

УТВЕРЖДЕНО
ВУ.РТНК.45006-01 34 01-ЛУ

Программный продукт
«Система централизованного управления
BeI VPN КР 4.5»

Руководство пользователя

ВУ.РТНК.45006-01 34 01

Листов 161

Содержание

1. Описание программного продукта «Система централизованного управления Bel VPN KP 4.5»	4
1.1. Назначение	4
1.2. Возможности продукта	5
1.3. Характеристика продукта	7
2. Сценарии управления	9
2.1. Сценарий первого обновления	9
2.2. Сценарий последующих обновлений	9
3. Установка Сервера управления	10
3.1. Инсталляция Сервера управления	10
4. Настройка Сервера управления	26
4.1. Настройка механизма идентификации и аутентификации в Сервер управления	26
4.2. Настройка Сервера управления	29
4.2.1. Ввод лицензии	30
4.2.2. Создание СА сертификата	31
4.2.3. Создание рабочего сертификата	32
4.2.4. Задание адресов Сервера управления	33
5. Настройка и управление центральным шлюзом	34
5.1. Создание учетной записи Клиента для Центрального шлюза	34
5.2. Подготовка скриптов для Клиента управления и Bel VPN Gate 4.5/4.1	46
5.3. Доставка и запуск скриптов	48
6. Настройка и управление устройством с Bel VPN Client-P 4.1	53
6.1. Создание учетной записи клиента на Сервере управления	53
6.2. Создание инсталляционных файлов Клиента управления и Bel VPN Client-P 4.1	66
6.3. Инсталляция Клиента управления и Bel VPN Client-P 4.1	67
7. Сценарий перехода на аутентификацию с использованием сертификатов	70
7.1. Создание обновления с параметрами ключевой пары и запроса на сертификат	71
7.2. Просмотр запроса на сертификат	73
7.3. Получение сертификата по запросу	74
7.4. Создание обновления с новым сертификатом для клиента Bel VPN Gate 4.1/4.5	75
7.5. Создание обновления с новым сертификатом для устройства с клиентом	83
8. Информация о клиенте на Сервере управления	92
9. Отправка команд на выполнение управляемому устройству	97
10. Восстановление конфигурации управляемого устройства из резервной копии ...	101
11. Сценарий включения в систему управления работающего устройства с Bel VPN Gate 4.5/4.1/Client-P 4.1	104
12. Групповые операции на Сервере управления	108
12.1. Создание шаблона проекта	108
12.2. Использование шаблона проекта	112

13.	Управление с использованием командной строки – утилита urmgr	114
14.	Изменение готового проекта с настройками VPN агента – утилита vpnmaker	120
15.	Настройки Сервера управления.....	122
16.	Настройки Клиента управления	127
17.	Описание интерфейса Сервера управления.....	133
17.1.	Вкладка Клиенты	133
17.2.	Меню Файл.....	136
17.3.	Меню Группы	136
17.4.	Меню Клиенты	137
17.5.	Меню Инструменты	142
17.5.1.	Задание политики и настроек с использованием вкладок.....	143
	Сохранение и загрузка настроек продукта	149
17.5.2.	Задание политики и настроек с использованием мастера	149
17.5.3.	Конвертирование политики	157
17.5.4.	Создание носителя с образом диска для восстановления.....	158
17.5.5.	Редактирование настроек базы данных	159
17.6.	Меню Помощь.....	159
17.7.	Панель инструментов	159
18.	Протоколирование событий.....	161
18.1.	Сервер управления	161
18.2.	Клиент управления.....	161
18.3.	Продукт Bel VPN Gate 4.5/4.1/Client-P 4.1	161

1. Описание программного продукта «Система централизованного управления Bel VPN КР 4.5»

1.1. Назначение

Программный продукт «Bel VPN КР 4.5» (далее - ПП Bel VPN КР) является самостоятельным Продуктом, но поставляется и работает только совместно с программными и программно-аппаратными продуктами линейки Bel VPN Gate и Bel VPN Client, а именно:

- программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1», комплекс программно-аппаратный «Шлюз безопасности Bel VPN Gate 4.5»;
- программные комплексы «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1», «Шлюз безопасности Bel VPN Gate 4.5»;
- устройство программно-аппаратное «Клиент ДСП 4.5»;
- программный продукт «Клиент безопасности Bel VPN Client-P 4.1».

ПП Bel VPN КР предназначен для централизованного удаленного управления программными и программно-аппаратными продуктами линейки Bel VPN Gate и Bel VPN Client, а именно:

- программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1», комплекс программно-аппаратный «Шлюз безопасности Bel VPN Gate 4.5»;
- программный комплекс «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1», «Шлюз безопасности Bel VPN Gate 4.5»;
- устройство программно-аппаратное «Клиент ДСП 4.5»;
- программный продукт «Клиент безопасности Bel VPN Client-P 4.1»;

ПП Bel VPN КР состоит из трех компонент (рисунок 1):

- **Программный продукт «Сервер управления Bel VPN Update Server 4.5» (далее – Сервер управления)** – серверная часть продукта, устанавливается на выделенный компьютер и предназначена для управления процессом обновления продуктов Bel VPN Gate/Client и их настроек, установленных на управляемых устройствах;
- **Программный продукт «Клиент управления Bel VPN Update Client 4.5 для ОС семейства Microsoft Windows» (далее – Клиент управления Windows)** – клиентская часть продукта, устанавливается на управляемое устройство с установленным продуктом линейки Bel VPN Client и предназначена для его управления;
- **Программный продукт «Клиент управления Bel VPN Update Client 4.5 для ОС семейства Linux» (далее – Клиент управления Linux)** – клиентская часть продукта, устанавливается на управляемые устройства с установленным продуктом Bel VPN Gate/Client и предназначена для его управления.

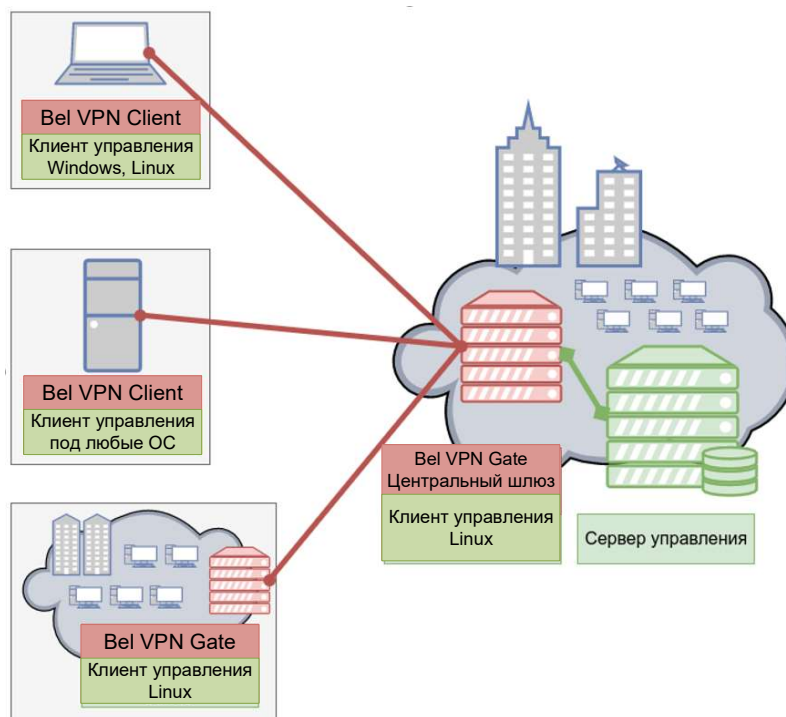


Рисунок 1

Сервер управления устанавливается на физическую или виртуальную аппаратную платформу в архитектуре Intel (x86/x86-64 совместимую) и функционирует под управлением одной из перечисленных операционных систем:

- Windows Server 2003 (32-bit);
- Windows Server 2008 (32-bit, 64-bit);
- Windows Server 2012 (64-bit);
- Windows Server 2016 (64-bit);
- Windows Server 2019 (64-bit).

Сервер управления должен размещаться в локальной сети, защищенной продуктом линейки Bel VPN.

Для каждого управляемого устройства создается Клиент управления, который устанавливается на управляемое устройство.

Все обмены между Сервером управления и Клиентом управления осуществляются по протоколу FTP и UDP (передаются оповещения/нотификации), трафик передается по защищенному IPsec VPN-соединению, организуемому управляемыми Продуктами.

Инициатором сетевого взаимодействия между Клиентом управления и Сервером управления всегда выступает Клиент управления. В случае временной потери соединения на Клиенте управления предусмотрена возможность “дозагрузки” данных с Сервера управления.

1.2. Возможности продукта



Все функциональные возможности Сервера управления и Клиента управления, описанные для продуктов версии 4.5 справедливы и для версии 4.1.

На управляемом устройстве с установленным продуктом Bel VPN Gate/Client и **Клиентом управления** могут быть изменены следующие настройки:

- локальная политика безопасности, предписанная данному устройству (в текстовом виде или в виде cisco-like конфигурации);

- политика драйвера по умолчанию продукта Bel VPN Gate/Client;
- настройки драйвера продукта Bel VPN Gate/Client;
- предопределенные ключи продукта Bel VPN Gate/Client;
- локальные сертификаты продукта Bel VPN Gate/Client, CA-сертификат, сертификаты партнеров, список отозванных сертификатов;
- контейнеры с ключами сертификатов;
- метод аутентификации партнеров;
- настройки сетевых интерфейсов;
- настройки сетевых маршрутов;
- настройки регистрации событий продукта Bel VPN Gate/Client;
- лицензия на продукт Bel VPN Gate/Client;
- настройки Клиента управления.

На **Сервере управления** имеются возможности:

- выполнения групповых операций, например, одновременное создание обновлений для нескольких устройств;
- использования шаблонов проекта при создании обновлений для устройств.

На **Сервере управления** ведется мониторинг состояния и настроек всех управляемых устройств, предоставляемых **Клиентами управления**, а именно:

- дата и время последнего успешного соединения каждого устройства с Сервером управления;
- IP-адреса устройств, с которых было осуществлено последнее успешное соединение;
- версия Клиента управления;
- версия Bel VPN Gate/Client;
- среднее значение загрузки процессора;
- количество активных IPSec-сессий;
- продолжительность сессии;
- дата последнего обновления;
- локальная политика безопасности продукта Bel VPN Gate/Client (в текстовом виде или в виде cisco-like конфигурации);
- настройки драйвера продукта Bel VPN Gate/Client;
- локальные сертификаты продукта Bel VPN Gate/Client, списки отозванных сертификатов, CA сертификаты, сертификаты партнеров;
- имена контейнеров с ключами сертификатов (если нет возможности сбора информации обо всех контейнерах, допускается сбор информации только о контейнерах, созданных с использованием Клиента управления);
- ближайшее время и дата истечения срока действия одного из сертификатов, размещенных в базе продукта Bel VPN Gate/Client на каждом устройстве;
- запросы на локальные сертификаты;
- имена предопределенных ключей продукта Bel VPN Gate/Client;
- настройки сетевых интерфейсов;
- настройки сетевых маршрутов;
- настройки регистрации событий продукта Bel VPN Gate/Client;
- журнал регистрации событий продукта Bel VPN Gate/Client и Клиента управления;

- информация о лицензиях продуктов Bel VPN Gate/Client;
- статистические данные о работе системы управляемого устройства;
- использование окон мастера для создания несложной политики безопасности продукта Bel VPN Gate/Client управляемого устройства;
- включение в систему управления уже работающего устройства с Bel VPN Gate/Client;
- создание клонов клиента для устройства с Bel VPN Gate, отличающихся локальными сертификатами, лицензиями и т. д.;
- изменение настроек готового проекта для Bel VPN Gate/Client.

1.3. Характеристика продукта

На Сервере управления каждый Клиент управления имеет уникальный идентификатор, а создаваемые обновления имеют порядковые номера. Уникальный идентификатор и порядковый номер входят в состав данных, загружаемых с Сервера управления. Полученные данные используются Клиентом управления только в том случае, если содержат верный идентификатор Клиента управления и, если номер обновления больше последнего установленного обновления.

Продукт обеспечивает защиту от злоумышленника, пытающегося с помощью механизма обновления запустить на компьютере с Клиентом управления “чужеродное” ПО. Защита осуществляется на основе ЭЦП, позволяющей осуществить аутентификацию и проверить целостность пересылаемых данных от Сервера управления к Клиенту управления. Предполагается, что злоумышленник не имеет доступа к управлению компьютером с Сервером управления и доступа к управлению устройствами с Клиентами управления.

Перед тем как предоставить данные для скачивания Клиентам управления, Сервер управления формирует ЭЦП для этих данных с использованием рабочего сертификата Сервера управления. Клиент управления перед использованием полученных данных с Сервера управления проверяет ЭЦП, используя открытый ключ рабочего сертификата Сервера управления.

Рабочий сертификат Сервера управления распространяется среди Клиентов управления в составе скачиваемых данных. Подлинность рабочего сертификата Сервера управления проверяется на основе построения цепочки сертификатов до СА сертификата Сервера управления. СА сертификат Сервера управления устанавливается на каждый Клиент управления во время инсталляции Клиента управления на устройство.

Перевыпуск рабочего сертификата Сервера управления производится по мере необходимости на Сервере управления. Время жизни рабочего сертификата, среди прочего, зависит и от объема подписываемых данных, то есть от количества обслуживаемых Клиентов управления и частоты обновлений. Рекомендуемое время жизни рабочего сертификата - от 1 месяца до 1 года.

В комплект поставки продукта Bel VPN KP 4.5 входят каталоги и файлы:

```

setup.exe
setup.ini
updater_server.cab
updater_server.msi
upweb.war
LINUXDEBIAN9
OTHERS
WINDOWS
    
```



Note

Если на управляемом устройстве уже инсталлирован продукт Bel VPN Client-P 4.1 то рекомендуется его деинсталлировать, а затем создать заново его инсталляционный файл и файл Клиента управления, как описано в данном документе.



Шлюз безопасности Bel VPN Gate 4.5/4.1 поставляется с установленным Клиентом управления, который перед использованием необходимо инициализировать. На Шлюзе безопасности старой версии 4.1 необходимо обновить Клиент управления. Обновление Клиента безопасности проводится с помощью Сервера управления.

В дальнейшем описании документа приведены примеры для стенда (Рисунок 2), в который включен Шлюз безопасности Bel VPN Gate 4.5, защищающий подсеть с конечным устройством, на котором установлен Сервер управления. Взаимодействие между управляемым устройством и Сервером управления осуществляется по IPsec-туннелю.

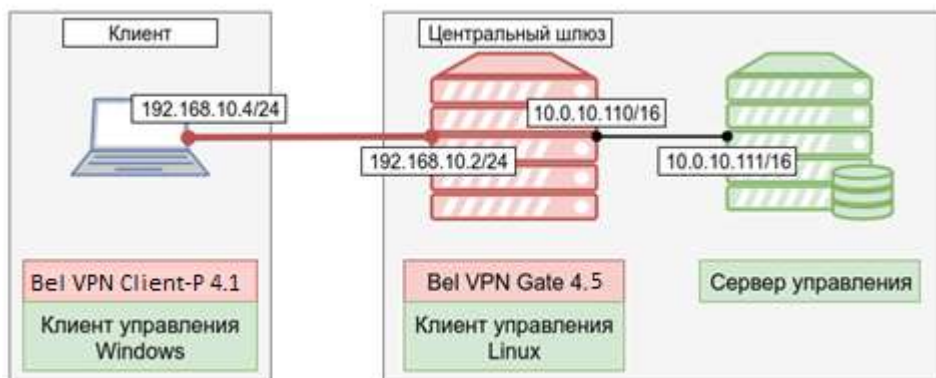


Рисунок 2

Далее по тексту управляемые устройства будем называть клиентами, на которые устанавливается (установлен) продукт Bel VPN Gate 4.5/4.1/Client-P 4.1 и Клиент управления.

Шлюз безопасности Bel VPN Gate 4.5, защищающий подсеть с Сервером управления, будем называть центральным шлюзом.

2. Сценарии управления

Выделяется два последовательных сценария обновления продукта Bel VPN Gate/Client 4.1/4.5 на управляемом устройстве.

Сценарий первого обновления (при первом обращении к управляемому устройству):

- для Bel VPN Client-P 4.1 – подготовка инсталляционных файлов Клиента управления и Bel VPN Client-P 4.1, доставка и локальная установка на управляемом устройстве;
- для Bel VPN Gate 4.1/4.5 – подготовка скриптов для инсталляции (инициализации) Клиента управления и настройки установленного продукта Bel VPN Gate 4.1/4.5, доставка и локальный запуск на управляемом устройстве

Сценарий последующих обновлений (все последующие взаимодействия с управляемым устройством) – создание обновлений на Сервере управления и передача их по защищенному VPN соединению.

Опишем подробно приведенные выше два сценария.

2.1. Сценарий первого обновления

- Шаг 1:** Установите Сервер управления на выделенный компьютер с установленной ОС Windows Server 2003/2008/2012/2016/2019, выполните настройку в соответствии с разделом [«Установка и настройка Сервера управления»](#).
- Шаг 2:** Настройте центральный шлюз - на Сервере управления подготовьте скрипты, доставьте их и запустите локально (см. раздел [«Настройка и управление центральным шлюзом»](#)).
- Шаг 3:** На Сервере управления подготовьте инсталляционные файлы продукта Bel VPN Client-P 4.1 и Клиента управления, доставьте и установите локально на управляемое устройство (см. раздел [«Настройка и управление устройством с Bel VPN Client-P 4.1»](#))
- Шаг 4:** Установленный Клиент управления автоматически выполнит проверку возможности устанавливать соединение с Сервером управления и получать обновления.

2.2. Сценарий последующих обновлений

- Шаг 1:** На Сервере управления сформируйте обновление для управляемого устройства., В заданное время пакет обновления будет создан автоматически и сразу будет доступен для скачивания.
- Шаг 2:** Клиент управления, периодически проверяя наличие доступных для него обновлений, скачает его с Сервера управления. Можно задать подряд несколько обновлений с указанием времени создания каждого, и они будут применены в том порядке, в котором и были созданы.

3. Установка Сервера управления

3.1. Инсталляция Сервера управления

Инсталляция Сервера управления осуществляется на выделенном компьютере с установленной ОС:

- Windows Server 2003 (32-bit);
 - Windows Server 2008 (32-bit, 64-bit);
 - Windows Server 2012 (64-bit);
 - Windows Server 2016 (64-bit);
 - Windows Server 2019 (64-bit).
1. Для инсталляции Сервера управления запустите файл `setup.exe` из состава дистрибутива. Появится окно с запросом на установку необходимых компонент, нажмите кнопку **Установить** (Рисунок 3).

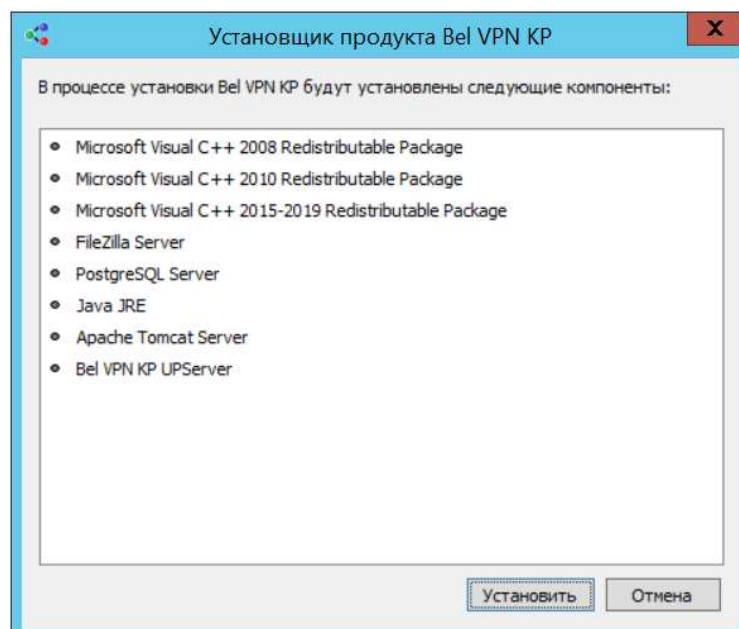


Рисунок 3

2. Выполняется сбор информации для Microsoft Visual C++ Redistributable Package и подготовка к инсталляции.

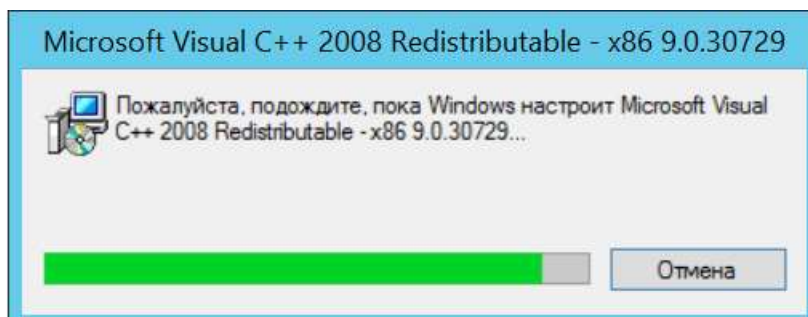


Рисунок 4

3. Установка Microsoft Visual C++ Redistributable Package выполняется без вмешательства администратора (Рисунок 5).

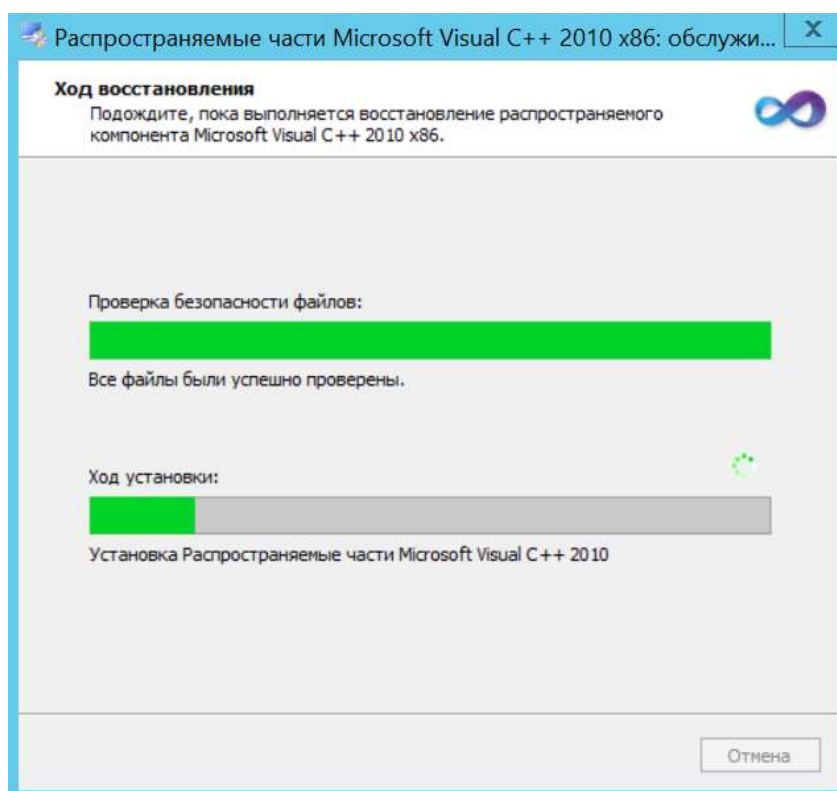


Рисунок 5

4. Далее устанавливается продукт FileZilla Server (Рисунок 6). Примите условия лицензионного соглашения – нажмите кнопку **I Agree**.

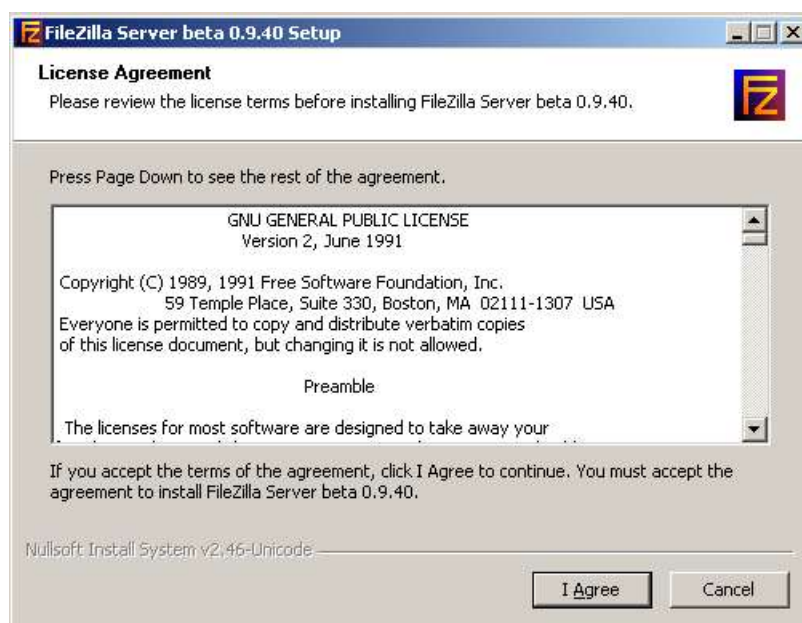


Рисунок 6

5. В следующем окне (Рисунок 7) предлагается выбрать компоненты для инсталляции. Оставьте настройки по умолчанию и нажмите кнопку [Next](#).

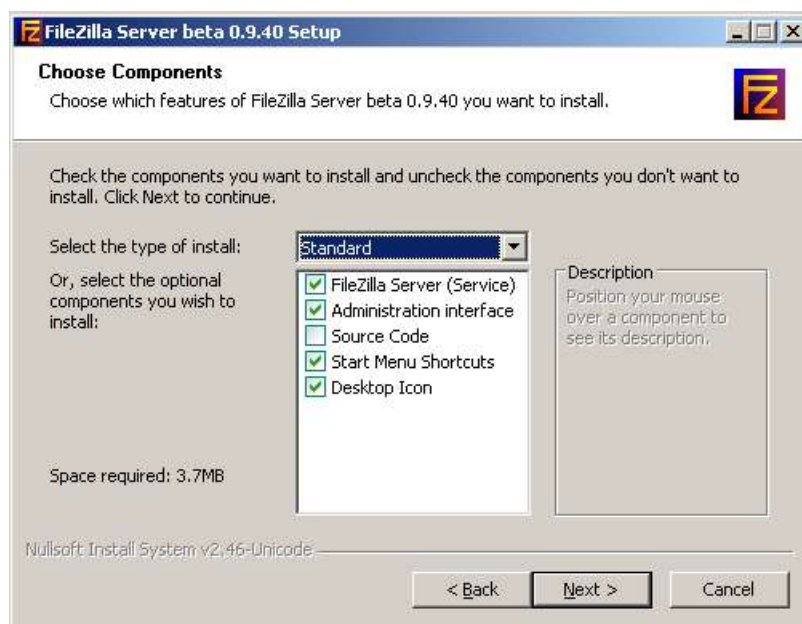


Рисунок 7

6. Укажите папку, в которую будет установлен продукт FileZilla Server (Рисунок 8).

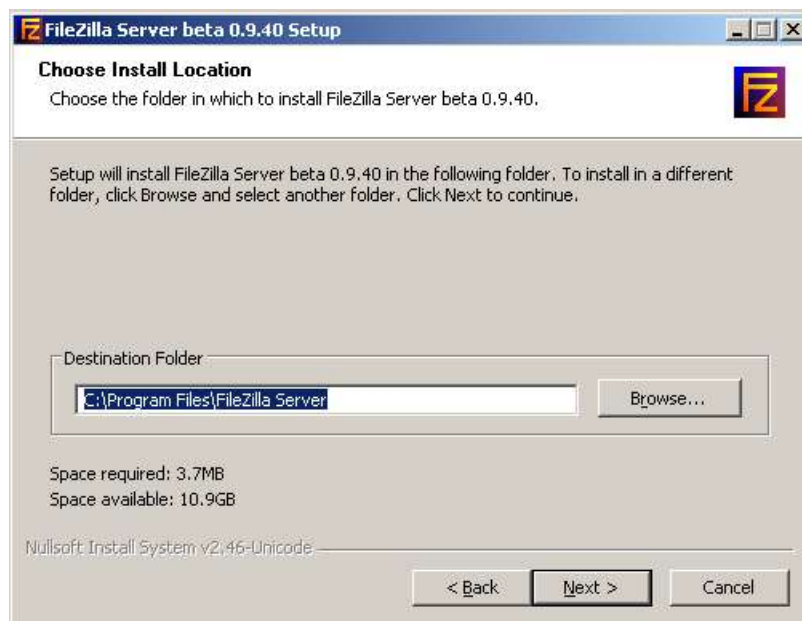


Рисунок 8

7. В окне выбора настроек для запуска сервиса продукта FileZilla Server оставьте значения по умолчанию и нажмите кнопку **Next** (Рисунок 9).

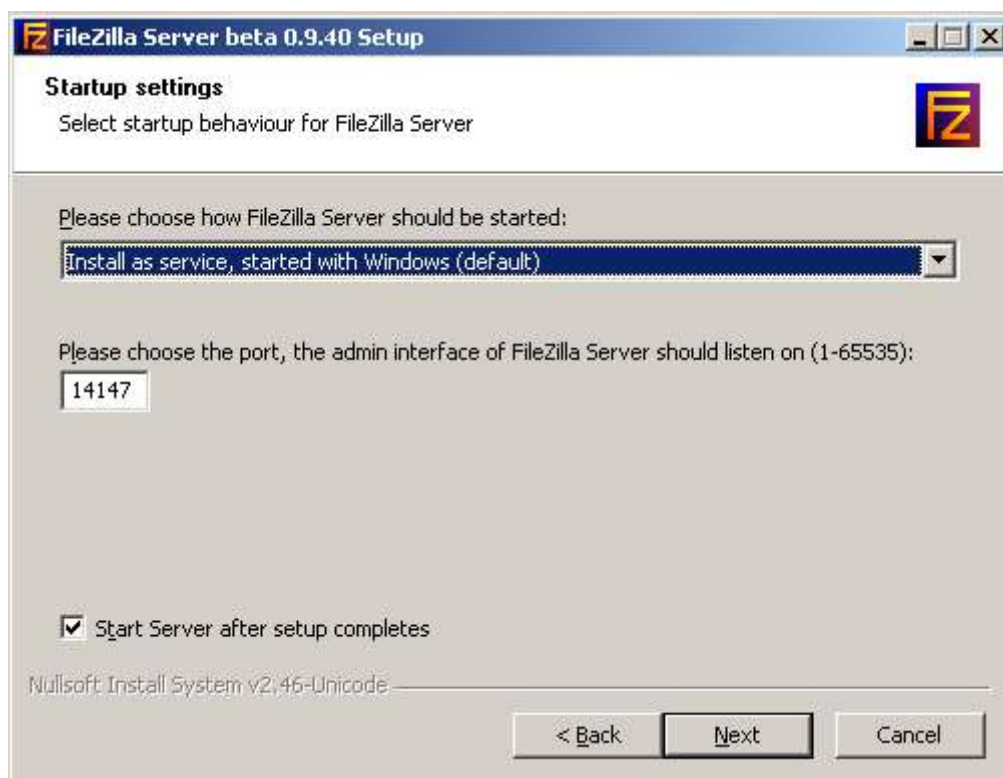


Рисунок 9

8. В окне с настройками старта консоли управления продуктом FileZilla Server оставьте значения по умолчанию и нажмите кнопку **Install** (Рисунок 10), после чего запустится процесс установки.

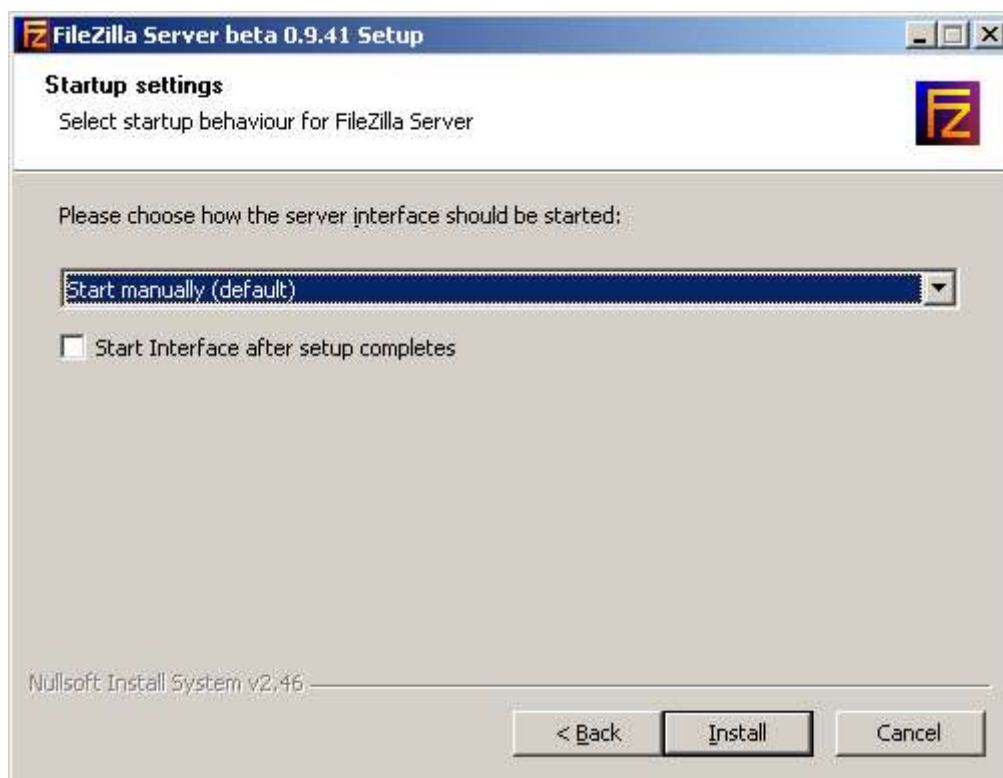


Рисунок 10

9. По завершению процесса установки FileZilla Server нажмите кнопку **Close** (Рисунок 11).

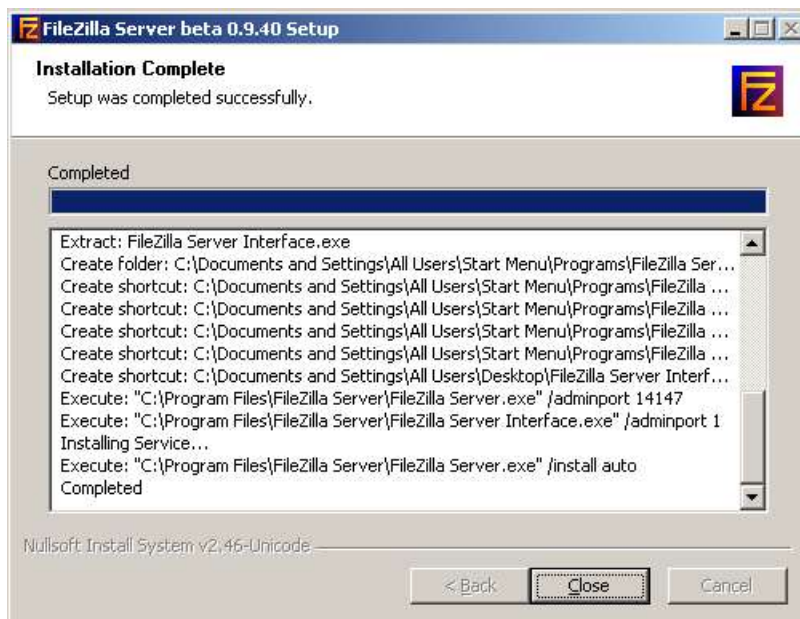


Рисунок 11

10. Далее устанавливается компонент PostgreSQL Server, нажмите кнопку **Next >** (Рисунок 12).

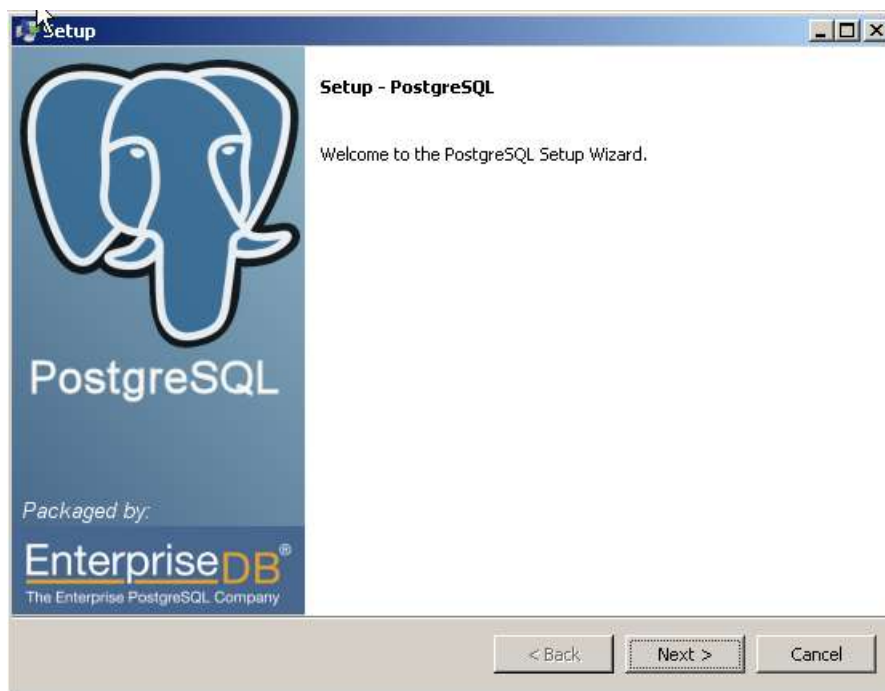


Рисунок 12

11. Задайте каталог установки продукта PostgreSQL Server, можно оставить по умолчанию или указать другой (Рисунок 13).

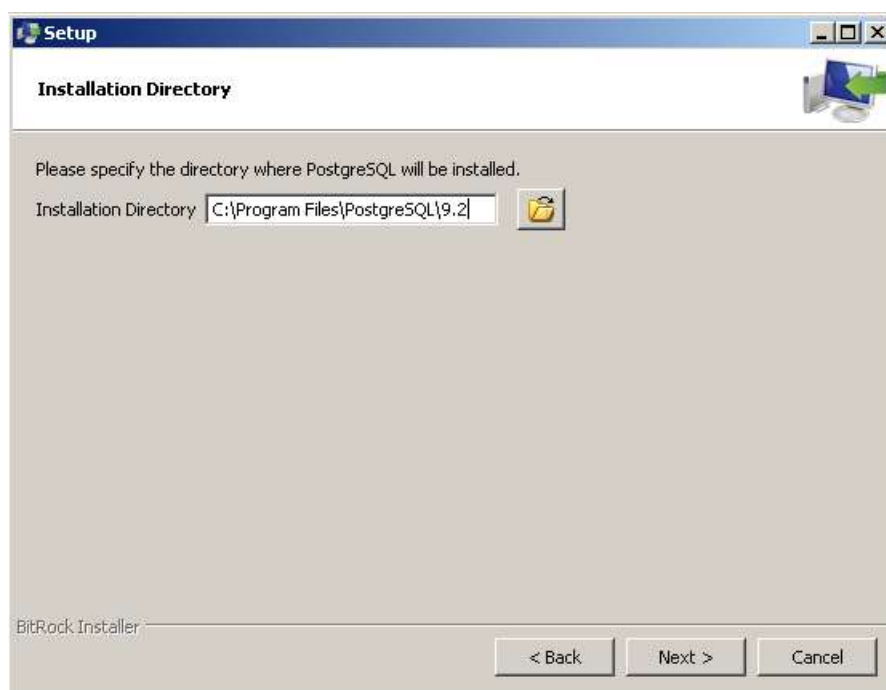


Рисунок 13

12. Задайте каталог инсталляции файлов базы данных (Рисунок 14).

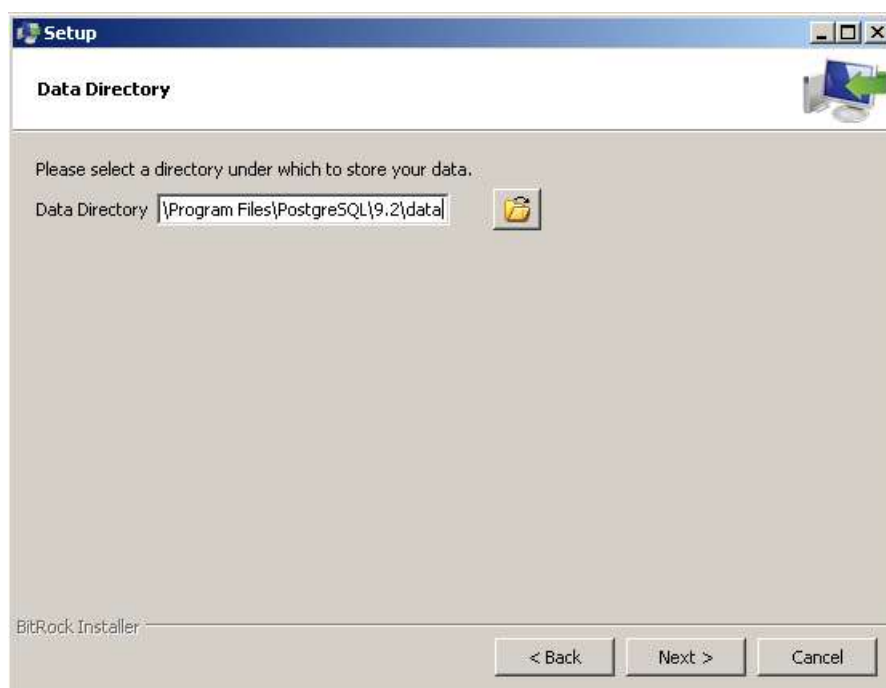


Рисунок 14

13. Далее появится окно с запросом пароля суперпользователя для работы с базой данных (Рисунок 15). По умолчанию задан пароль 1234567890. Этот пароль не должен изменяться администратором в процессе инсталляции, так как это не позволит модернизировать базу данных нужным образом в процессе инсталляции. Если есть потребность изменить этот пароль, администратор может это сделать **после** завершения инсталляции, изменив пароль в самой базе данных и в конфигурационном файле Сервера управления (чтобы Сервер управления мог взаимодействовать с базой данной).

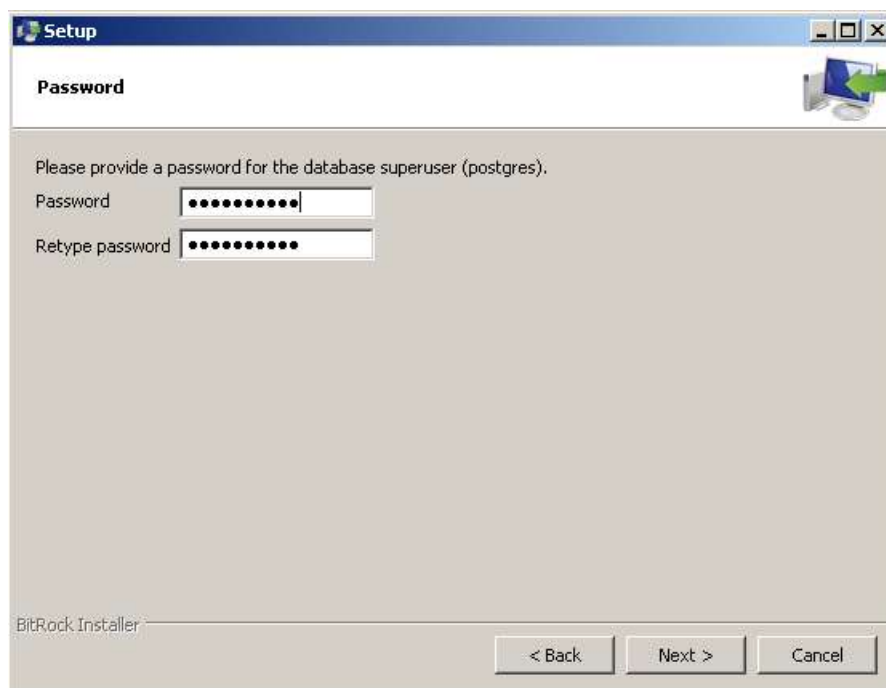


Рисунок 15

14. Далее появится окно с указанием порта - 5432, по которому будет происходить обращение к базе данных (Рисунок 16). Рекомендуется оставить это значение, в противном случае придется вносить новое значение в конфигурационный файл Сервера управления. Нажмите кнопку [Next](#).

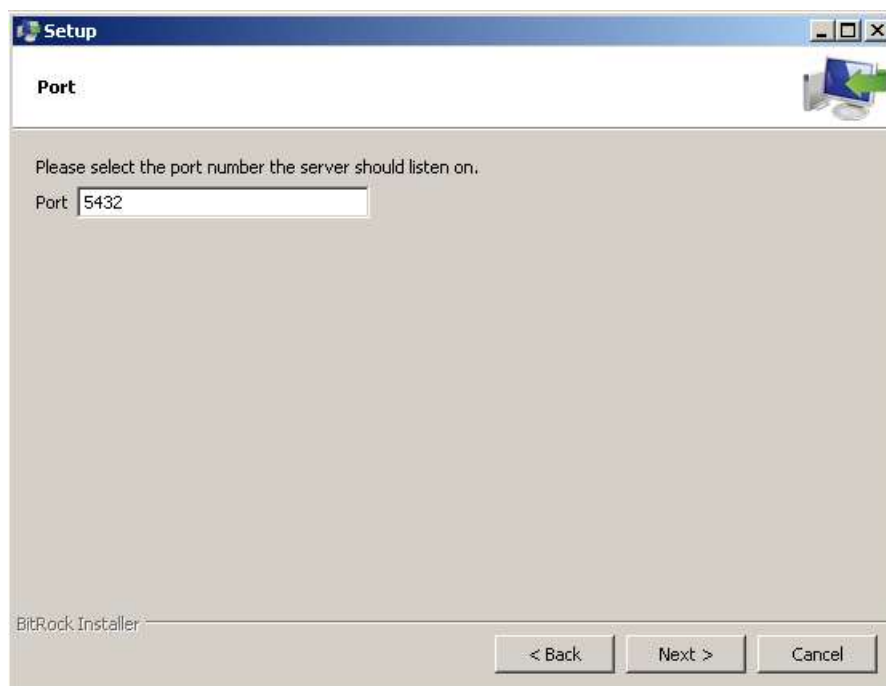


Рисунок 16

15. В окне задания языка хранения данных (Рисунок 17) оставьте значение по умолчанию.

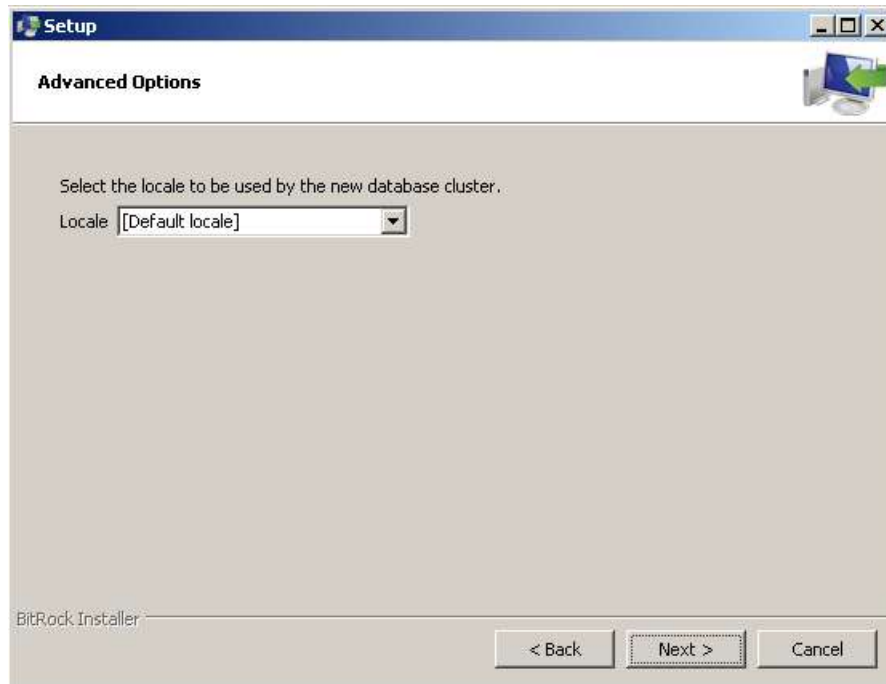


Рисунок 17

16. Далее начнется инсталляция PostgreSQL (Рисунок 18).

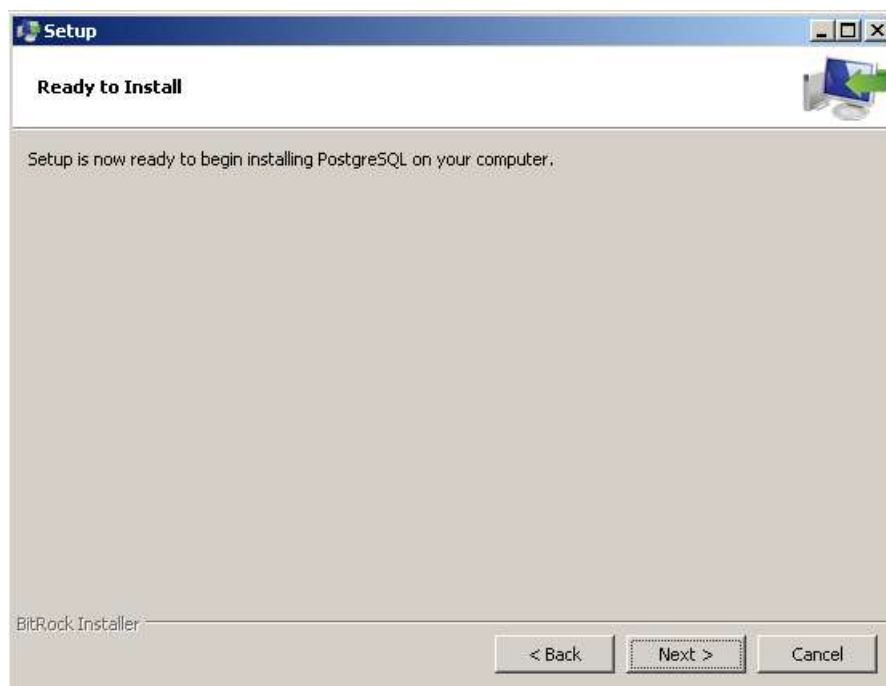


Рисунок 18

17. По окончании инсталляции PostgreSQL нажмите кнопку Finish (Рисунок 19).

