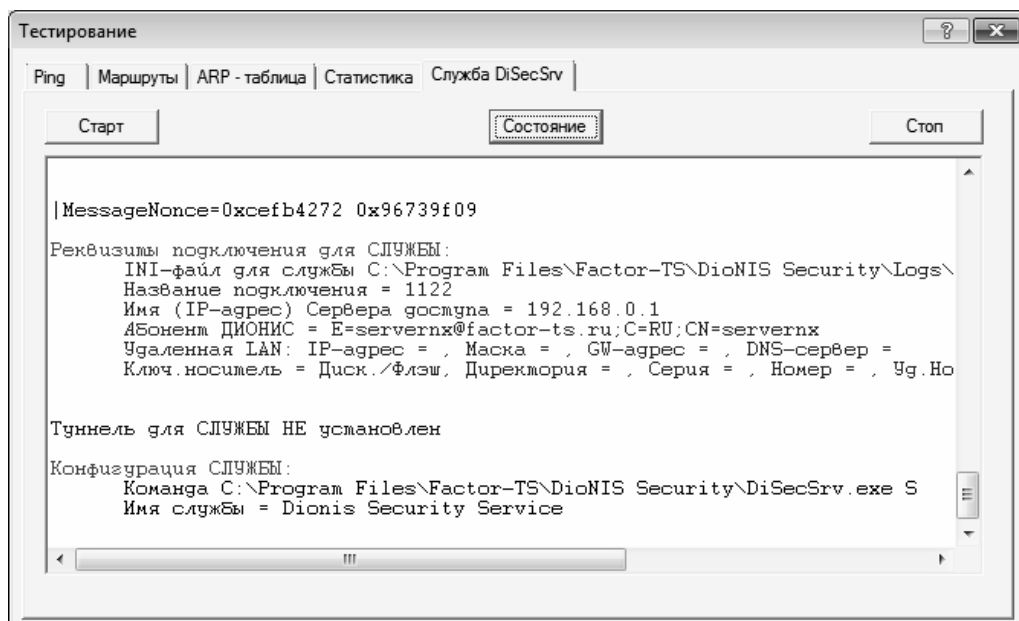


Рис. 63 Служба настроена, но не запущена (режим IPSEC-ФАКТОР)

Для режима IPSEC-ГОСТ состояние службы отображается следующим образом (Рис. 64):

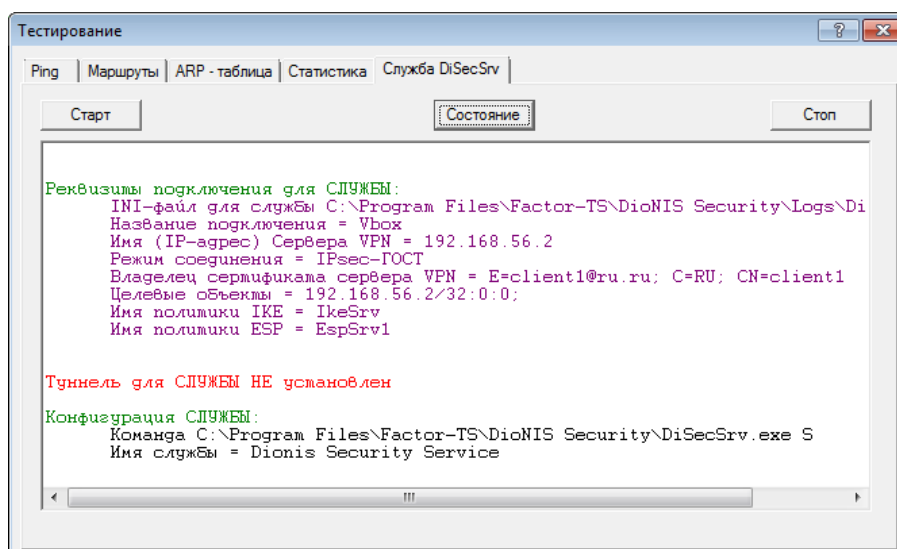


Рис. 64 Служба настроена, но не запущена (режим IPSEC-ГОСТ)

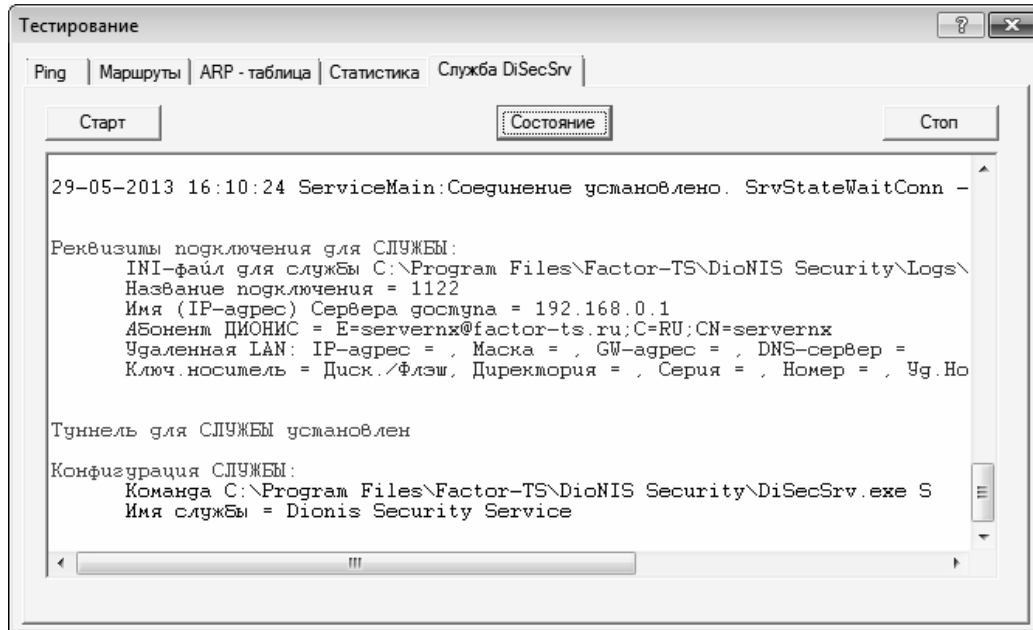


Рис. 65 Служба запущена, туннель установлен

11 Информационные команды

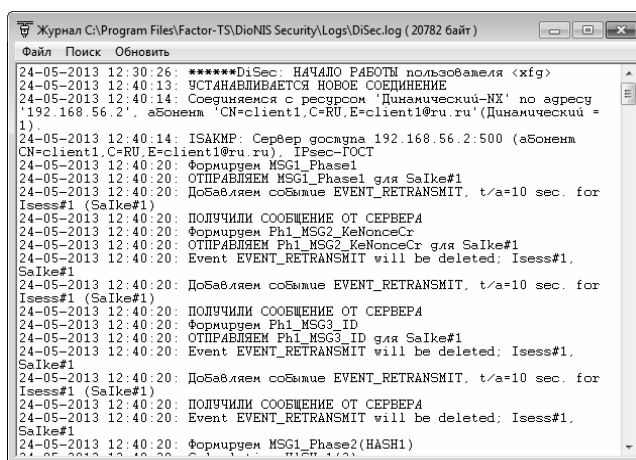
Информационные команды позволяют получить дополнительную информацию, необходимую для диагностики ситуаций невозможности установки подключения и/или возможных причин неработоспособности туннеля посредством изучения информации, выведенной в процессе установки и функционирования туннеля в окне **Диагностика** (раздел 11.2, с. 69) и **Протокол Сети** (раздел 11.3, с. 70), либо при нарушении регламента безопасности в Журнале работы DiSec (раздел 11.1, с. 69).

11.1 Команда Журналы

Команда Главного меню оболочки DiSec (Рис. 11) **Журналы** позволяет просмотреть на экране журнал работы оболочки DiSec и журнал работы службы DiSecSvc. 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. раздел 7.1, с. 27).