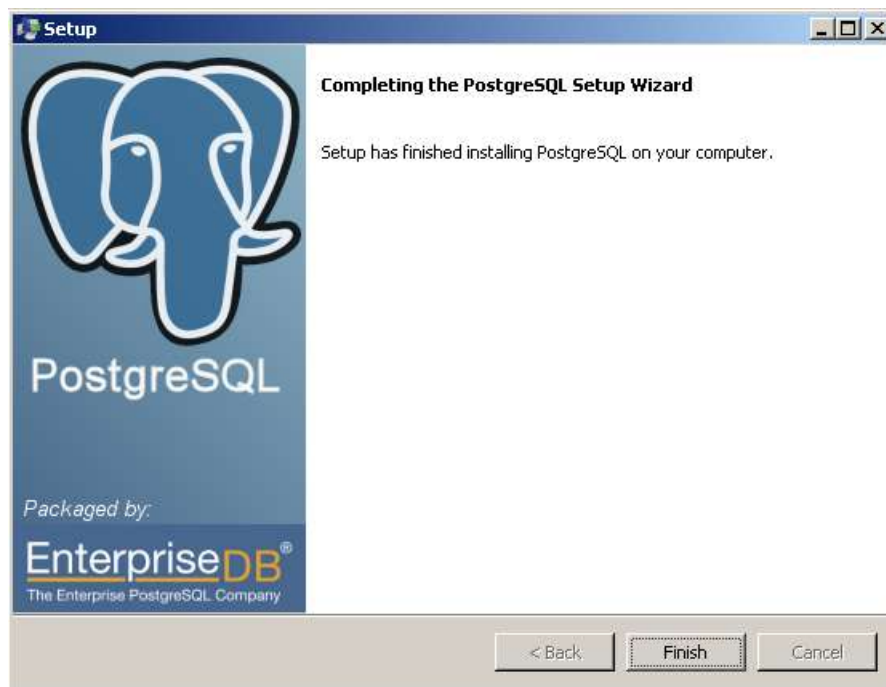


Рисунок 19

18. Далее устанавливается Java JRE (Рисунок 20). Нажмите кнопку [Install](#).



Рисунок 20

19. Инсталляция занимает некоторое время (Рисунок 21).



Рисунок 21

20. По окончании инсталляции Java JRE нажмите кнопку [Close](#) (Рисунок 22).



Рисунок 22

21. Устанавливается компонента Apache Tomcat Server, нажмите кнопку [Next](#) (Рисунок 23).



Рисунок 23

22. Согласитесь с лицензионным соглашением, нажав кнопку **I Agree** (Рисунок 24).

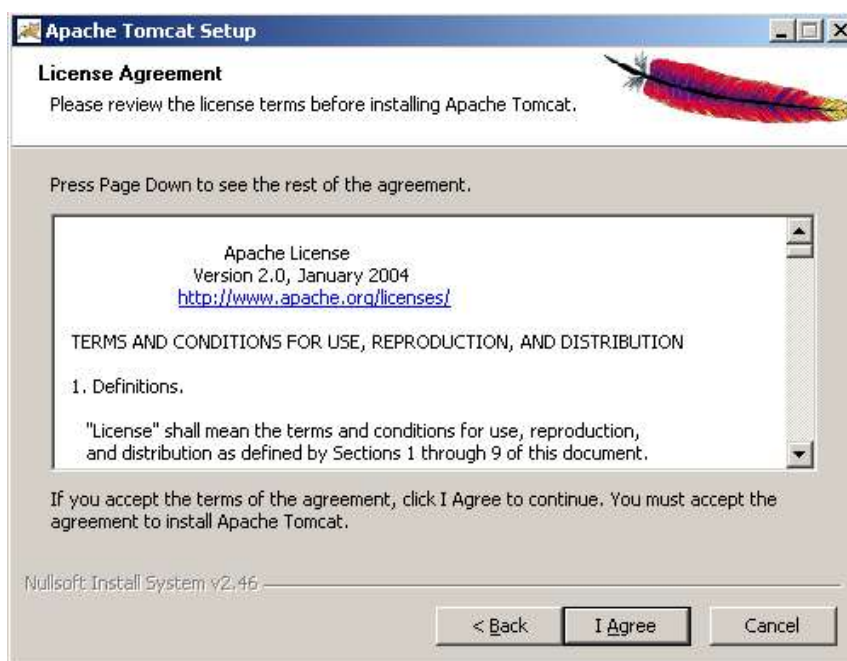


Рисунок 24

23. Выбранные компоненты для инсталляции по умолчанию можно оставить и нажать [Next >](#) (Рисунок 25).

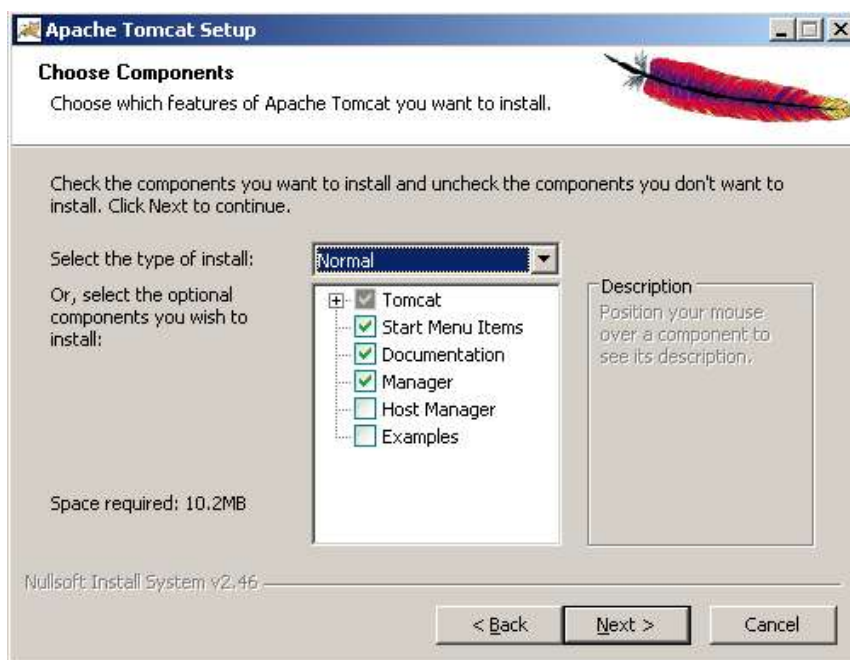


Рисунок 25

24. Основные параметры работы продукта оставьте по умолчанию (Рисунок 26).

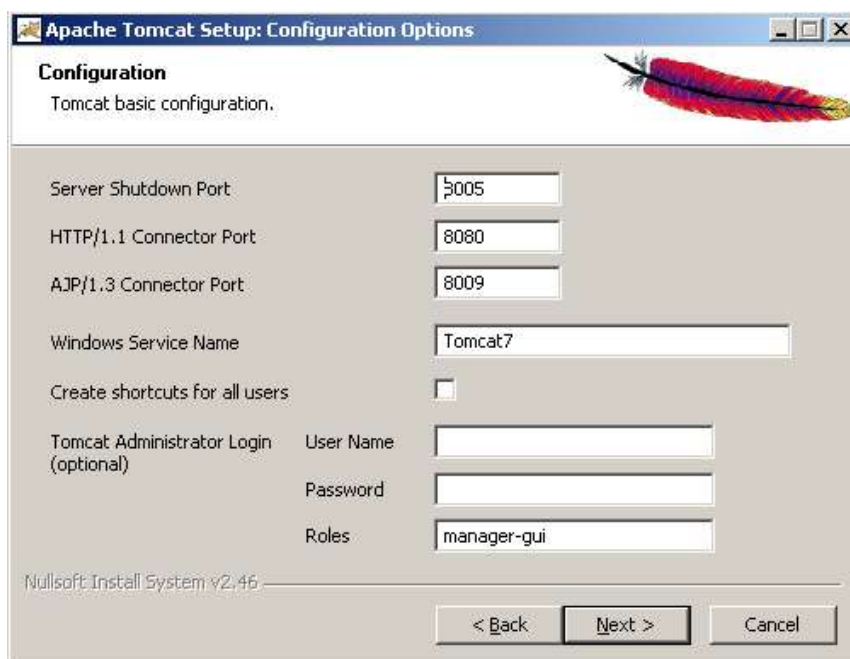


Рисунок 26

25. Укажите папку, в которую был инсталлирован Java SE, можно оставить путь по умолчанию и нажать кнопку Next > (Рисунок 27).

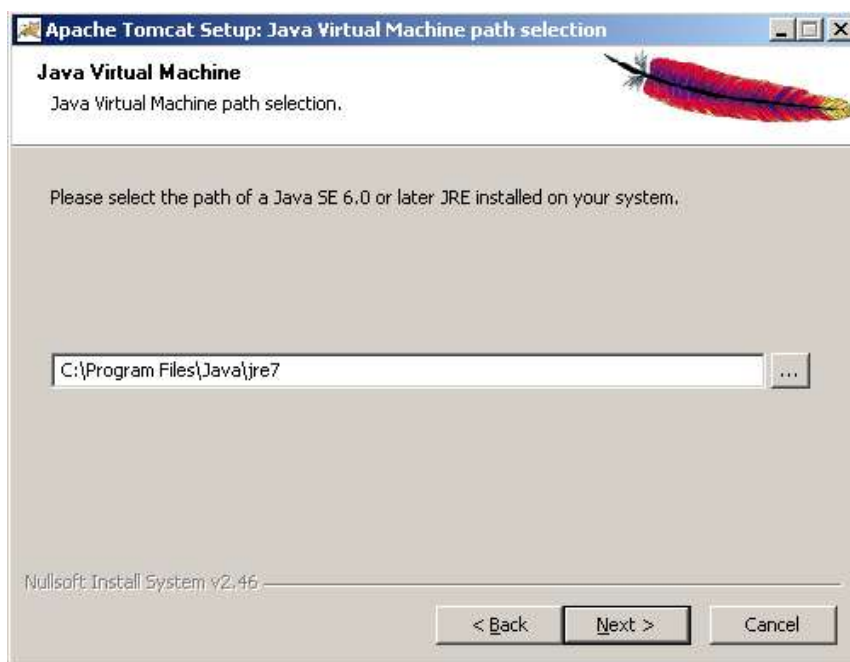


Рисунок 27

26. Для инсталляции бинарных кодов Apache Tomcat Server папку можно оставить по умолчанию и нажать **Install** (Рисунок 28).

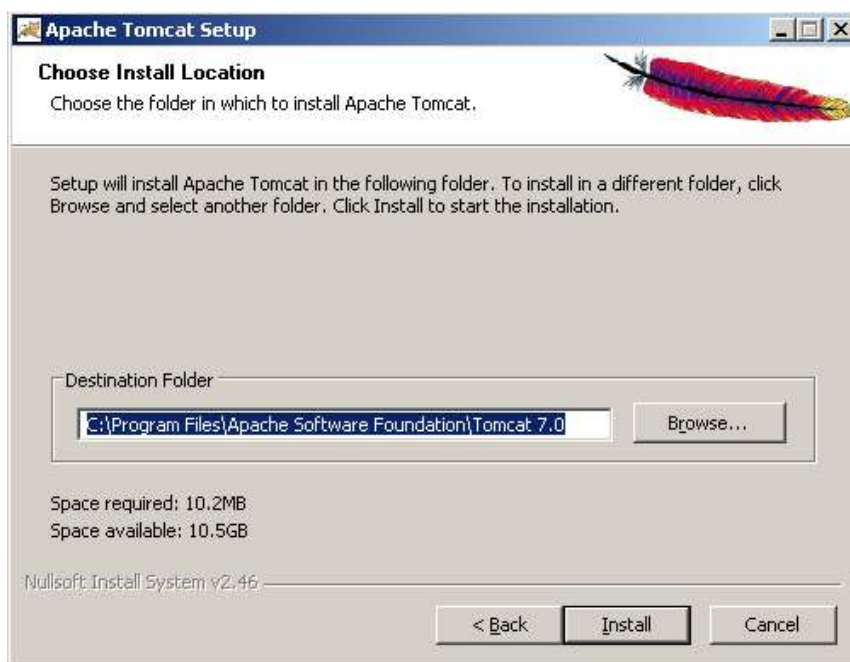


Рисунок 28

27. Начнется процесс инсталляции (Рисунок 29).

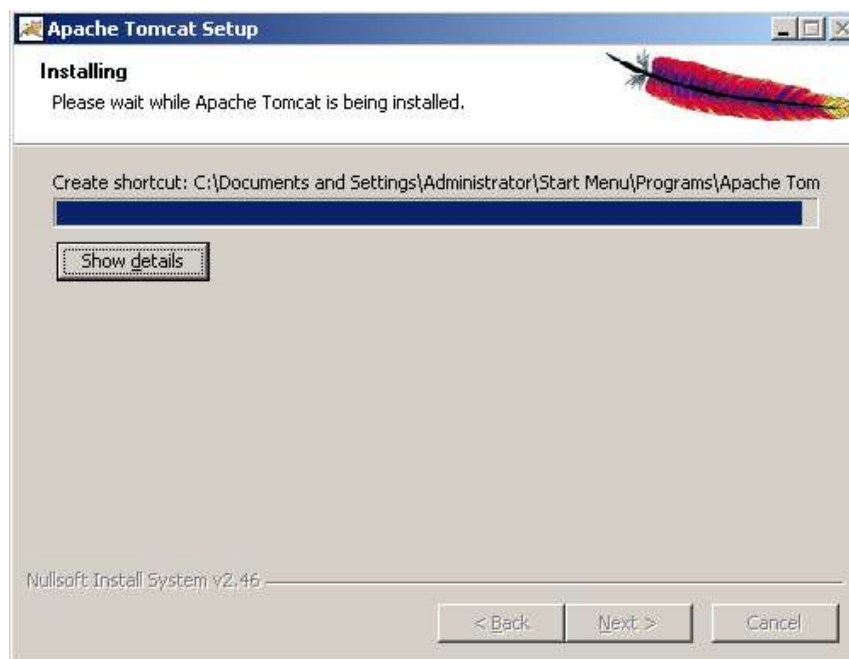


Рисунок 29

28. По окончании инсталляции нажмите кнопку **Finish**, предварительно отменив запуск сервиса Apache и показа информации о продукте, если нужно (Рисунок 30).



Рисунок 30

29. Если запуск сервиса Apache не был отменен, то происходит его запуск (Рисунок 31).

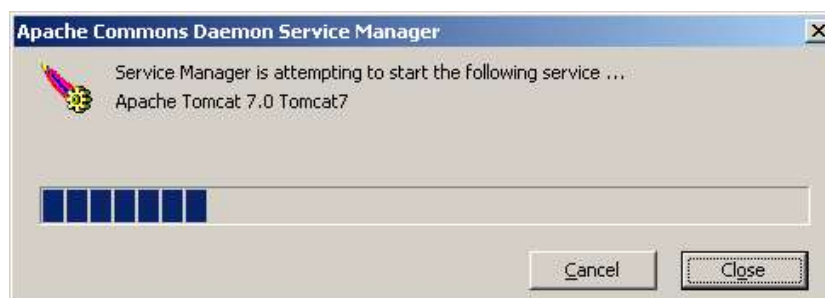


Рисунок 31

30. Появляется окно с адресом лицензионного соглашения и ограничениями к применению.

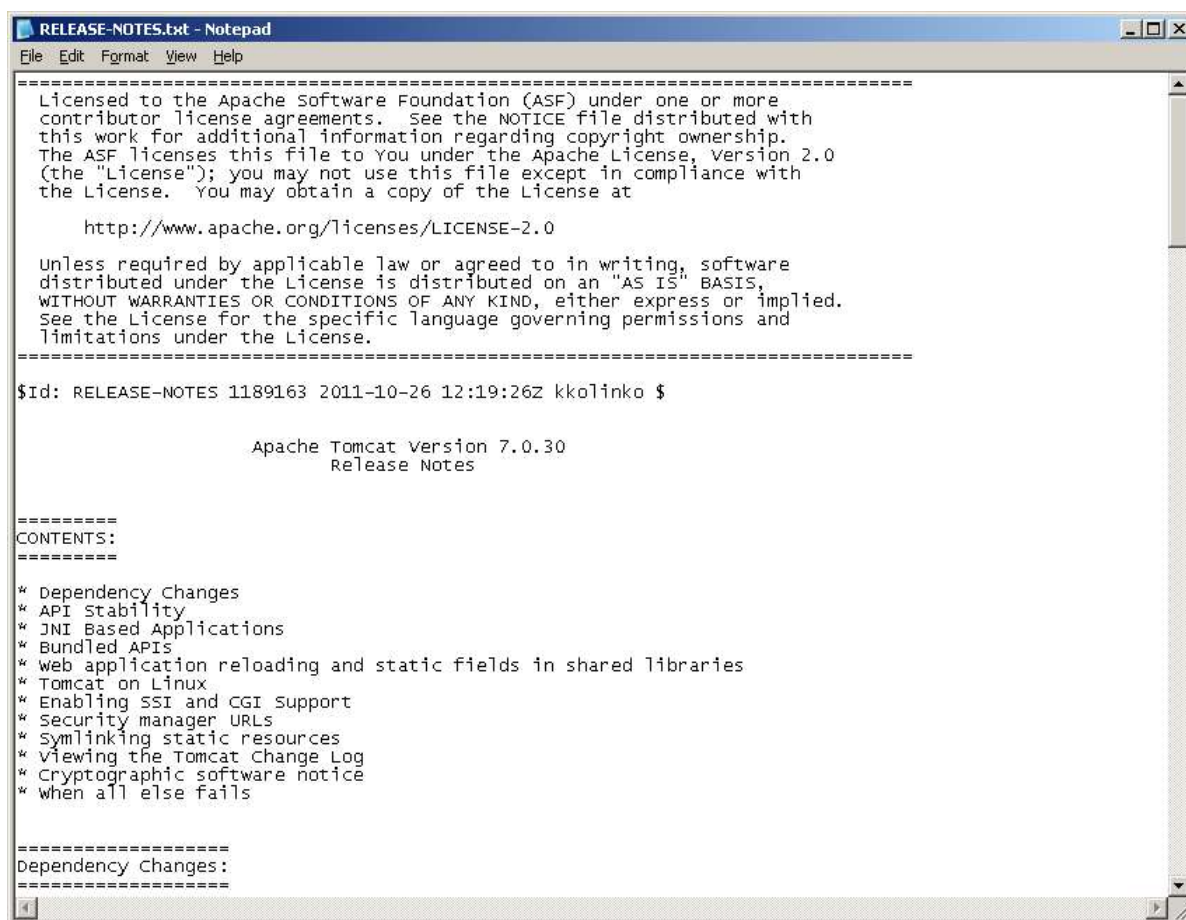


Рисунок 32

31. Начинается инсталляция Сервера управления (Рисунок 33). Нажмите кнопку **Next >**.

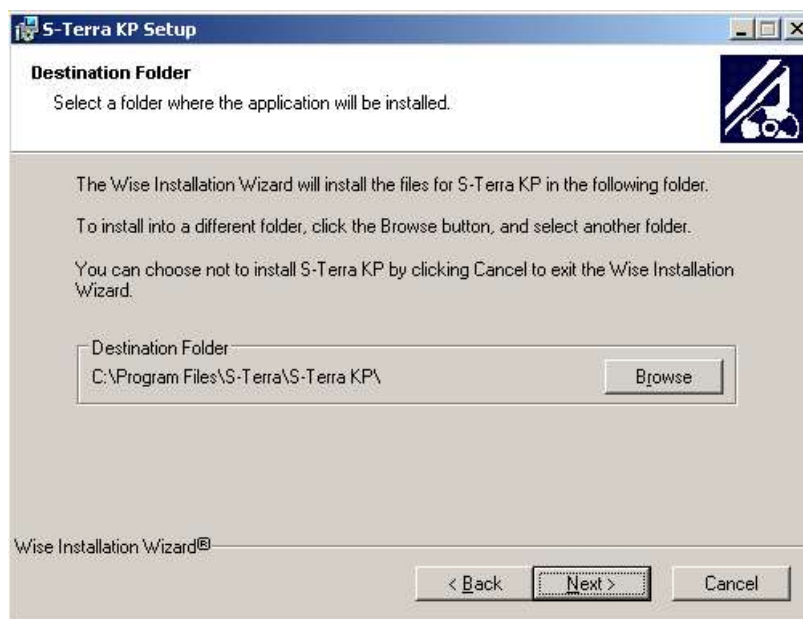


Рисунок 33

32. Каталог, в который устанавливается Сервер управления, можно оставить по умолчанию и нажать **Next >** (Рисунок 34).

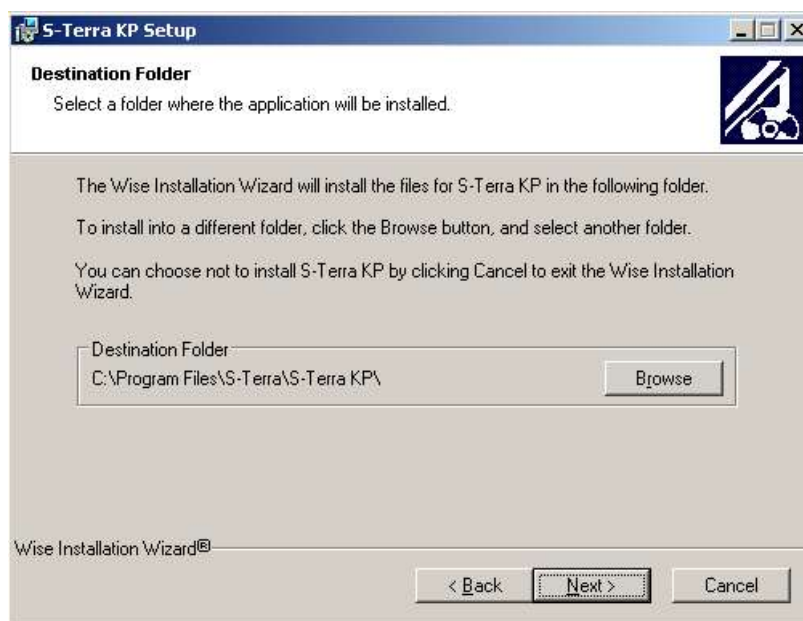


Рисунок 34

33. После установки Сервера управления и запуска сервиса, который может быть продолжительным порядка двух минут, так как проверяется целостность файлов программной части, выдается окно об окончании установки, нажмите в нем кнопку **Finish**.



Рисунок 35

4. Настройка Сервера управления

4.1. Настройка механизма идентификации и аутентификации в Сервер управления

Для настройки механизма идентификации и аутентификации для доступа к Серверу управления выполните следующее:

1. Запустите консоль Сервера управления – **Bel VPN UPServer Console** (Пуск→Программы→S-Terra Bel→Bel VPN KP→UPServer Console).
2. В консоли выберите меню **Инструменты** и предложение **User editor...** (Рисунок 36).

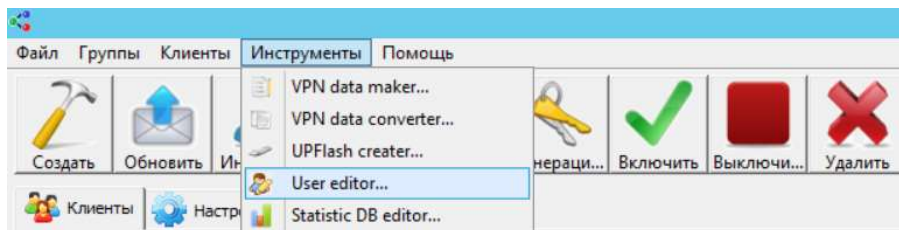


Рисунок 36

3. Появится окно **UPServer вход** для ввода пароля пользователя с именем «superuser». Для этого пользователя (по умолчанию) предустановлен пустой пароль. Нажмите кнопку **OK** (Рисунок 37).

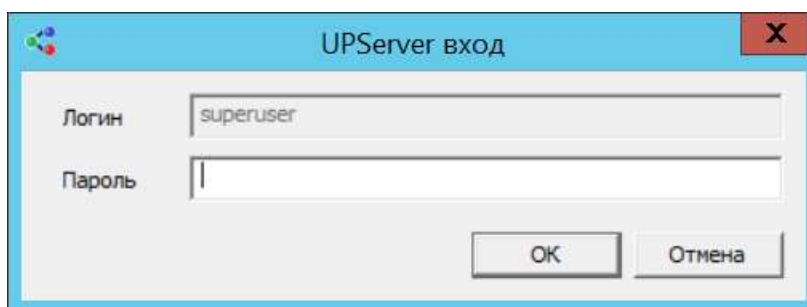


Рисунок 37

4. Замените пароль пользователю «superuser», если будете создавать новых пользователей (Рисунок 37).

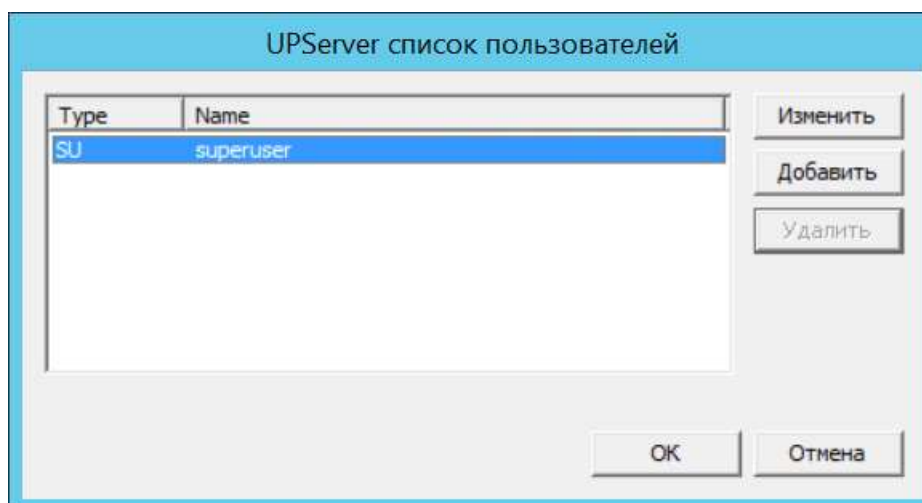


Рисунок 37

- В окне **UPServer пользователь** введите пароль дважды и нажмите ОК (Рисунок 38).

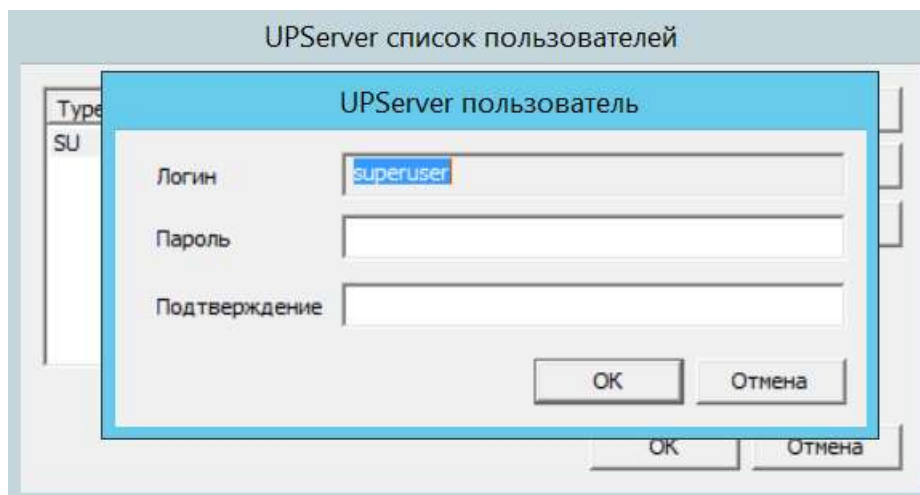


Рисунок 38

- Только пользователь с идентификатором «superuser» и знающий его пароль может в дальнейшем назначать администратора, имеющего право доступа к Серверу управления.
- Для назначения администратора нажмите кнопку **Добавить** (Рисунок 39).

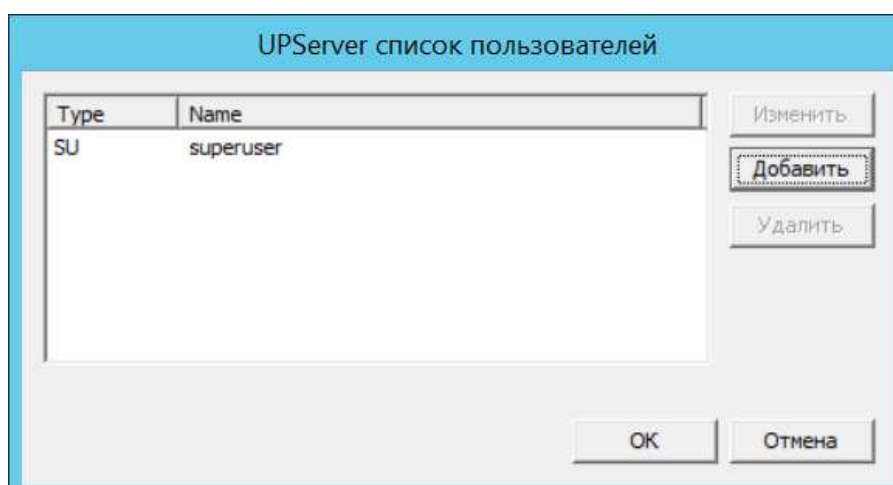


Рисунок 39

- Назначьте имя и пароль администратору и нажмите кнопку **OK** дважды (Рисунок 40).

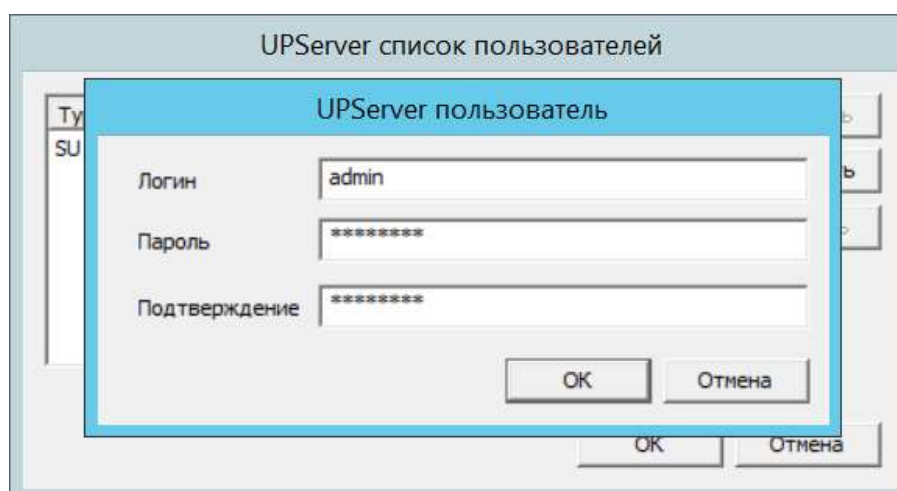


Рисунок 40

- Закройте консоль Сервера управления - **VPN UPServer Console**.

10. В дальнейшем при запуске консоли Сервера управления (Пуск→Программы→S-Terra_Bel→Bel VPN КР→UPServer Console) будет появляться окно **UPServer вход** для ввода имени и пароля администратора для доступа к Серверу управления (Рисунок 41).

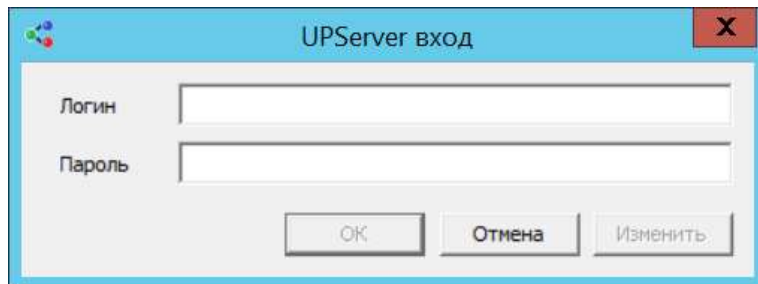


Рисунок 41

11. В этом же окне назначенный администратор может изменить свой пароль, нажав кнопку **Изменить** (Рисунок 42).

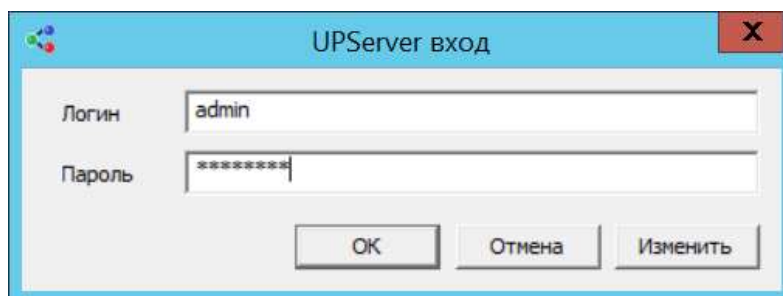


Рисунок 42

12. После нажатия кнопки **ОК** при успешном вводе данных запустится консоль Сервера управления - **VPN UPServer Console** (Рисунок 43).
13. После трех общих неуспешных попыток ввода идентификатора и пароля администратора, окно консоли Сервера управления не откроется, а появится сообщение о трех неуспешных попытках ввода данных и закрытии системы.
14. Если администратор с именем «superuser» не назначит еще одного администратора, кроме себя, для доступа к Серверу управления, то при запуске консоли Сервера управления окно **UPServer вход** появляться не будет.

4.2. Настройка Сервера управления

Начальная настройка Сервера управления производится во вкладке **Настройки**, а настройка и управление клиентами – во вкладке **Клиенты** (Рисунок 43).

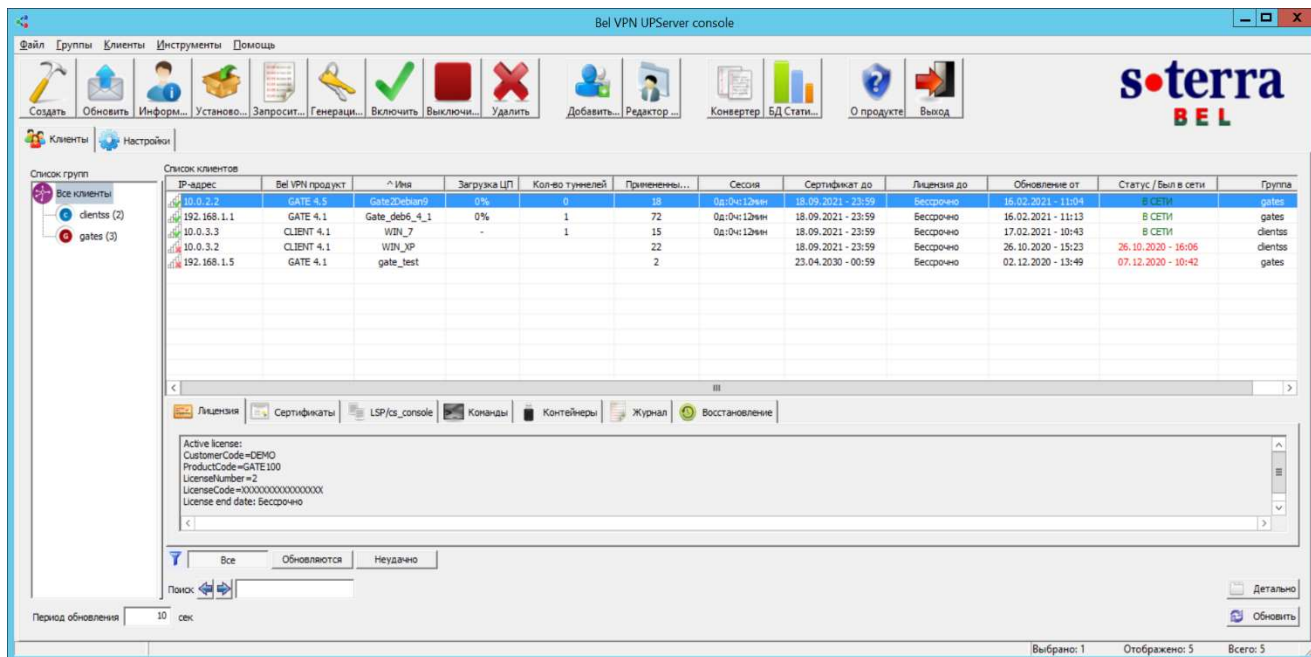


Рисунок 43

Меню графического интерфейса описано в главе «Описание интерфейса Сервера управления».

При первом запуске приложения **VPN UPSever Console** выводится предупреждение о необходимости задать настройки продукта **Сервер управления** (Рисунок 44).

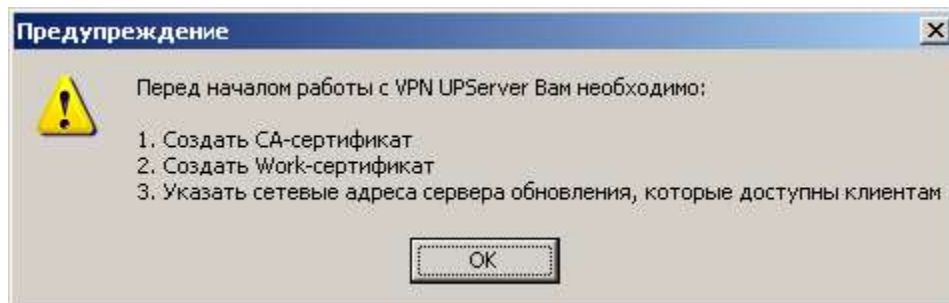


Рисунок 44

Нажмите кнопку **OK**, откроется окно настроек продукта Сервер управления (Рисунок 45). Во вкладке **Настройки** введите данные лицензии, создайте CA-сертификат и рабочий сертификат Сервера управления, а также задайте сетевые адреса Сервера управления, что далее описано подробно по пунктам.

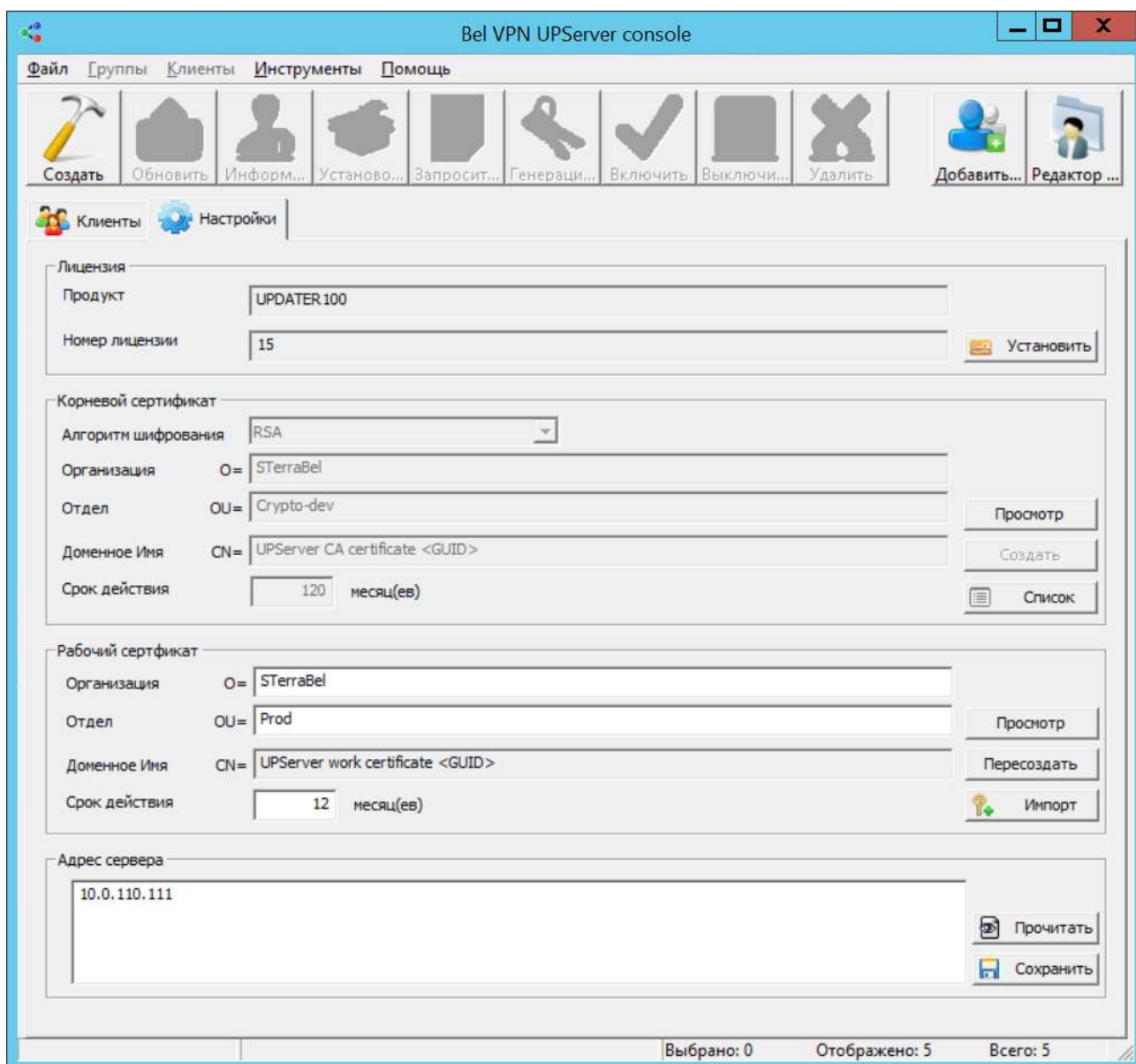


Рисунок 45

4.2.1. Ввод лицензии

Для ввода лицензии на продукт Сервер управления нажмите кнопку **Установить** (Рисунок 45).

В появившемся окне **Ввод лицензии** (Рисунок 46):

в поле **Продукт** выберите тип продукта из выпадающего списка:

UPDATER100 – продукт будет работать с количеством Клиентов управления не более 10;

UPDATER1000 – продукт будет работать с количеством Клиентов управления не более 50;

UPDATER3000 – продукт будет работать с количеством Клиентов управления не более 1000;

UPDATER7000 – продукт будет работать с неограниченным количеством Клиентов управления

в поле **Клиентский код** укажите название организации, которой выдана лицензия

в поле **Номер лицензии** введите номер лицензии

в поле **Лицензионный код** введите код лицензии.

Все эти данные можно взять с бланка лицензии, поставляемой вместе с продуктом.

Если лицензия была получена в виде файла, то нажмите кнопку **Открыть файл** и данные для заполнения полей будут взяты из этого файла.



Если лицензия на продукт не введена, то продукт будет работать максимум с двумя Клиентами управления.

Рисунок 46

4.2.2. Создание CA сертификата



Создать CA сертификат и рабочий сертификат Сервера управления можно с помощью доверенного УЦ, а потом импортировать их на Сервер управления. Существует одно ограничение: поле CN такого сертификата должно начинаться с зарезервированной строки **CN=UPServer CA certificate**.

Можно выполнить создание CA сертификата прямо на Сервере управления.

1. В группе **Корневой сертификат** (Рисунок 45) нажмите кнопку Создать и заполните поля в окне **Создание нового CA сертификата**:

Алгоритм открытого ключа – алгоритм генерации открытого ключа CA сертификата и ЭЦП¹, доступен алгоритм:

RSA - длина открытого ключа – 2048 бит

Организация – название организации

Отдел – название отдела в организации

Доменное имя – имя владельца сертификата, заполняется автоматически

Срок действия – срок действия сертификата в месяцах.

2. После этого нажмите кнопку **Создать**, будет выдано **Предупреждение** (Рисунок 47), нажмите **ОК**.

¹ Данная ЭЦП используется только для контроля целостности и авторства файлов обновления, и НЕ применяется для построения защищенного канала связи

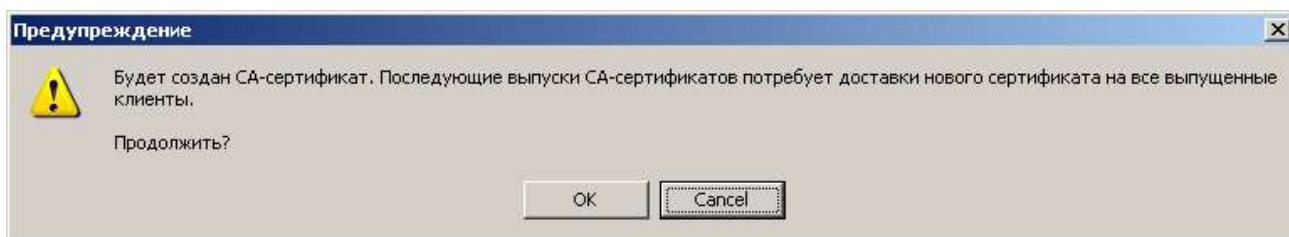


Рисунок 47

3. СА сертификат создан и хранится в сертификатном хранилище операционной системы, нажмите **ОК**.

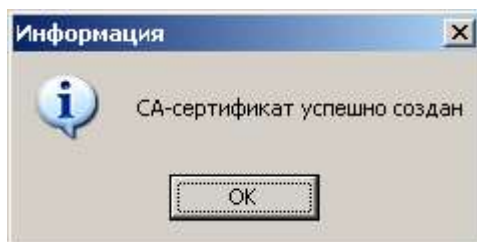


Рисунок 48



Note

Рекомендуется СА сертификат и секретный ключ к нему сохранить на другом компьютере для предотвращения потери СА-сертификата при поломке компьютера, на котором установлен Сервер управления.

4.2.3. Создание рабочего сертификата

1. В группе **Рабочий сертификат** (Рисунок 45) заполните поля рабочего (локального) сертификата Сервера управления и нажмите кнопку **Создать**. Перед созданием будет выдано **Предупреждение** (Рисунок 49):

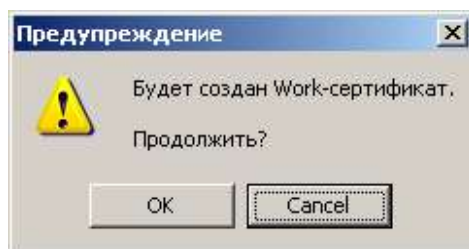


Рисунок 49

2. Если поля заполнены верно – нажмите кнопку **ОК**.
3. После успешного создания сертификата будет выдано подтверждение, нажмите кнопку **ОК** (Рисунок 50).

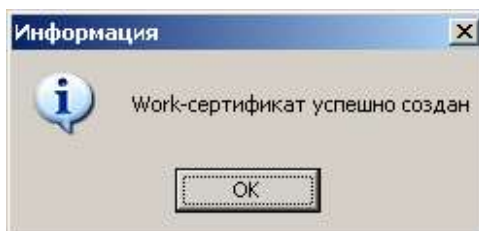


Рисунок 50

После этого кнопка **Создать** в группе **Рабочий сертификат** изменится на **Пересоздать**.

По истечению срока действия рабочего сертификата пересоздайте его, нажав кнопку **Пересоздать**.

4.2.4. Задание адресов Сервера управления

1. В группе **Адрес сервера** (Рисунок 45) задайте список сетевых адресов Сервера управления, которые доступны с управляемых устройств, следуя при этом следующим правилам:
 - ♦ каждый адрес должен располагаться на отдельной строке, перевод строки осуществляется нажатием клавиши **Enter** или **Ctrl-Enter**
 - ♦ сетевой адрес представляет собой IP-адрес или DNS-имя, которое будет транслироваться в IP-адрес на устройстве в момент создания соединения с Сервером управления
 - ♦ Сервер управления должен размещаться в подсети, защищенной шлюзом безопасности (центральным). Согласно Рисунку 2 адрес Сервера управления – 10.0.10.111.
2. После задания адресов обязательно нажмите кнопку **Сохранить**, появится предупреждение (Рисунок 51).
3. Если адреса введены верно, то нажмите кнопку **OK**, при этом происходит проверка введенных данных и только после этого во все создаваемые дистрибутивы Клиентов управления по умолчанию будет вноситься список адресов Сервера управления.

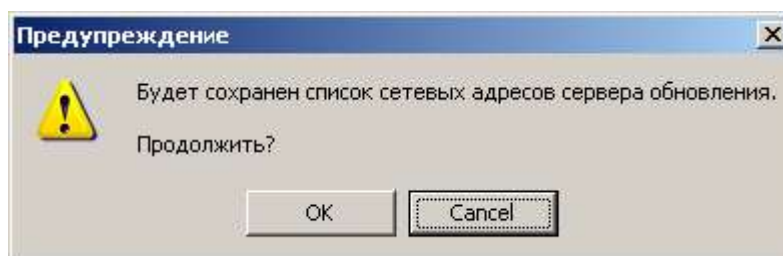


Рисунок 51



Note

На данном этапе категорически не рекомендуется задавать адреса, не принадлежащие Серверу управления. Адреса, не принадлежащие Серверу управления, могут быть указаны только при процедуре перевода клиентов на другой Сервер управления. Инструкция по переводу клиентов на другой Сервер управления будет выдаваться по запросу пользователя при появлении такой потребности.

Далее перейдите во вкладку **Клиенты** и выполните настройки для центрального шлюза.

5. Настройка и управление центральным шлюзом

Создание и удаление учетных записей клиентов управляемых устройств, создание для них Клиентов управления, обновлений будем выполнять во вкладке **Клиенты** (Рисунок 52) Сервера управления, интерфейс которой описан в разделе «Описание интерфейса Сервера управления».

Во вкладке **Клиенты** отражается информация обо всех управляемых устройствах. Далее, будет выполняться настройка центрального шлюза для стенда, приведенного на рисунке 2.

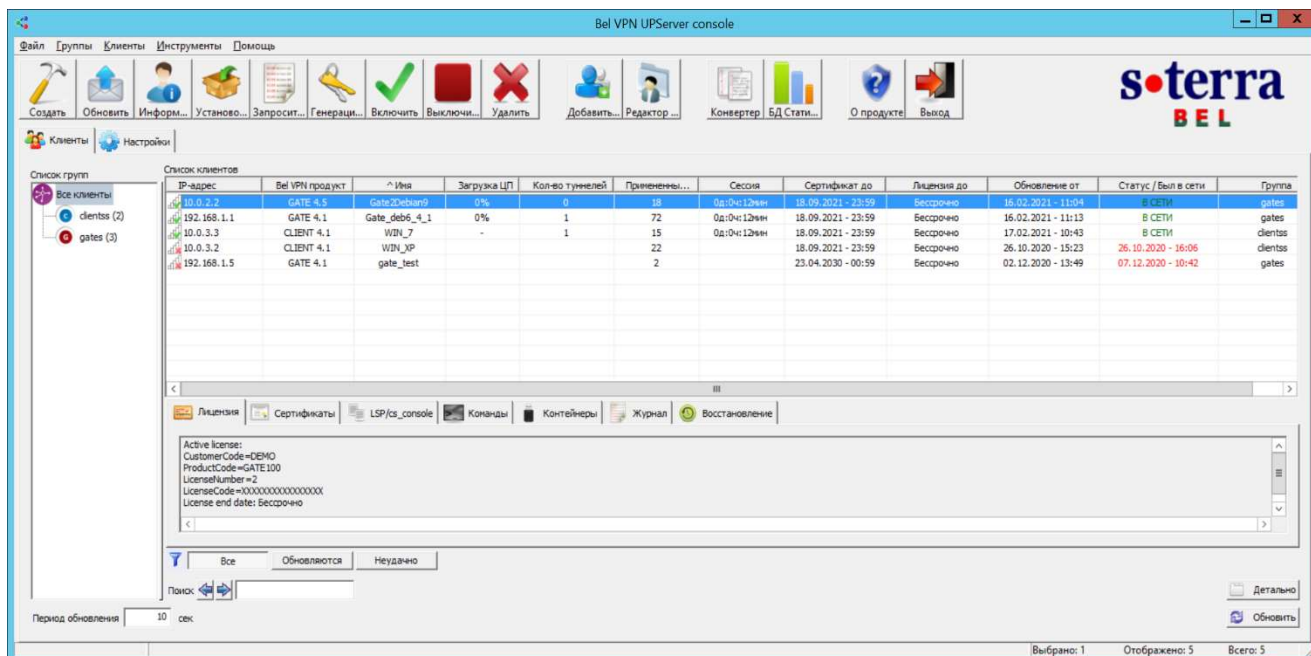


Рисунок 52

5.1. Создание учетной записи Клиента для Центрального шлюза

1. В меню **Клиенты** выберите предложение **Создать** (Рисунок 53).