Вид журнала на экране может быть, например, таким (Рис. 66):



```
Журнал C:\Program Files\Factor-TS\DiONIS Security\Logs\DiSec.log (20782 байт)
Файл Поиск Обновить
24-05-2013 12:30:26: *****DiSec: НАЧАЛО РАБОТЫ пользователя <xif>
24-05-2013 12:40:13: УСТАНОВЛИВАЕТСЯ НОВОЕ СОЕДИНЕНИЕ
24-05-2013 12:40:14: Соединяемся с ресурсом 'Динамический-NX' по адресу
'192.168.56.2', абонент 'CN=client1.C=RU.E=client1@ru.ru' (Динамический =
1)
24-05-2013 12:40:14: ISAKMP: Сервер гослана 192.168.56.2:500 (абонент
CN=client1.C=RU.E=client1@ru.ru), IPsec-ГОСТ
24-05-2013 12:40:20: Формируем MSG1_Phase1
24-05-2013 12:40:20: ОТПРАВЛЯЕМ MSG1_Phase1 для SaIke#1
24-05-2013 12:40:20: Добавляем событие EVENT_RETRANSMIT, t/a=10 sec. for
IseSS#1 (SaIke#1)
24-05-2013 12:40:20: ПОЛУЧИЛИ СООБЩЕНИЕ ОТ СЕРВЕРА
24-05-2013 12:40:20: Формируем Ph1_MSG2_KeNonceCr
24-05-2013 12:40:20: ОТПРАВЛЯЕМ Ph1_MSG2_KeNonceCr для SaIke#1
24-05-2013 12:40:20: Event EVENT_RETRANSMIT will be deleted: IseSS#1,
SaIke#1
24-05-2013 12:40:20: Добавляем событие EVENT_RETRANSMIT, t/a=10 sec. for
IseSS#1 (SaIke#1)
24-05-2013 12:40:20: ПОЛУЧИЛИ СООБЩЕНИЕ ОТ СЕРВЕРА
24-05-2013 12:40:20: Формируем Ph1_MSG3_ID
24-05-2013 12:40:20: ОТПРАВЛЯЕМ Ph1_MSG3_ID для SaIke#1
24-05-2013 12:40:20: Event EVENT_RETRANSMIT will be deleted: IseSS#1,
SaIke#1
24-05-2013 12:40:20: Добавляем событие EVENT_RETRANSMIT, t/a=10 sec. for
IseSS#1 (SaIke#1)
24-05-2013 12:40:20: ПОЛУЧИЛИ СООБЩЕНИЕ ОТ СЕРВЕРА
24-05-2013 12:40:20: Event EVENT_RETRANSMIT will be deleted: IseSS#1,
SaIke#1
24-05-2013 12:40:20: Формируем MSG1_Phase2(HASH1)
```

Рис. 66

В командной строке окна две команды и одно меню:

Файл – команда служит для переключения между файлами, содержащими журнал работы оболочки DiSec или службы DiSecSvc (при активизации команды **Журналы** всегда открывается текущий файл работы оболочки DiSec – тот, в который ведется запись в настоящий момент);

Поиск – меню 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 журнала в системный буфер обмена;
- команда **Выделить все** (или клавиши <Ctrl+A>) - скопировать весь текст в системный буфер обмена.

Обновить – команда обновляет окно просмотра, т.е. выводит те записи, которые накопились в журнале с момента активизации команды **Журналы**.

11.2 Команда Диагностика

Активизация команды Главного меню оболочки DiSec (Рис. 11) **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. 67).

Примечание - Такое же окно выводится на экран при организации динамического туннеля при установке флажка **Выводить окно диагностических сообщений** в окне **Подключиться** (см. раздел 8.1, с. 56).

В окне **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 **Закреть 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**.