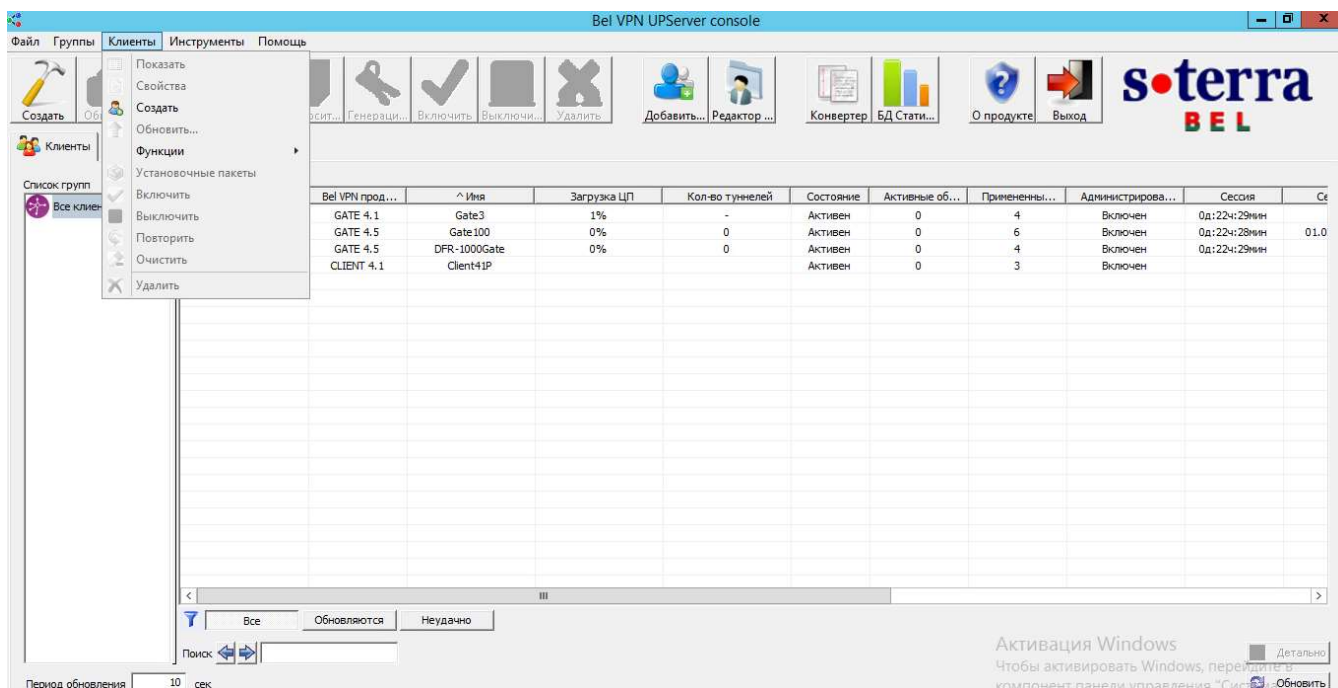


Рисунок 53

Появившееся окно **Создание нового клиента** (Рисунок 54) создания нового клиента имеет следующие поля:

ИД клиента – уникальный идентификатор клиента, может состоять из любых символов, за исключением следующих: <ПРЯМОЙ СЛЕШ>, <ОБРАТНЫЙ СЛЕШ>, <ДВОЕТОЧИЕ>, <ЗВЕЗДОЧКА>, <СИМВОЛ ВОПРОСА>, <ДВОЙНЫЕ КАВЫЧКИ>, <ЗНАК МЕНЬШЕ>, <ЗНАК БОЛЬШЕ>, <ВЕРТИКАЛЬНАЯ ЧЕРТА>, <ТАБУЛЯЦИЯ>. Идентификатор не должен начинаться или заканчиваться символами <ПРОБЕЛ> или <ТОЧКА>, и не должен быть равен “NUL” или “CON”, или “PRN”, или “AUX”, или “COMx”, где $x \in [1..9]$, или “LPTx”, где $x \in [1..9]$

Пакет продукта – имя инсталляционного файла Bel VPN Gate 4.1, созданного с помощью окна **VPN data maker**, вызываемого кнопкой **E**

Кнопка **E** – вызывает окно **VPN data maker** (Рисунок 55) для задания политики безопасности и настроек продукта Bel VPN Gate 4.5/4.1

Пароль устройства – пароль устройства для выполнения дополнительных действий на нем, в данной версии поле не используется

Настройки UPAgent settings – имя файла с настройками Клиента управления, по умолчанию имя файла уже задано (см. главу «[Настройки Клиента управления](#)»).

Рисунок 54

2. В поле **ИД клиента** введите идентификатор клиента, например, gate0.
3. Поле Настройки **UPAgent'a** оставьте без изменений, в нем указано имя файла с настройками Клиента управления.
4. В поле **Пакет продукта** нажмите кнопку **E**, появится окно **VPN data maker** (Рисунок 55).

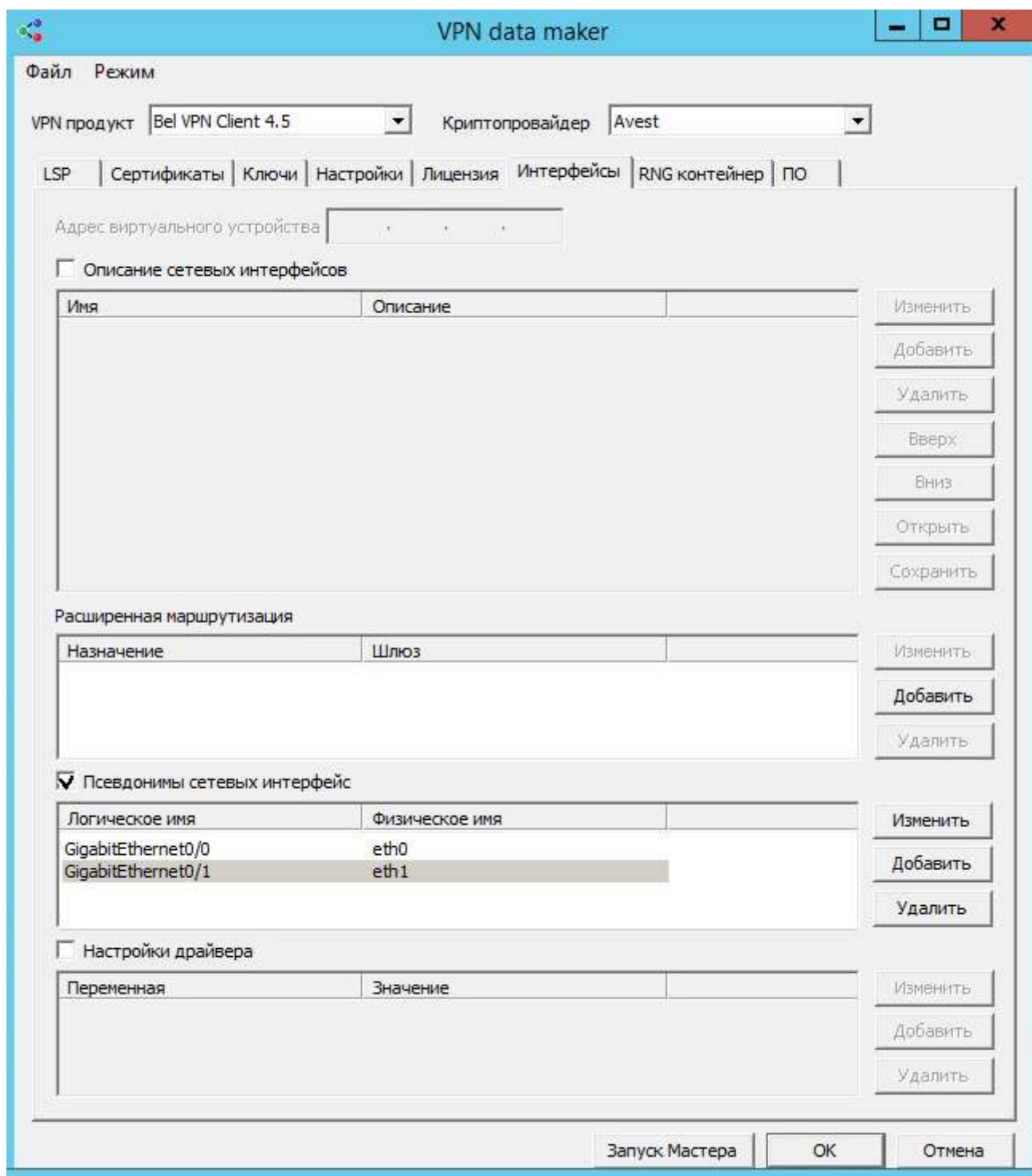


Рисунок 55

5. В окне **VPN data maker** выберите продукт Bel VPN Gate 4.5 (Рисунок 55).

6. Далее нужно задать политику безопасности для шлюза и другие настройки.

Сложную политику можно задать во вкладке **LSP** (Рисунок 55) в текстовом виде или в виде cisco-like конфигурации (или загрузить из ранее созданного файла).

Для создания несложной политики можно использовать окна мастера, нажав кнопку **Запуск Мастера** в окне **VPN data maker**, появится окно для выбора метода аутентификации шлюза при взаимодействии со своими партнерами (Рисунок 56). Интерфейс этого окна описан в разделе «[Задание политики и настроек с использованием мастера](#)».

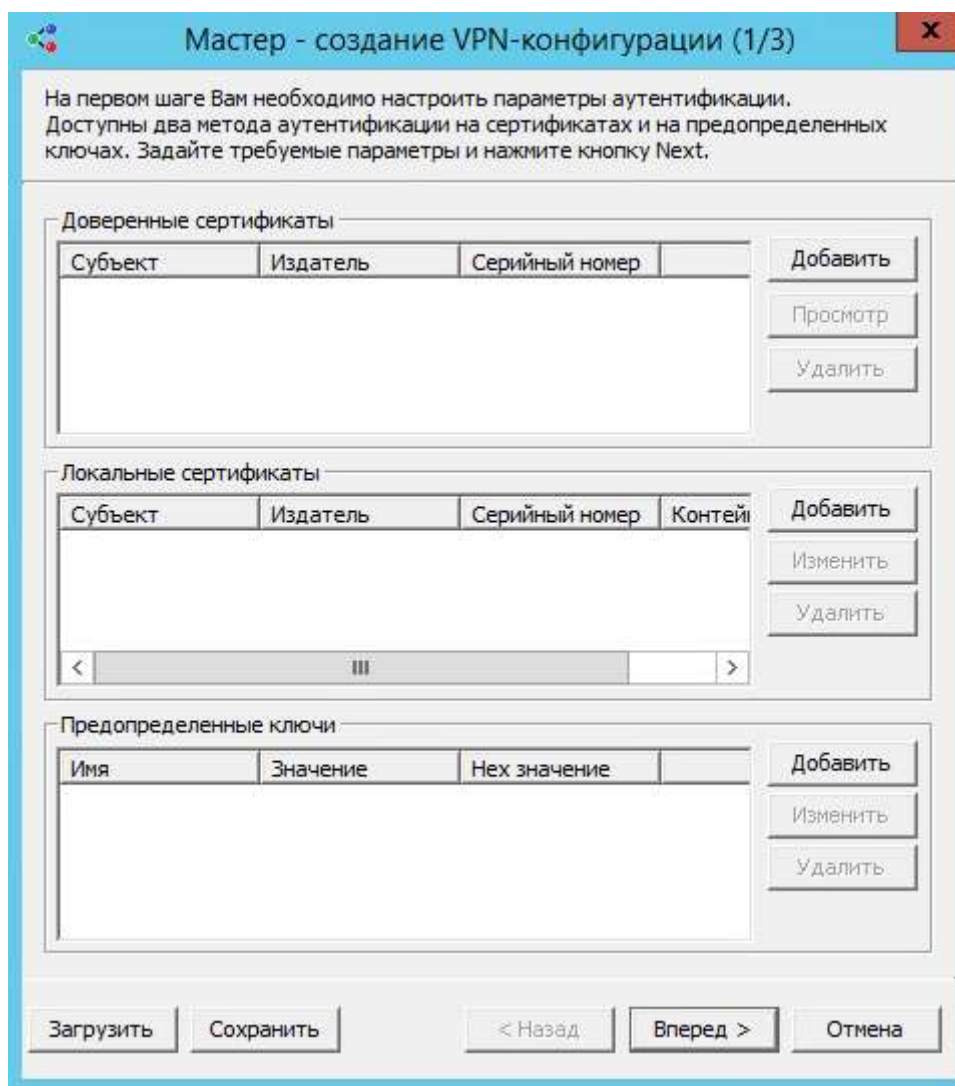


Рисунок 56

- Для примера выберем аутентификацию с использованием предопределенного ключа. В разделе **Предопределенные ключи** нажмите кнопку **Добавить** (Рисунок 56).

8. В открывшемся окне **Предопределенный ключ** (Рисунок 57) введите имя ключа, например, key0, и значение ключа, нажмите кнопку **OK**.

Рисунок 57

9. Предопределенный ключ добавился в проект, нажмите кнопку **Вперед** (Рисунок 58).

Имя	Значение	Hex значение
key0	1234567890key0	31 32 33 34 35 ...

Рисунок 58

10. В следующем окне задайте правила обработки трафика, согласно которым центральный шлюз будет пропускать трафик от управляемых устройств к Серверу управления и обратно. При этом трафик между управляемыми устройствами и центральным шлюзом должен быть защищен (Рисунок 59). Для создания правила нажмите кнопку [Добавить](#).

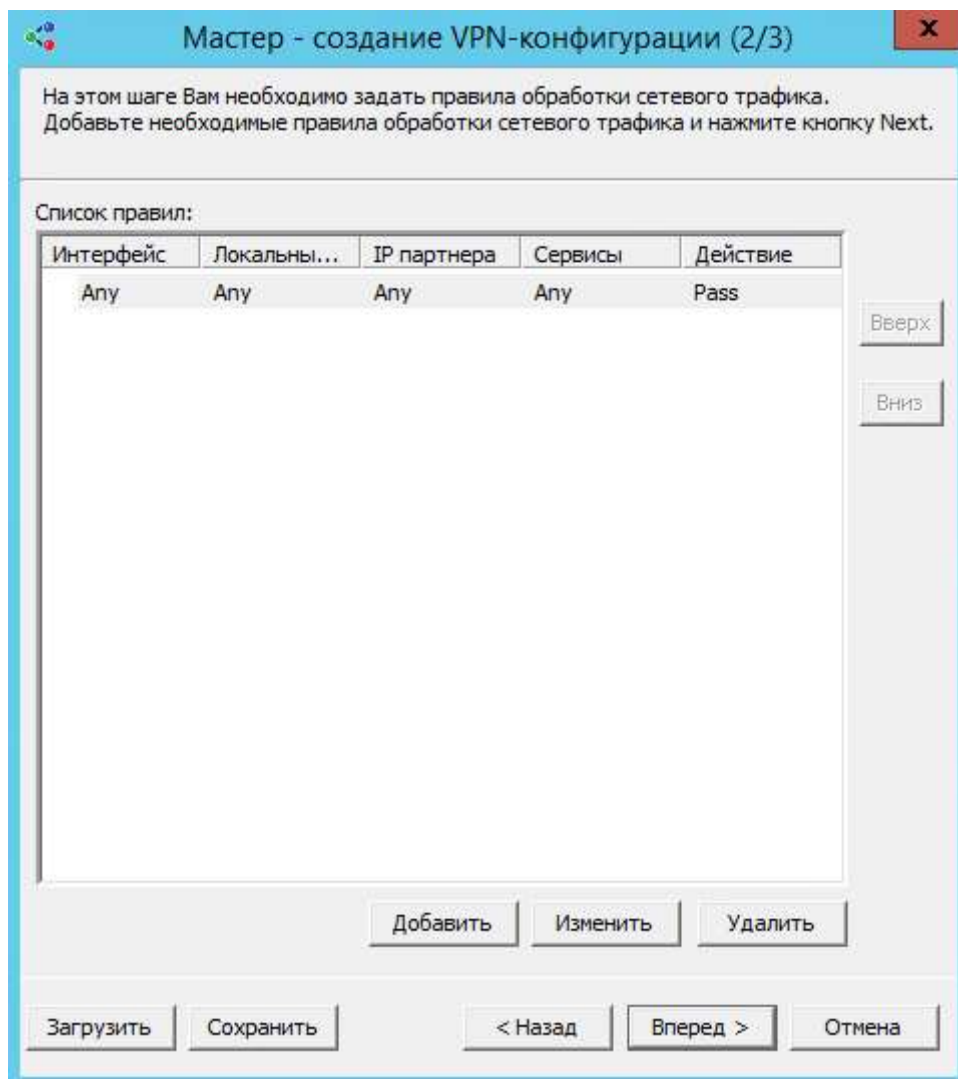


Рисунок 59

Добавить Правило

Псевдоним сетевого интерфейса: FastEthernet0/0

Локальные IP-адреса: ☐ Любой ☒ Задать

IP-адрес	Маска подсети
10.0.0.0	255.255.0.0

Добавить Изменить Удалить

Партнерские IP-адреса: ☒ Любой ☐ Задать

IP-адрес	Маска подсети
----------	---------------

Добавить Изменить Удалить

Сервисы и Протоколы: ☒ Любой ☐ Задать

Имя	Порты
-----	-------

Добавить Изменить Удалить

Действие: Protect using IPsec

Аутентификация: Preshared key: key0

Локальный ID: Local IP address

ID партнера: Accept any ID

Туннельные IP-адреса партнера

☐ Использовать IP-адреса в случайном порядке

Вверх Вниз

Добавить Изменить Удалить

Расширенные настройки

☐ Логировать совпадения

OK Отмена

Рисунок 60

- Создаваемое правило привяжите к интерфейсу шлюза с логическим именем FastEthernet0/0, который смотрит во внешнюю сеть (Рисунок 2). В области **Локальные IP-адреса** (Рисунок 60) укажите адрес защищаемой подсети - 10.0.0.0/16, в эту подсеть смотрит интерфейс шлюза с именем eth1. Шлюз должен взаимодействовать с любыми партнерами, поэтому в области **Партнерские IP-адреса** поставьте переключатель в положение Любой. В области **Действие** - переключатель в положение **Protect using IPsec**, не указывая адрес IPsec партнера (адрес может быть любым).
- После нажатия кнопки **OK** появится предупреждение (Рисунок 61). Нажмите кнопку **Да**.

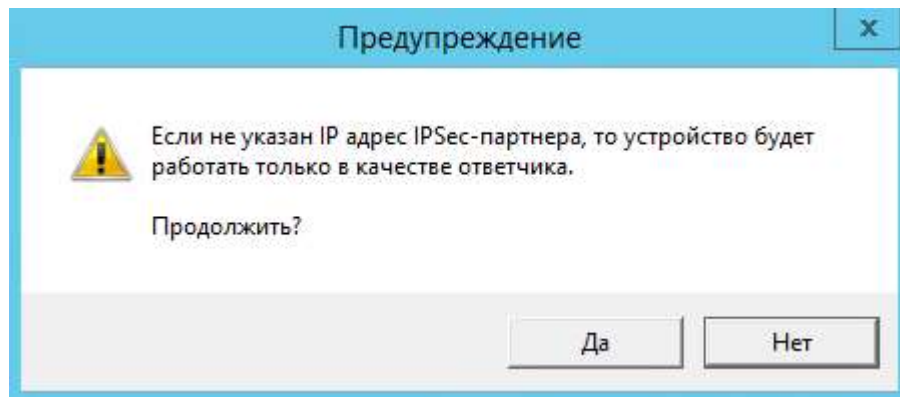


Рисунок 61

13. Увеличьте приоритет созданного правила (Рисунок 62), нажав кнопку [Вверх](#).

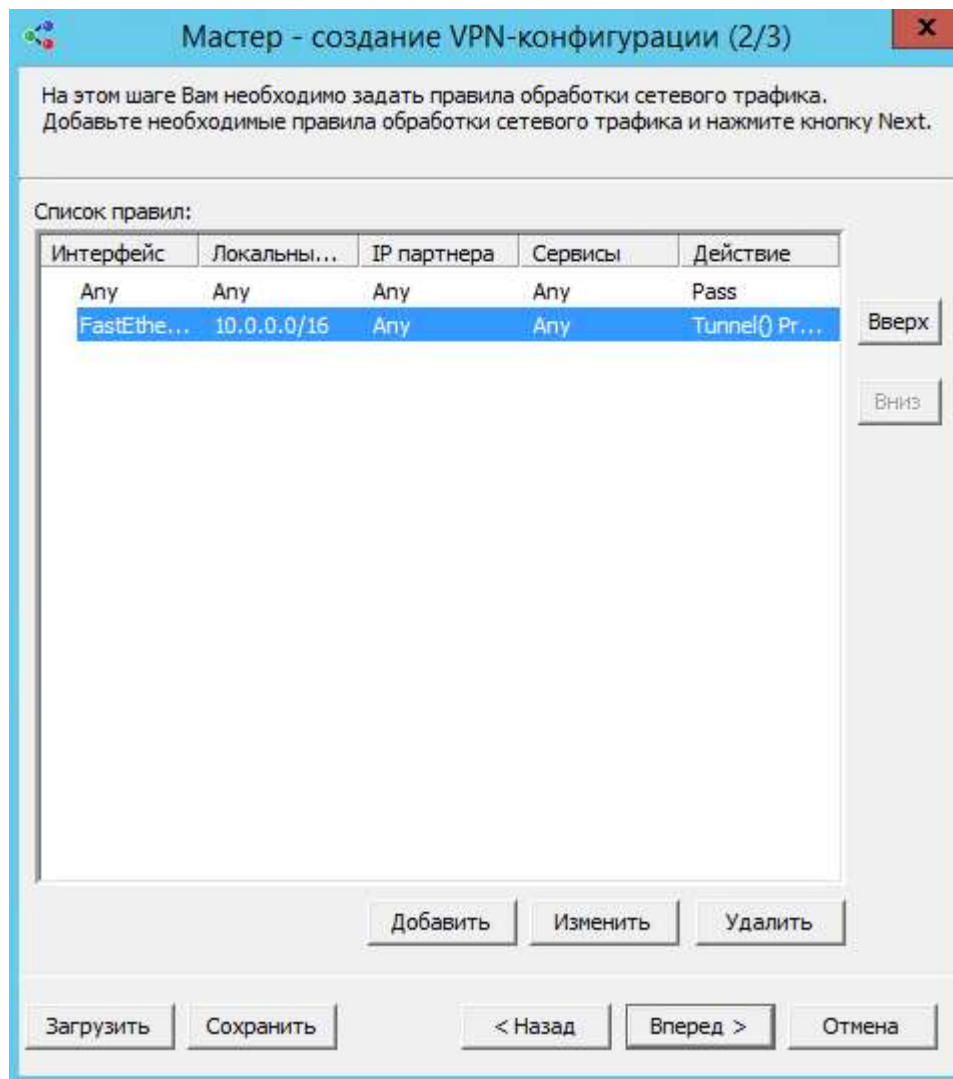


Рисунок 62

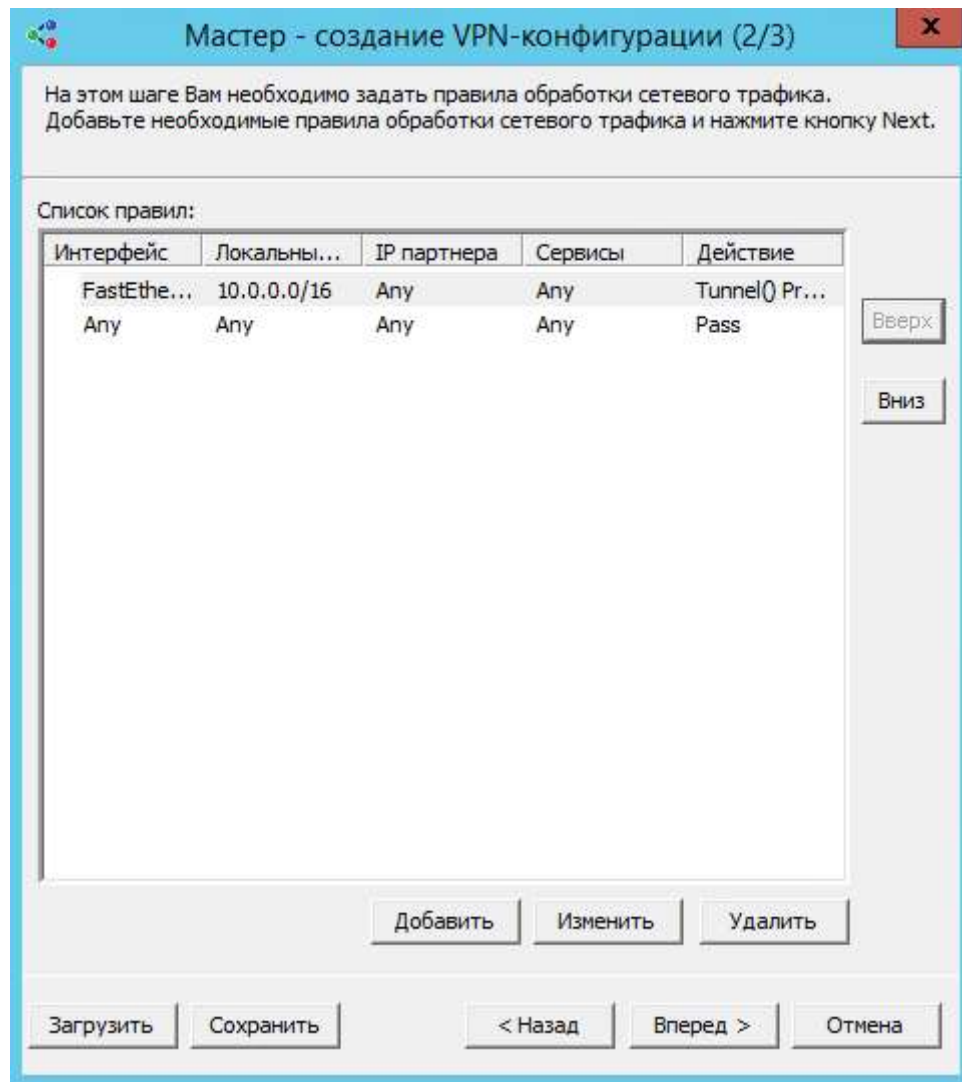


Рисунок 63

14. Нажмите кнопку **Вперед** (Рисунок 63).
15. Введите Ваши данные лицензии на продукт Bel VPN Gate 4.5/4.1 (Рисунок 64).

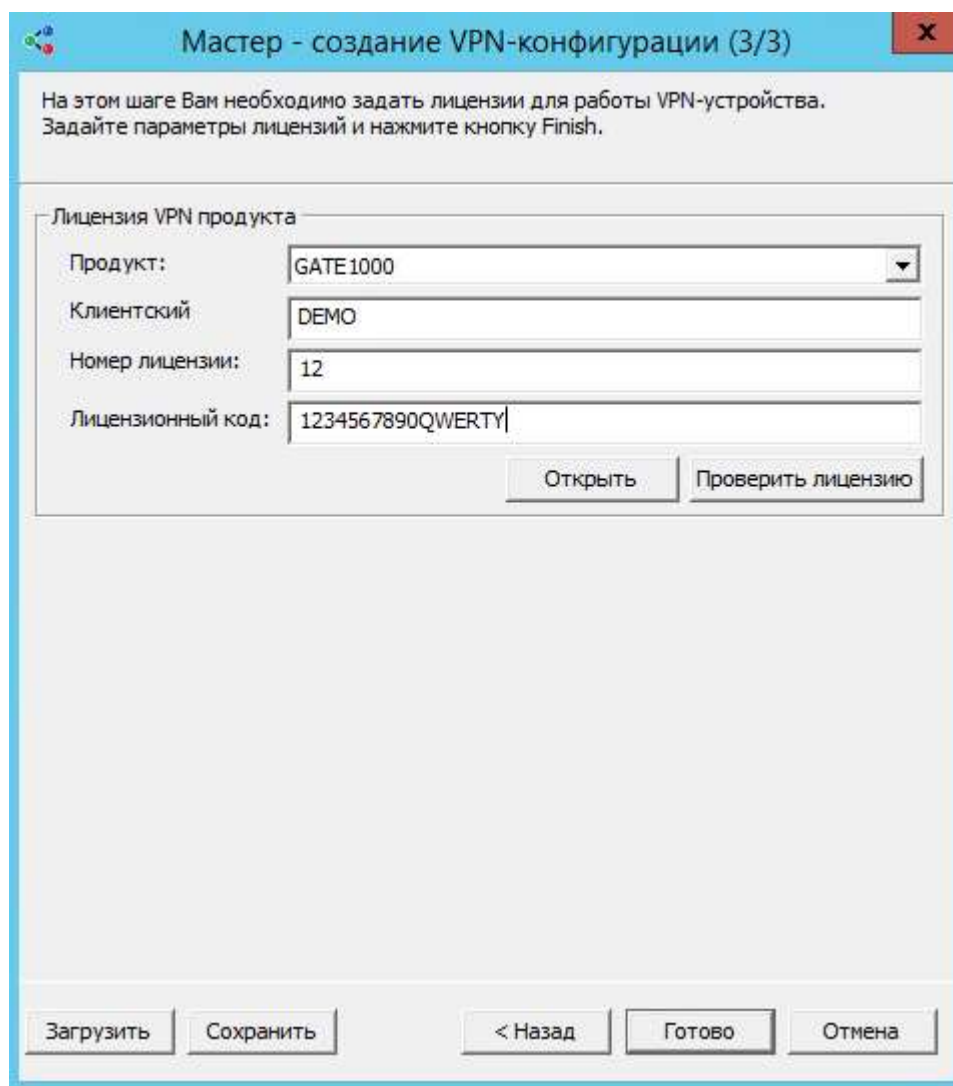


Рисунок 64

16. Сохраните введенные данные в окна мастера, нажав кнопку **Сохранить** (Рисунок 64), и укажите имя файла-проекта в любом созданном вами каталоге (Рисунок 65).

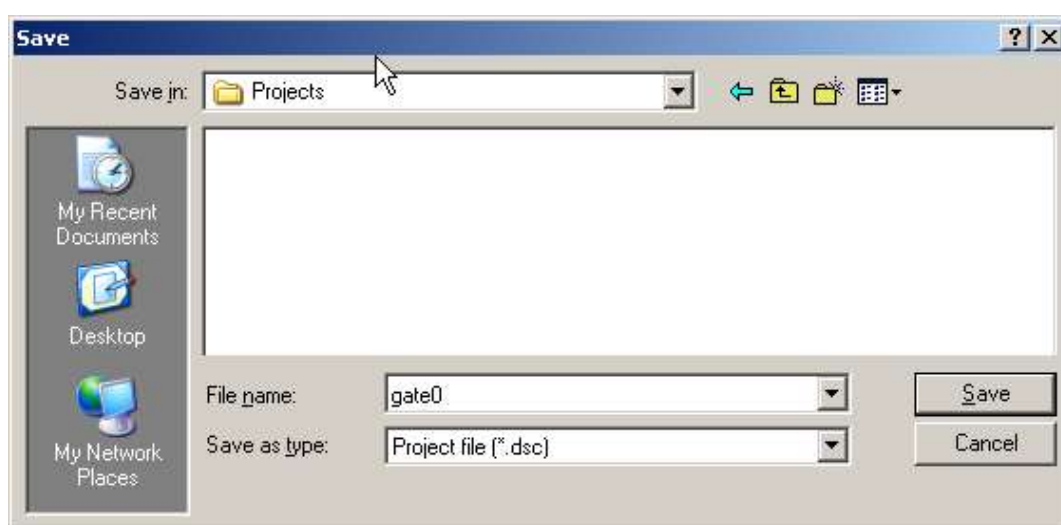


Рисунок 65

17. В окне мастера нажмите кнопку **Готово** (Рисунок 64). Все введенные данные будут отражены во вкладках проекта (Рисунок 66), за исключением вкладки **Интерфейсы**.

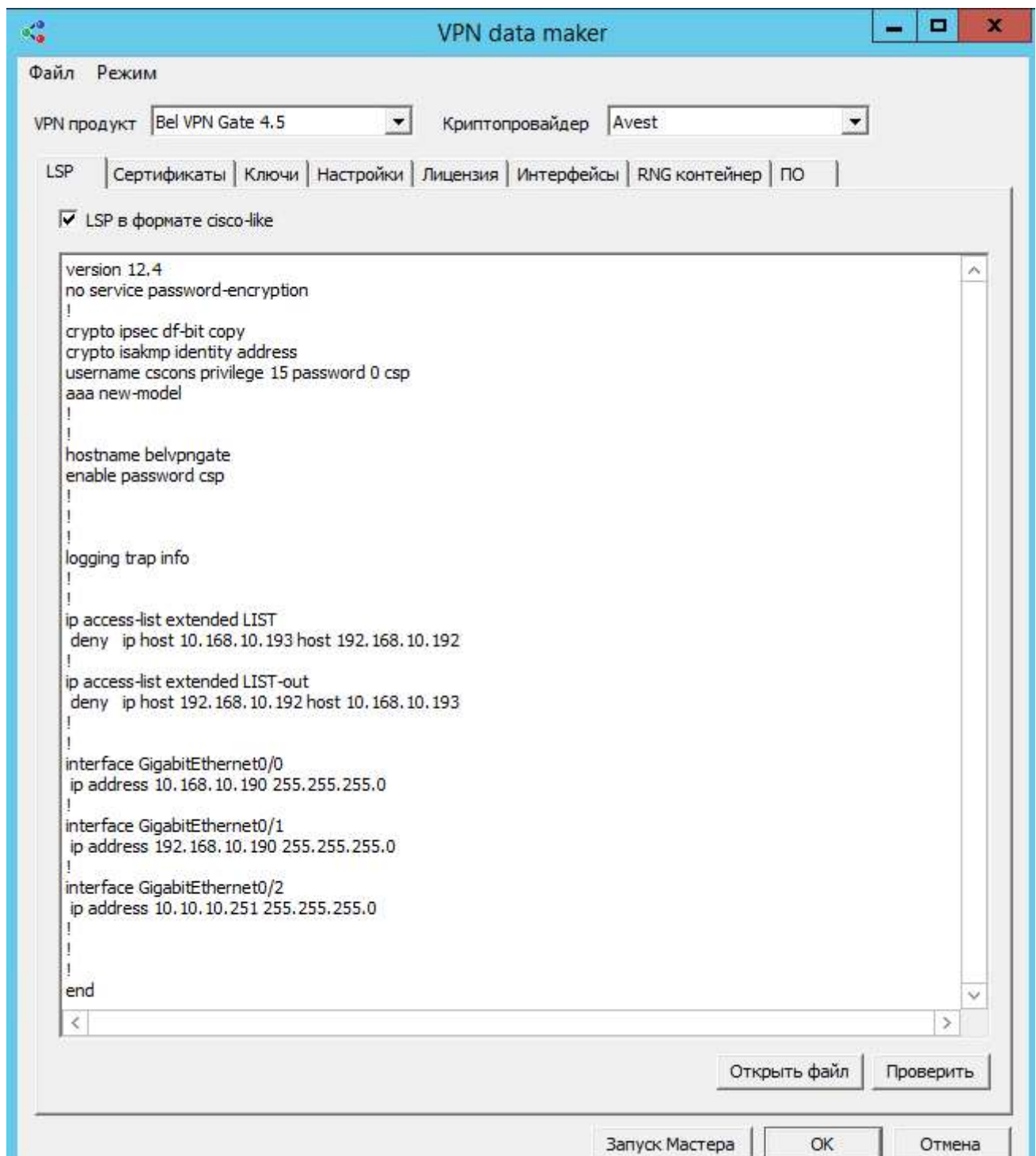


Рисунок 66

18. Перейдите во вкладку **Интерфейсы** и задайте соответствие между логическими и физическими именами интерфейсов шлюза безопасности. Для получения имен интерфейсов используйте:

утилиту `/opt/VPNagent/bin/if_show` – для Gate 4.5/4.1.

Во вкладке **Интерфейсы** установите флажок **Псевдонимы сетевых интерфейсов**, нажмите кнопку **Добавить** и в окне **Псевдонимы сетевых интерфейсов** введите логическое и физическое имя интерфейсов (Рисунок 67).

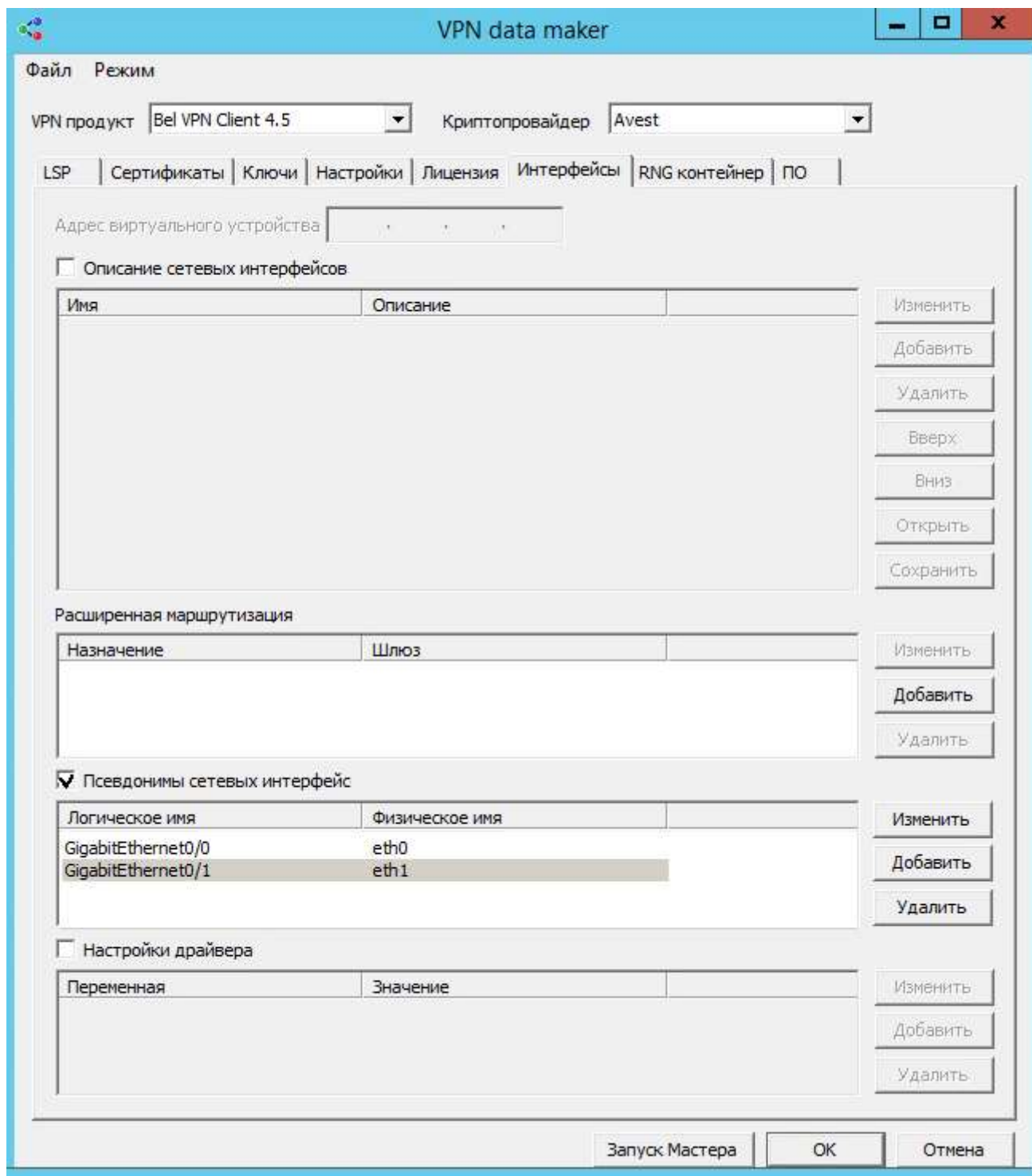


Рисунок 67

19. Во вкладке **Интерфейсы** нажмите кнопку **OK**, появится окно с настройками нового клиента (Рисунок 68), опять нажмите кнопку **OK**.

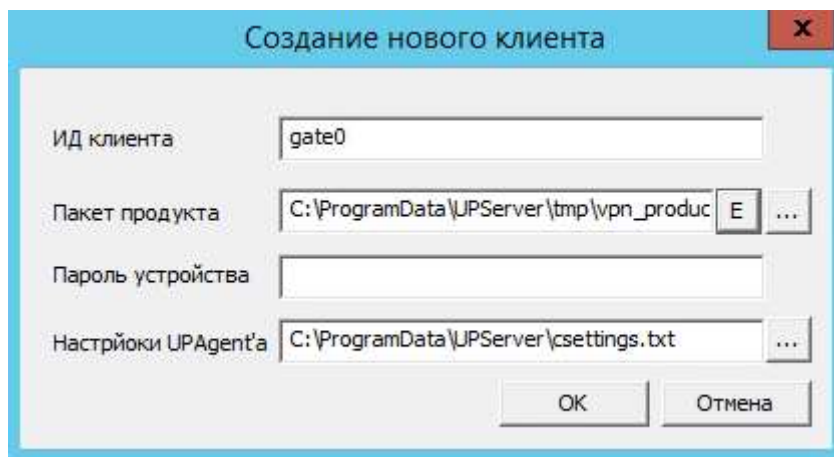


Рисунок 68

20. На Сервере управления в таблице клиентов появился новый клиент `gate0`. Переведите его в активное состояние, выбрав в контекстном меню предложение **Включить** (Рисунок 69).

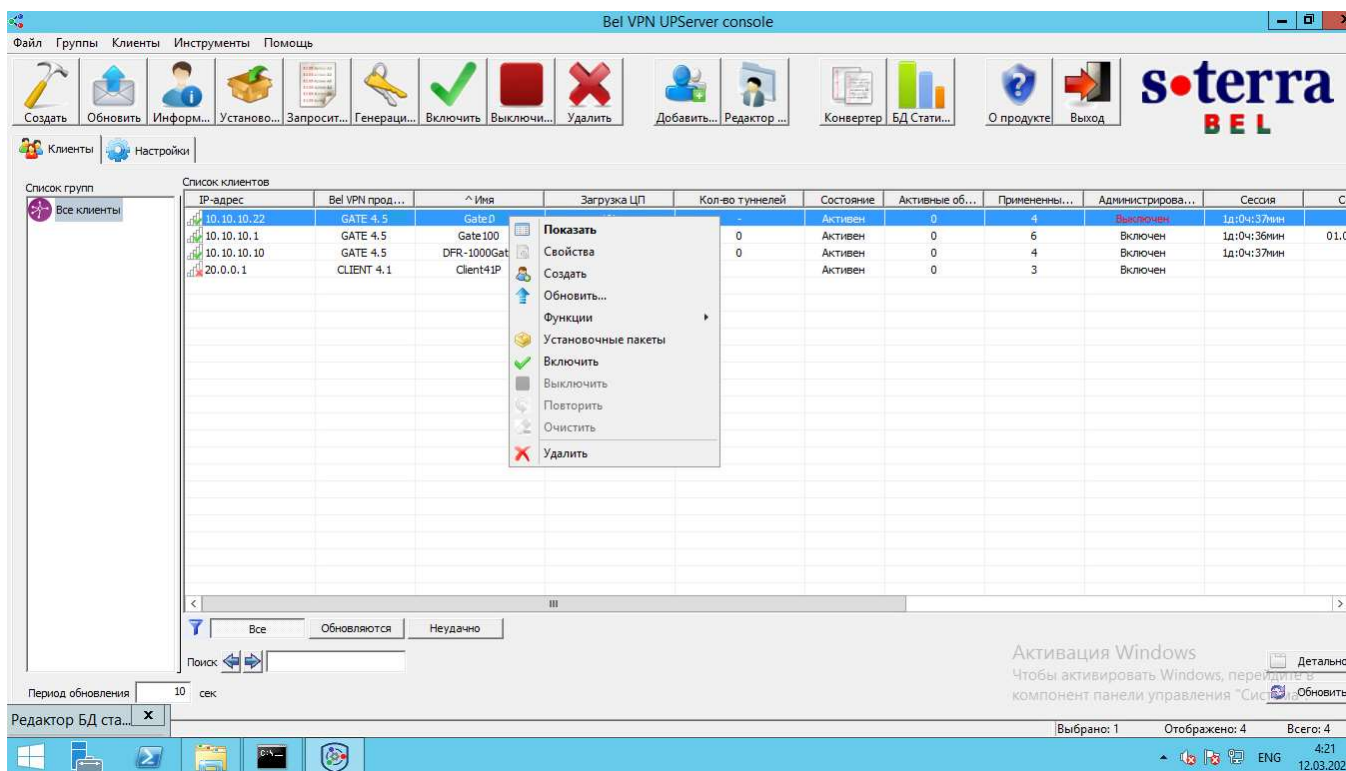


Рисунок 69

5.2. Подготовка скриптов для Клиента управления и Bel VPN Gate 4.5/4.1

1. Для установки Клиента управления, дистрибутив которого размещен на шлюзе в каталоге /packages, и обновления настроек Bel VPN Gate 4.5/4.1 следует подготовить два скрипта. Для клиента `gate0` выберите предложение **Установочные пакеты** в контекстном меню (Рисунок 70).

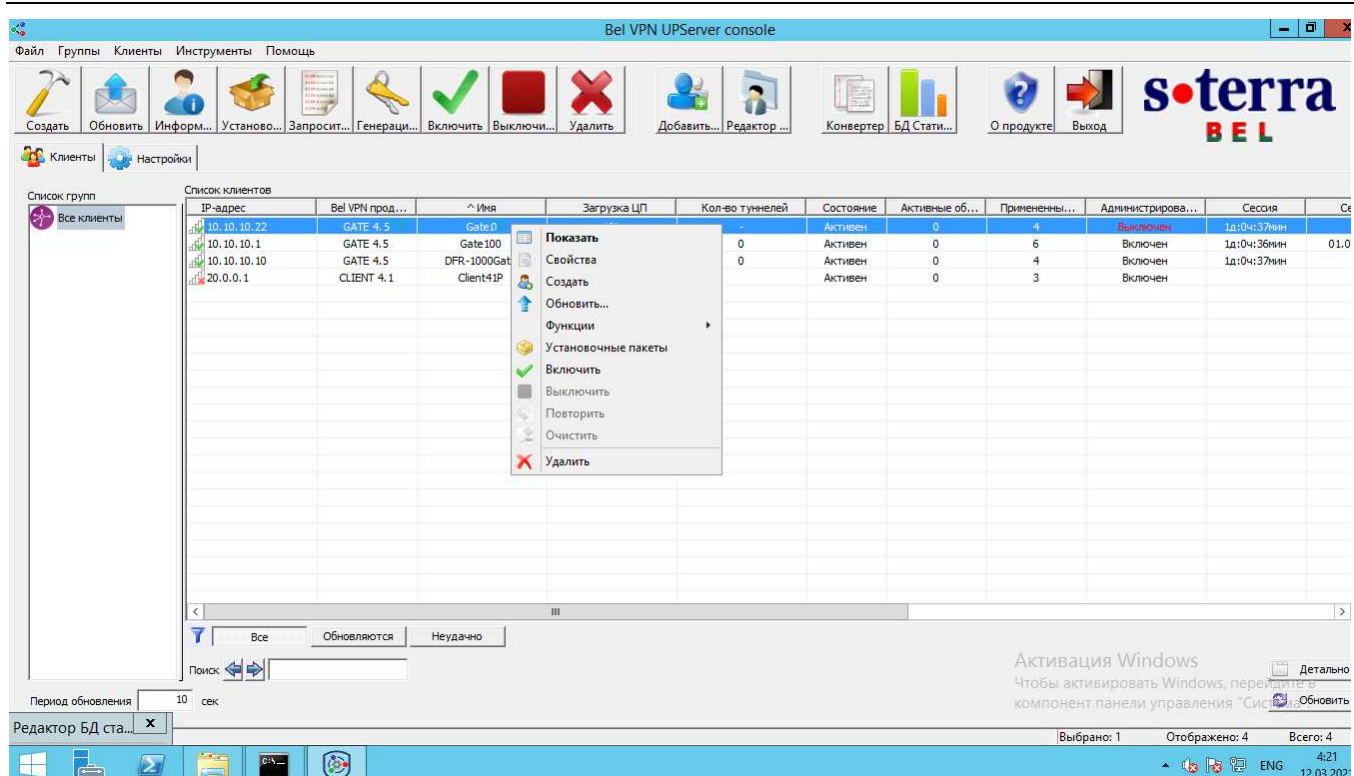


Рисунок 70

2. В открывшемся окне укажите каталог для сохранения скриптов (Рисунок 71).

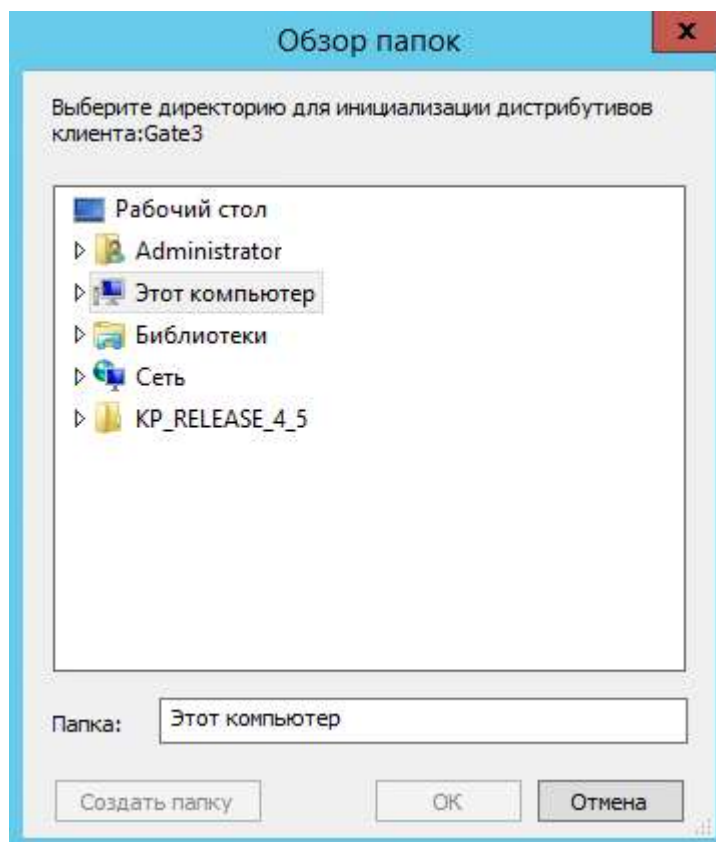


Рисунок 71

В указанный каталог будут сохранены два файла (Рисунок 72), (Рисунок 73):

- `setup_upagent.sh` – скрипт для инициализации Клиента управления
- `setup_product.sh` – скрипт для настройки продукта Bel VPN Gate 4.5/4.1.