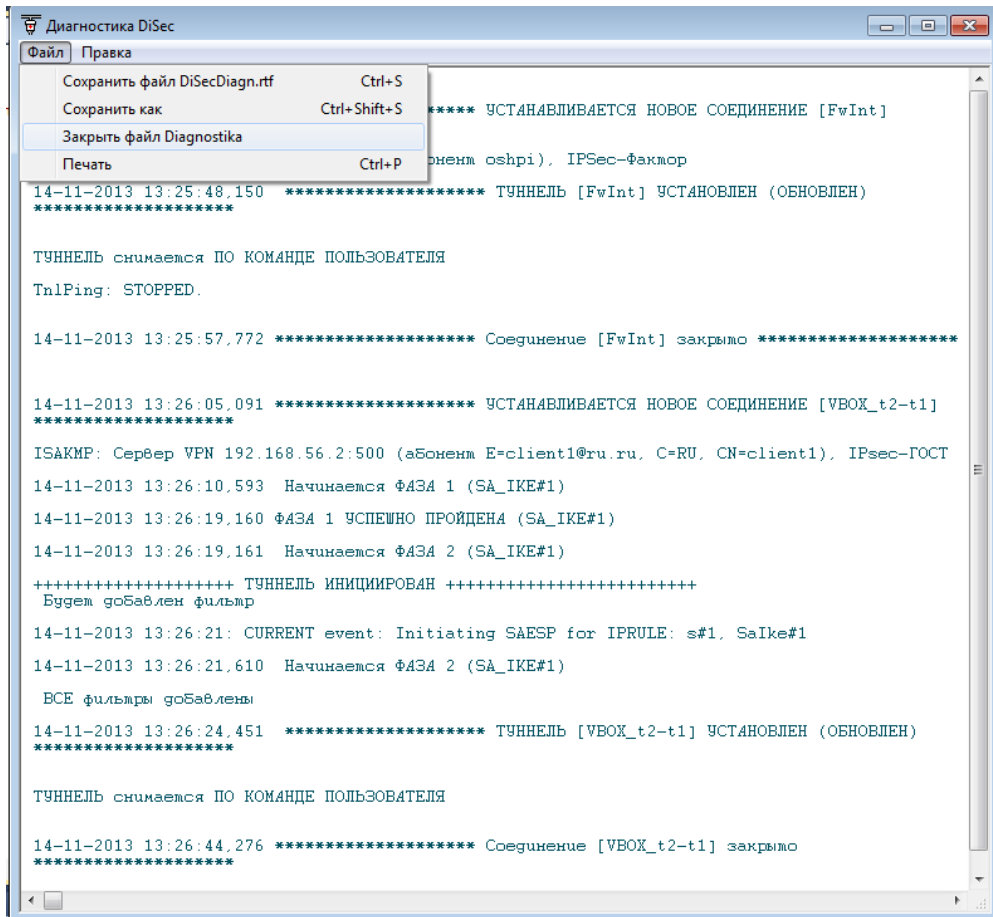


Рис. 67

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 **Закреть файл Diagnostika**) и переслать ОБА файла администратору Сервера VPN или разработчикам ПО DiSec.

11.3 Команда Протокол сети

Команда Главного меню оболочки **DiSec** (Рис. 11) **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, помещенный в директории установки программы в поддиректории **Logs**.

Количество и тип записываемой в протокол информации определяется настройкой (см. раздел 7.4.2, с. 46).

В верхней строке после названия окна (Рис. 68) выводится имя файла, содержащего протокол, и его размер.

В командной строке окна одно меню и одна команда.

Поиск – меню 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 – команда обновляет окно просмотра, т.е. выводит те записи, которые накопились в журнале с момента активизации команды **Протокол сети**.

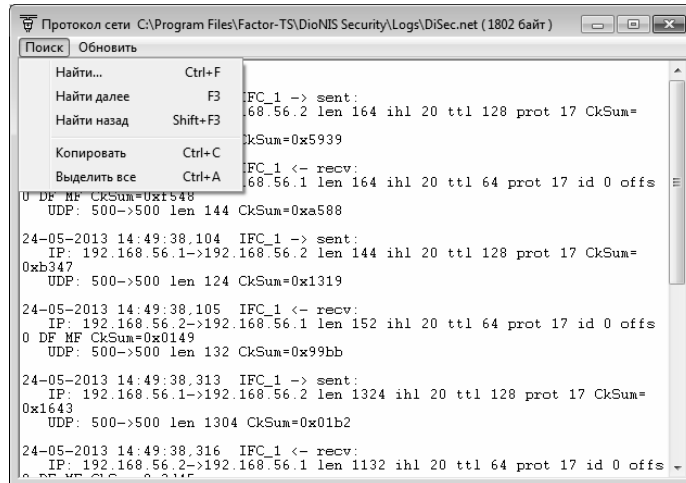


Рис. 68

В протокол сети записывается результат работы межсетевых экранов – фиксируются не прошедшие проверку сетевые пакеты. Пример протокола:

```
29-08-2012 15:21:55,812 IFC_2 -> sent:
  IP: 192.168.32.166->192.168.32.156 len 60 ihl 20 ttl 128 prot 1 CkSum=0x1dfb
  ICMP: Echo Reply code 0
  REJECTED FW Packet!

29-08-2012 15:21:58,125 IFC_2 -> sent:
  IP: 192.168.32.166->192.168.32.156 len 60 ihl 20 ttl 128 prot 1 CkSum=0x1bfb
  ICMP: Echo Reply code 0
  REJECTED FW Packet!
```

12 Справочная информация

Справка

Оболочка DiSec снабжена стандартной для программ под управлением WINDOWS справочной подсистемой, вызываемой по команде Главного меню оболочки DiSec (Рис. 11) **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>.

О программе

По команде Главного меню оболочки DiSec (Рис. 11) **О программе** на экран выводится краткая информация о версии и компонентах ПО DiSec, а также о фирме-разработчике.

13 Команда Выход

По команде Главного меню оболочки DiSec (Рис. 11) **Выход** выполняются следующие действия:

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