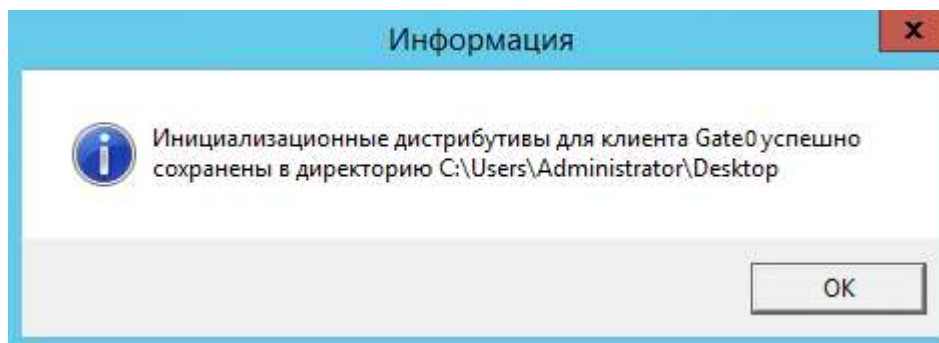


Рисунок 72



	setup_product.sh	12.03.2021 4:26	Файл "SH"	2 КБ
	setup_upagent.sh	12.03.2021 4:26	Файл "SH"	3 КБ

Рисунок 73

5.3. Доставка и запуск скриптов

Установка созданных скриптов на центральном шлюзе осуществляется в следующем порядке:

- 1) `setup_upagent.sh`;
- 2) `setup_product.sh`.

Такой порядок обусловлен тем, что для успешного выполнения скрипта `setup_product.sh`, необходим установленный и инициализированный Клиент управления.

Примечание: продукт *Bel VPN Gate 4.5/4.1*, поставляется на устройстве в инсталлированном состоянии вместе с Клиентом управления, требуется инициализировать только Клиента управления.

Если на устройстве уже работает продукт *Bel VPN Gate 4.5/4.1* и не предполагается изменение его политики безопасности, то инициализируйте (инсталлируйте) только Клиент управления!

Установка созданных скриптов осуществляется локально, так как Клиент управления на этом устройстве еще не инициализирован (инсталлирован). Поэтому доставьте скрипты на шлюз безопасности по заслуживающему доверия каналу связи и запустите локально.

1. Для доставки можно использовать:

- утилиту `pscp.exe` из распространяемого бесплатно пакета Putty;
- терминальную программу, например, Putty;
- USB-флеш
- FTP-сервер (FileZilla Server) на Сервере управления.

- а) При использовании утилиты `pscp.exe` на Сервере управления выполните команды, предварительно создав каталог `/tmp` на шлюзе:

```
pscp setup_upagent.sh root@10.0.10.110:/tmp
pscp setup_product.sh root@10.0.10.110:/tmp
```

Далее перейдите к [пункту 2](#).

- б) При использовании терминальной программы, например, Putty, укажите адрес интерфейса шлюза eth1 - 10.0.10.110 (Рисунок 74).

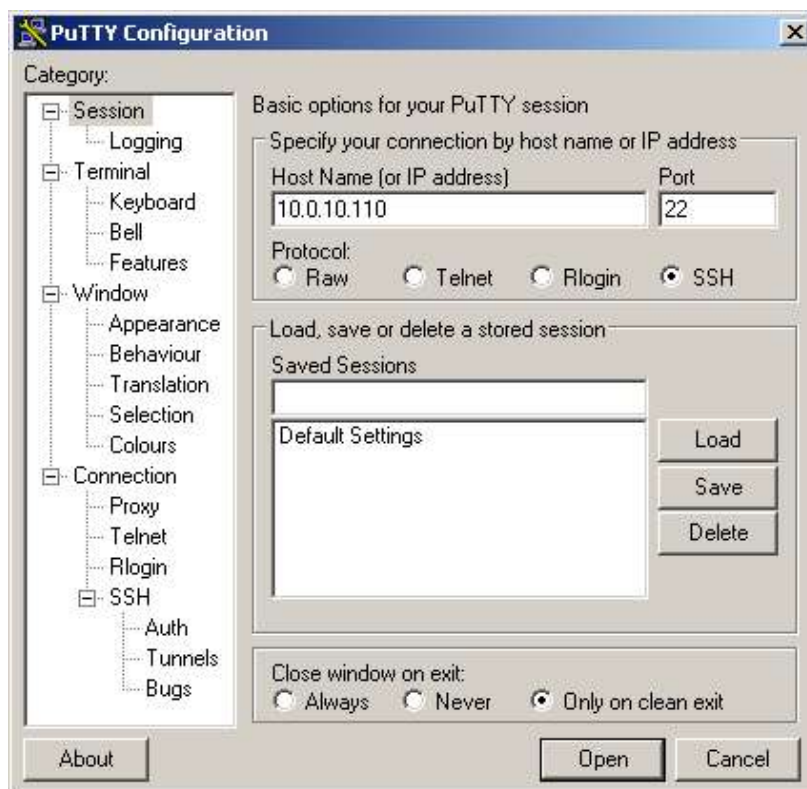


Рисунок 74

На шлюзе создайте каталог, например, /tmp. Скопируйте каждый скрипт в буфер, предварительно открыв его, например, в Wordpad, так как они являются текстовыми файлами. После открытия терминальной сессии со шлюзом задайте команду:

```
cat > /tmp/setup_upagent.sh
```

После нажатия **Enter** вставьте скопированный скрипт и нажмите **Ctrl-D** (Рисунок 75).


```

root@cspgate:~
login as: root
Sent username "root"
root@10.0.10.110's password:
Last login: Wed Nov 30 16:33:06 2011 from 192.168.2.111
[root@cspgate ~]# cat > /tmp/setup_upagent.sh
if [ -e /packages/VPNUPAgent/install.sh ] ; then
    cd /packages/VPNUPAgent; /packages/VPNUPAgent/install.sh
    if [ $? != 0 ] ; then
        echo Error: Cannot install VPNUPAgent
        exit 1
    fi
fi
FILE_NAME=/tmp/vpnupagent.txt
echo "PDw8PCBTRlggMS4wUkxJQiAgICBUaXRzZT1FeHRyYWN0IGRpc3RyaWJ1dG12
ZQpRdWVzdGlvbj1WUE4gVVBZ2Z2VudCBmb3IgZ2FOZTAgd2lsbCBiZSBpbmNO
YWxsZWQuIERvIGVbnRpbmVlPwptZXR1cD1zZXR1cC5zaCBDTElFT1RfSUQ9
ImdhGdUwIiBDTElFT1RfUdEPSJiYzAyNDE5NDEOYjc4NzMxYzgz1ZjQ5NGQw
YmM3YjA1OSIgVVBfTU9ERT0id2luZG93bGVzcyIgVVFU19BU0tftTU9ERT0i
YXV0byIAeNpzM05MTi0qOQMSDAMzHcNmpHvGjQxHV3AzMTIxQWw3B+vuOx
LwtcFTZfmyiV/dGak41Vm4+ZS2aVwSDeUMFAjo051IV2WDw0IDi1qCy1SMH2
UQFkXmZaZnJiSaghvIES3AW3sFhIaNGJQn5RemJeZlViSWZ+nkJPXmaJoZSB
BEGb17AghgIDOXFeQwMDSyMTQyMjCxCOTKHFeIwTXOIr2DmhiVDLgZePUavNo
+87LymJiYsDcxMjPABTnYmpizGTyBFFntZ7/bj2XT7b9spzGXbM+dEe6XHnO
mm04ZtPtsFt/nizsXOvUVXhr4YdDR52kjiWteMX/SO5SZ/ehDwIZwpcdmrfX3
K/JYndx+4CbDjkfa58V4fj7dL7NNlvvQPY+Dmk6VqHK65I4ujXu6THf5dFP
iV9zv+1jsKCJ2duo1Sui+qW+FLBrX9EXTdUXmrKMOq0TePD/iZ3ZeaGmQyv
Ldi36nKGrPTSm7jgH3/H9NtpsgqHr9Xfm/66ozR01fTk+BtzXO797ud78/yc
Fic740IbT/kHV9bxbBtv7dv29vriRiCvz78Xvui98vSWTY1fnUtZ3HrDI/G3
Xt803P/rOsdME5eLvX5Gr2ne99nYmZkYFzcOMOgcapB4yRgMMoysjR2GTS2
Nwj02Joo6fhhXhrLurDhqsj3+IWJNI+uJnyp1RkUX/59nh+jTs+YvCfwOH+2
ma2GB7prfx965rNa2HfaYpHfK3ok/qbFDfxQq9gYbWa2e6262vbn19p4Pz+O
Xbl2tvTs9zcMA+qrvIqDwzSt41Wk1+3o8NU22MRoXfTBavOL+NA2ExsHO5/6
7QvXflk7ob42azbzZGFZ+wfhlly6JmZ2dXLQ68OsNOza5PGbhGZsbVd7OyuIx
iDFRW2Ba+25/ZsOPY65MEOuK1HdbtXk7ZC6WrY8yYRHNq+rdfeHH8sD3Q7++
X1z77pCDUmVCWaKdRJYD/zzRrQdXGSR9VPiU9jU8Z80Js8qzP1b91fy+euD+
PKvPK3W3bHw1/Xv97H8H1zpv8axMOyV7OEEk+nLca7ei1HS9kooSYE5n2B8d
7O8WEu4Y5BoTGuCYnppXEsV5eliw6MBgNertDi1CK/xNxUZH5AYnFxeX5R
im1SsgEwF1qaGJoKmVuYGxsmW5immViapBgkJSznGZha8nIFJJZk2OrnF5To
Qw3n5fLNTOm1Lc/MS8kvz0ktLoYY6VicDR2PLC3J5+Xi5UI4KizATwHmLIRp
QNFEiHfuxak1JZ156cUwD+2J9s1PByp2y8xJ9U2sCM6sSrU1NTQyABsbWpAC
9AdQ1jkjNTkbbqCOgtSgzP8XWDCLtFgJNjOAVwQWpqSk+mbmZJbZASaBJIUWV
zvmleSW2xrxcQDZUJ9hksGxiGjDxhmTnpuaXltgaWgCFHVNSioBeNLA1NNAz
OAMShoaGYHs889Ly8HagB4BohfsSEMzXi4ANKcHKwAAABVgAAAAAIFNGWCA+
Pj4+
" > $FILE_NAME
/opt/UPAgent/bin/init.sh $FILE_NAME
RET=$?
rm -f $FILE_NAME
exit $RET
[root@cspgate ~]#
    
```

Рисунок 75

Аналогичным образом доставьте на шлюз второй скрипт `setup_product.sh`.

- Измените права доступа к скриптам, выполнив локально на шлюзе команды:

```

[root@cspgate ~]# chmod +x /tmp/setup_upagent.sh
[root@cspgate ~]# chmod +x /tmp/setup_product.sh
    
```

- Запустите локально скрипты на выполнение (для класса защиты КС1 и КС2):


```
[root@cspgate ~]# /tmp/setup_upagent.sh
warning: /packages/VPNUPAgent/libidn-0.6.5-1.1.i386.rpm: Header V3
DSA signature: NOKEY, key ID e8562897
Info: libidn is installed successfully
Info: Link /var/log/upagent to /tmp is created successfully
Info: VPNUPAgent is installed successfully
Adding new rndm:
Nick name: cpsd
Name device: CPSD RNG
Level: 1
Succeeded, code:0x0
File decompression...

cacert.cer
reg.txt
settings.txt

...Done
Starting VPN UPAgent watchdog daemon.done.
Initialization is successful
```

При запуске скрипта `setup_upagent.sh` выполняется проверка - установлен ли продукт VPNUPAgent (Клиент управления). Если он еще не установлен, то устанавливаются необходимые дистрибутивы и настраивается среда функционирования. В процессе установки дистрибутивов возможны интерактивные запросы на подтверждение действий.

Если Клиент управления не установлен, то на поставленном шлюзе будет непустой каталог `/packages/VPNUPAgent` с дистрибутивом продукта VPNUPAgent. Если Клиент управления установлен, то каталог `/packages` отсутствует. Если Клиент управления не установлен и каталог пустой, то на установленном Сервере управления имеется архив `vpnupagent.tar`, который размещен:

```
для ОС Debian/Linux6 (64-bit)
C:\Program Files\S-Terra\S-Terra KP\upagent\LINUXDEBIAN6\amd64\
vpnupagent.tar

для ОС Debian/Linux6 (32-bit)
C:\Program Files\S-Terra\S-Terra KP\upagent\LINUXDEBIAN6\i686\
vpnupagent.tar

для ОС Red Hat Enterprise Linux 5
C:\Program Files\S-Terra\S-Terra
KP\upagent\LINUXRHEL5\i486\vpnupagent.tar

для ОС Solaris 10
C:\Program Files\S-Terra\S-Terra KP\
UPServer\upagent\SOLARIS\i386\vpnupagent.tar
```

Перед запуском скриптов самостоятельно доставьте архив `vpnupagent.tar` на шлюз, предварительно создав на шлюзе каталог:

```
mkdir /packages
```

Для доставки архива используйте, например, утилиту `pscp.exe` из пакета Putty:

```
pscp vpnupagent.tar root@10.0.10.110:/packages
```

И на шлюзе выполните команды:

```
cd /packages
tar xvf vpnupagent.tar
```

Запустите второй скрипт:

```
[root@cspgate ~]# /tmp/setup_product.sh
```

- При успешном выполнении скриптов установится соединение с Сервером управления для проверки возможности скачивания обновлений. Состояние клиента сначала изменится с **Ожидание** на **Обновление**.

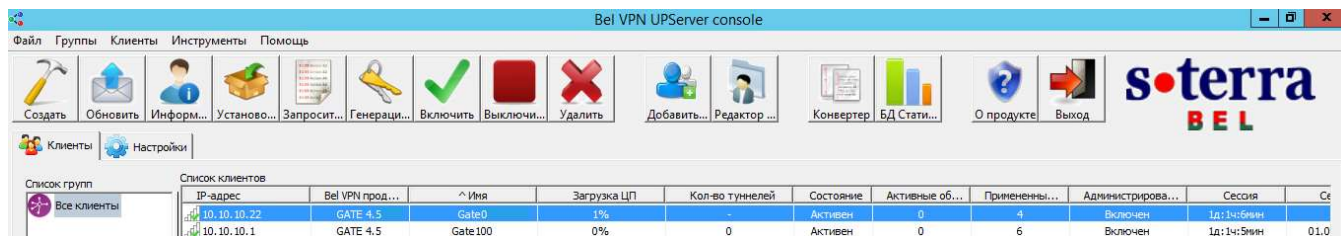


Рисунок 76

- А затем с **Обновление** на **Активен**. В состоянии **Активен** клиент готов для получения новых обновлений.

6. Настройка и управление устройством с Bel VPN Client-P 4.1

6.1. Создание учетной записи клиента на Сервере управления

Во вкладке **Клиенты** создадим группу, в ней учетную запись клиента для управляемого устройства, на котором установлен или будет установлен продукт Bel VPN Client 4.1.

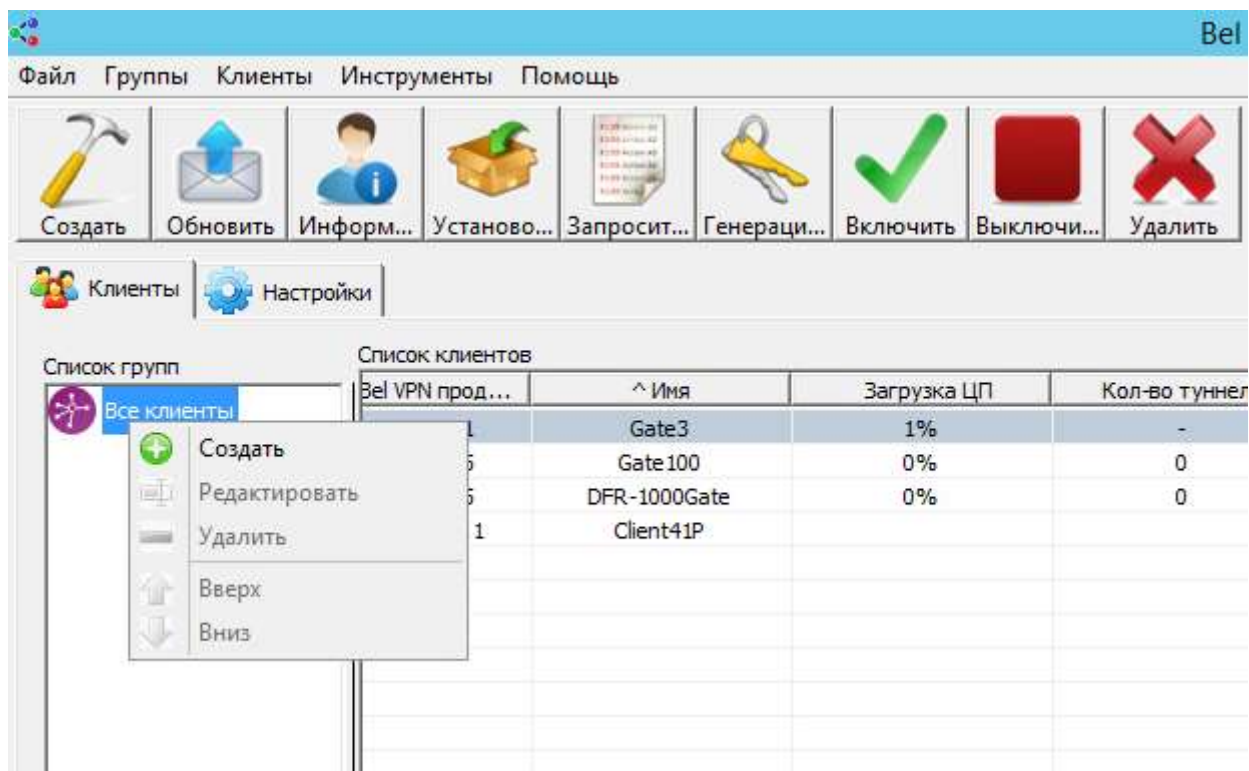


Рисунок 78

1. Для управляемых устройств можно создать отдельную группу. Для создания группы выделите группу **Все клиенты**, а в меню **Группы** выберите предложение **Создать** (Рисунок 79).

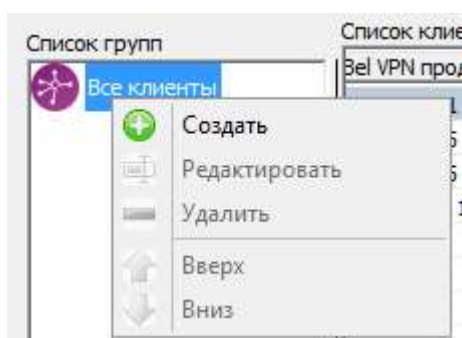


Рисунок 79

В поле **Имя группы** введите имя группы, например, Office1, в которой будут созданы в дальнейшем клиенты (Рисунок 80), затем выберите иконку группы для продуктов из предложенных и нажмите **OK**.

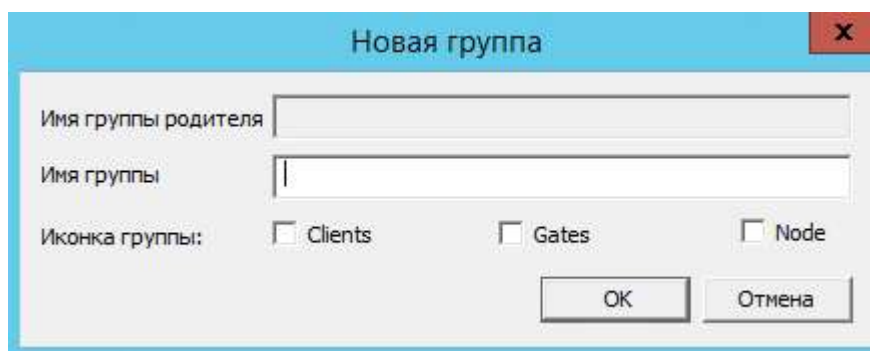


Рисунок 80

В меню **Clients** выберите предложение **Создать** (Рисунок 771).

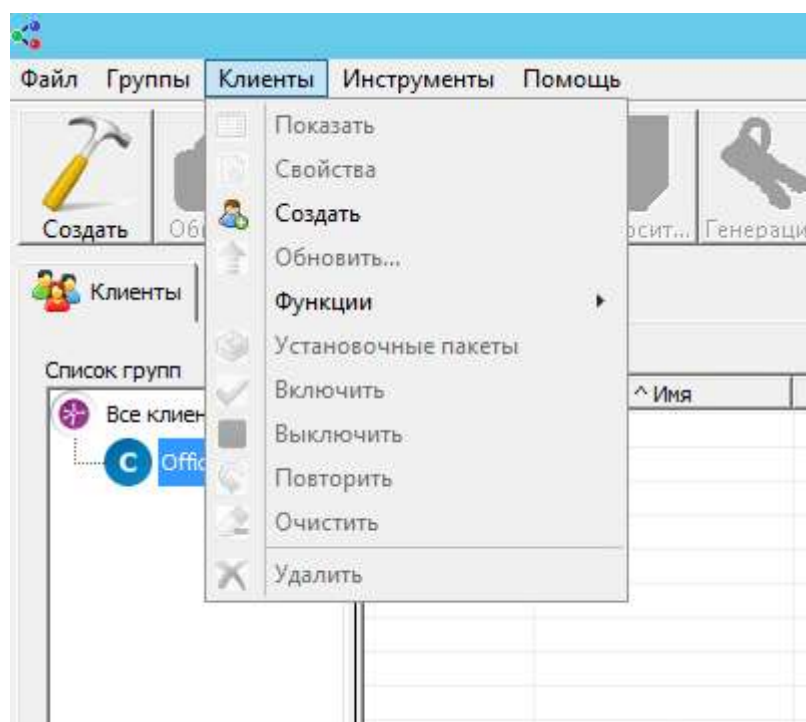


Рисунок 771

2. В окне создания нового клиента **Создание нового клиента** введите идентификатор клиента, например, `client01`, а в поле **Пакет продукта** нажмите кнопку **E** (Рисунок 782).

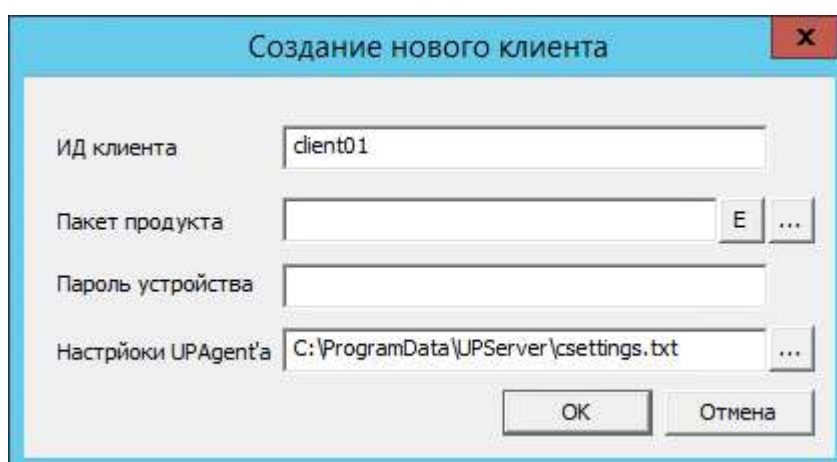


Рисунок 782

Далее описывается процесс создания начальной политики безопасности Bel VPN Client.

3. В окне **VPN data maker** (Рисунок 793) задайте политику безопасности и все настройки продукта.

Политику и настройки можно ввести / вставить в соответствующее поле вкладки или загрузить из файла, либо воспользоваться мастером настройки, нажав кнопку [Запуск Мастера...](#)

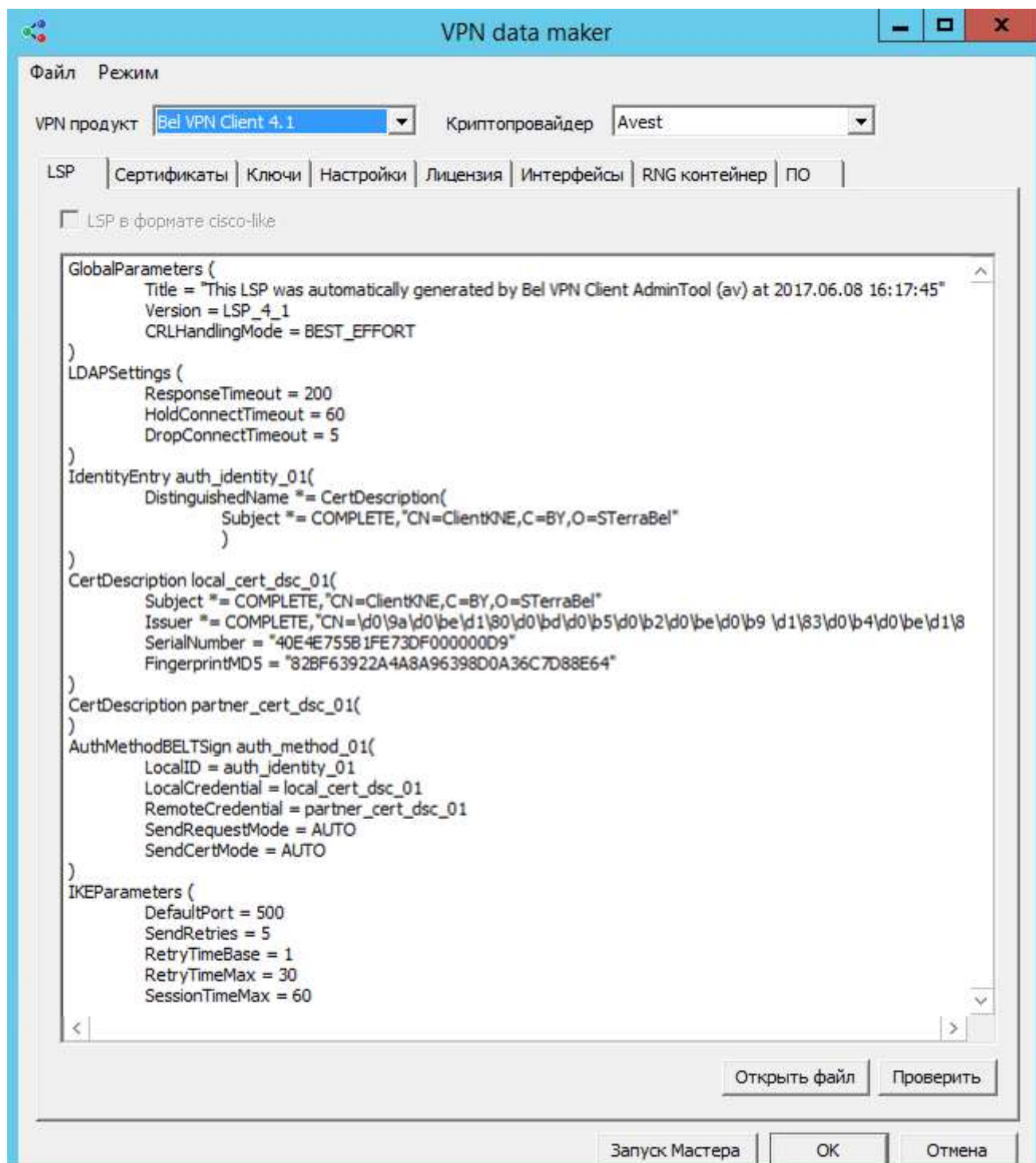
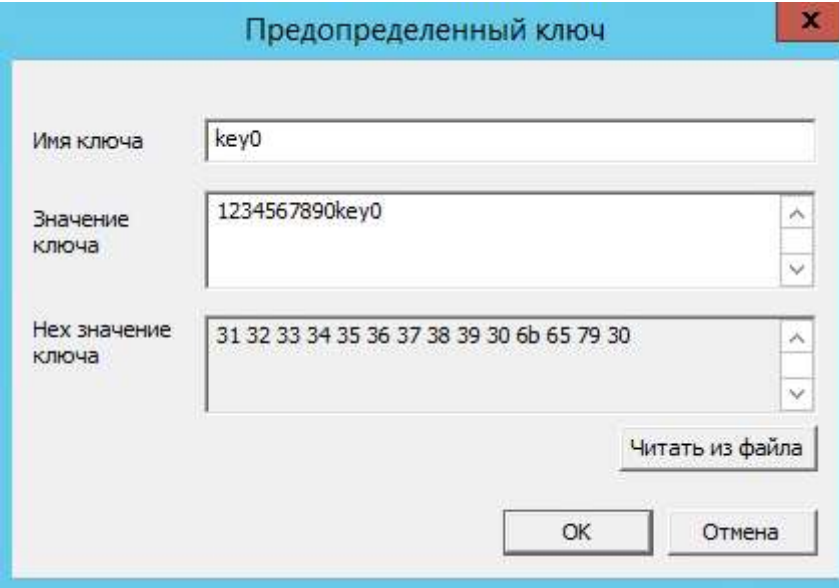


Рисунок 793

4. Выберите метод аутентификации такой же как и у партнера - шлюза Bel VPN Gate, введите такое же значение ключа (Рисунок 804), нажмите кнопку [Вперед](#).



Предопределенный ключ

Имя ключа: key0

Значение ключа: 1234567890key0

Hex значение ключа: 31 32 33 34 35 36 37 38 39 30 6b 65 79 30

Читать из файла

OK Отмена

Рисунок 804

5. В следующем окне задайте правило для создания соединения между устройством с установленным продуктом Bel VPN Client и Сервером управления, при этом соединение с центральным шлюзом должно быть защищенным, для этого нажмите кнопку [Добавить](#) (Рисунок 815).

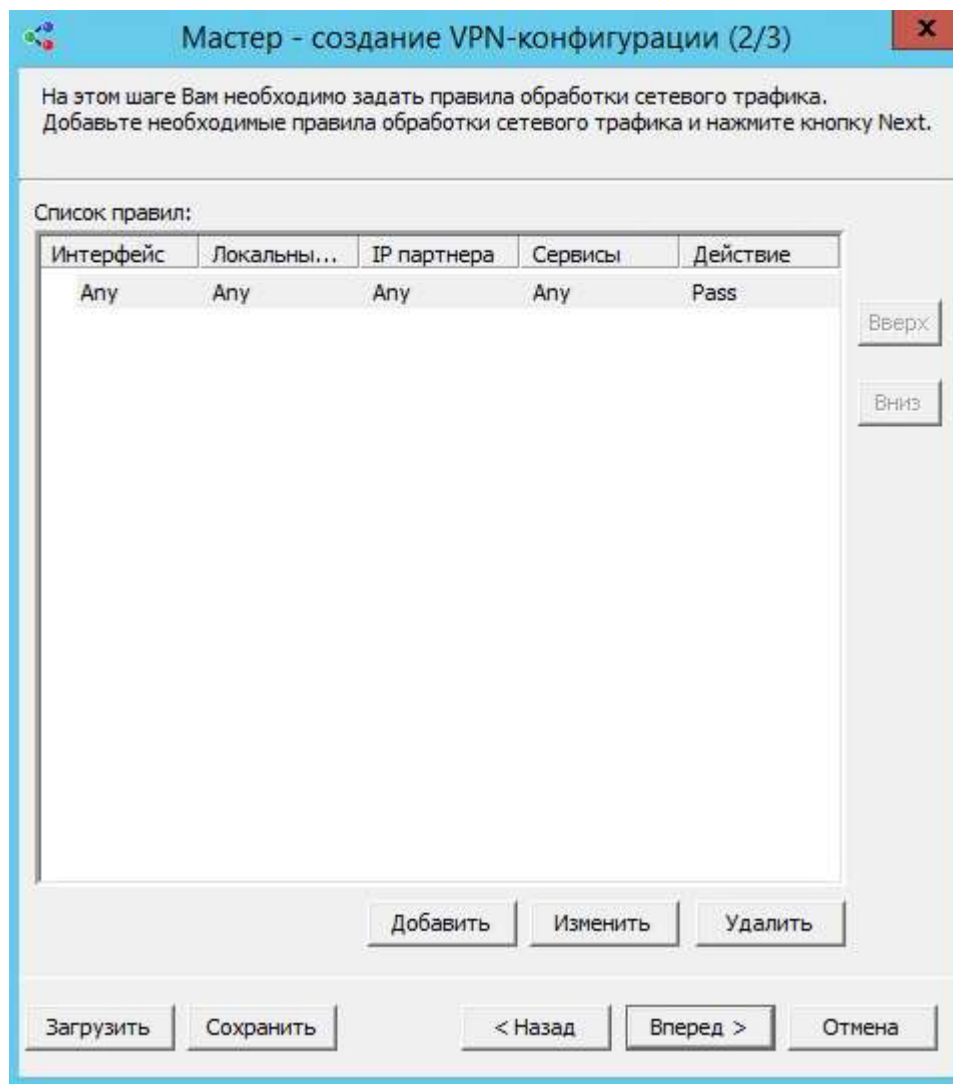


Рисунок 815.

6. Откроется окно **Добавить**, в котором необходимо указать правило для выбора защищаемого трафика (Рисунок 826).

Рисунок 826

Описание полей окна **Добавить правило**:

Псевдоним сетевого интерфейса – имя сетевого интерфейса, к которому применяется правило. Если имя не указано, то правило будет применять ко всем сетевым интерфейсам.

Локальные IP-адреса – локальные сетевые адреса. Правило применяется к сетевым пакетам, содержащим в поле *SourceIP* указанные адреса.

Партнерские IP-адреса – сетевые адреса партнеров. Правило применяется к сетевым пакетам, содержащим в поле *DestinationIP* указанные адреса/

Сервисы и протоколы – сетевые сервисы и протоколы. Правило применяется к сетевым пакетам указанные сервисов/протоколов.

Действие – действие. Описание действия, которое должно быть выполнение с сетевым пакетом, подпадающим под указанное правило. Варианты действий:

Pass – пропустить сетевой пакет

Drop – заблокировать сетевой пакет

Protect using IPsec – применить криптозащиту.

При выборе действия **Protect using IPsec** появится секция для ввода адреса Шлюза безопасности и параметров криптозащиты.

7. В поле **Псевдоним сетевого интерфейса** (Рисунок 82) имя интерфейса не задается – правило будет привязано ко всем интерфейсам. В области партнера укажите всю подсеть 10.0.0.0/16 Сервера управления, в качестве адреса, до которого будет построен IPsec-туннель, задайте адрес интерфейса шлюза 192.168.10.2, защищающего подсеть с Сервером управления. Нажмите кнопку **OK**

Добавить Правило

Псевдоним сетевого интерфейса

Локальные IP-адреса

☒ Любой ☐ Задать

IP-адрес	Маска подсети

Партнерские IP-адреса

☐ Любой ☒ Задать

IP-адрес	Маска подсети
10.0.0.0	255.255.0.0

Рисунок 837

ВНИМАНИЕ!
ЛОКАЛЬНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ ВСЕГДА ДОЛЖНА
ВКЛЮЧАТЬ ПРАВИЛО²
ДЛЯ ЗАЩИТЫ СЕТЕВОГО ОБМЕНА МЕЖДУ
КЛИЕНТОМ УПРАВЛЕНИЯ И СЕРВЕРОМ УПРАВЛЕНИЯ
(Рисунок 88)

Добавить Правило

Псевдоним сетевого интерфейса

Локальные IP-адреса

☒ Любой ☐ Задать

IP-адрес	Маска подсети
----------	---------------

Добавить Изменить Удалить

Партнерские IP-адреса

☐ Любой ☒ Задать

IP-адрес	Маска подсети
10.0.0.0	255.255.0.0

Добавить Изменить Удалить

Сервисы и Протоколы

☒ Любой ☐ Задать

Имя	Порты
-----	-------

Добавить Изменить Удалить

Действие

Protect using IPsec

Аутентификация: Preshared key: key0

Локальный ID: Local IP address

ID партнера: Accept any ID

Туннельные IP-адреса партнера

☐ Использовать IP-адреса в случайном порядке

192.168.10.2

Вверх Вниз

Добавить Изменить Удалить

Расширенные настройки

☐ Логировать совпадения

OK Отмена

Рисунок 84 Пример политики для защиты обмена между Клиентом управления и Сервером управления

² Данное правило можно пропустить только при условии, что адрес Сервера управления попадает в диапазон адресов, защищаемый другим правилом

8. Увеличьте приоритет созданного правила, используя кнопку **Вверх** (Рисунок 85), затем нажмите **Вперед**.

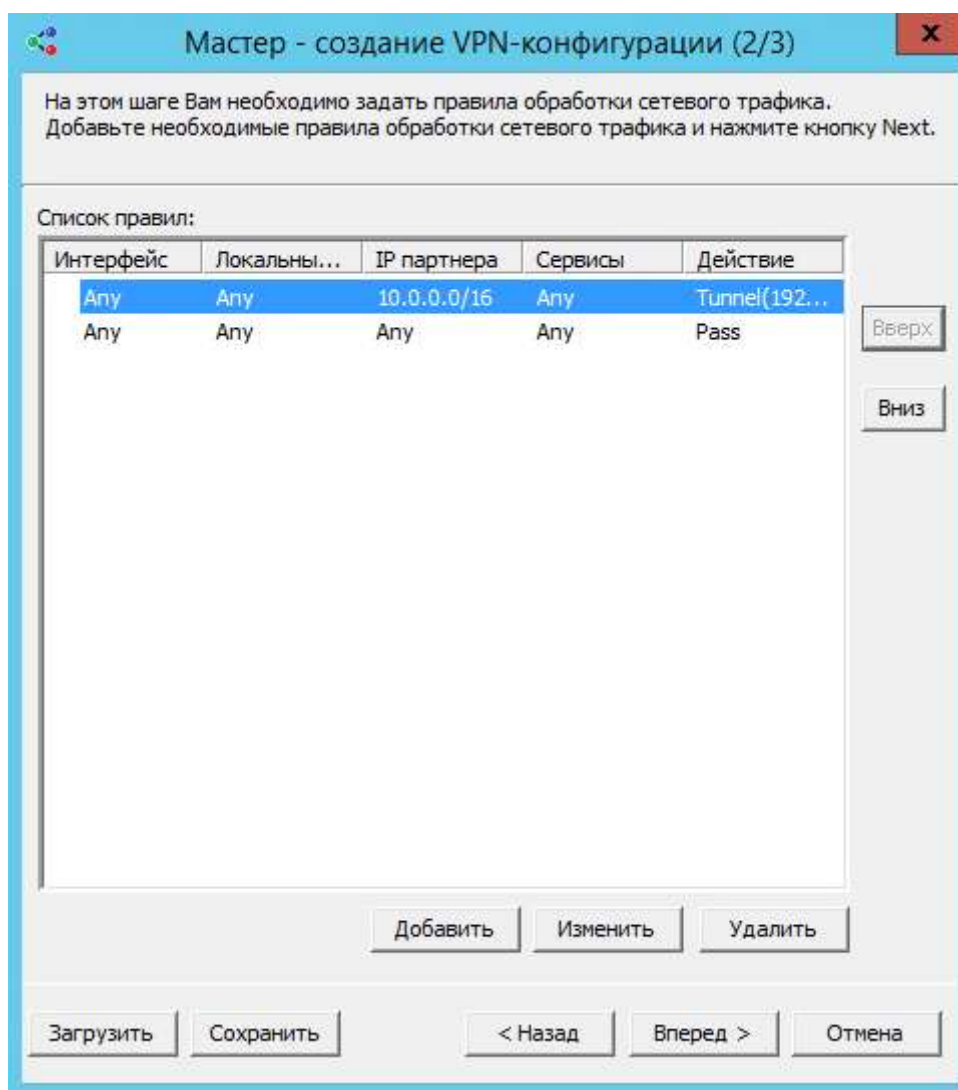


Рисунок 85

9. Введите данные лицензии на продукт Bel VPN Client 4.1 (Рисунок 86).

Мастер - создание VPN-конфигурации (3/3)

На этом шаге Вам необходимо задать лицензии для работы VPN-устройства. Задайте параметры лицензий и нажмите кнопку Finish.

Лицензия VPN продукта

Продукт: CLIENT

Клиентский: test

Номер лицензии: 1

Лицензионный код:

Открыть Проверить лицензию

Загрузить Сохранить < Назад Готово Отмена

Рисунок 86

8

10. Сохраните все введенные данные, нажав кнопку **Сохранить**, и укажите имя файла-проекта в любом созданном вами каталоге (Рисунок 87).

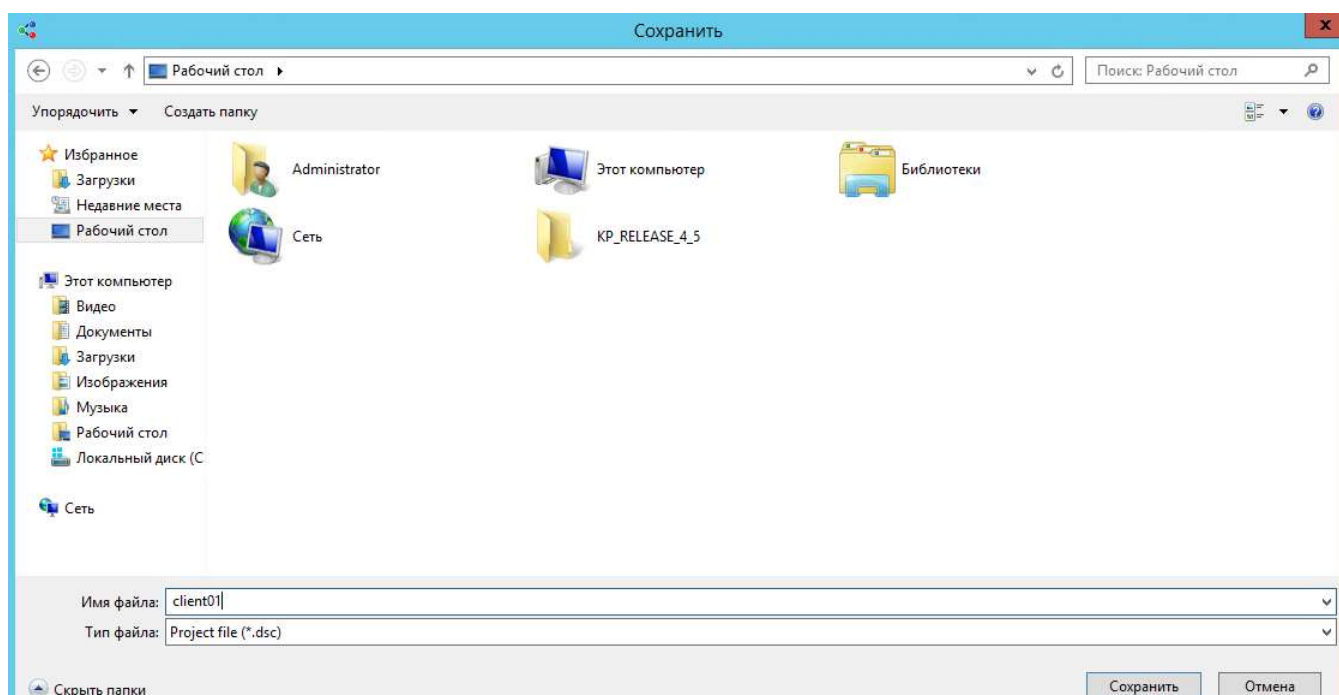


Рисунок 87

11. В окне мастера нажмите кнопку **Готово** (Рисунок 86). Все введенные данные будут отражены во вкладках проекта (Рисунок 88). Нажмите кнопку **ОК**.

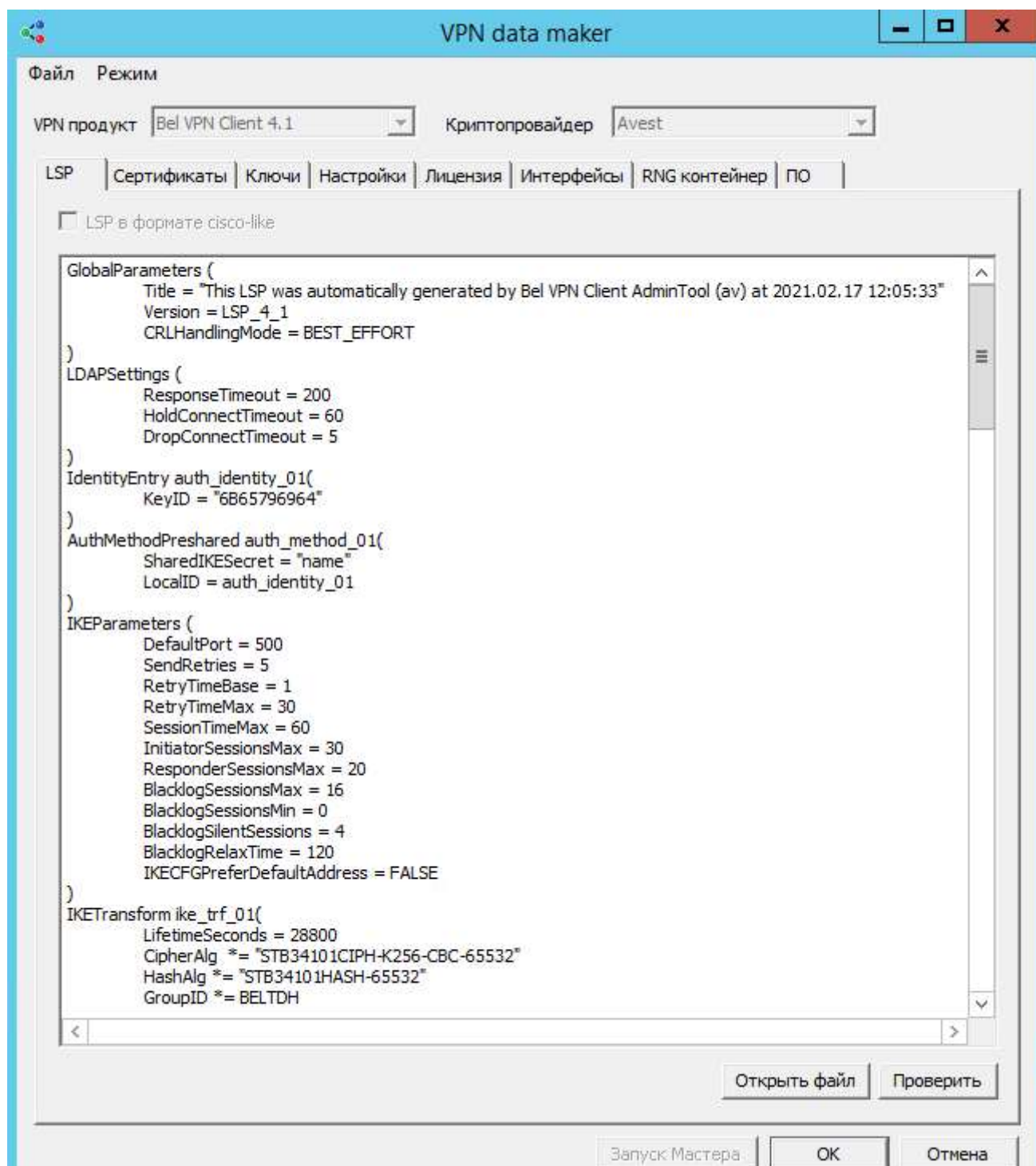


Рисунок 88

12. В окне создания нового клиента server01 также нажмите **ОК** (Рисунок 89).

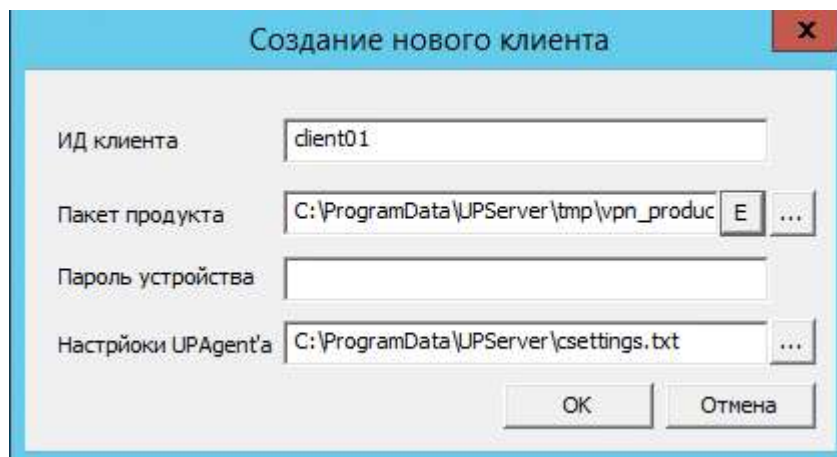


Рисунок 89

13. Созданного клиента переведите в активное состояние, выбрав в контекстном меню предложение **Включить** (Рисунок 90). Процедура **Включить** необходима для того, чтобы в момент инсталляции Клиента управления он смог связаться с Сервером управления и провести проверку возможности получения обновлений. После изменения статуса клиента на **Включен**, для него будет сформировано проверочное (тестовое) обновление, и состояние клиента изменится на **Ожидает**.

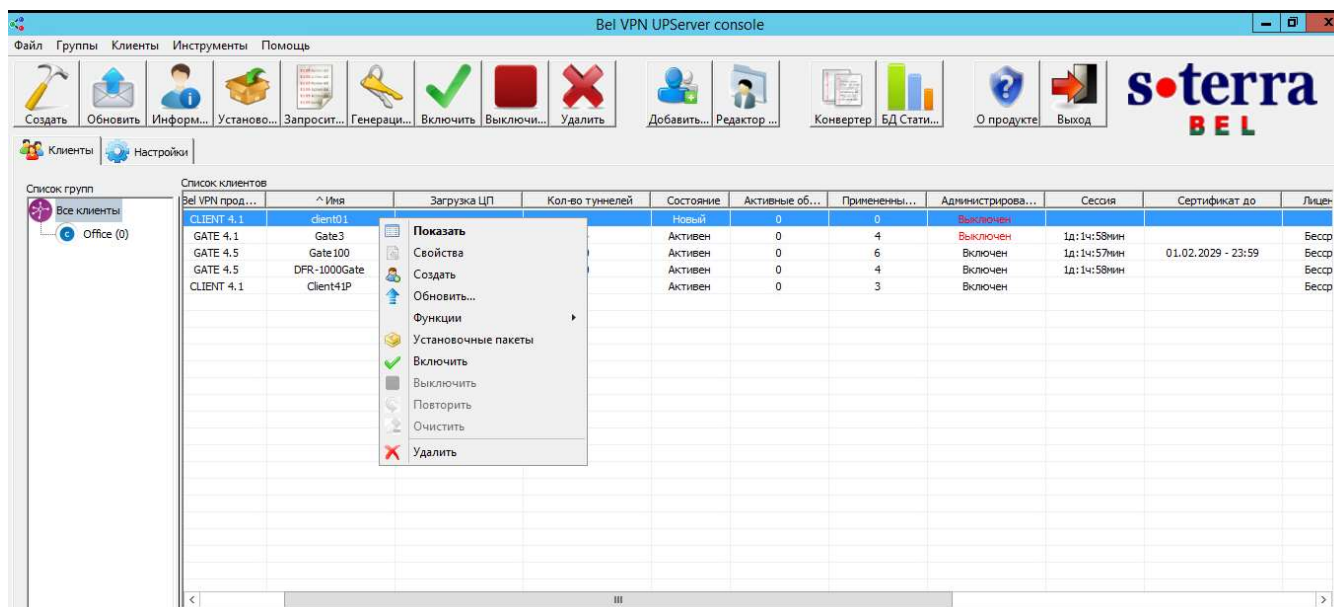


Рисунок 90

6.2. Создание инсталляционных файлов Клиента управления и Bel VPN Client-P 4.1

1. Для создания инсталляционных файлов Клиента управления и Bel VPN Client для учетной записи клиента client01 выберите предложение **Установочные пакеты** (Рисунок 91).

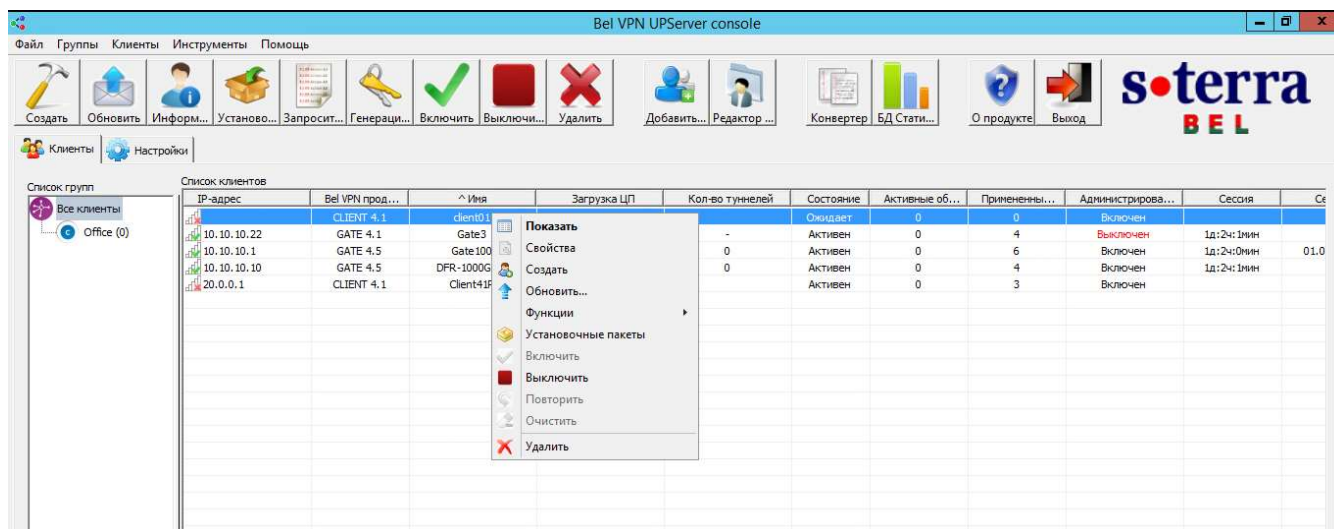


Рисунок 91

2. Укажите каталог для сохранения инсталляционных файлов (Рисунок 92) и нажмите **ОК**.

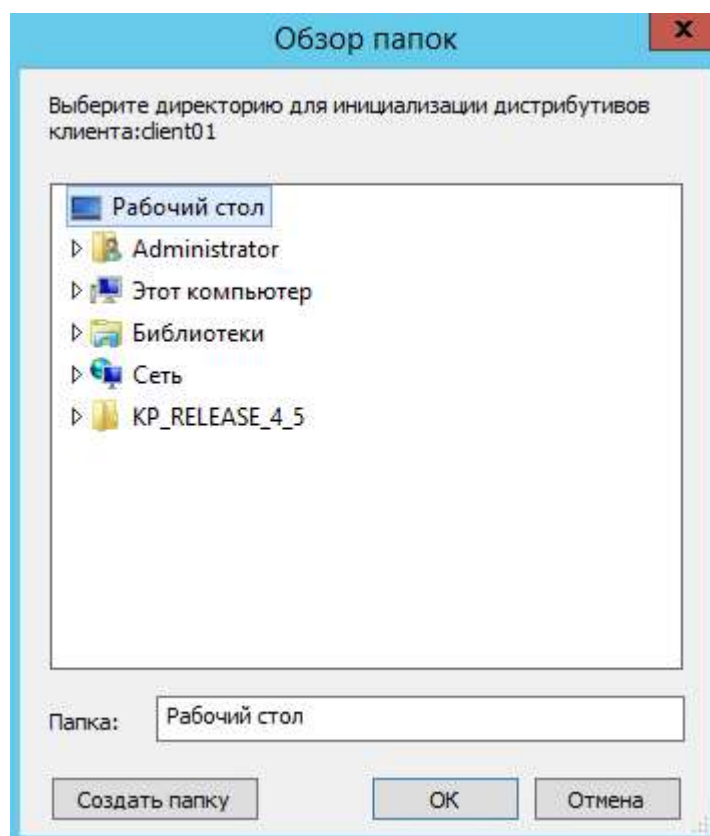


Рисунок 92

3. В указанный каталог будут сохранены два файла (Рисунок 93):
setup_product.exe – инсталляционный файл Клиента безопасности Bel VPN Client-P 4.1
setup_upagent.exe – инсталляционный файл Клиента управления Bel VPN KP 4.5.



 setup_product	12.03.2021 5:47	Приложение	16 395 КБ
 setup_upagent	12.03.2021 5:47	Приложение	19 647 КБ

Рисунок 93

6.3. Инсталляция Клиента управления и Bel VPN Client-P 4.1

Установка подготовленных файлов на управляемое устройство осуществляется локально. Доставьте на устройство два файла и запустите инсталляцию в следующем порядке:

- 1) **setup_product.exe** – установка Клиента безопасности
- 2) **setup_upagent.exe** – установка Клиента управления

ВНИМАНИЕ! УСТАНОВЛИВАТЬ СТРОГО В УКАЗАННОМ ПОРЯДКЕ!
Если порядок изменить, то Клиент управления сразу после установки попытается выйти на связь с Сервером управления по незащищенному соединению

Установка:

1. Процесс установки продукта Bel VPN Client-P 4.1 описан в документе «Программный продукт «Клиент безопасности Bel VPN Client-P 4.1» Руководство администратора. Общее руководство».
2. Перезагрузите операционную систему и введите пароль для доступа к продукту Bel VPN Client-P 4.1 (изначально установлен пустой пароль, измените его значение) (Рисунок 94).



Рисунок 94

3. Инсталляция Клиента управления (продукт Bel VPN КР 4.1) запускается программой setup_upagent.exe. В появившемся окне (Рисунок 95) нажмите кнопку **Да**.



Рисунок 95

4. Для продолжения инсталляции нажмите кнопку [Next](#).



Рисунок 96

5. Выберите каталог для инсталляции Клиента управления (Рисунок 97).

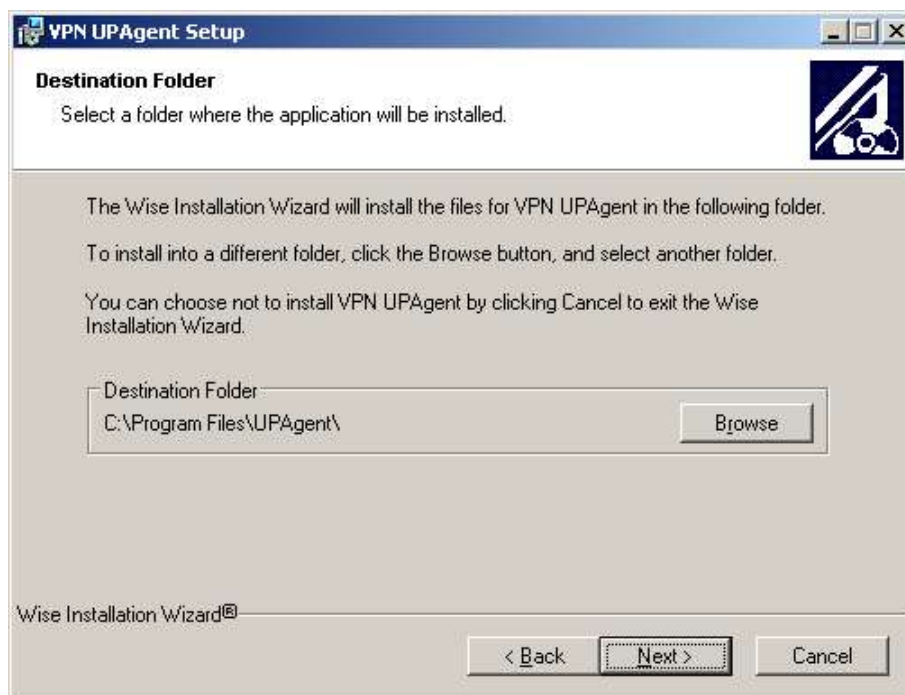


Рисунок 97

6. В следующем окне подтвердите готовность к установке и нажмите кнопку [Next](#).

7. По завершению инсталляции нажмите кнопку **Finish** (Рисунок 98).



Рисунок 98

8. По завершению установки Клиент управления попытается установить связь с Сервером управления. После успешного соединения и проверки возможности получения обновлений, состояние клиента на Сервере управления изменится с **Ожидает** на **Обновление**, а затем на **Активен**. Это означает, что Клиент управления готов к скачиванию обновлений (Рисунок 99).

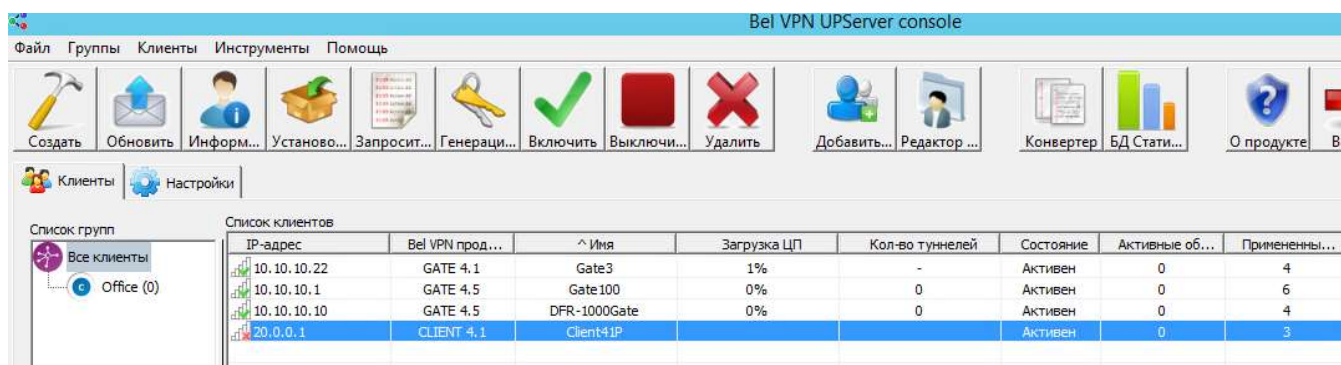


Рисунок 99



Note

Если пароль от VPN-продукта на управляемом устройстве отличается от нулевого, то по завершении установки Клиента управления и установки соединения с Сервером управления, на управляемом устройстве появится диалоговое окно **“VPN UPAgent – Пароль для VPN-продукта”** с запросом пароля от VPN-продукта. Введите пароль в поле **Пароль:** и нажмите **OK**.

Пароль от VPN-продукта запрашивается всякий раз, когда он отличается от нуля и/или неизвестен Клиенту управления: при изменении пароля от VPN-продукта, при запуске UPAgent'a и установке соединения с Сервером управления, при обновлении UPAgent'a.

7. Сценарий перехода на аутентификацию с использованием сертификатов

Далее предполагается, что:

- 1) На управляемом устройстве установлен Клиент управления и Клиент безопасности Bel VPN Client-P 4.1.
- 2) На центральном Шлюзе безопасности Bel VPN Gate 4.1/4.5 также установлен Клиент управления.
- 3) Для аутентификации оба продукта используют predetermined ключ.

Требуется изменить метод аутентификации – использовать на обоих устройствах локальные сертификаты.

Сценарий перехода на аутентификацию с использованием сертификатов осуществляется в несколько этапов:

1. На Сервере управления для управляемых устройств готовится обновление, которое включает имя контейнера для ключевой пары, пароль для доступа к контейнеру и параметры для запроса на сертификат открытого ключа.
2. После применения данного обновления, на управляемом устройстве создается ключевой контейнер (с ключевой парой) и запрос на сертификат.
3. На Сервере управления появится новая информация о соответствующем Клиенте управления – создан ключевой контейнер и запрос на сертификат.
Информацию о запросе на сертификат необходимо передать в Удостоверяющий центр.
4. После получения сертификата открытого ключа из Удостоверяющего центра, необходимо на Сервере управления подготовить обновление, включающее новый локальный сертификат, сертификат УЦ и отредактированную политику для данного клиента.

Далее эти этапы расписаны подробно.

7.1. Создание обновления с параметрами ключевой пары и запроса на сертификат

1. На Сервере управления сразу для двух устройств создайте обновления для генерации ключевой пары и запроса на сертификат на этих устройствах. Поэтому выделите в таблице строки с клиентами и выберите предложение **Функции – Ключевая пара – Генерация** (Рисунок 100).

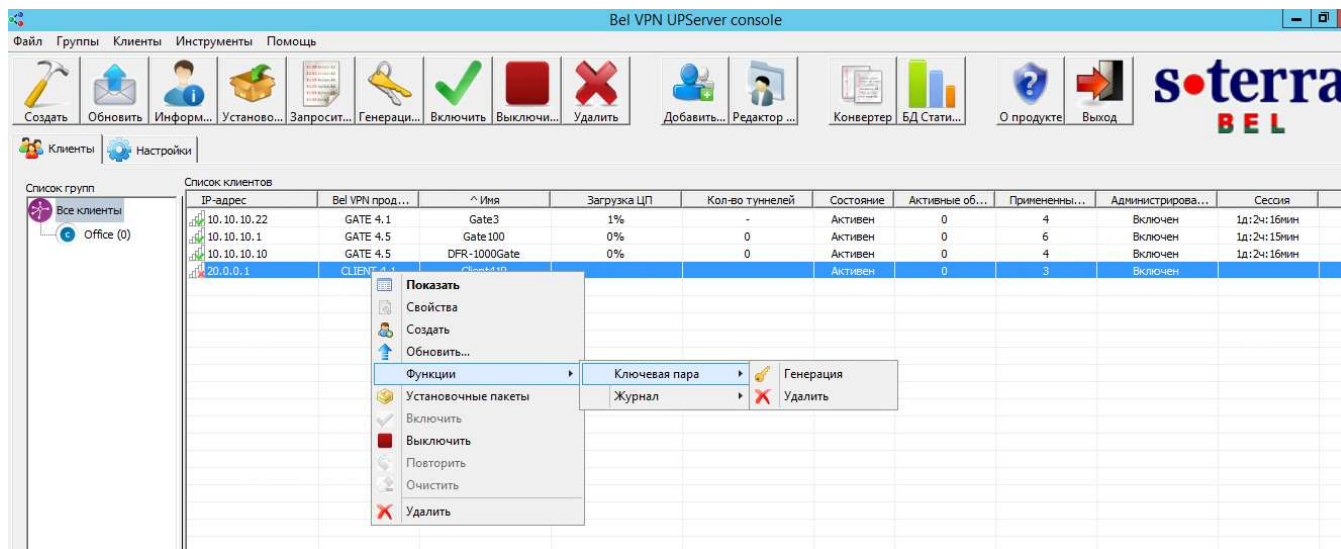


Рисунок 100

2. В открывшемся окне (Рисунок 101) заполните только два поля – задайте пароль на контейнер и его подтверждение, в который будет размещена ключевая пара для локального сертификата.

Рисунок 101

Окно **Создание ключевой пары** имеет следующие поля:

- ♦ **Время создания** – время, когда Сервер управления сделает доступным для Клиента управления обновление, содержащее необходимые данные для создания ключевой пары и запроса на сертификат

- ♦ **Имя контейнера** – имя контейнера на управляемом устройстве³, в который будет записана ключевая пара. Если это поле не задано, то имя контейнера будет подобрано автоматически. При указании имени оно должно быть уникальным и включать имя считывателя, если на управляемом устройстве установлено несколько считывателей. Например,

<i>av:AVP2050050123:Client50123.cont</i>	Формат записи названия контейнера для ПП Bel VPN Client-P 4.1 с ключевым носителем
<i>av:Gate50123.cont</i>	Формат записи названия контейнера для ПК, ПАК Bel VPN Gate 4.5/4.1 с ключевым носителем
<i>Client4754.cont</i>	Формат записи названия контейнера для ПП Bel VPN Client-P 4.1 без ключевого носителя

- ♦ **Пароль контейнера** – пароль для защиты контейнера. Если это поле не задано, то пароль для контейнера будет считаться пустым
 - ♦ **Подтверждение пароля** – поле для повторного ввода пароля. Должно совпадать со значением Container password
 - ♦ **Certificate subject** – строка, используемая в качестве поля Subject при создании запроса на сертификат. В этой строке можно использовать макросы, такие как %UPAgentID%, %UPAgentGroup% и т.п., которые будут заменены на их значения (список макросов, которые можно использовать, совпадает с переменными, передаваемыми в файл cook.bat при его запуске).
3. При нажатии кнопки **OK** предлагается выполнить «биологическую» инициализацию ДСЧ – понажимайте клавиши или перемещайте указатель мыши (Рисунок 102). Если на Сервере управления установлен аппаратный ДСЧ, то данное окно не выводится.

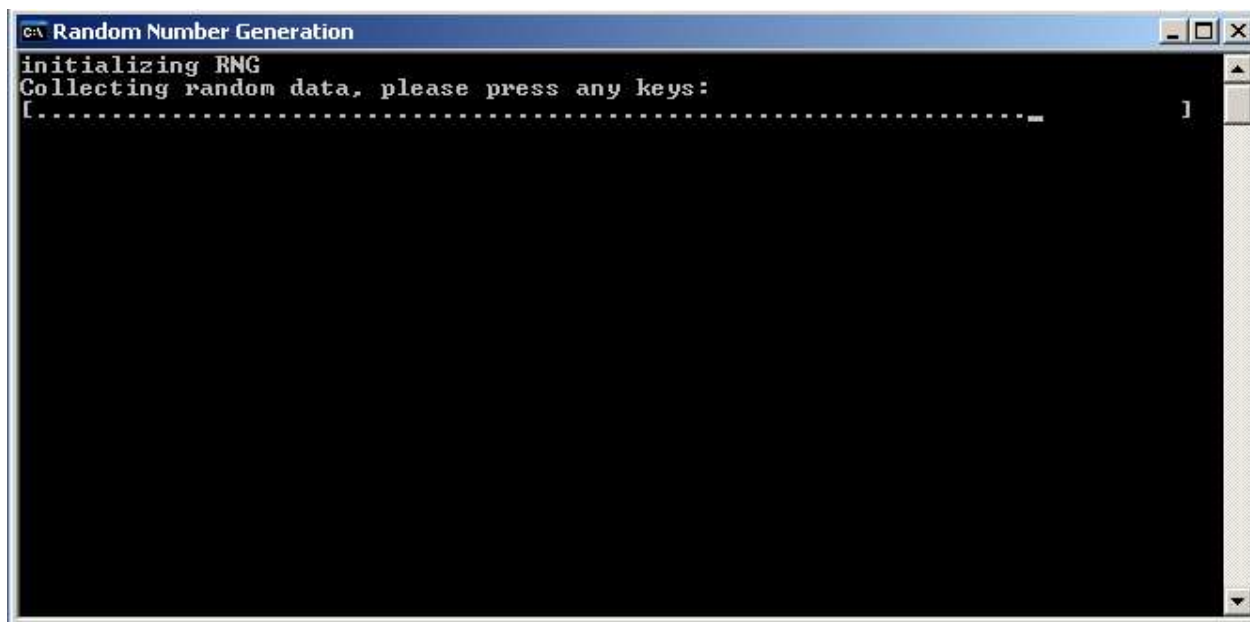


Рисунок 102

³ Подробнее о названии контейнера см. руководство администратора продуктов линейки Bel VPN Gate 4.5/4.1 и Bel VPN Client-P 4.1

4. После этого в таблице появятся новые обновления с параметрами ключевых пар и контейнеров для данных клиентов (Рисунок 103). Количество активных обновлений (столбец Active updates) увеличится на единицу.

Список клиентов

IP-адрес	Bel VPN прод...	Имя	Загрузка ЦП	Кол-во туннелей	Состояние	Активные об...
10.10.10.22	GATE 4.1	Gate3	1%	-	Активен	0
10.10.10.1	GATE 4.5	Gate100	0%	0	Активен	0
10.10.10.10	GATE 4.5	DFR-1000Gate	0%	0	Активен	0
20.0.0.1	CLIENT 4.1	Client41P			Ожидает	1

Рисунок 103

5. На устройстве с установленным Bel VPN Gate 4.5/4.1 обновление применяется автоматически.

На устройстве с установленным Bel VPN Client-P 4.1 запрашивается разрешение на применение обновления (подробнее, см. раздел «Действия администратора при обновлении»).

Через некоторое время обновления будут применены на устройствах, что отразится в таблице на Сервере управления (Рисунок 104). Количество успешных примененных обновлений увеличится на единицу, а количество готовых к скачиванию - уменьшится на единицу.

Список клиентов

IP-адрес	Bel VPN прод...	Имя	Загрузка ЦП	Кол-во туннелей	Состояние	Активные об...	Примененны...	Администрирова...
10.10.10.22	GATE 4.1	Gate3	1%	-	Активен	0	4	Включен
10.10.10.1	GATE 4.5	Gate100	0%	0	Активен	0	6	Включен

Рисунок 104

7.2. Просмотр запроса на сертификат

В результате на каждом устройстве будет создан контейнер с ключевой парой и запрос на сертификат, которые можно увидеть на Сервере управления. Для выделенного клиента в контекстном меню выберите предложение **Показать** (Рисунок 105).

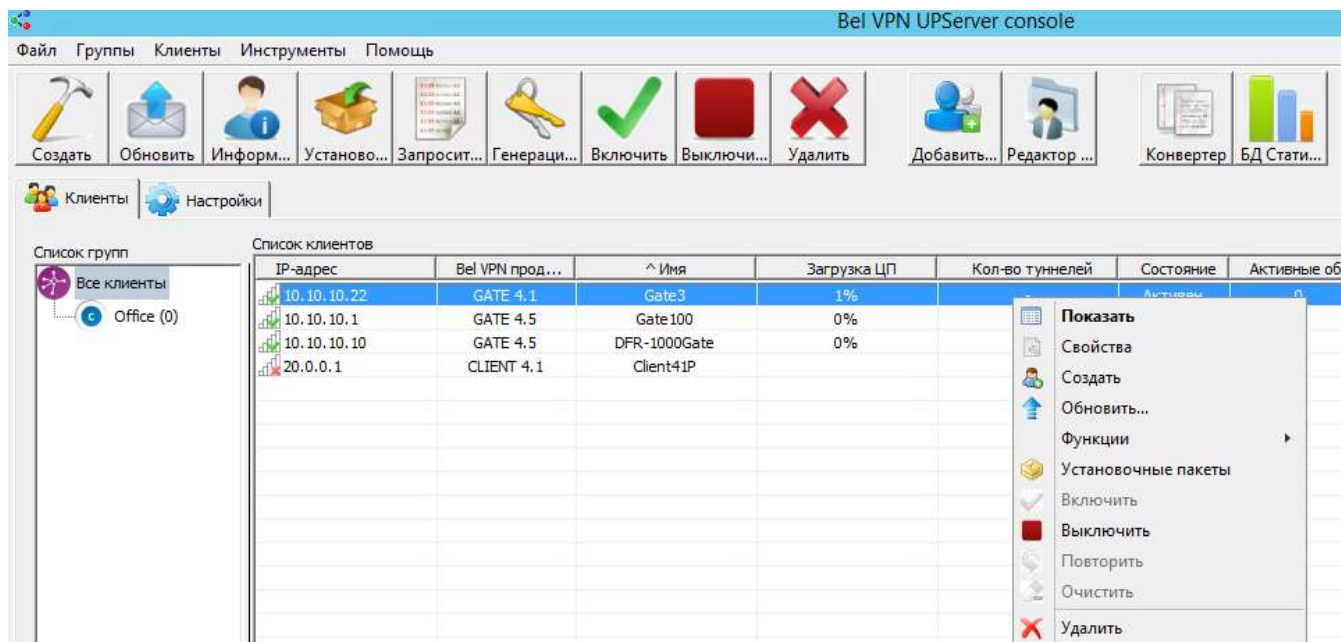


Рисунок 105

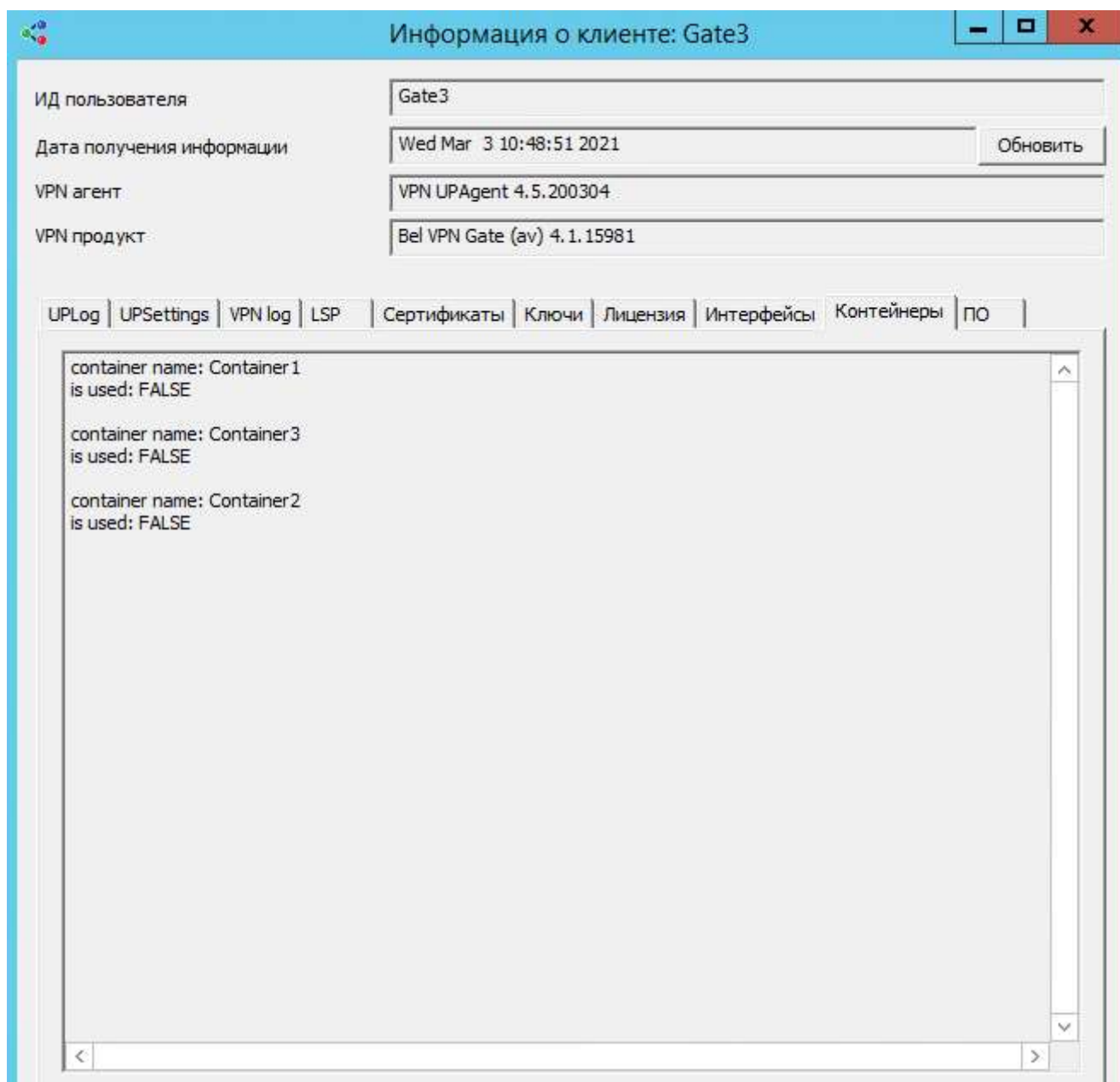


Рисунок 106

Во вкладке **Контейнеры** появилась запись о созданном контейнере и запросе на сертификат (Рисунок 106):

- **container name** – имя созданного контейнера на жестком диске
- **is used: FALSE** – признак того, что контейнер еще не используется продуктом Bel VPN Gate 4.1, так как сертификат не создан
- **password id** – уникальный идентификатор пароля к контейнеру
- **certificate subject** – строка, которая использовалась в качестве поля Subject при создании запроса на сертификат
- тело запроса на сертификат.

7.3. Получение сертификата по запросу

Для получения сертификата открытого ключа по сформированному запросу необходимо:

1. Скопировать текстовое представление запроса (формат base64) из вкладки **Контейнеры**, сохранить в текстовый файл.
2. Сформировать карточку открытого ключа, убедиться, что данные об организации и устройстве в запросе указаны верно.
3. Отправить в Удостоверяющий центр текстовый файл с запросом и карточку открытого ключа (если требуется по регламенту Удостоверяющего центра).

7.4. Создание обновления с новым сертификатом для клиента Bel VPN Gate 4.1/4.5

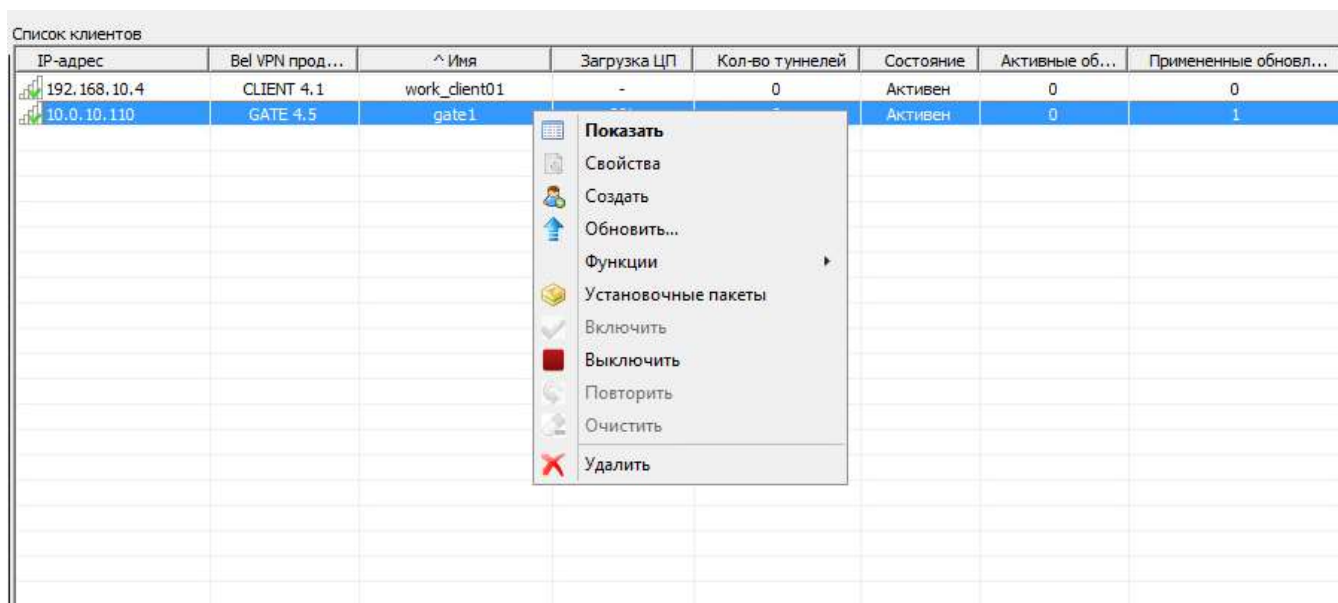


Рисунок 107

1. На Сервере управления в контекстном меню выберите предложение **Обновить** (Рисунок 107).
2. В открывшемся окне **Обновление для клиента** нажмите кнопку **E** (Рисунок 108).

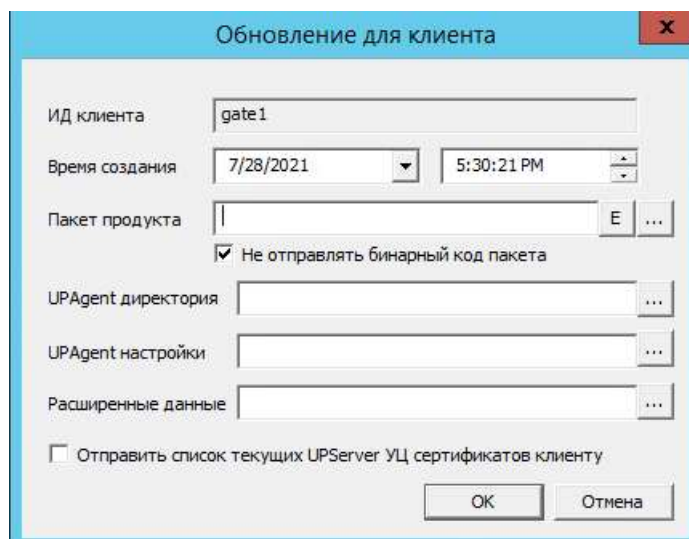


Рисунок 108

3. В окне **VPN data maker** (Рисунок 109) переходите на вкладки и вносите необходимые изменения.

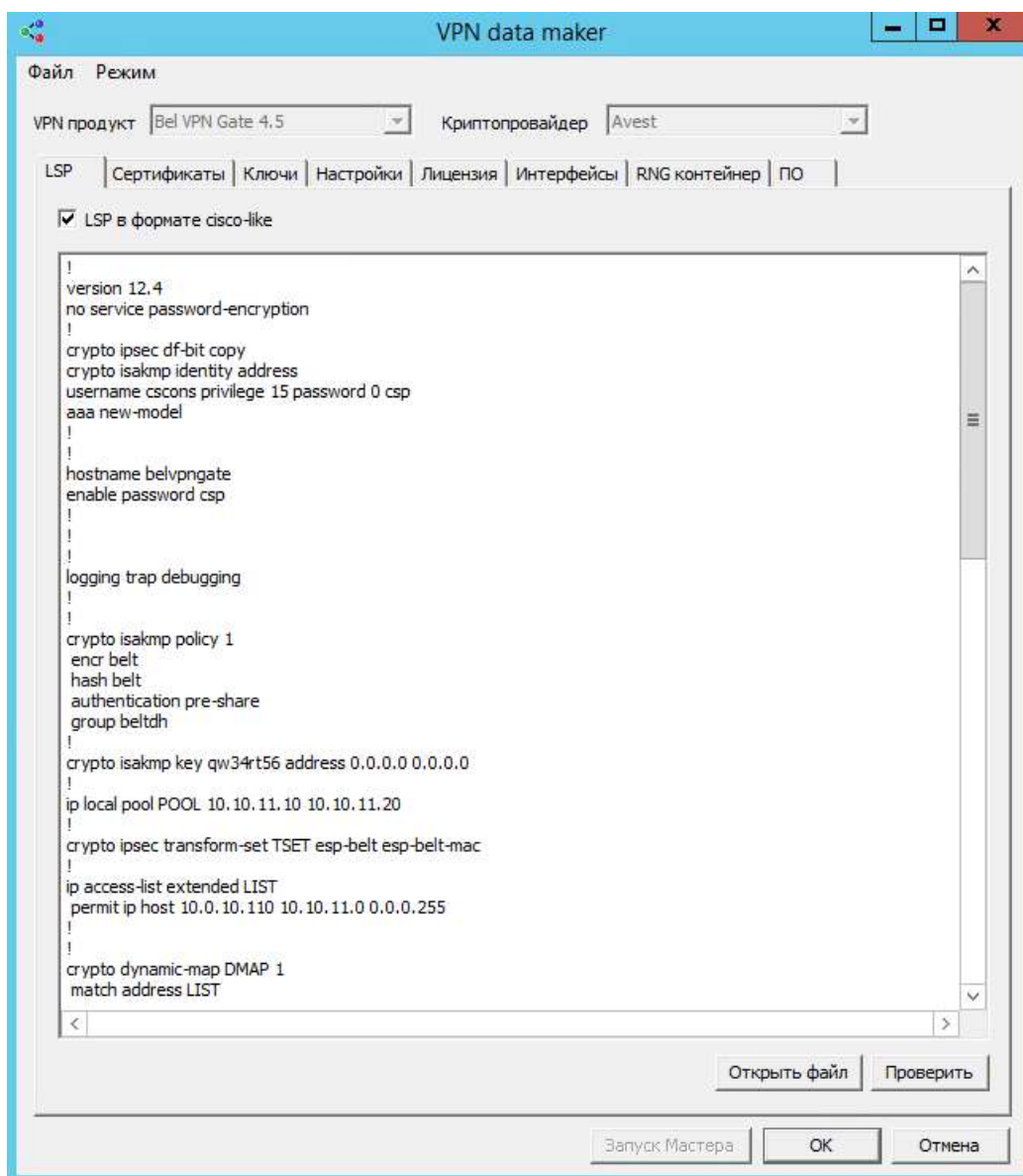


Рисунок 109

4. Для изменения сертификатов в открывшемся окне перейдите на вкладку **Сертификаты** и добавьте сертификат УЦ и локальный сертификат(Рисунок 110).

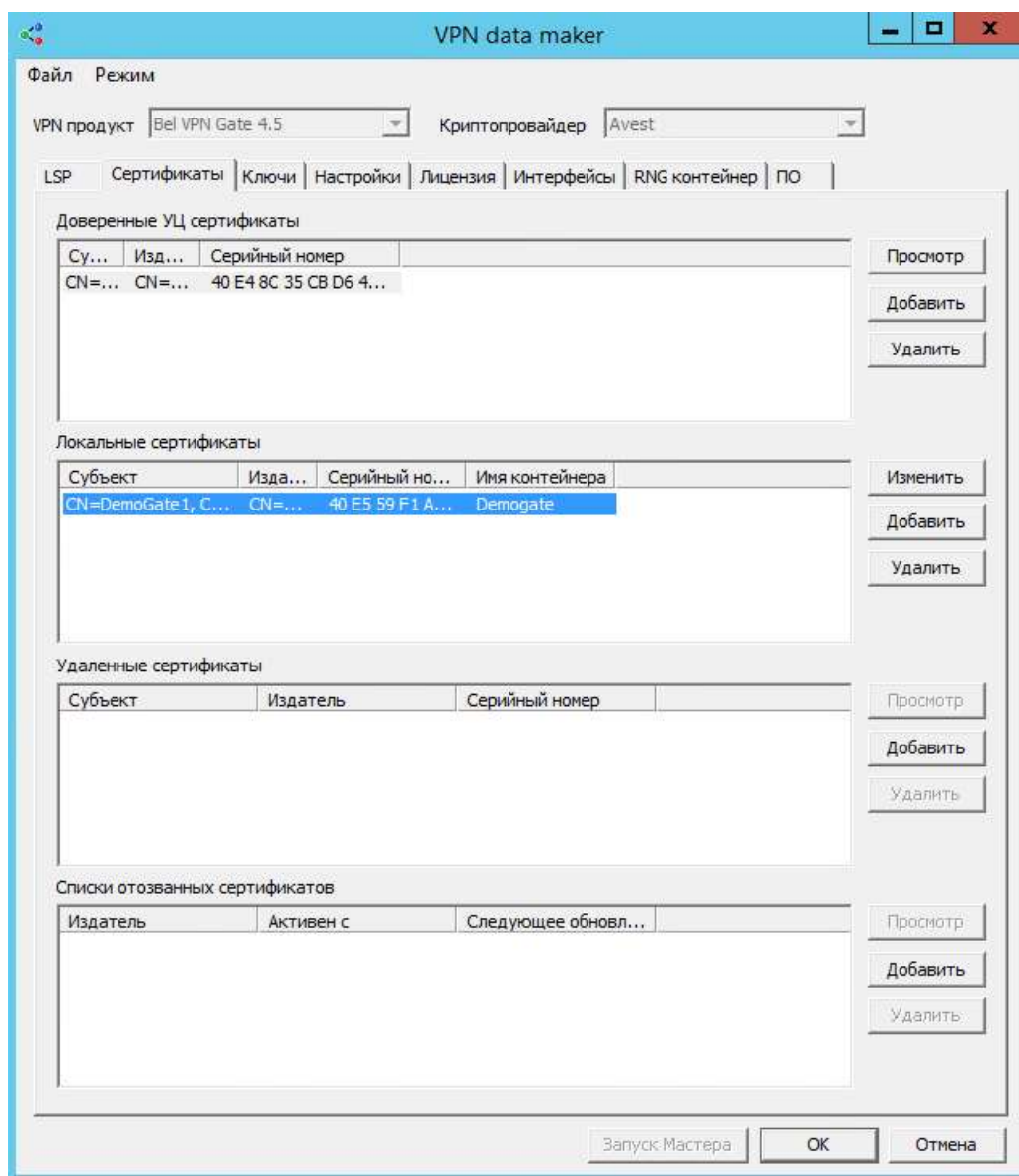


Рисунок 110

- Для обновления политики безопасности (переход с аутентификации PSK на сертификаты), обновления списков доступа, маршрутизации и т.п. перейдите на вкладку **LSP** (Рисунок 111).

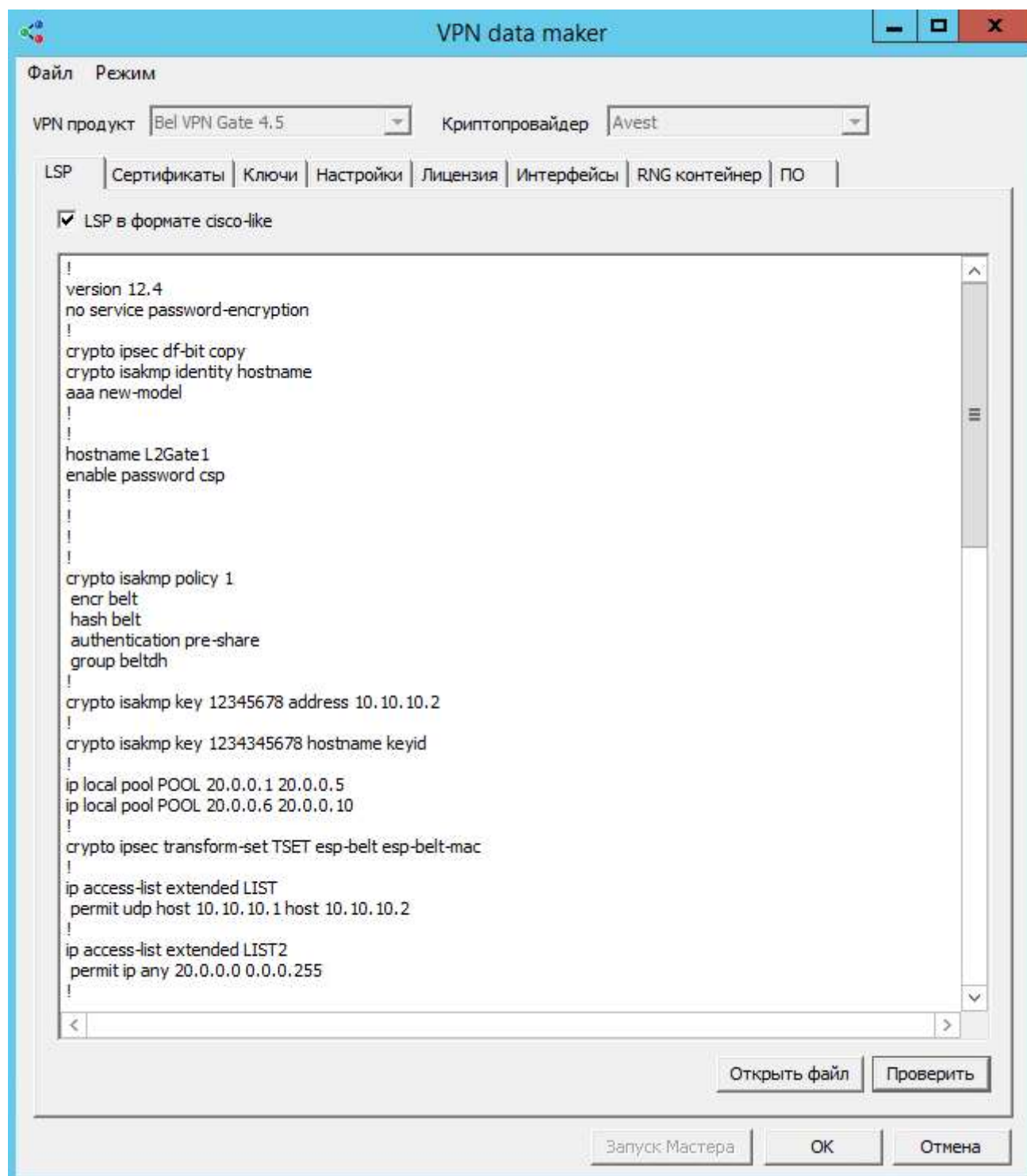


Рисунок 111

6. В окне вкладки **LSP** внесите необходимые изменения в формате cisco-like. При внесении изменений выберите чекбокс **LSP в формате cisco-like** (Рисунок 1125).
7. Убедиться, что внесенные Вами изменения имеют правильный формат при помощи кнопки **Проверить** (Рисунок 1126).

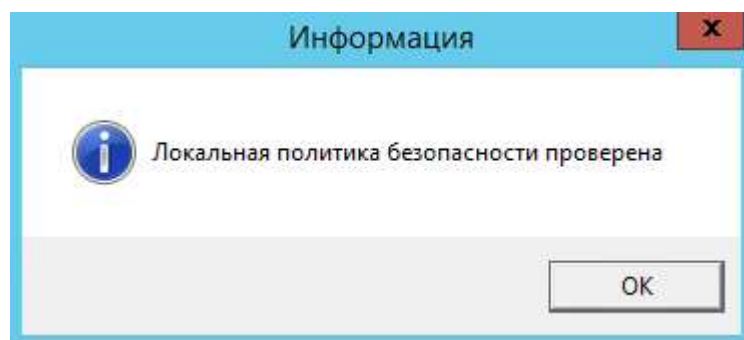


Рисунок 112

8. В окне с информацией нажмите кнопку **ОК** (**Ошибка! Источник ссылки не найден.**6).
9. При необходимости Вы можете изменить и лицензионные данные. Для этого перейдите на вкладку **Лицензия** Рисунок 7).

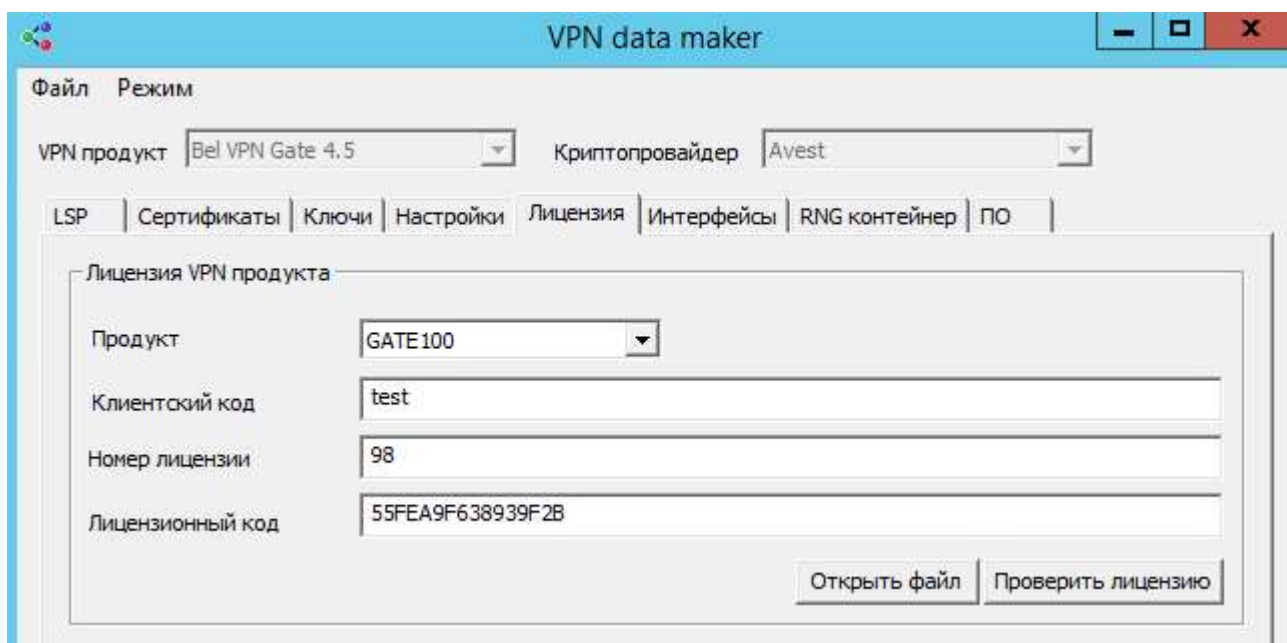


Рисунок 1137

10. После внесенных изменений нажмите на кнопку **Проверить лицензию** (Рисунок 8).

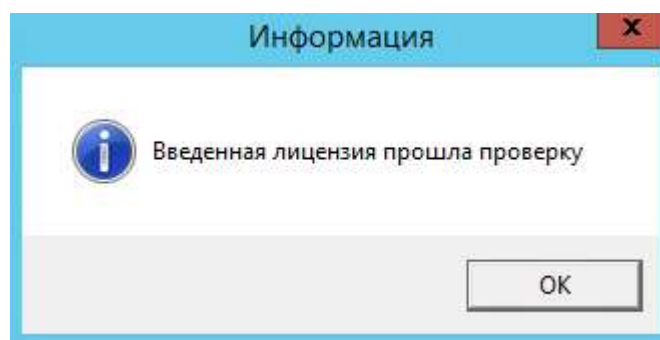


Рисунок 118

11. Проверьте все введенные данные во вкладках проекта, после чего нажмите кнопку **ОК** (Рисунок 11419).

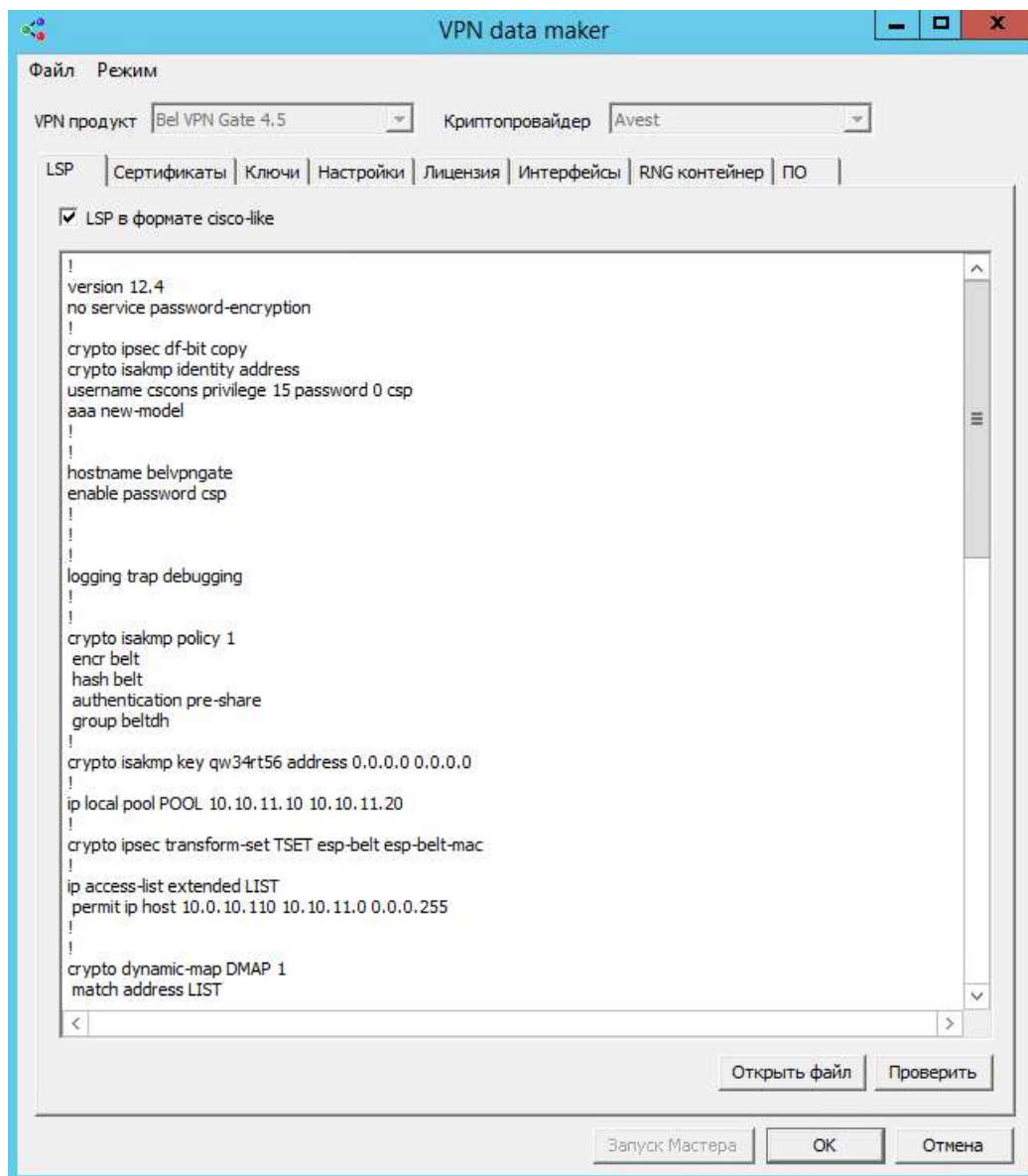


Рисунок 11419

12. В окне создания обновления нажмите кнопку **OK** (Рисунок 115).

Рисунок 115

13. Обновление с использованием локального сертификата для аутентификации создано (Рисунок 116).

IP-адрес	Bel VPN прод...	Имя	Загрузка ЦП	Кол-во туннелей	Состояние	Активные об...	Примененные обновл...
192.168.10.4	CLIENT 4.1	work_client01	-	0	Активен	0	0
10.0.10.110	GATE 4.5	gate1	0%	0	Обновляется	1	1

Рисунок 116

14. После того как центральный шлюз скачает подготовленное обновление и применит его, на Сервере управления можно посмотреть вкладку **Сертификаты**, выбрав в контекстном меню предложение **Show**, – CA и локальный сертификаты зарегистрированы в продукте и используются (Рисунок 117).

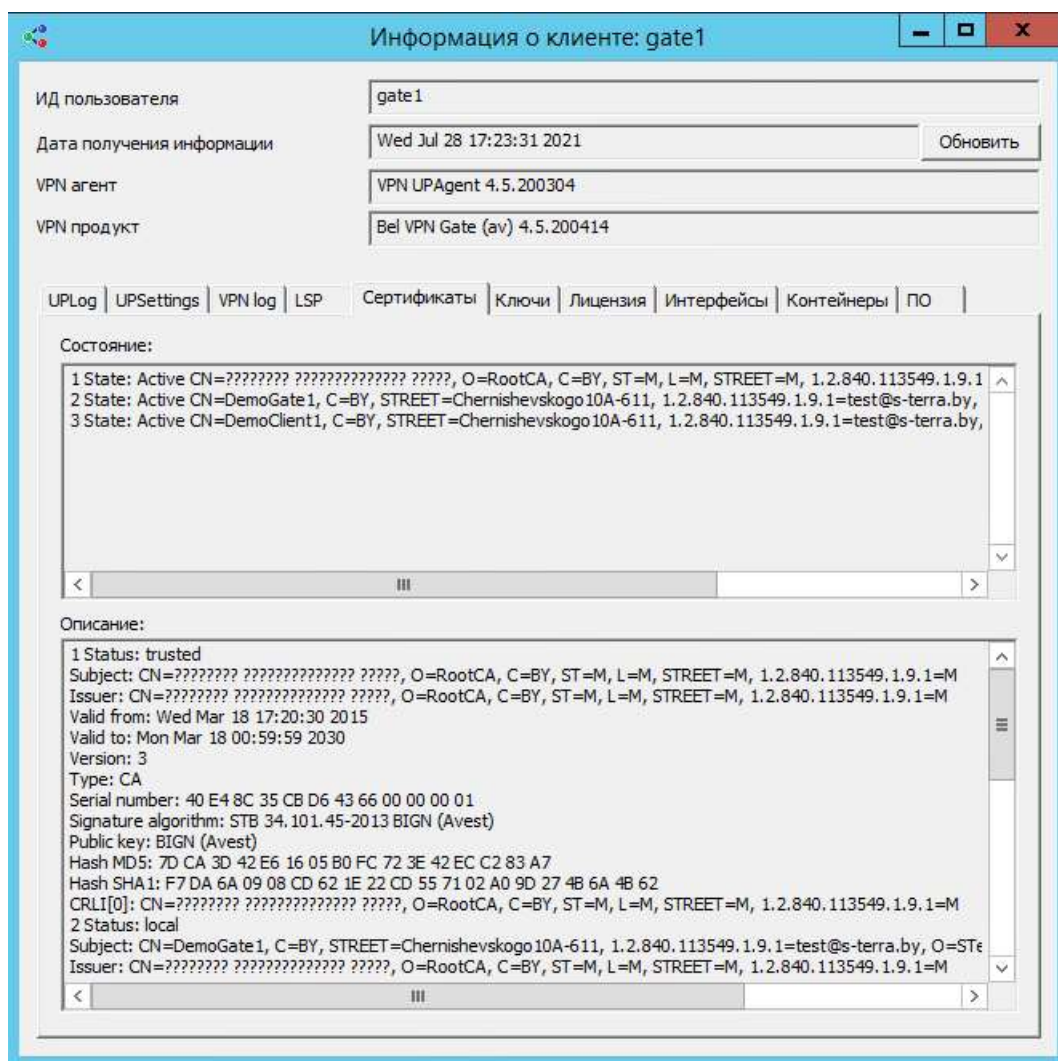


Рисунок 117

15. Во вкладке **Контейнеры** видно, что на центральном шлюзе используется контейнер с ключевой парой локального сертификата – `is used: TRUE`.

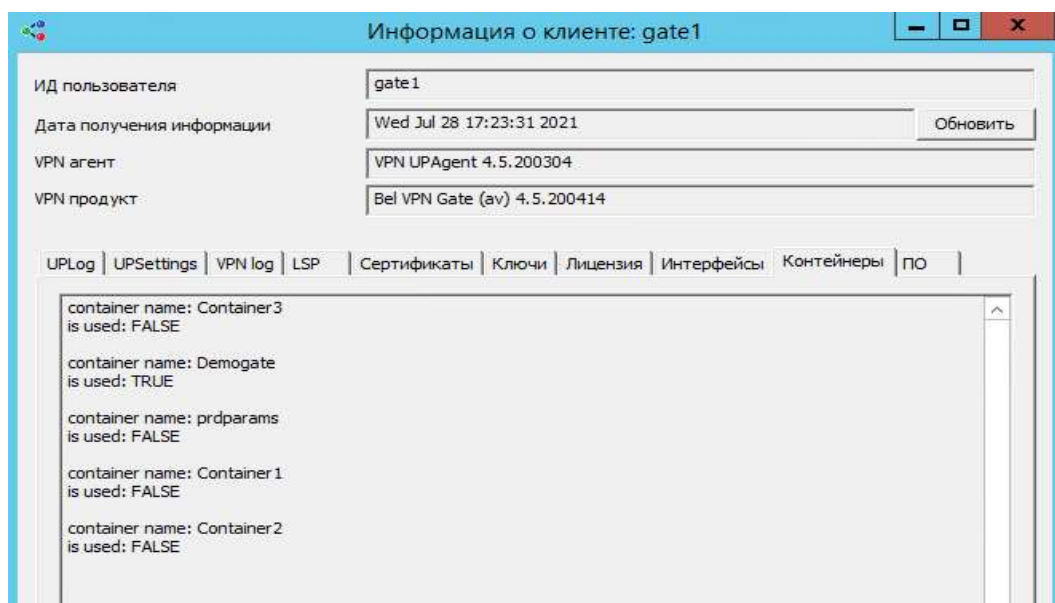


Рисунок 118

7.5. Создание обновления с новым сертификатом для устройства с клиентом



Note

Обратите внимание, что на момент замены сертификата на клиенте с Bel VPN Gate/Client-P 4.1, его партнеры уже должны быть настроены на работу с новым сертификатом на Bel VPN Gate/Client-P 4.1.

1. Создание обновления для устройства с клиентом выполняется также как и для центрального шлюза – в контекстном меню выберите предложение **Обновить** (Рисунок 119).

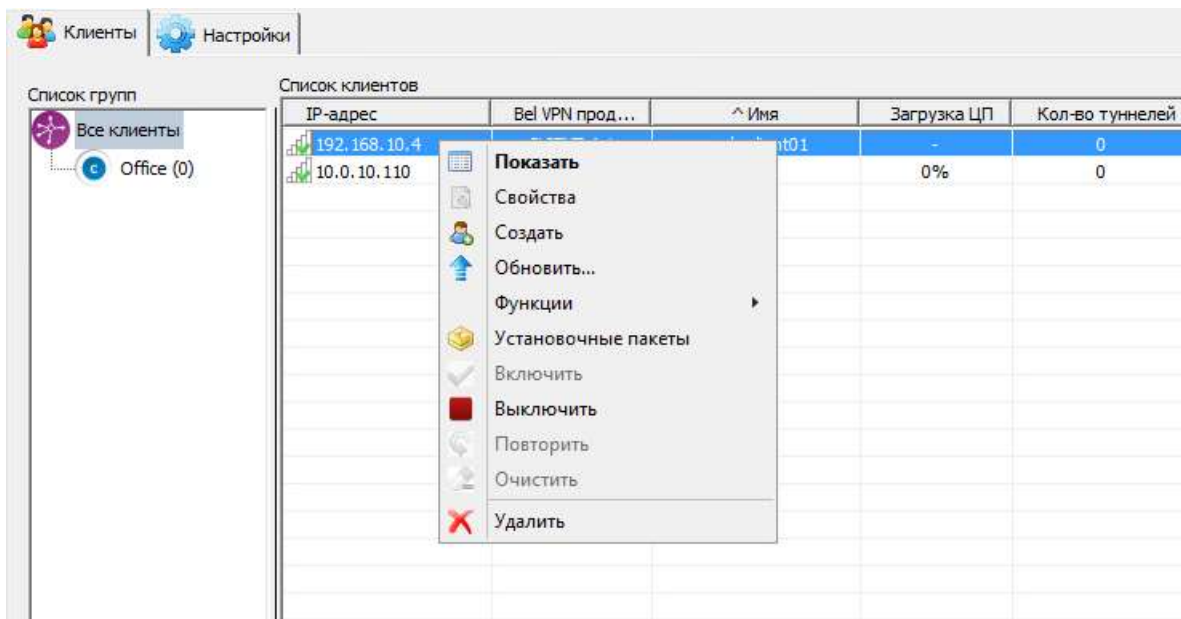


Рисунок 119

2. В следующем окне нажмите кнопку **E** для вызова окна для ввода данных (Рисунок 120).

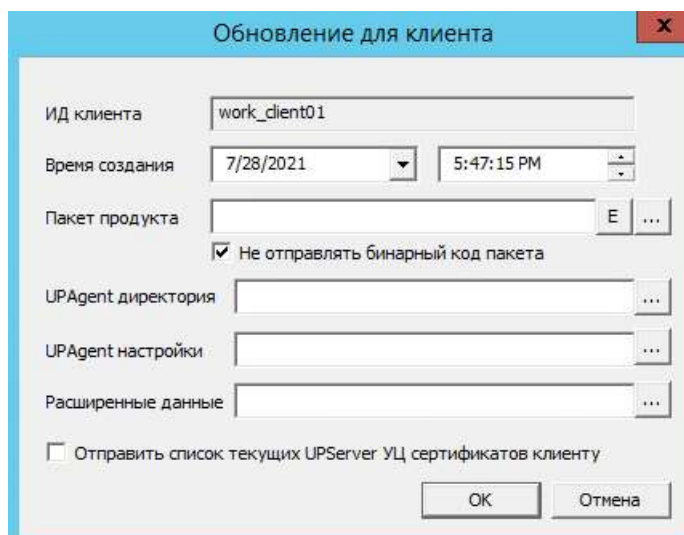


Рисунок 120

3. Появится окно **VPN data marker** с текущими настройками продукта Bel VPN Client-P 4.1.

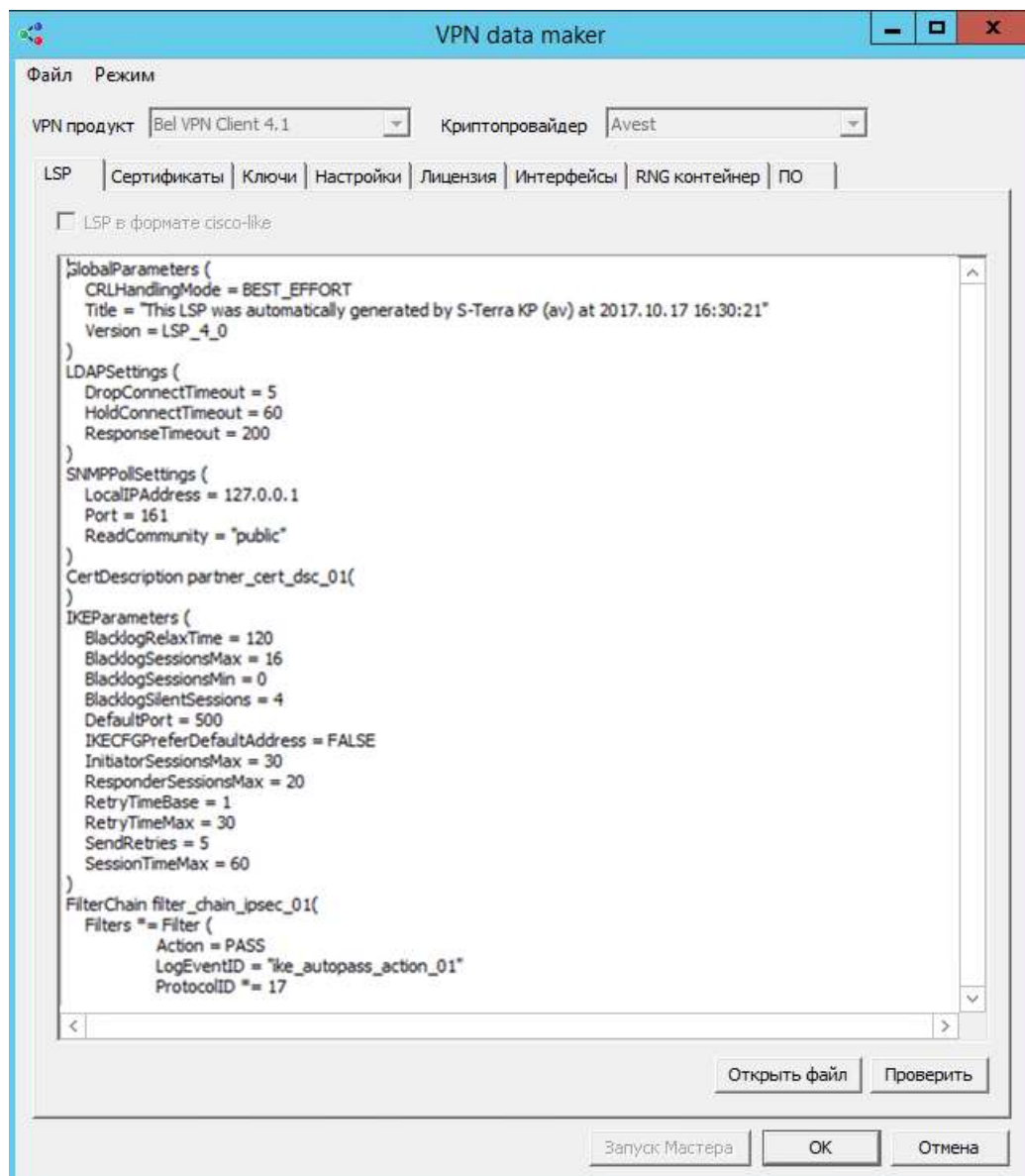


Рисунок 121

- В вкладке **Сертификаты** добавьте CA сертификат и локальный сертификат клиента client01, (Рисунок 122).

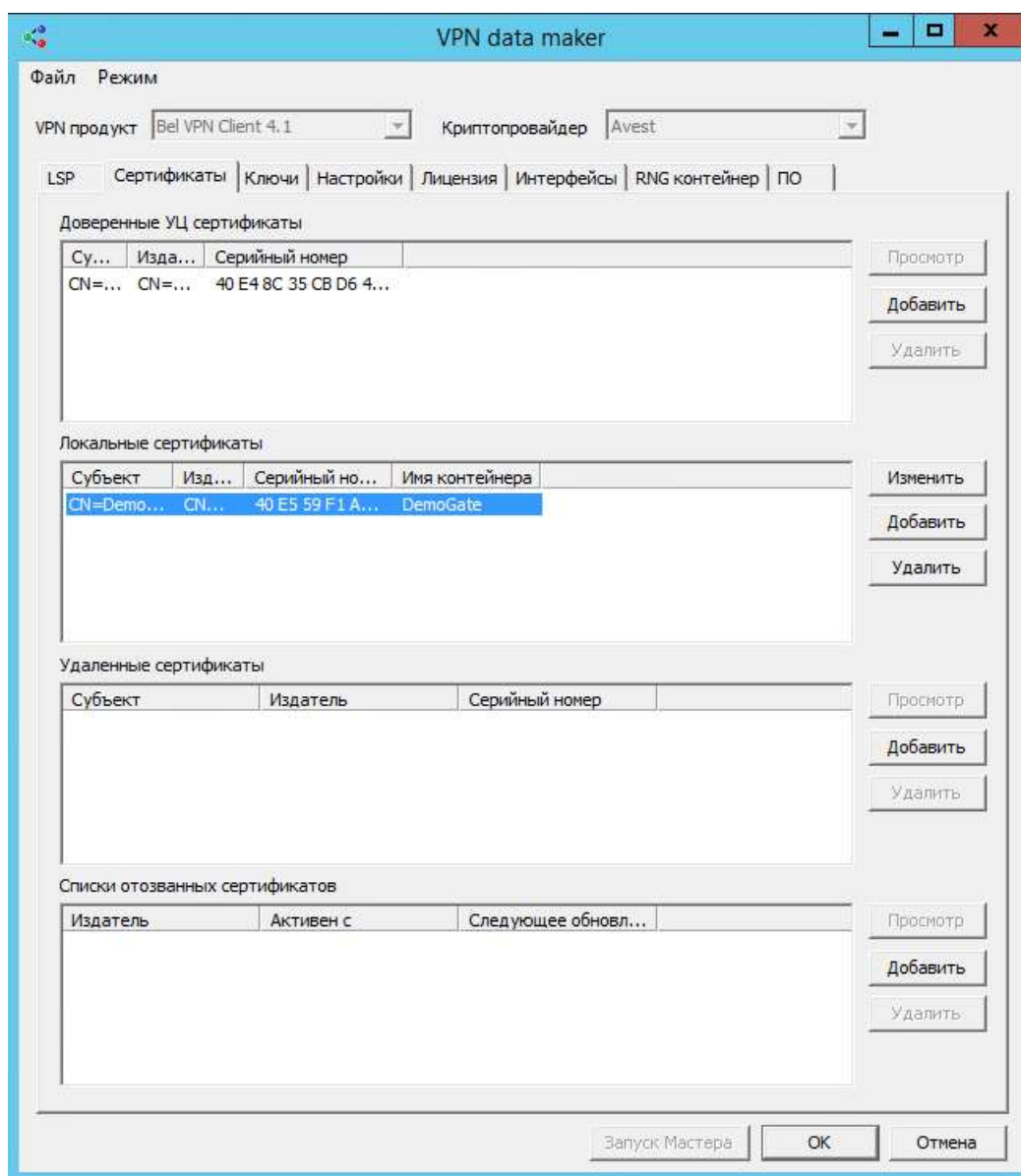


Рисунок 122

- При добавлении сертификатов выберите файл, в котором лежат два сертификата - CA сертификат и локальный сертификат для client01.

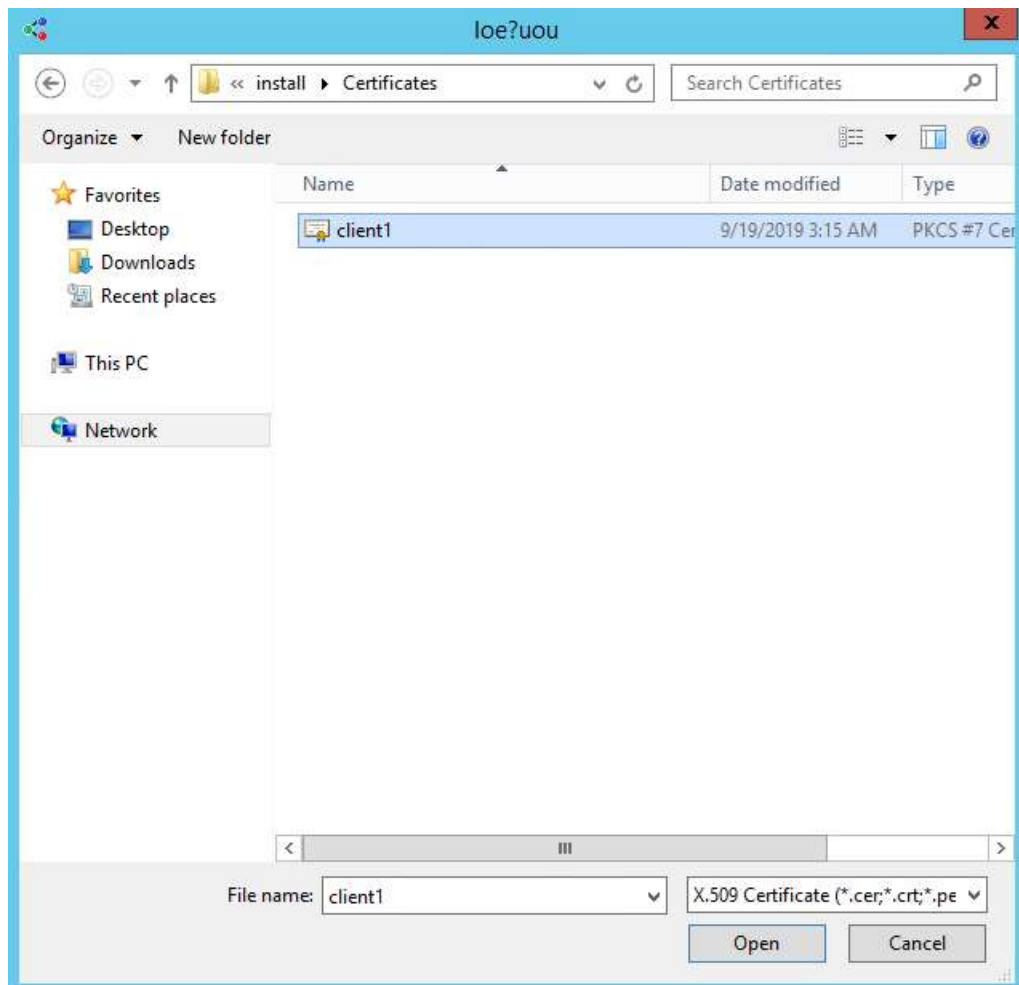


Рисунок 123

В открывшемся окне выберите CA сертификат или локальный и нажмите **OK**.

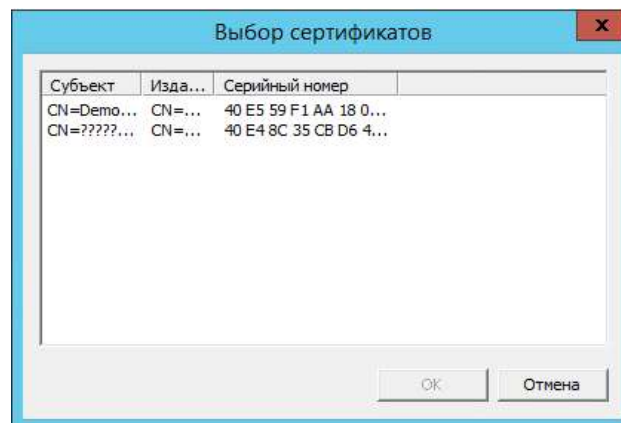


Рисунок 124

6. Лицензионные данные оставьте без изменений (Рисунок 1).

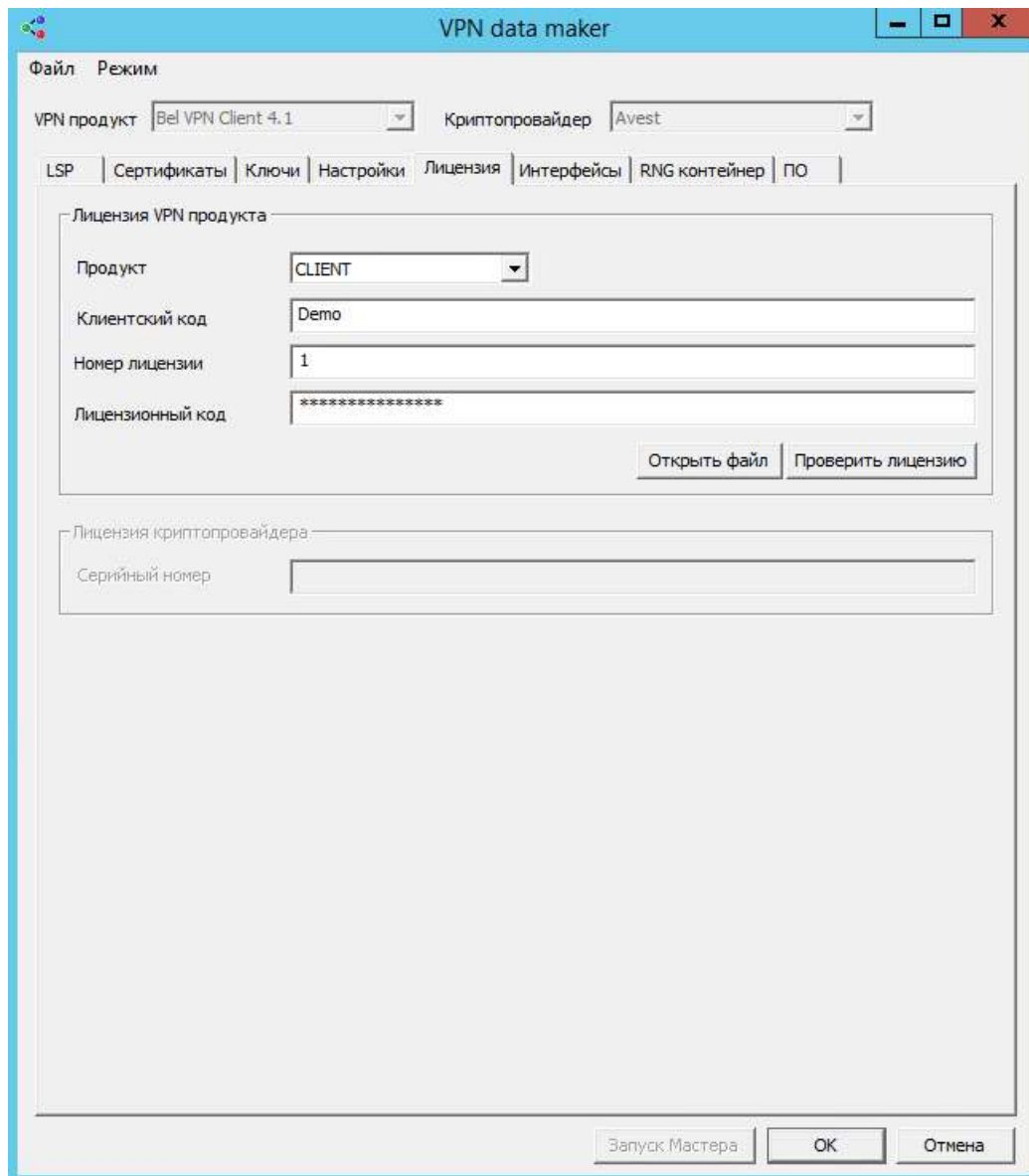


Рисунок 131

7. В окне **VPN data maker** со вкладками нажмите кнопку **OK** (Рисунок 132).

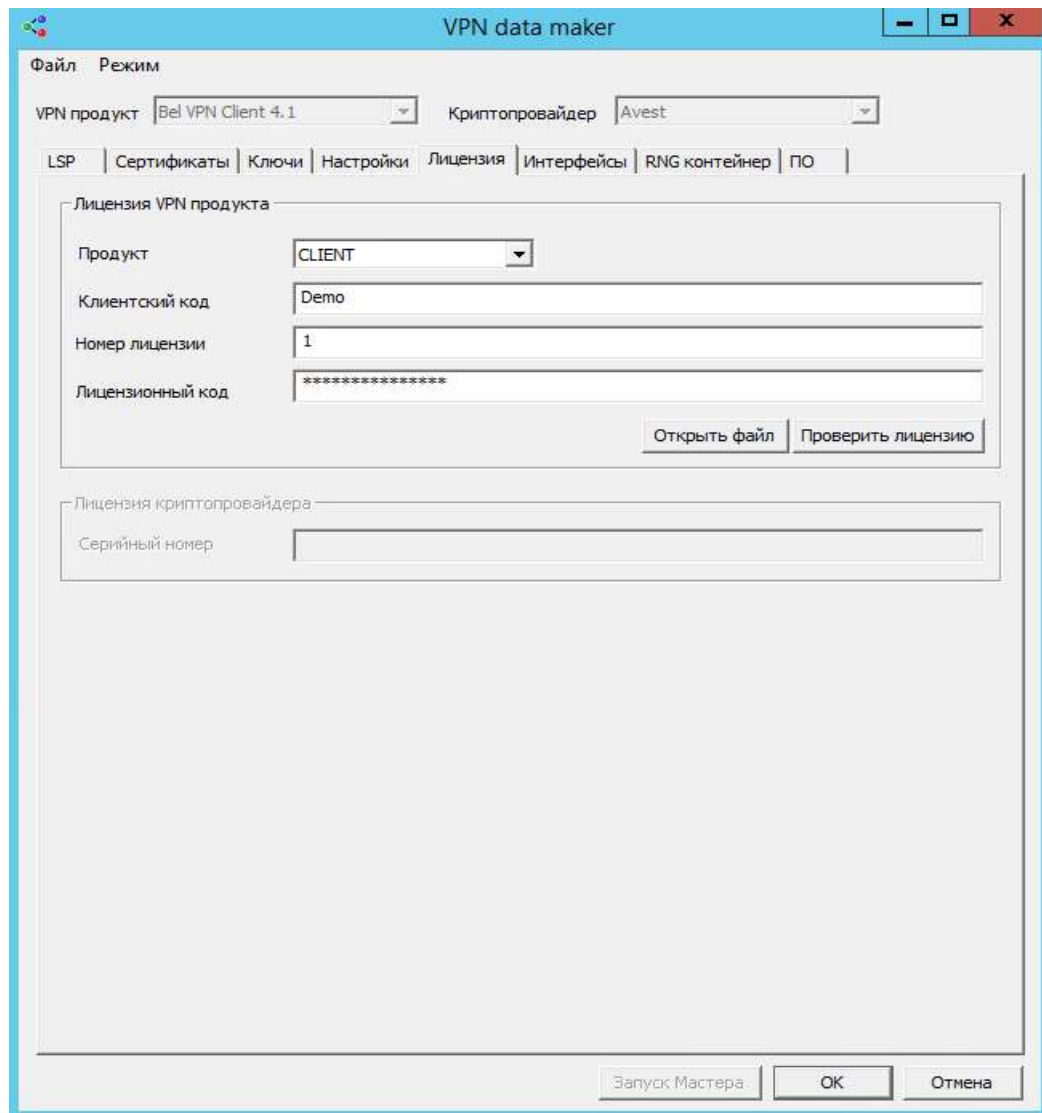


Рисунок 132

8. В окне создания обновления **Обновление для клиента** также нажмите кнопку **OK** (Рисунок 3).

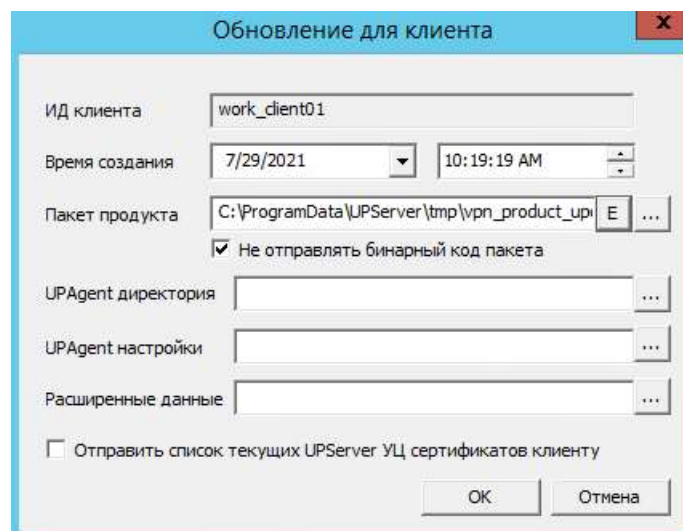


Рисунок 133

9. Обновление для client01 создано (Рисунок). Помните, что на рабочем месте клиента требуется дать разрешение на применение обновления (Рисунок 135).

Список клиентов							
IP-адрес	Bel VPN прод...	Имя	Загрузка ЦП	Кол-во туннелей	Состояние	Активные об...	Примененные обновл...
192.168.10.4	CLIENT 4.1	work_client01	-	1	Обновляется	1	1
10.0.10.110	GATE 4.5	gate1	0%	1	Активен	0	2

Рисунок 125

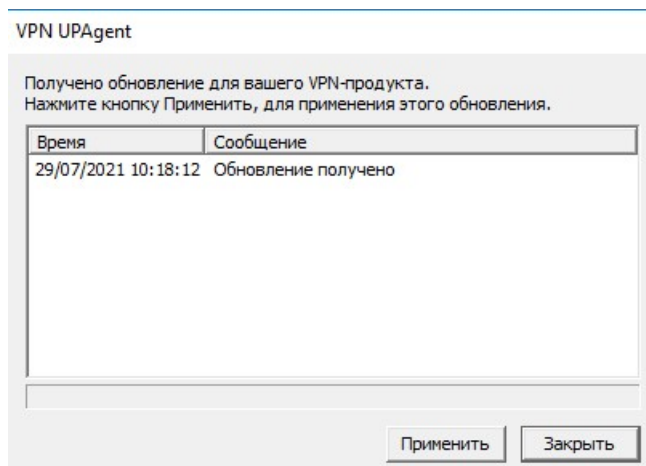


Рисунок 135

10. После нажатия на кнопку **Применить** на клиенте начнется обновление (Рисунок 136).

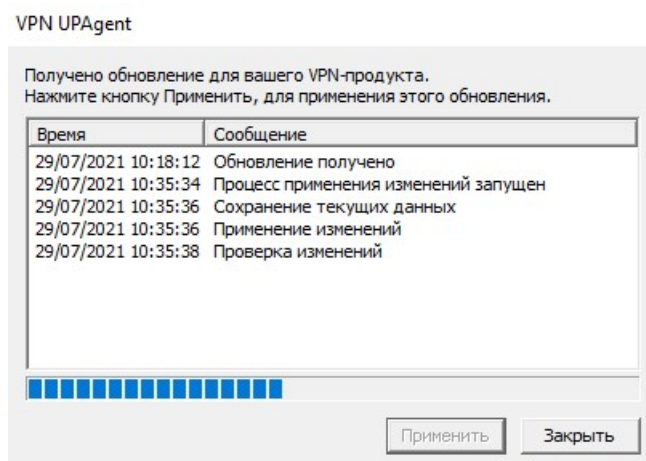


Рисунок 136.

11. После применения обновления на клиенте (Рисунок), Клиент управления пришлет на Сервер управления информацию о настройках клиента.

Список клиентов							
IP-адрес	Bel VPN прод...	Имя	Загрузка ЦП	Кол-во туннелей	Состояние	Активные об...	Примененные обновл...
192.168.10.4	CLIENT 4.1	work_client01	-	1	Активен	0	1
10.0.10.110	GATE 4.5	gate1	0%	1	Активен	0	2

Рисунок 126

В контекстном меню по команде **Показать** (Рисунок 138) откройте вкладку **Сертификаты** (Рисунок 127). Видно, что на устройстве с клиентом зарегистрировано 3 сертификата, при создании соединения с центральным шлюзом он прислал по IKE свой сертификат.

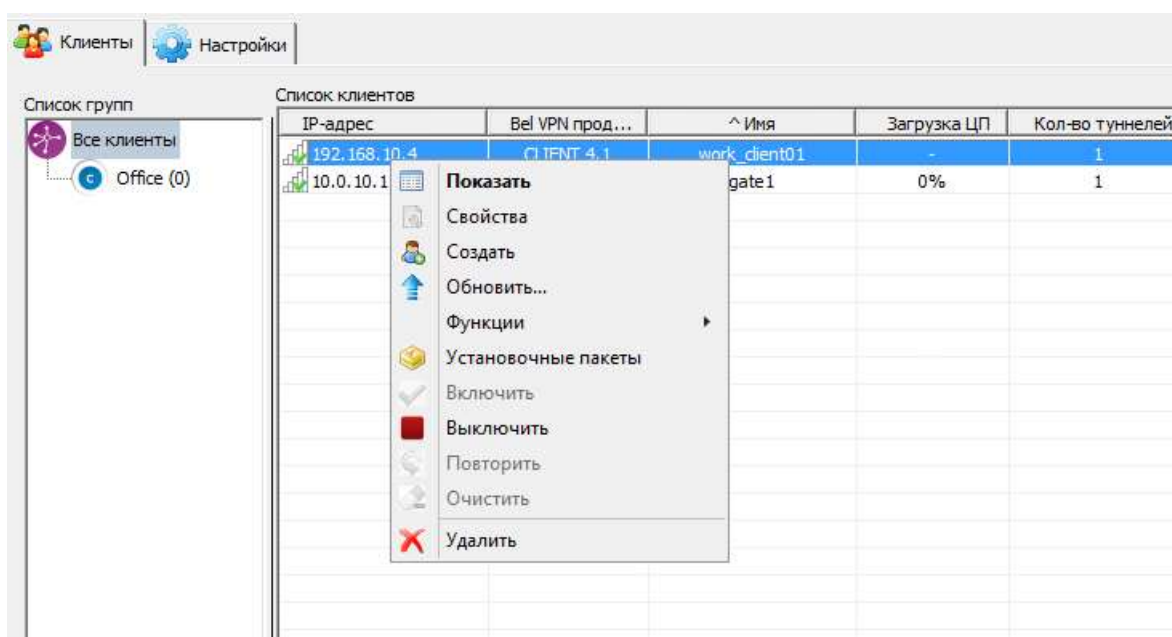


Рисунок 138

12.

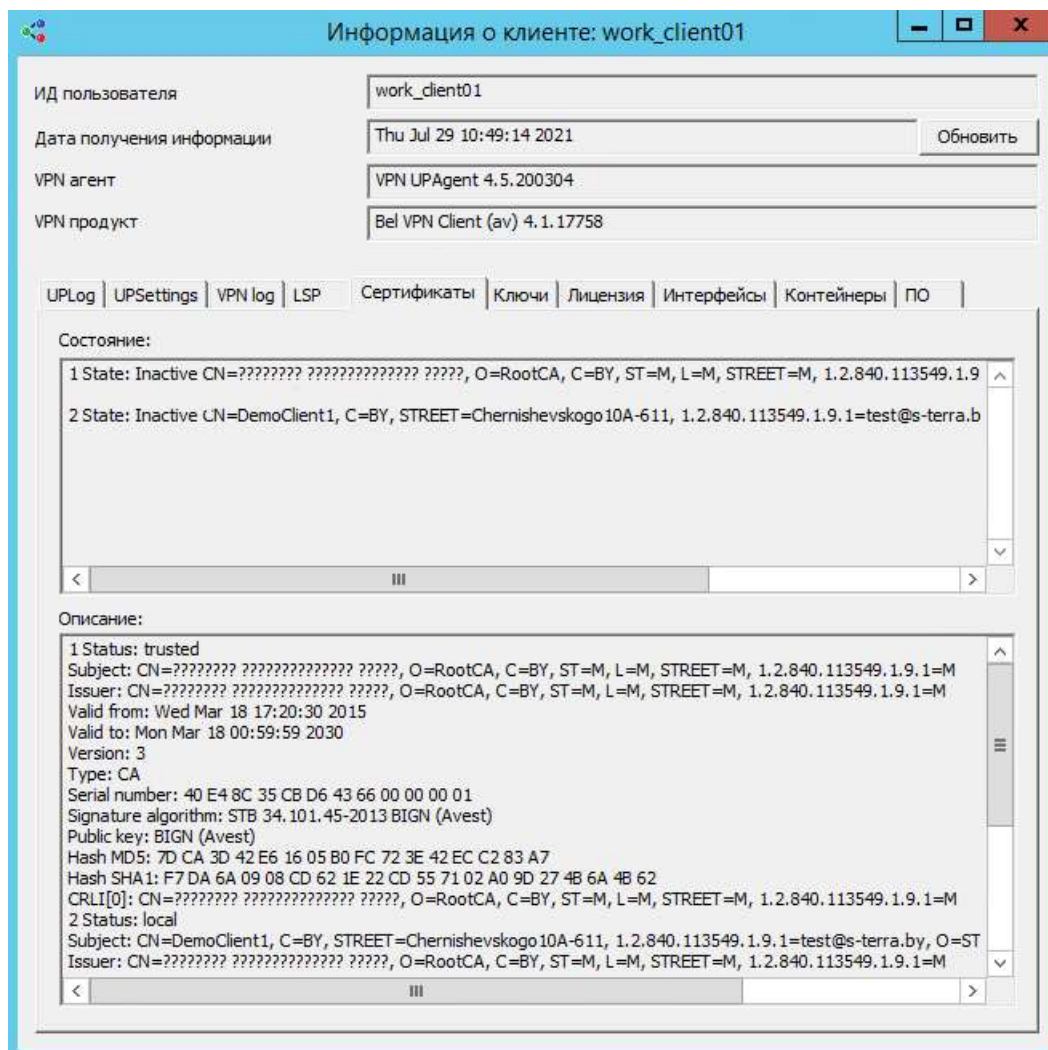


Рисунок 127

8. Информация о клиенте на Сервере управления

1. Клиент управления на управляемом устройстве собирает информацию о его настройках и передает ее на Сервер управления, где ведется мониторинг состояния и настроек всех управляемых устройств. Для выделенного клиента выберите предложения **Показать** меню **Clients** или в контекстном меню.

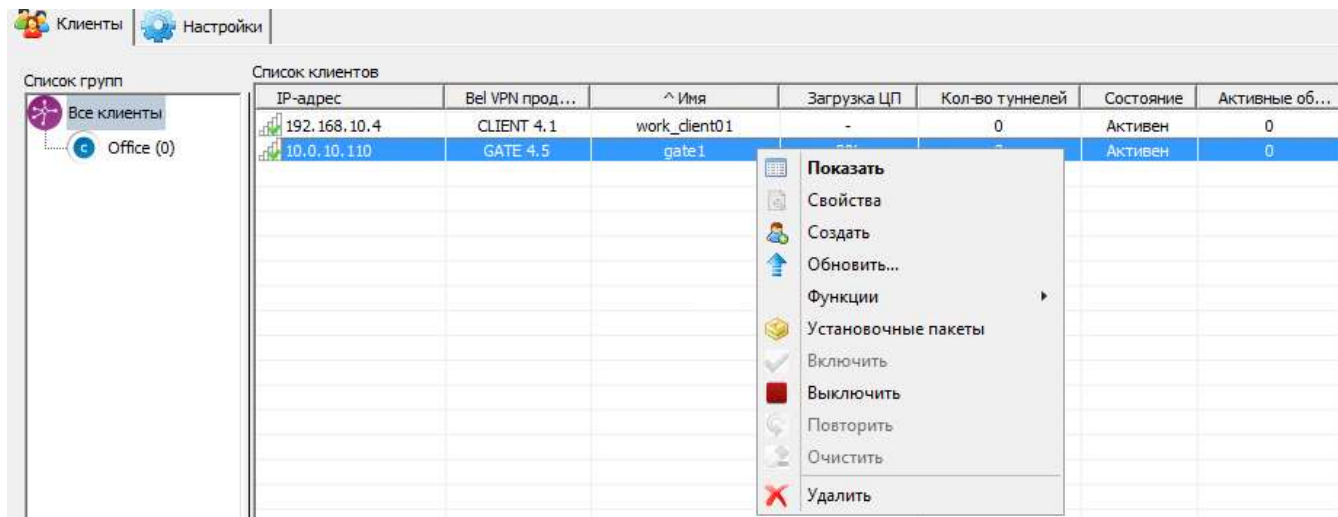


Рисунок 128

2. В результате будет выдано окно с разными вкладками (Рисунок 129), в которых отражена информация о проведенных обновлениях, настройках Клиента управления, действующей в данный момент политике безопасности на устройстве, используемых предопределенных ключах или сертификатах, об интерфейсах устройства, таблице маршрутизации и т.п.
3. Во вкладке **UPLog** ведется регистрация событий при обновлении клиента.

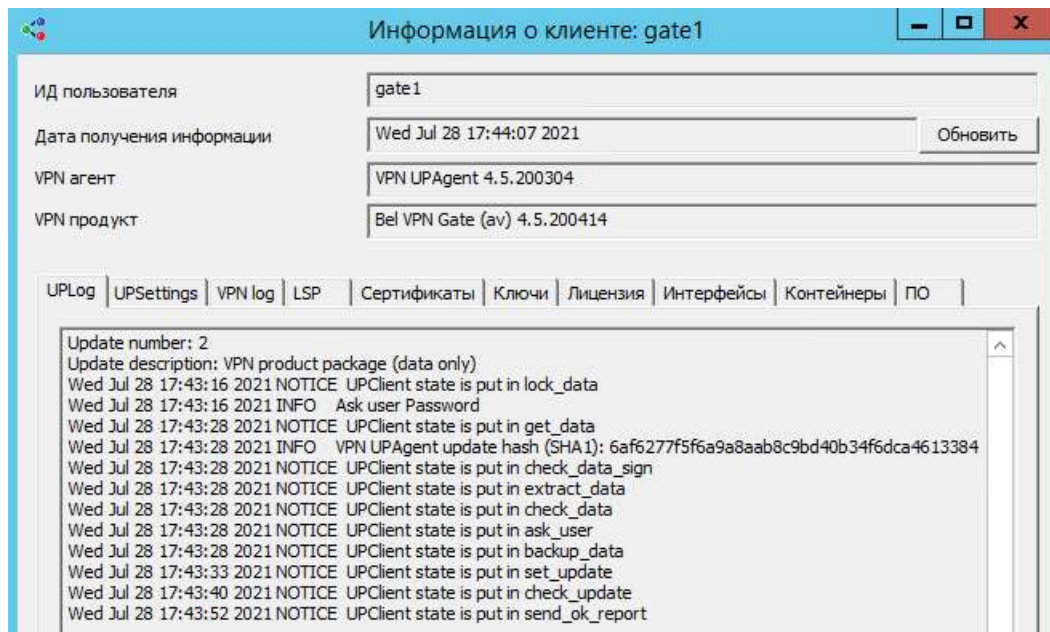


Рисунок 129

4. Во вкладке **UPSettings** (Рисунок 130) отражены настройки Клиента управления. Описание этих настроек дано в главе «[Настройки Клиента управления](#)».

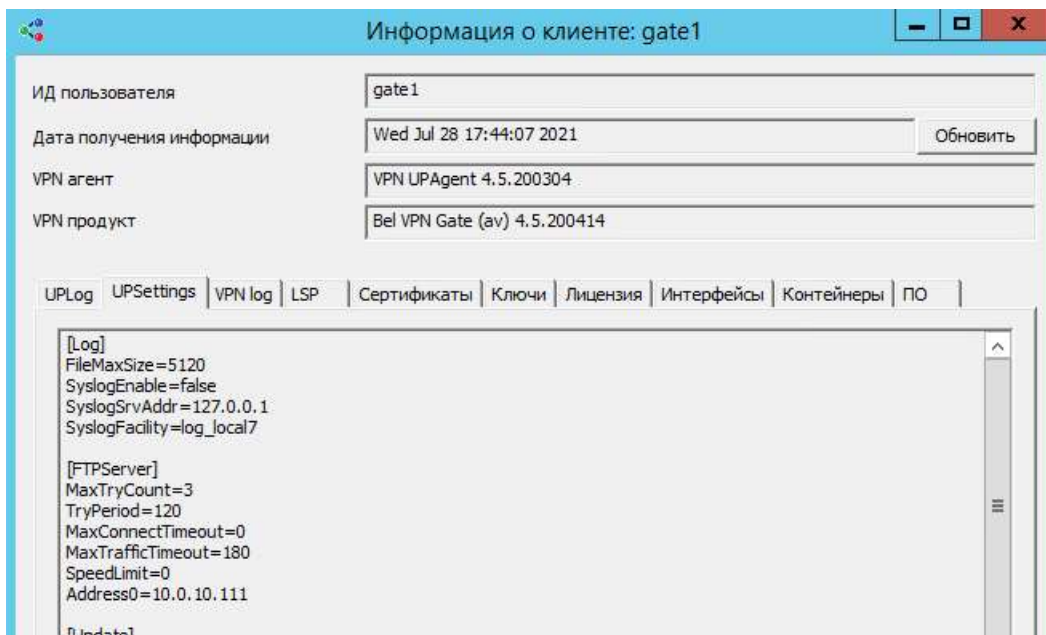


Рисунок 130

5. Во вкладке **VPN log** отражается регистрация событий, связанных с работой VPN-продукта, в частности, Bel VPN Gate, и настройки syslog-клиента.

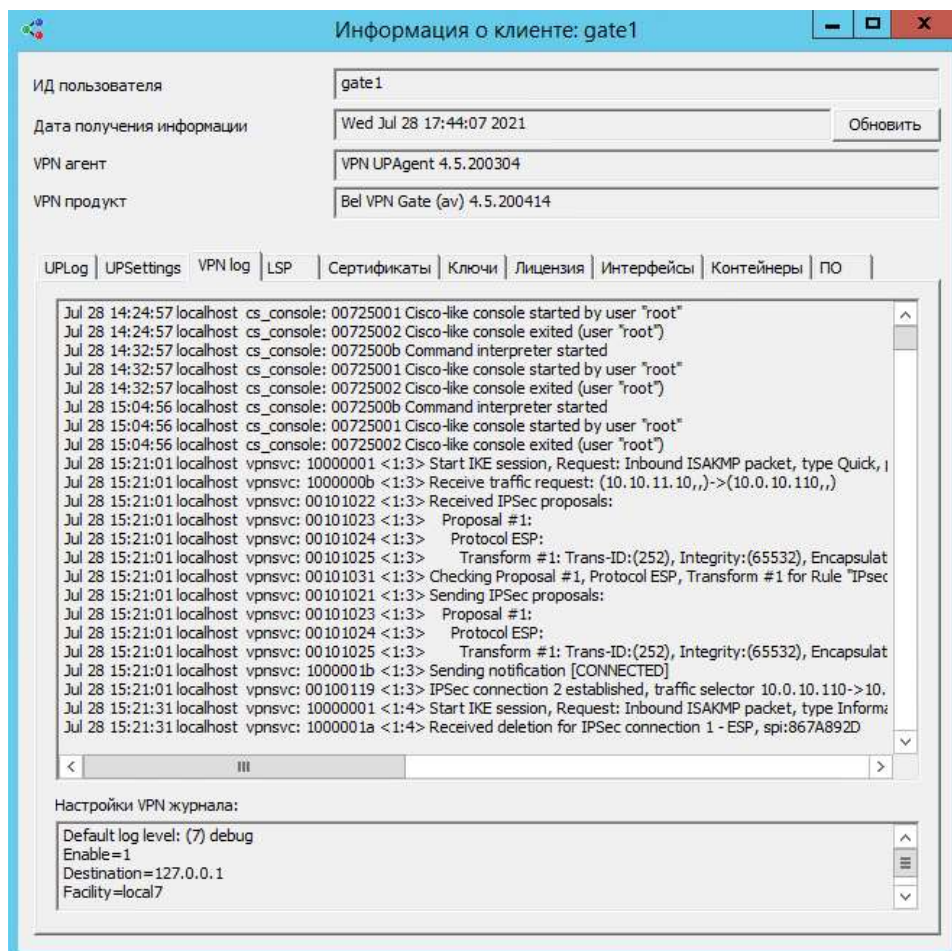


Рисунок 131

6. Вкладка **LSP** показывает загруженную политику безопасности на управляемом устройстве в виде текстового файла и в виде cisco-like конфигурации, а также политику по умолчанию (Рисунок 132).

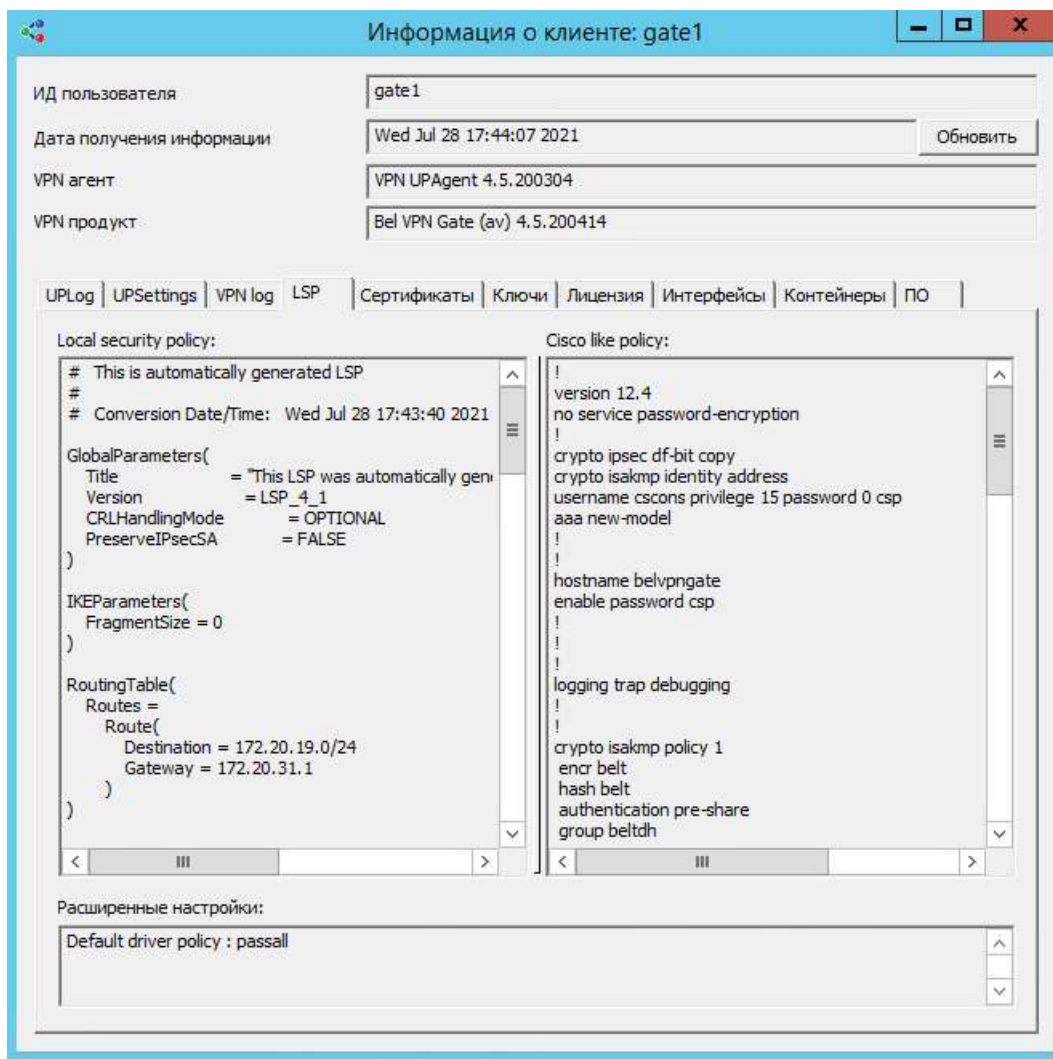


Рисунок 132

7. Вкладка **Ключи** показывает только имена предопределенных ключей, используемых при работе с партнерами, не выдавая их значений.

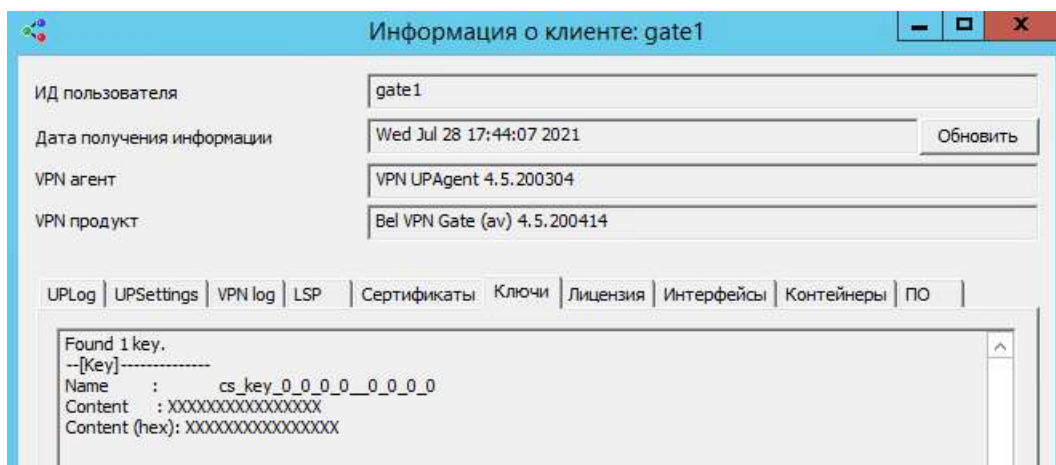


Рисунок 133

8. Вкладка **Сертификаты** показывает все зарегистрированные в продукте Bel VPN Gate сертификаты и их статус.

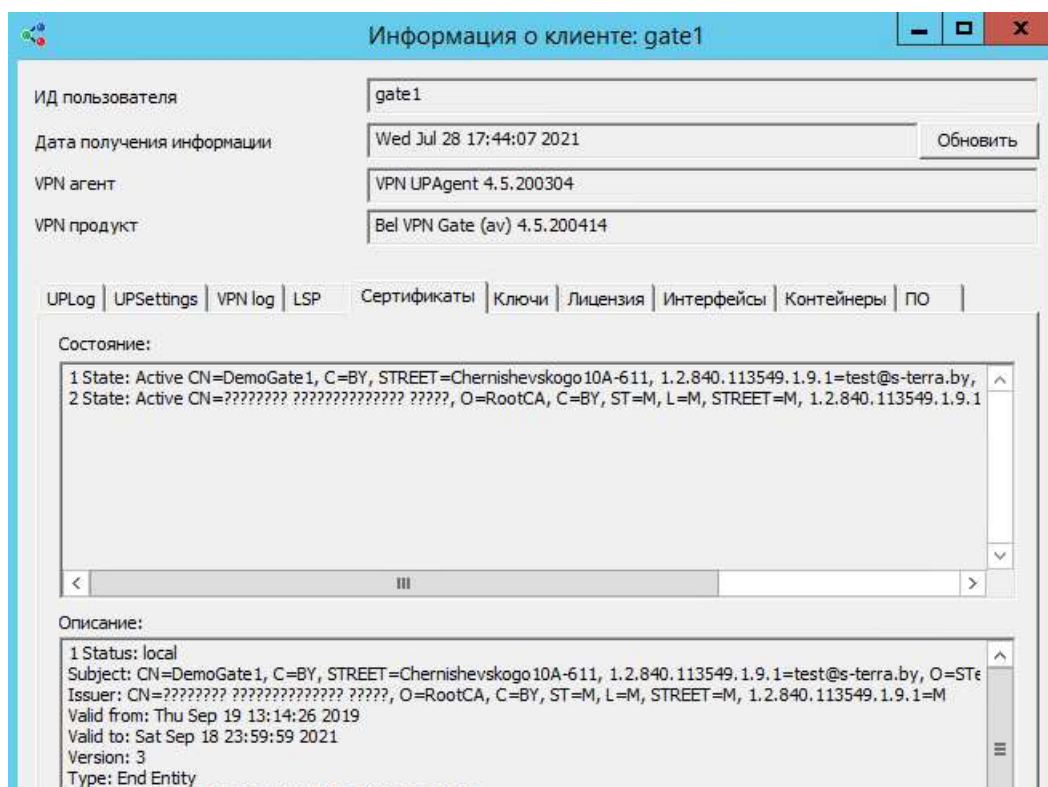


Рисунок 134

9. Во вкладке **Лицензия** отражена информация о Лицензиях на продукты.



Рисунок 135

10. Вкладка **Интерфейсы** содержит информацию обо всех сетевых интерфейсах управляемого устройства, маршрутах, а раздел Driver settings показывает настройки IPsec драйвера (для продуктов Bel VPN Gate 4.5/4.1, Bel VPN Client-P 4.1).

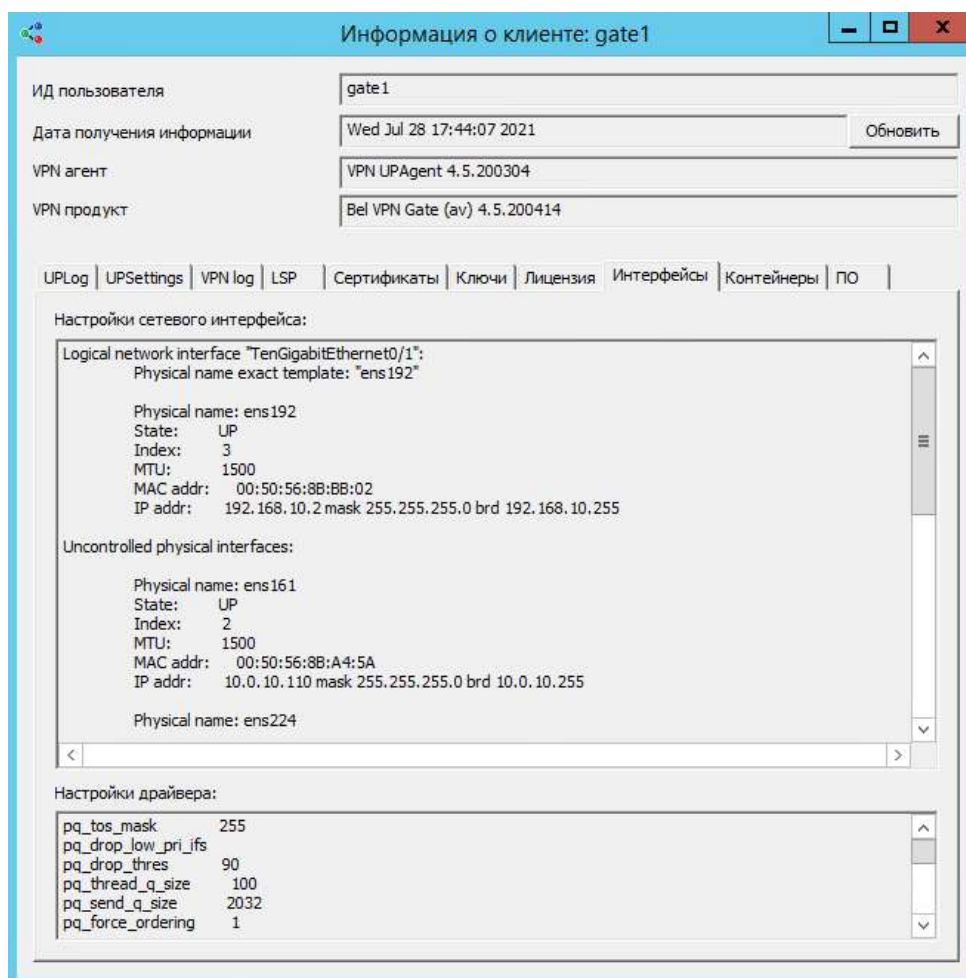


Рисунок 136

11. Вкладка **Контейнеры** показывает созданные на управляемом устройстве запросы на сертификаты, используемые и неиспользуемые контейнеры с ключевыми парами.

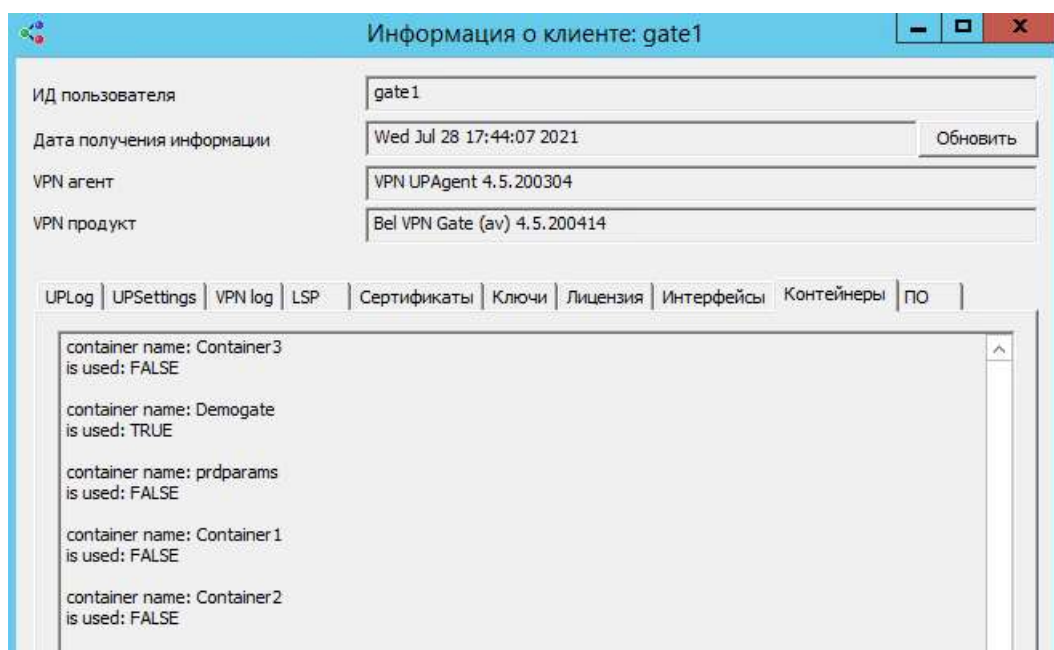


Рисунок 137

12. Вкладка **ПО** резервирована для будущего использования.

9. Отправка команд на выполнение управляемому устройству

Описанную выше задачу для выбранного управляемого устройства можно выполнить через вкладку **Команды**, доступную в информационной панели, отображающейся при нажатии на кнопку **Детально**, находясь во вкладке **Клиенты**.

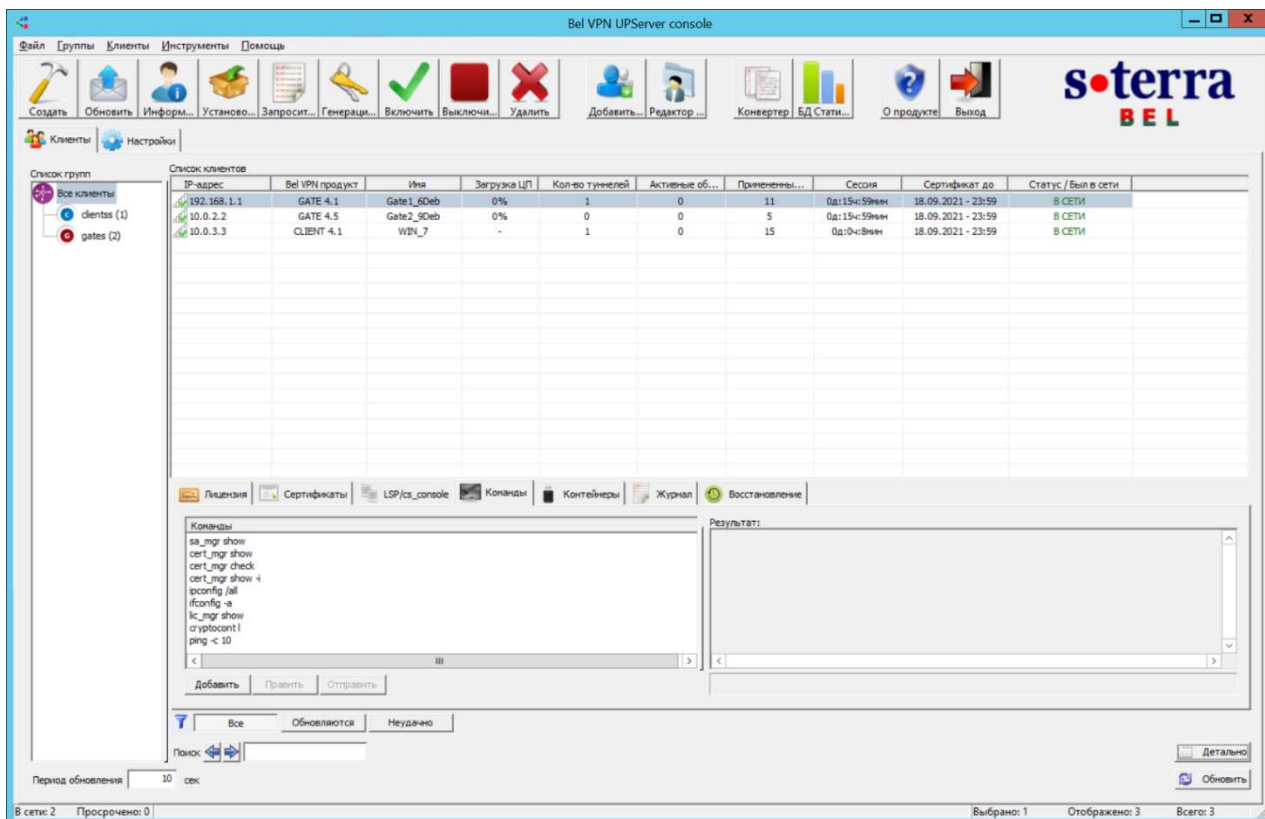


Рисунок 1387

Для добавления новой команды в окне **Команды** выберите **Добавить**, в открывшемся диалоговом окне **Добавить команду** в поле **Команда:** введите команду для выполнения на управляемом устройстве и выберите **Добавить**.

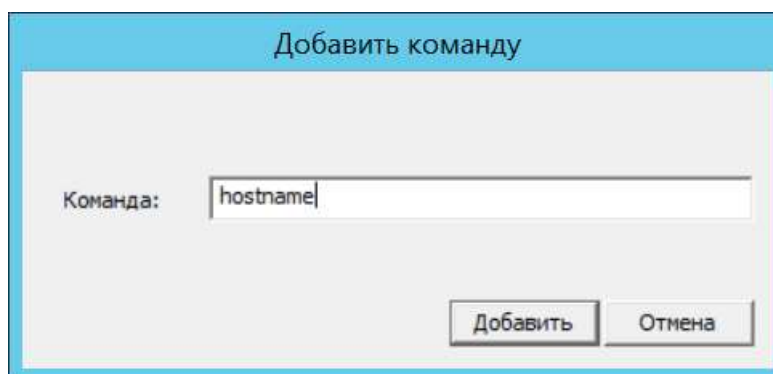


Рисунок 168

Новая команда отобразится в списке **Команды**, выберите ее и нажмите **Отправить**.

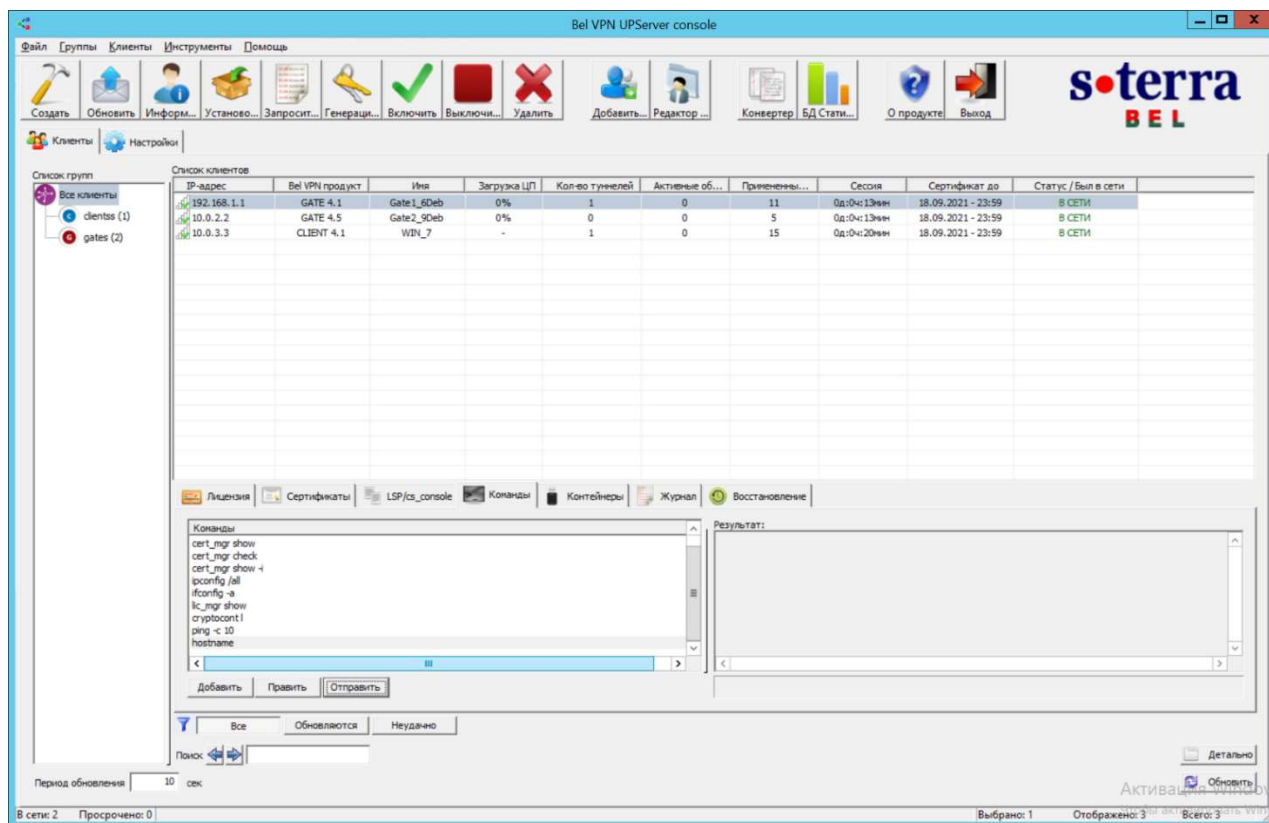


Рисунок 169

В появившемся диалоговом окне **Предупреждение** выберите **OK**.

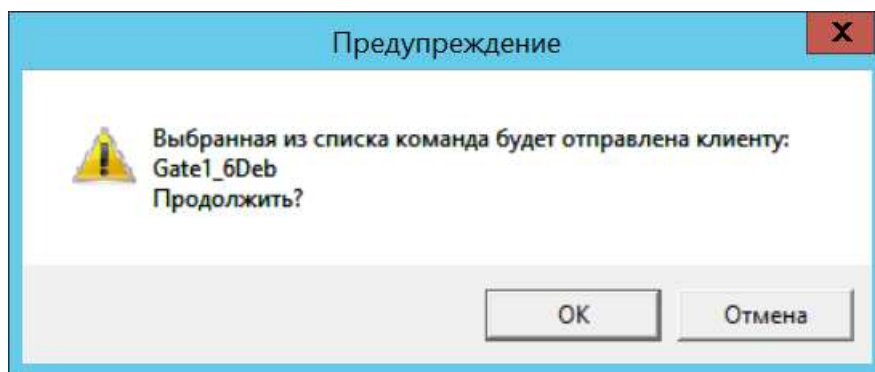


Рисунок 170

В результате, для выбранного клиента, будет сформировано расширенное обновление с выбранной командой. Количество активных обновлений изменится на 1. Индикатор выполнения, расположенный под окном **Результат**, отображает ход выполнения данного обновления.

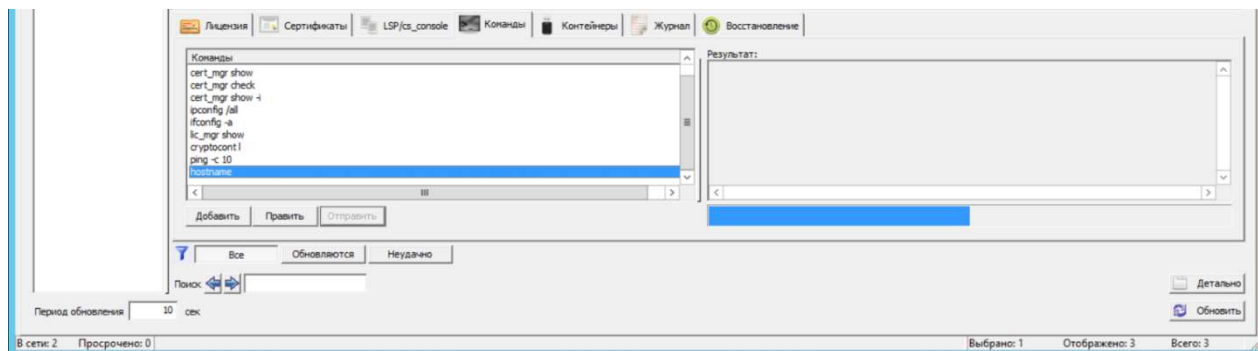


Рисунок 171

По мере полного заполнения индикатора выполнения в окне **Результат:** появится результат выполнения команды на управляемом устройстве.

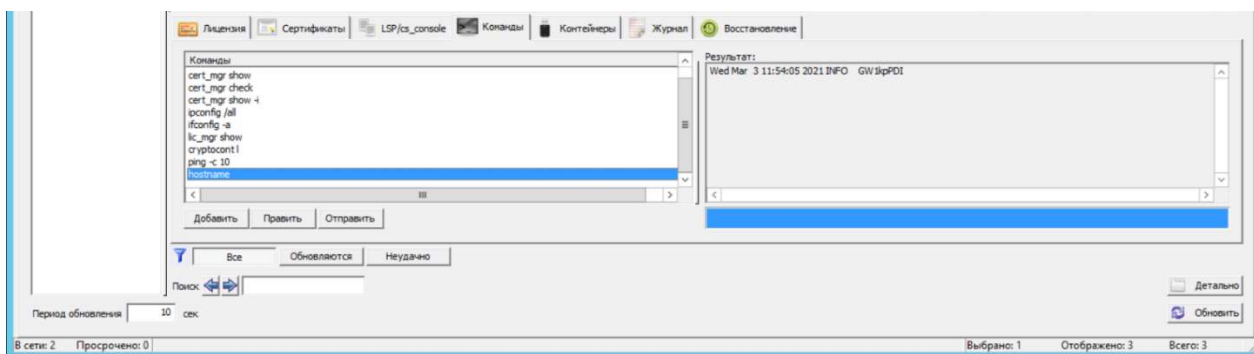


Рисунок 172

В случае успешного выполнения команды на управляемом устройстве количество примененных обновлений увеличится на один, а в окне **Результат** появится результат ее выполнения. В случае неудачного выполнения команды, в столбце **Состояние** списка клиентов появится запись **Неудачно**, а в окне Результат будут отражены сообщения об ошибке.

Для команд, содержащих внутри себя, переменные значения необходимо явно указывать последние перед отправкой команды.

Например, необходимо отправить команду **ping 192.168.1.50** выбранному управляемому устройству: Выберите соответствующую команду из списка команд и выберите **Править**.

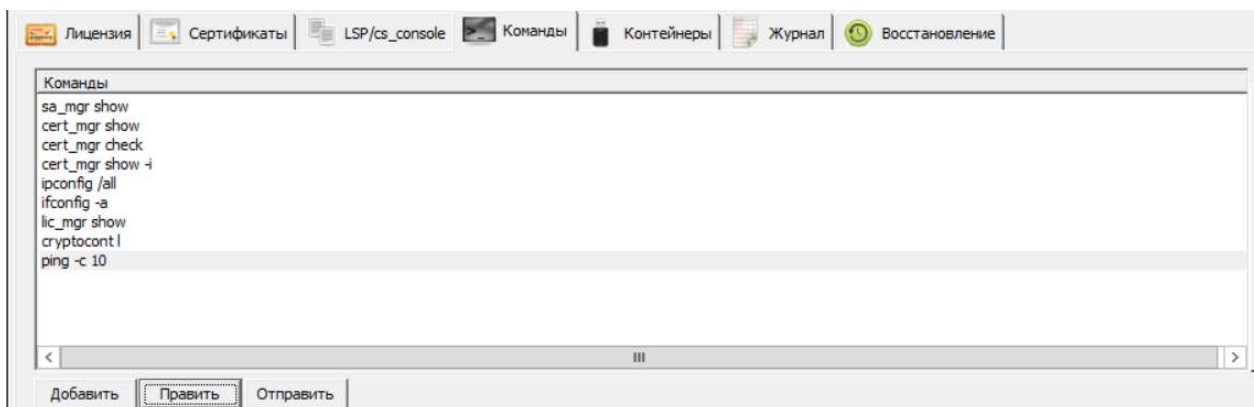


Рисунок 173

В появившемся диалоговом окне **Изменение команды**, в поле **Команда:** скорректируйте имеющееся значение и выберите **Сохранить**.

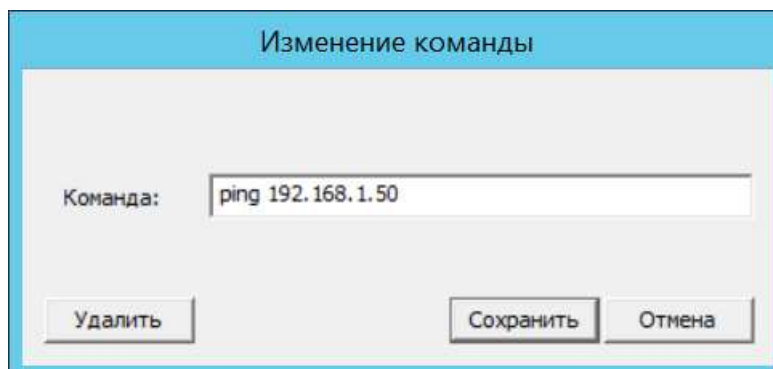


Рисунок 174

Скорректированная команда отобразится в списке команд. Выберите ее и **Отправить**.

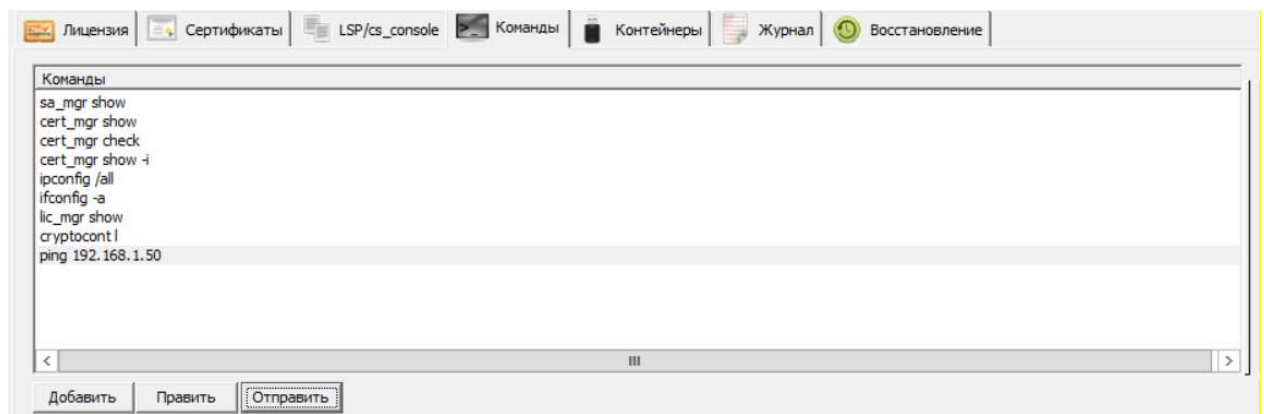


Рисунок 175

Для удаления команды из списка выберите **Править** и **Удалить**.

10. Восстановление конфигурации управляемого устройства из резервной копии

Список резервных копий выбранного управляемого устройства доступен во вкладке **Восстановление**, доступной в информационной панели, отображающейся при нажатии на кнопку **Детально**, находясь во вкладке **Клиенты**.

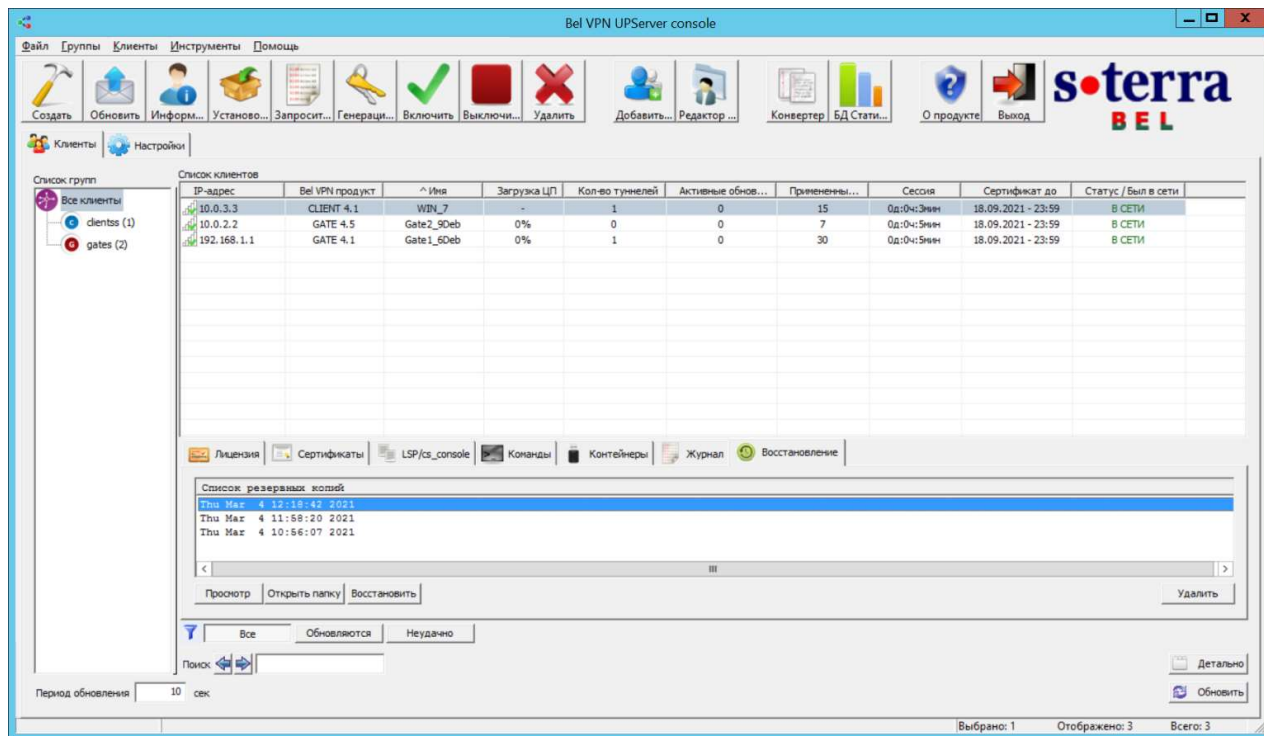


Рисунок 176

Список резервных копий состоит из записей, расположенных в обратном хронологическом порядке, представляющих дату и время создания резервной копии. Резервные копии создаются автоматически, всякий раз когда успешно проводится обновление управляемого устройства, содержащее в себе изменение VPN-конфигурации (isp/cisco-like).

Для доступа к расположению файла с резервной копией выберите соответствующую запись из списка и выберите **Открыть папку**.

Для удаления резервной копии выберите соответствующую запись из списка и выберите **Удалить**.

Для просмотра конфигурации, содержащейся в резервной копии выберите соответствующую запись из списка и выберите **Просмотр**. Появится диалоговое окно утилиты **VPN data maker** с отображаемой конфигурацией выбранной резервной копии.

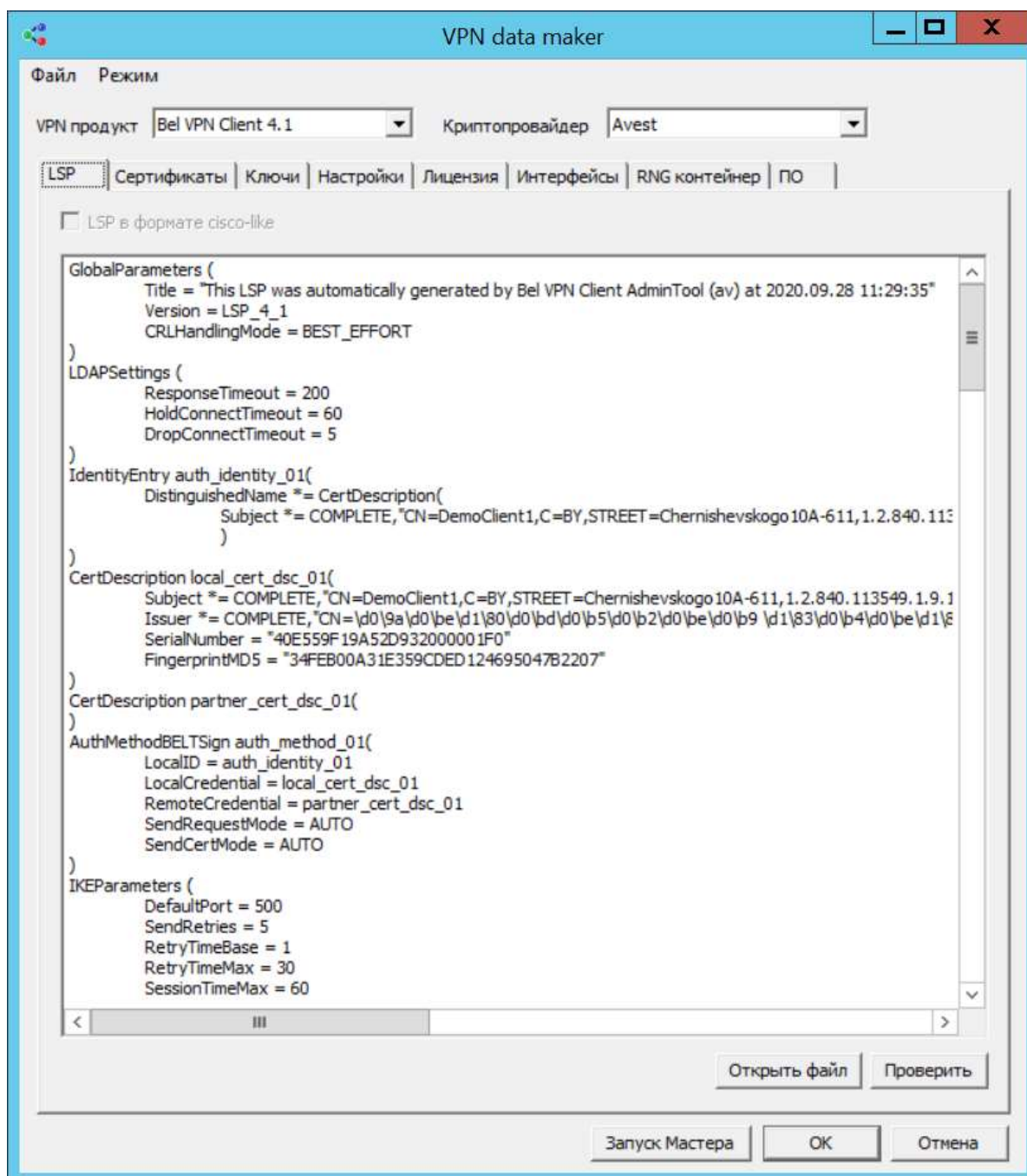


Рисунок 177

Для восстановления управляемого устройства из резервной копии выберите соответствующую запись из списка и выберите **Восстановить**. В появившемся окне с предупреждением выберите **OK**.

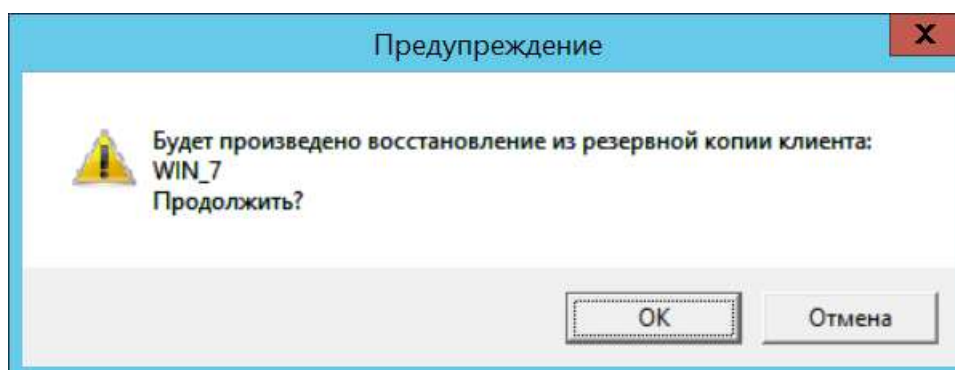


Рисунок 178

Будет сформирован пакет обновления для выбранного управляемого устройства с конфигурацией, загруженной из выбранной резервной копии. Количество активных обновлений увеличится на один, а управляемое устройство перейдет в состояние **Ожидает**. Процесс восстановления успешно завершен в случае успешного применения обновления.



Для восстановления управляемого устройства через Сервер управления на управляемом устройстве должен быть установлен Клиент управления (UPagent). Управляемое устройство должно быть доступно Серверу управления.

11. Сценарий включения в систему управления работающего устройства с Bel VPN Gate 4.5/4.1/Client-P 4.1

Имеется устройство с установленной ОС и продуктом Bel VPN Gate 4.5/4.1/Client-P 4.1, которое настроено сторонними методами и включено, например, в подсеть 192.168.10.0/24 с адресом 192.168.10.2. Устройство настроено так, что может создавать защищенные соединения с партнерами в сети 10.0.0.0/16, в которой также размещен Сервер управления. Данный сценарий описывает включение работающего устройства в систему управления с использованием Сервера управления.

1. На Сервере управления создайте учетную запись клиента для работающего устройства, например, с установленным продуктом Bel VPN Gate 4.5/4.1 - work_gate01.

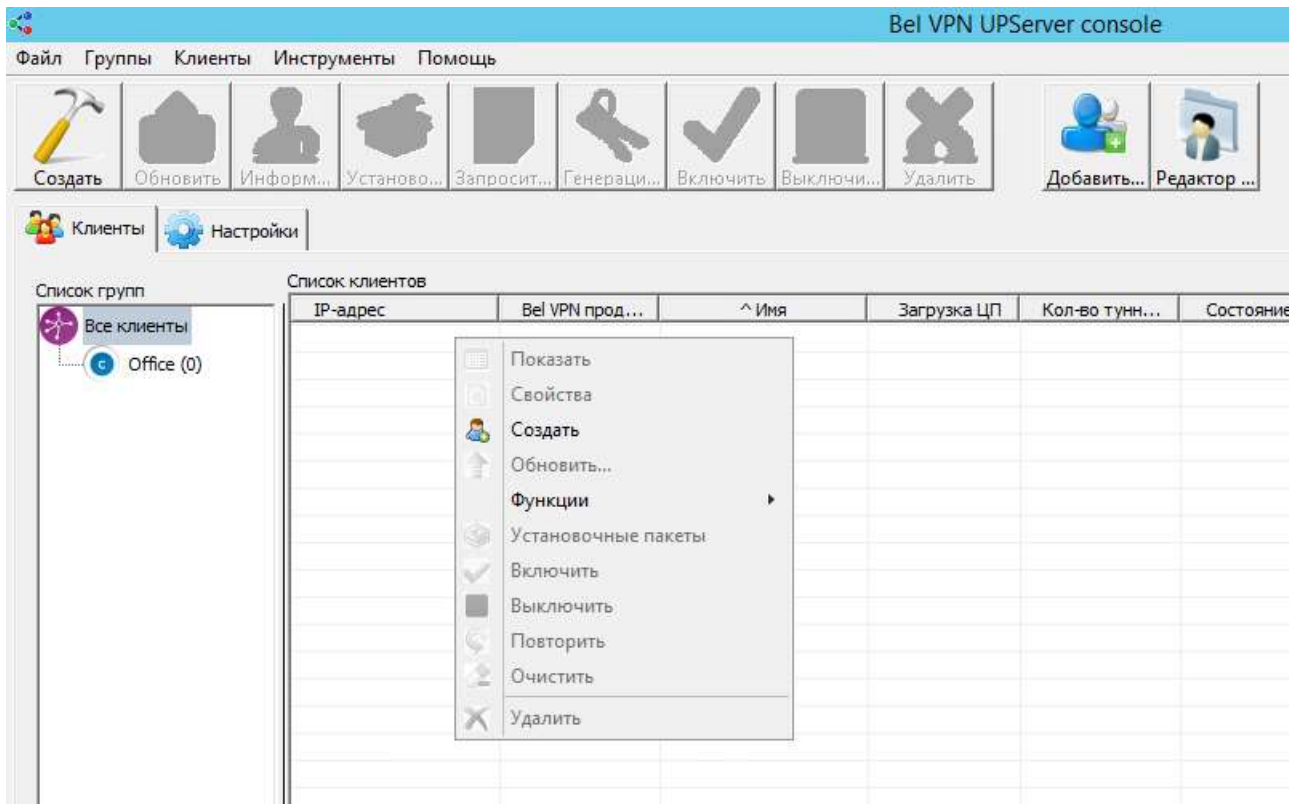


Рисунок 139

1. Введите уникальное имя клиента и нажмите кнопку **E**.

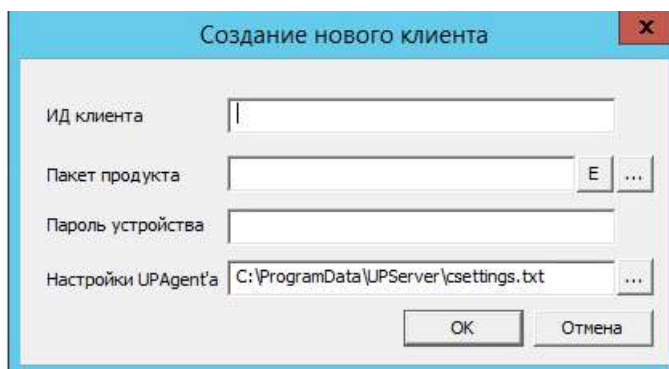


Рисунок 140

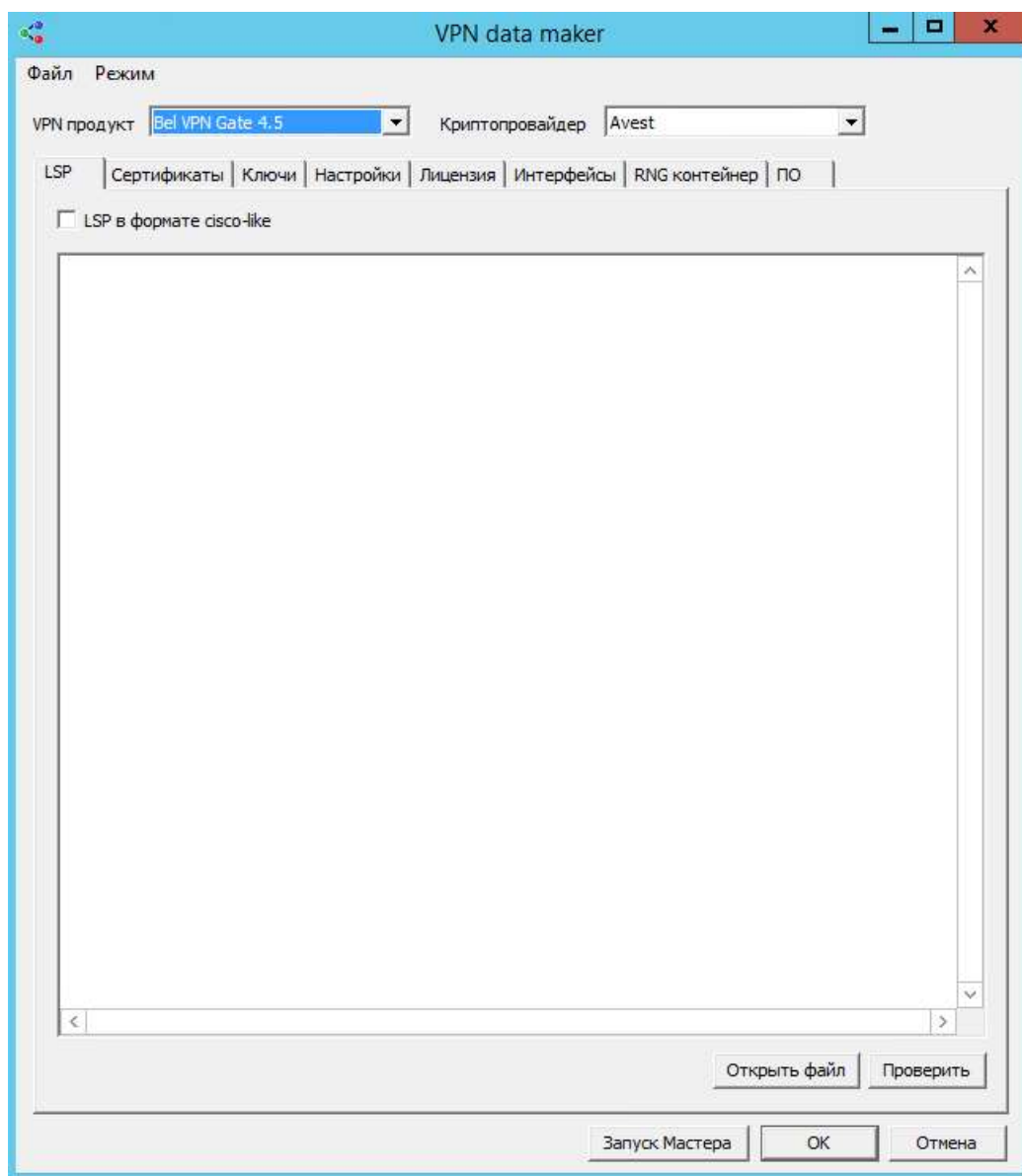


Рисунок 141

2. Выберите продукт, установленный на работающем устройстве, Avest и нажмите кнопку **OK**.
3. Создается фиктивный проект, настройки на устройстве уже заданы, поэтому в предупреждении нажмите кнопку **OK**.

Рисунок 142

4. В следующем предупреждении также нажмите **OK**.

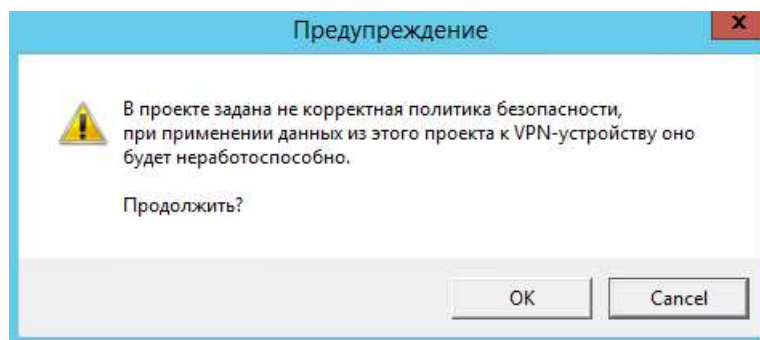


Рисунок 143

5. В окне создания клиента нажмите **OK**.

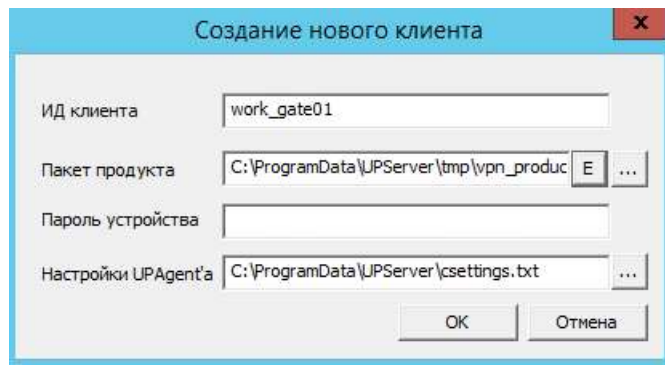


Рисунок 144

6. Для нового клиента в контекстном меню выберите операцию **Enable**, а затем **Get packages** для создания скриптов.

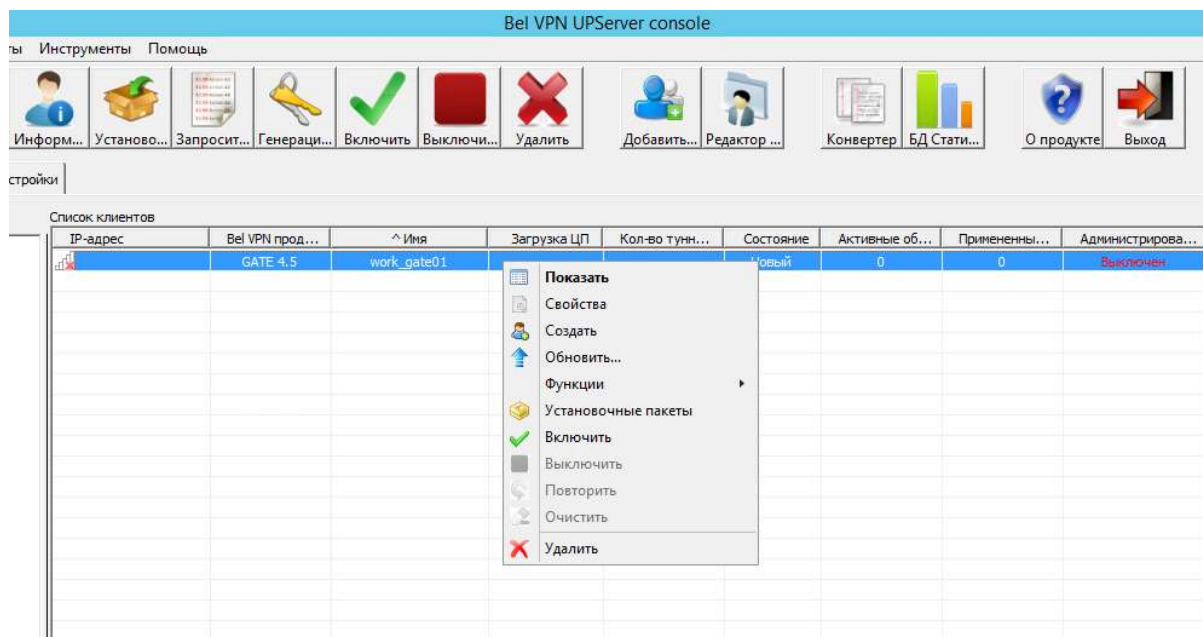


Рисунок 145

7. Выберите каталог для сохранения настроечных скриптов и нажмите **OK**.

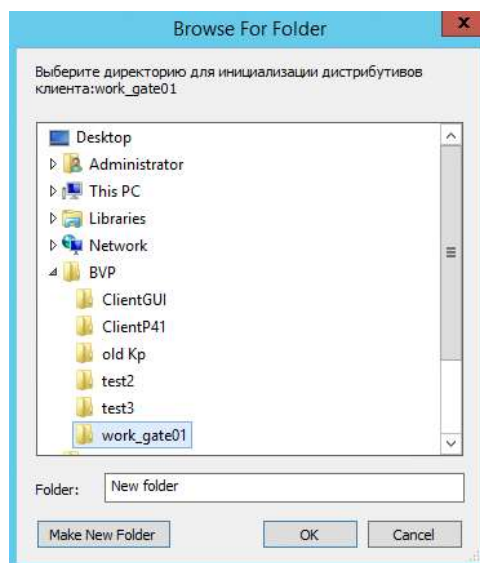


Рисунок 146

8. Два скрипта созданы. Требуется только один скрипт `setup_upagent.sh` для инсталляции (инициализации) Клиента управления, продукт Bel VPN Gate уже настроен.

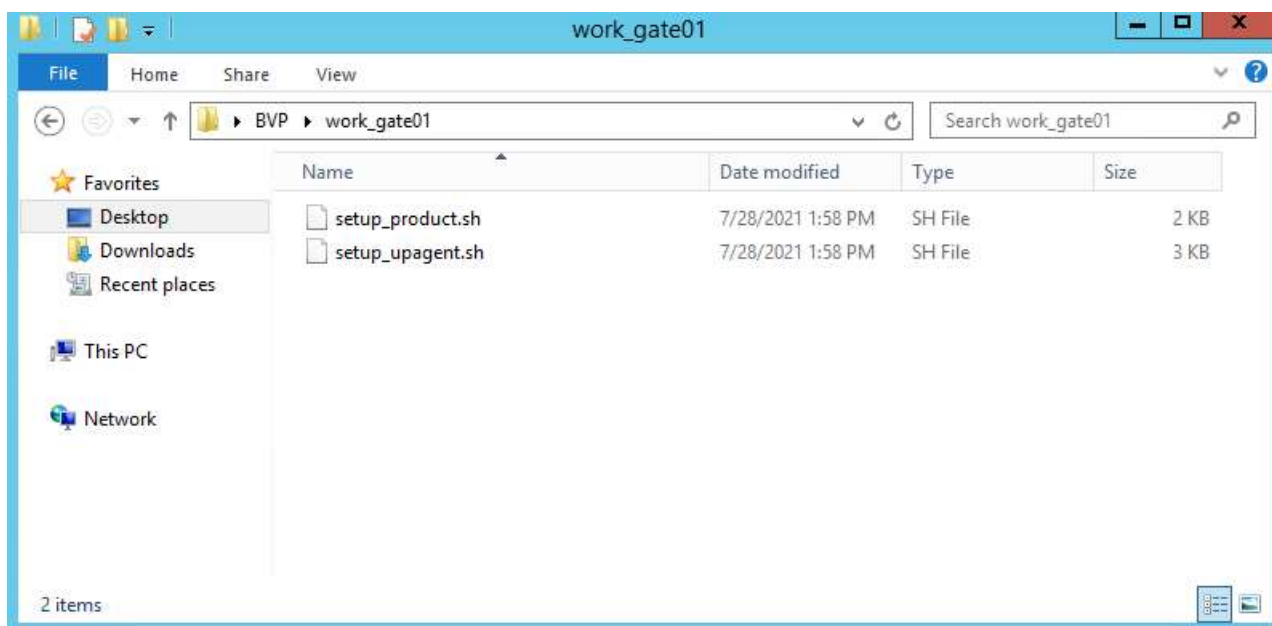


Рисунок 147

9. Доставьте скрипт `setup_upagent.sh` на работающий шлюз с адресом 192.168.10.2, например, с использованием утилиты `pscp` в предварительно созданный каталог `/tmp`:

```
pscp setup_upagent.sh root@192.168.10.2:/tmp
```

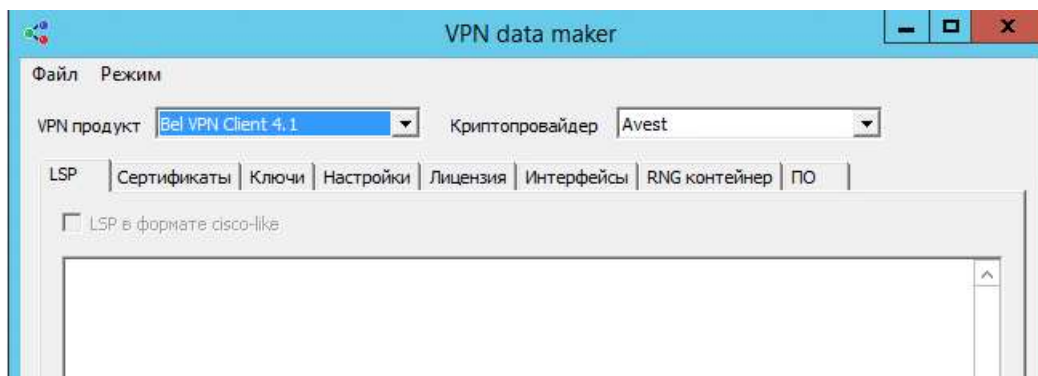
10. Измените права доступа к скрипту, выполнив локально на шлюзе команду:

```
chmod +x /tmp/setup_upagent.sh
```

11. Запустите локально скрипт на выполнение:

```
/tmp/setup_upagent.sh
```

Аналогично выполняется настройка и для клиента Bel VPN Client-P 4.1, за исключением п.2, где в поле VPN продукт необходимо выбрать Bel VPN Client 4.1.



После успешной инициализации Клиента управления, на управляемом устройстве будет запущен процесс сбора информации о его текущей конфигурации, по окончании которого, на Сервер управления будет выслан пакет обновления с собранной информацией.

Когда управляемое устройство станет доступно (**В СЕТИ**) на Сервере управления, а пакет обновления от клиента управления получен, Сервер управления начнет процесс обновления для управляемого устройства, тем самым синхронизируя информацию о его конфигурации.

После успешного завершения процесса обновления Сервер управления располагает достоверными данными о работающем устройстве. При внесении изменений в конфигурацию управляемого устройства сторонними методами (локально), синхронизация данных производится таким же образом, автоматически и без участия администратора Сервера управления.

12. Групповые операции на Сервере управления

В таблице на Сервере управления можно выделить несколько клиентов и применить к ним операции меню **Клиенты**, за исключением **Создать** и **Установочные пакеты**.

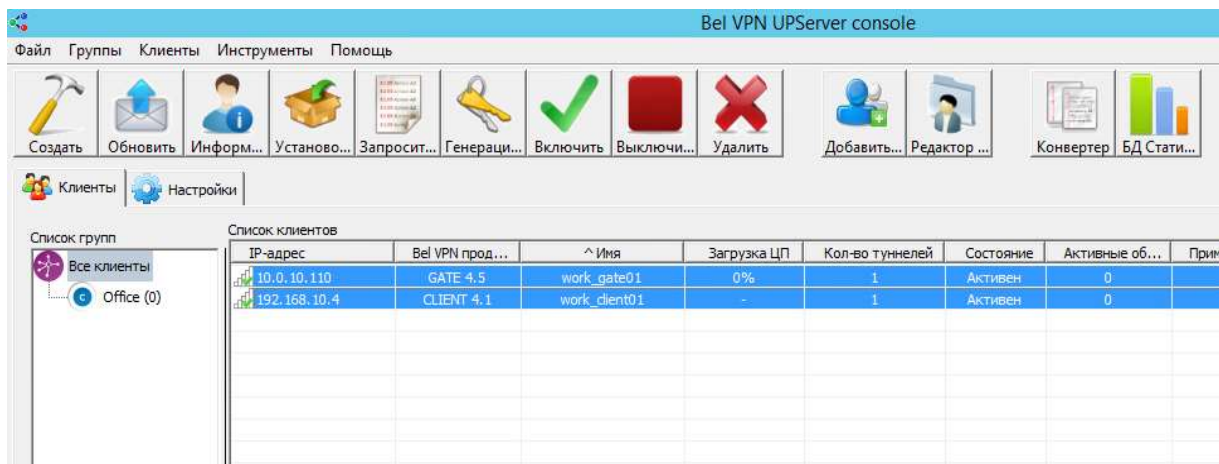


Рисунок 148

Каждый клиент на Сервере управления создается отдельно и для каждого клиента скрипты Клиента управления и Bel VPN Gate 4.5/4.1/Client-P 4.1 также создаются отдельно.

Остальные операции могут применяться к любой выделенной группе клиентов.

Подробно операции меню **Клиенты** описаны в разделе [«Меню Клиенты»](#) главы [«Описание интерфейса Сервера управления»](#).

При выборе операции **Обновить** для нескольких клиентов будут созданы одинаковые обновления. После применения этих обновлений клиенты будут иметь, например, одинаковую политику безопасности, одинаковый список predeterminedных ключей, свой локальный сертификат. Если в базе продукта лежит список локальных сертификатов, клиент не сможет создать соединение с партнером, так как будет использоваться первый сертификат списка. Чтобы избежать таких проблем с локальными сертификатами, используйте **шаблон проекта**, при котором происходит отбор локального сертификата из списка для каждого клиента при обновлении. Такой отбор локального сертификата возможен только при наличии на управляемом устройстве запроса на локальный сертификат, который и будет использоваться для поиска нужного сертификата из списка.

12.1. Создание шаблона проекта

1. Не выделяя в таблице клиентов, в меню **Инструменты** выберите предложение **VPN data maker**.

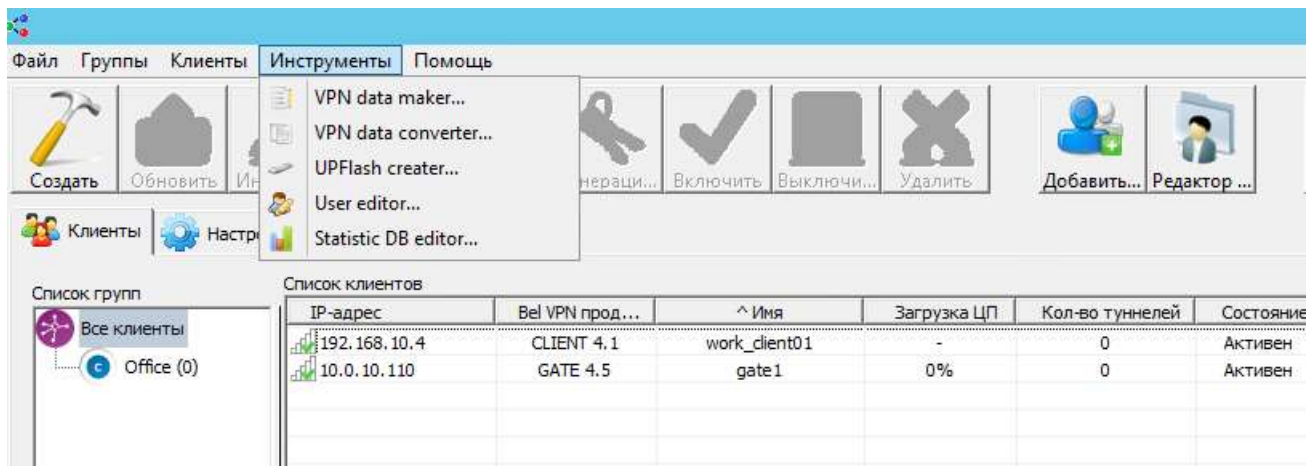


Рисунок 149

- В открывшемся окне **VPN data maker** заполните необходимые вкладки для настройки продукта Bel VPN Gate 4.5/4.1/Client-P 4.1.

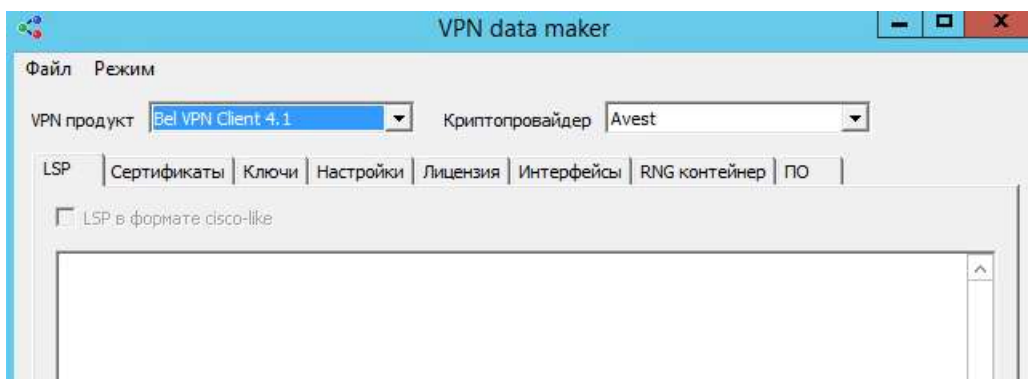


Рисунок 150

- Во вкладке **Сертификаты** можно задать **список локальных сертификатов**, для которых были созданы запросы на клиентах, список сертификатов партнеров, список удаленных сертификатов (CRL).

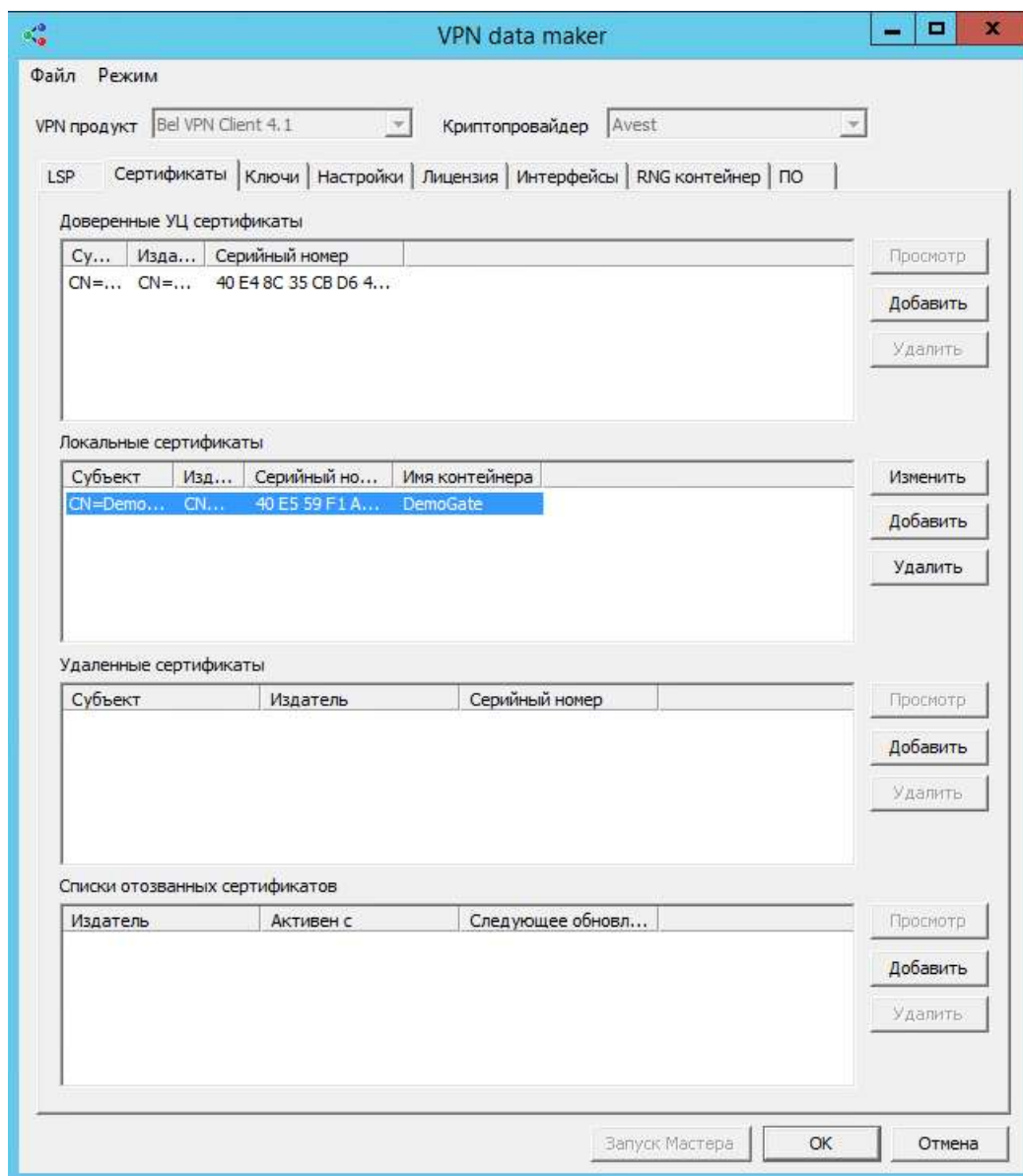


Рисунок 151

При задании локальных сертификатов появляется окно **Описание сертификата**, в котором надо указать имя контейнера и пароль к нему на управляемом устройстве. В этих двух полях можно указать значение «*», которое при применении обновления будет заменено на действительные значения.

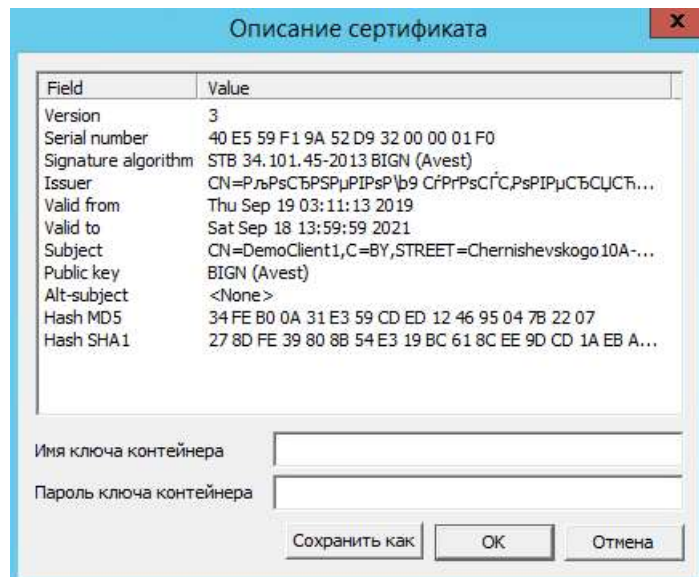


Рисунок 152

4. Заполнив вкладки, перейдите в режим шаблона проекта, выбрав в меню **Режим** предложение **Включить режим шаблона**.

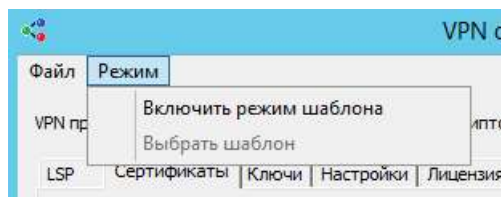


Рисунок 153

5. Затем в меню **Режим** выберите предложение **Выбрать шаблон** (это предложение доступно только в режиме шаблона проекта).

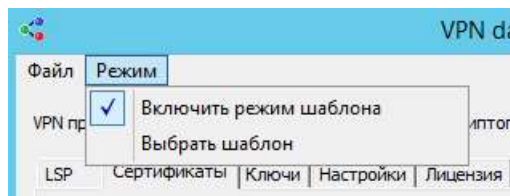


Рисунок 154

6. Появилось окно **Типы данных обновления** со списком данных, которые могут входить в шаблон проекта. Пометьте флажком данные, которые будут входить в шаблон. При применении обновления, созданного с использованием шаблона, только входящие в него данные будут изменяться на клиенте.

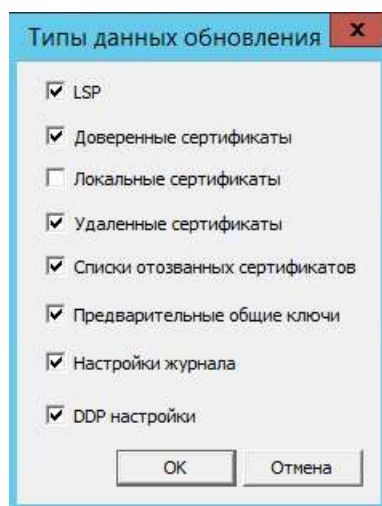


Рисунок 155

Состав окна **Типы данных обновления**:

LSP – при установке флажка локальная политика безопасности, указанная во вкладке **LSP**, будет входить в состав шаблона проекта

Доверенные сертификаты – при установке флажка все доверенные СА-сертификаты, указанные во вкладке **Сертификаты**, будут входить в шаблон проекта

Локальные сертификаты – при установке флажка все локальные сертификаты, указанные во вкладке **Сертификаты** в разделе **Локальные сертификаты**, будут входить в шаблон проекта

Удаленные сертификаты – при установке флажка все сертификаты партнеров, указанные во вкладке **Сертификаты** в разделе **Удаленные сертификаты**, будут входить в шаблон проекта

Списки отозванных сертификатов – при установке флажка все списки отозванных сертификатов, указанные во вкладке **Сертификаты** в разделе **Списки отозванных сертификатов**, будут входить в шаблон проекта

Предварительные общие ключи – при установке флажка все предопределенные ключи, указанные во вкладке **Ключи**, будут входить в состав шаблона проекта

Настройки журнала – при установке флажка настройки протоколирования, указанные во вкладке **Настройки**, будут входить в шаблон проекта

DDP настройки - при установке флажка политика DDP, указанная во вкладке **Настройки**, будет входить в шаблон проекта.

Выбрав данные, которые будут входить в шаблон, нажмите кнопку **OK**.

7. Заполнив ранее вкладки для этих данных, сохраните созданный шаблон в файл, используя предложение **Сохранить как** меню **Файл**.

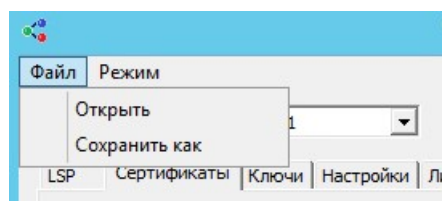


Рисунок 156

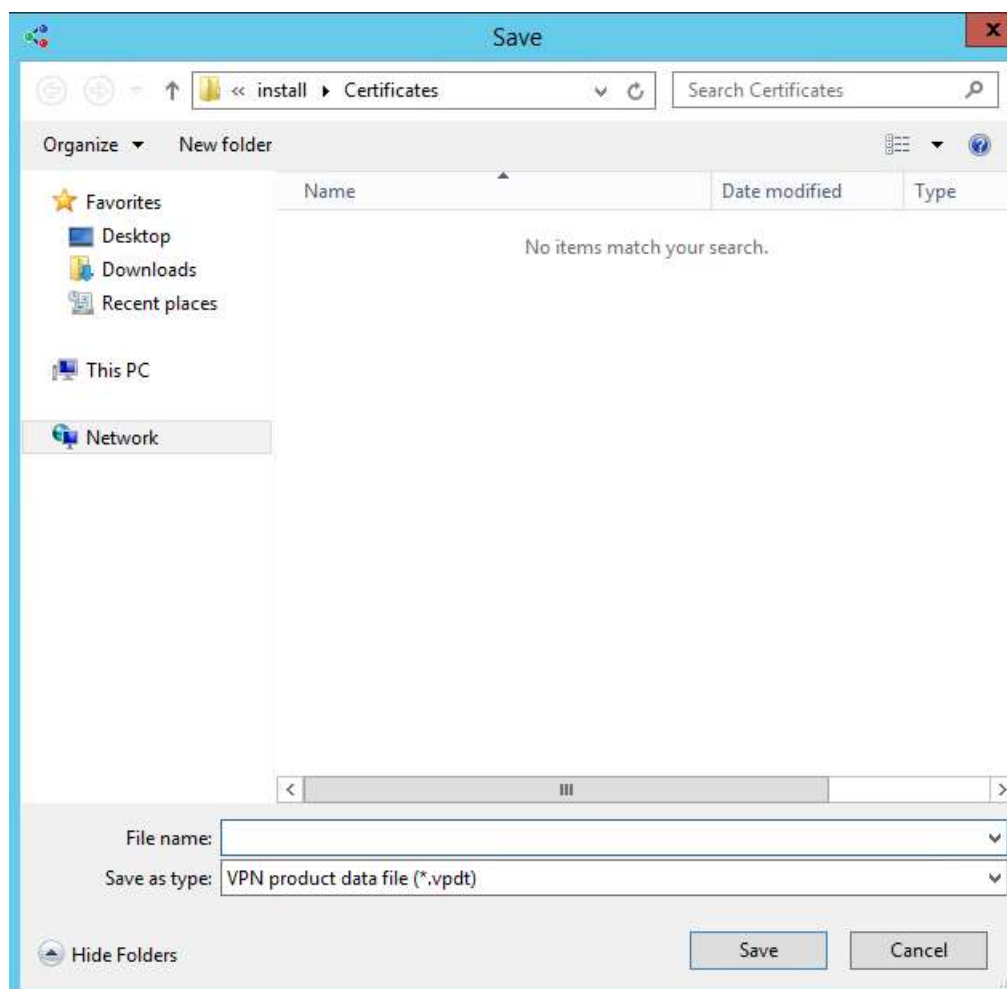


Рисунок 157

12.2. Использование шаблона проекта

Шаблон проекта удобно использовать при создании обновления сразу для нескольких клиентов.

1. Для этого выделите в таблице несколько клиентов, в контекстном меню выберите предложение **Обновить**.

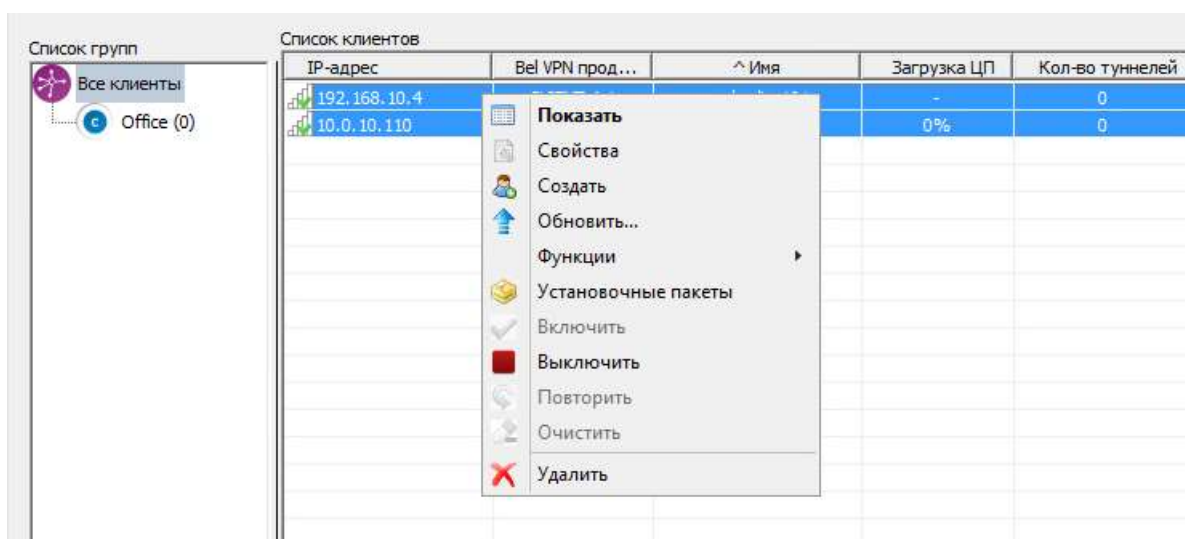


Рисунок 158

- В открывшемся окне **Обновление для клиентов** в поле **Пакет продукта** нажмите кнопку [...] и в стандартном окне открытия файла укажите файл с шаблоном проекта, например, `client_template.vpdt`.

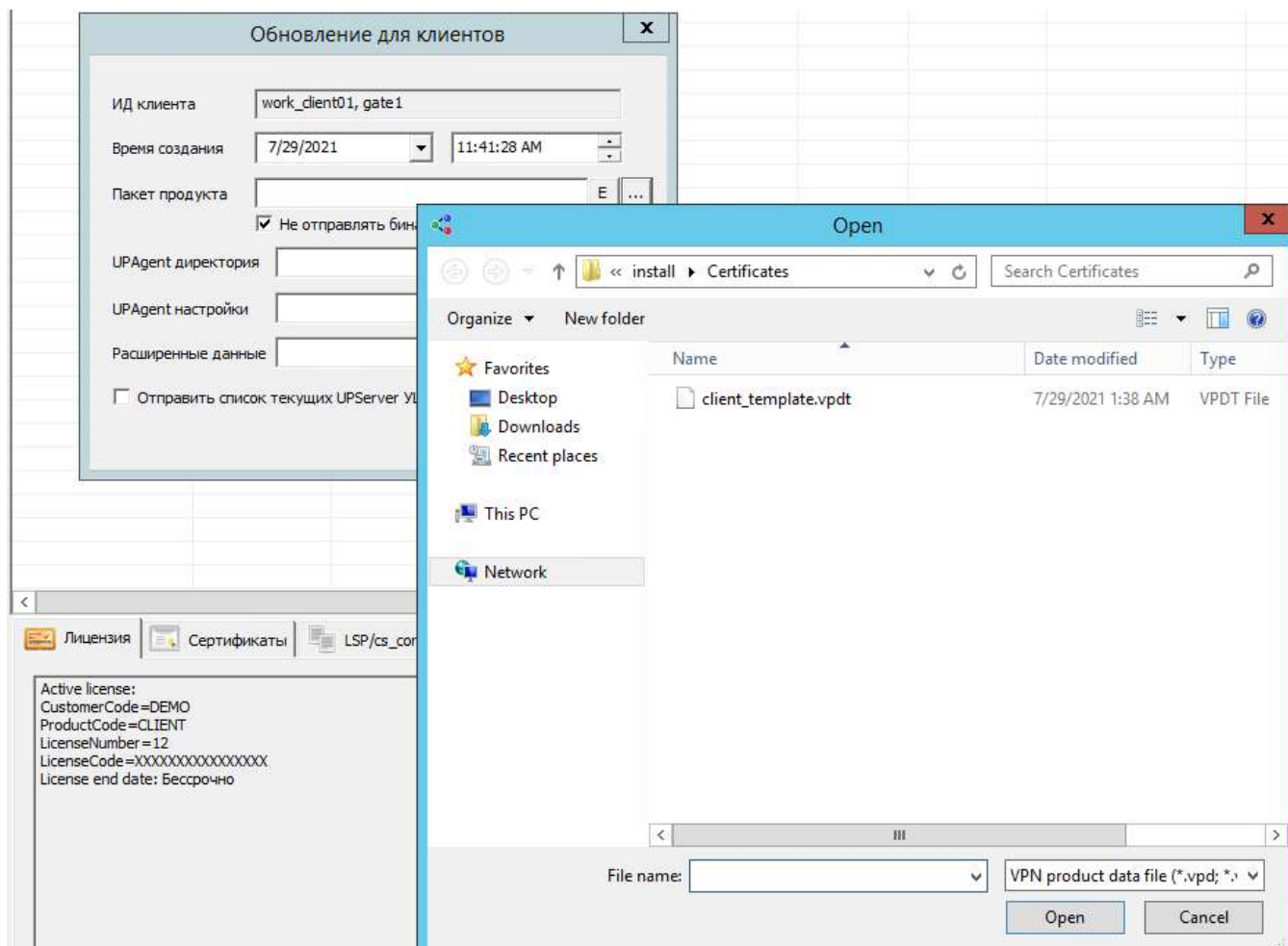


Рисунок 159

- Если в шаблон входит список локальных сертификатов, то при применении обновления для каждого клиента будет отбираться локальный сертификат из списка с выполнением проверки соответствия имеющегося у него запроса на сертификат и открытого ключа в сертификате. Такая проверка будет выполняться только при использовании шаблона. При отсутствии на клиенте запроса на его локальный сертификат такая проверка не выполняется и локальный сертификат на клиенте не обновляется.

13. Управление с использованием командной строки – утилита upmgr

Для автоматизации процесса управления клиентами удобно использовать интерфейс командной строки. В состав продукта **VPN UPSever** входит командно-строчная утилита `upmgr.exe`, размещенная в каталоге продукта – `C:\Program Files\S-Terra Bel\Bel VPN KP`.

Команды утилиты upmgr.exe

Команда show

Команда show выводит информацию о клиенте, аналогичную таблице клиентов (Рисунок).

```
upmgr show [-i CLIENT_ID [-s SECTION_NAME]]
```

CLIENT_ID	уникальный идентификатор клиента, может состоять из любых символов, за исключением следующих: \?/:.">*<, не должен начинаться или заканчиваться символами пробел, табуляция или точка, и не должен быть равен "NUL" или "CON" или "PRN" или "AUX" или "COMx" или "LPTx", где x [1..9]; Если не указывать ключ <code>-i</code> выводится краткая информация обо всех клиентах При указании ключа <code>-i</code> выводится расширенная информация для указанного клиента.
SECTION_NAME	имя секции данных о клиенте. Например, "---VPN PRODUCT---", "---LSP---", "---LICENSE---" и т.п.

Пример

```
upmgr show
client01 active 0 3 enabled unknown 14/05/2012 00:21:38 40.0.0.101 none
```

Команда create

Команда create позволяет создать нового клиента на Сервере управления

```
upmgr create -i CLIENT_ID -p PRODUCT_PKG [-g CLIENT_GROUP] [-s AGENT_SETTINGS] [-dev_pwd DEVICE_PWD]
```

PRODUCT_PKG	имя файла (здесь и далее имя файла включает полный путь к нему), содержащего настройки VPN продукта, который был создан с помощью окна консоли управления VPN data maker, или имя файла дистрибутива продукта Bel VPN Gate 4.5/4.1/Client-P 4.1, который был создан с помощью продукта Bel VPN Gate/Client AdminTool
CLIENT_GROUP	имя группы, к которой принадлежит клиент (формат SUB1/SUB2/NAME);
AGENT_PKG	каталог, в котором размещен дистрибутив Клиента управления (указывается, если получена новая версия Клиента управления от разработчика, текущая версия размещена в каталоге upagent)
AGENT_SETTINGS	имя файла, содержащего настройки Клиента управления
DEVICE_PWD	в данной версии не используется

Пример создания нового клиента с идентификатором "client02", с именем дистрибутива продукта Bel VPN Client 4.1 "e:\share\test_pkg.exe"

```
upmgr create -i client02 -p e:\share\test_pkg.exe
```

Команда remove

Команда remove позволяет удалить клиента из таблицы клиентов на Сервере управления

```
upmgr remove -i CLIENT_ID
```

Пример удаления клиента с идентификатором " client02":

```
upmgr remove -i client02
```

Команда get

Команда get позволяет получить инициализационные файлы для управляемого устройства в указанный каталог

```
upmgr get -i CLIENT_ID -d PRODUCT_DIR [-s UPAGENT_SETTINGS] [-ask_user_mode ASK_USER_MODE] [-check_mode CHECK_MODE] [-notify_client_port NOTIFY_CLIENT_PORT]
```

PRODUCT_DIR	каталог, в который будут сохранены дистрибутивы для Клиента управления
UPAGENT_SETTINGS	файл с настройками <i>Клиента управления</i> . Если он не указан будет использоваться конфигурационный файл по умолчанию (C:\Documents and Settings\All Users\Application Data\UPServer\csettings.txt)
ASK_USER_MODE	режим запроса подтверждения у пользователя о начале обновления, устанавливаемый в пакете Клиента управления, может принимать значения: auto – подтверждение запрашивается, если установлен Bel VPN Client (значение по умолчанию) never – подтверждение никогда не запрашивается always – подтверждение запрашивается всегда. Если значение другое, то оно трактуется как auto.
CHECK_MODE	режим проверки исполняемых модулей, подписанных ЭЦП, при получении обновления, может принимать значения: <пустая строка> - исполняемые модули не проверяются none – исполняемые модули не проверяются full – проверяются присланные в обновлении расширенные обновления и бинарные коды нового Клиента управления Если значение отсутствует, то оно приравнивается к значению none
NOTIFY_CLIENT_PORT	сетевой порт, который <i>Клиент управления</i> будет использовать для обмена сообщениями с <i>Сервером управления</i> . Если он не указан, то будет использоваться порт, указанный в конфигурационном файле <i>Клиента управления</i> (по умолчанию порт 43011);

Пример получения дистрибутивов для клиента с идентификатором "client02", с записью их в каталог "e:\share\#init\client02", Клиенту управления никогда не запрашивать подтверждение о начале обновления и всегда проверять на ЭЦП присланные обновления:

```
upmgr.exe get -i client02 -d e:\share\#init\client02 -ask_user_mode never -check_mode full
```

Команда update

Команда update позволяет создать обновление на Сервере управления для клиента

```
upmgr update -i CLIENT_ID [-p[d] PRODUCT_PKG] [-a AGENT_PKG] [-s
AGENT_SETTINGS] [-sca (UPCACERTS_FILE|*)] [-e EXTENDED_DATA] [-date
CREATION_DATE] [-time CREATION_TIME]
```

PRODUCT_PKG	имя файла (здесь и далее имя файла включает полный путь к нему), содержащего настройки VPN продукта, который был создан с помощью окна консоли управления VPN data maker, или имя файла дистрибутива продукта Bel VPN Gate 4.5/4.1/Client-P 4.1, который был создан с помощью продукта Bel VPN Gate/Client AdminTool Если вместо ключа -p указать ключ -pd, то Клиенту управления будут пересылаться только данные, без бинарных кодов продукта Bel VPN Gate 4.5/4.1/Client-P 4.1.
AGENT_PKG	каталог, в котором размещен дистрибутив Клиента управления (указывается, если получена новая версия Клиента управления от разработчика, текущая версия размещена в каталоге upagent)
AGENT_SETTINGS	имя файла, содержащего настройки Клиента управления
UPCACERTS_FILE *	имя файла в формате PKCS#7 (.p7b) со списком CA сертификатов Сервера управления, которые передаются клиенту в составе обновления. Если передается один CA сертификат, то файл может быть с расширением .cer. Если нужно передать весь актуальный список CA сертификатов Сервера управления, то следует указать «*»
EXTENDED_DATA	каталог, в котором расположены расширенные данные и скрипты обновления
CREATION_DATE	формат: dd/mm/yy, hh:mm
CREATION_TIME	дата и время, когда Сервер управления сформирует пакет обновления и сделает его доступным для скачивания Клиентом управления. Если указанное время уже прошло, то пакет обновления будет сформирован и открыт для скачивания сразу после создания обновления (если параметры не указаны, то используются текущая дата и время).

Пример создания для клиента с идентификатором "client02" обновления данных продукта Bel VPN Gate/Client, находящихся в дистрибутиве этого продукта "e:\share\test_pkg.exe":

```
upmgr update -i client02 -p e:\share\test_pkg.exe
```

Команда retry

Команда retry позволяет снять с обновления признак неудачного обновления, тем самым указывая системе, что это обновление должно быть применено Клиентом управления еще раз

```
upmgr retry -i CLIENT_ID
```

Пример снятия признака неудачного обновления для клиента с идентификатором "00000002":

```
upmgr retry -i 00000002
```

Команда clear

Команда clear позволяет отменить все непримененные и незавершенные обновления для клиента

```
upmgr clear -i CLIENT_ID [-force]
```

force флаг для команды clear, позволяющий произвести отчистку всех непримененных и незавершенных обновлений, не взирая на их статус.

Пример удаления всех непримененных обновлений для клиента с идентификатором "00000002":

```
upmgr clear -i 00000002 -force
```

Команда *disable*

Команда *disable* блокирует все сетевые обмены Сервера управления с клиентом

```
upmgr disable -i CLIENT_ID
```

Пример запрета всех сетевых обменов с клиентом с идентификатором "client02":

```
upmgr disable -i client02
```

Команда *enable*

Команда *enable* разрешает Серверу управления сетевые обмены с клиентом

```
upmgr enable -i CLIENT_ID
```

Пример разрешения сетевых обменов Серверу управления с клиентом с идентификатором "client02":

```
upmgr enable -i client02
```

Команда *set_group*

Команда *clear* изменяет группу у заданных клиентов

```
upmgr set_group -g CLIENT_GROUP {-i CLIENT_ID|-go OLD_CLIENT_GROUP}
```

CLIENT_GROUP имя группы, к которой принадлежит клиент (формат SUB1/SUB2/NAME)

OLD_CLIENT_GROUP имя группы, которая должна быть заменена на CLIENT_GROUP (формат PARENT0/PARENT1[NAME][*]);

Пример включения клиента "client02" в группу "Minsk/Office01":

```
upmgr.exe set_group -g Minsk/Office01 -i client02
```

Команда *set_prop*

Команда *set_prop* добавляет описание свойств у заданного клиента

```
upmgr set_prop -i CLIENT_ID [-dev_pwd DEVICE_PWD] [-client_desc CLIENT_DESC] [-ex_var_file FILE]
```

DEVICE_PWD зарезервировано для будущих версий

CLIENT_DESC произвольная строка для описания клиента, вносимая в поле Description

FILE имя файла, в котором указаны строки с переменными и их значениями, описывающие свойства клиента, которые передаются скрипту cook.bat при его запуске в процессе подготовки расширенного обновления. Формат строки:
_ex_имя_переменной=значение_переменной

Пример добавления в описание client02 свойства «может работать с токеном» со значением «AvPass 11-E-02/04».

```
upmgr.exe set_prop -i client02 -client_desc "в одной сети с client01" -  
ex_var_file "C:\Program Files\S-Terra Bel\Bel VPN КР\prop_client02.txt"
```

В файле prop_client02.txt записана строка – «может работать с токеном= AvPass 11-E-02/04»

Команда show_cert

Команда show_cert запускает стандартную GUI программу операционной системы для отображения рабочего сертификата Сервера управления

```
upmgr show_cert
```

Пример показа рабочего сертификата Сервера управления:

```
upmgr show_cert
```

Команда renew_cert

Команда renew_cert запускает перевыпуск рабочего сертификата Сервера управления (начало срока действия сертификата - за день до текущей даты, время жизни сертификата - 1 месяц)

```
upmgr renew_cert [-expired_only]
```

-expired_only рабочий сертификат Сервера управления пересоздается, если у него истек срок действия

Пример пересоздания рабочего сертификата Сервера управления только в том случае, если у него истек срок действия.

Команда check_files

Команда check_files запускает

```
upmgr check_files
```

check_files проверка целостности файлов Сервера управления

Команда backup

Команда backup запускает процесс сохранения данных о Клиентах управления и настройках Сервера управления в файл. В процессе сохранения архивируются данные Сервера управления, кроме контейнеров с секретными ключами сертификатов Сервера управления и статистической информации о Клиентах управления, хранимой в базе данных статистики.

```
upmgr backup -f BACKUP_FILE_NAME
```

BACKUP_FILE_NAME имя файла для сохранения данных о Клиентах управления и настройках Сервера управления.

Пример сохранения данных о клиентах управления и настройках Сервера управления:

```
upmgr.exe backup -f c:\backup01.bin
```

Команда restore

Команда restore запускает процесс восстановления данных о Клиентах управления и настройках Сервера управления из файла. В процессе будут восстановлены данные Сервера управления, кроме контейнеров с секретными ключами сертификатов Сервера управления и статистической информации о Клиентах управления, хранимой в базе данных статистики

```
upmgr restore -f BACKUP_FILE_NAME
```

BACKUP_FILE_NAME имя файла с данными о Клиентах управления и настройках Сервера управления.

Пример восстановления данных Сервера управления из файла C:\backup01.bin:

```
upmgr.exe restore -f c:\backup01.bin
```

При успешном завершении команды – код возврата равен 0, а при неуспешном - отличен от 0.

14. Изменение готового проекта с настройками VPN агента – утилита `vpnmaker`

Для внесения изменений в готовый проект можно использовать утилиту `vpnmaker`, расположенную в каталоге продукта – `C:\Program Files\S-Terra\Bel VPN KP`.

Назначение – изменение данных в готовых проектах, созданных с помощью Сервера управления, или создание новых проектов-шаблонов.

Предполагается, что утилита будет использоваться для создания большого количества похожих проектов для клиентов, незначительно отличающихся друг от друга (например, локальным сертификатом и номером лицензии агента).

Параметры утилиты:

```
vpnmaker replace -fi IN_FILE -fo OUT_FILE [-lsp LSP_TXT_FILE|-clp CISCO-
LIKE_POLICY] [-keyname KEY_NAMEON -keybody KEY_FILEON] [-lic LIC_FILE] [-
cert CERT_FILE [-certpwd PWD] [-certnum NUM] [-certkey KEY_CONT [-
certkeypwd KEY_PWD]] [-trust]] [-ifdesc IF_FILE] [-ifaliases IF_FILE]
```

```
vpnmaker make_template -fo OUT_FILE [-cert LOCAL_CERT_FILE01] [-cert
LOCAL_CERT_FILEON] [-cp CP_VENDOR]
```

You can enter many keys and many certificates.

В режиме работы **replace** некоторые старые данные проекта заменяются новыми. Старые сертификаты удаляются из базы, но не все, а только тех типов, которые добавляются. Например, при замене только локального сертификата CA-сертификаты сохраняются. Можно добавить/заменить несколько сертификатов разных типов.

Параметры режима **replace**:

<code>-fi IN_FILE</code>	полный путь к файлу с проектом, который надо изменить. Расширение <code>.exe</code> или <code>.vpd</code>
<code>-fo OUT_FILE</code>	полный путь к файлу с измененным проектом. Расширение <code>.exe</code> или <code>.vpd</code>
<code>-lsp LSP_TXT_FILE</code>	полный путь к текстовому файлу с локальной политикой безопасности. Эта опция не может применяться одновременно с опцией <code>-clp</code> . Старые политики безопасности LSP и cisco-like из проекта удаляются. Новая LSP сохраняется в базе данных проекта.
<code>-clp CISCO_LIKE_POLICY</code>	полный путь к текстовому файлу с cisco-like политикой безопасности. Эта опция не может применяться одновременно с опцией <code>-lsp</code> . Опция допустима только для шлюзов безопасности. Старые политики безопасности LSP и cisco-like из проекта удаляются. Старые настройки лога (файлы <code>"log_set.dsc"</code> , <code>"syslog.ini"</code> , <code>"syslog_3_1.ini"</code> , <code>"syslog_4_1.ini"</code>) удаляются. Новая cisco-like политика сохраняется в базе данных проекта.
<code>-keyname KEY_NAME</code>	имя ключа. После имени обязательно должна следовать опция <code>-keybody</code>
<code>-keybody KEY_FILE</code>	полный путь к файлу с телом ключа.
<code>-lic LIC_FILE</code>	полный путь к текстовому файлу с лицензией на продукт. Пример файла: <pre>[license] CustomerCode=bank ProductCode=GATE100 LicenseNumber=1 LicenseCode=AAAAAAAAAAAAAAAAAA</pre>
<code>-cert CERT_FILE</code>	полный путь к файлу с сертификатом (расширение <code>.cer</code> , <code>.p7b</code> , <code>.pfx</code>). Для этого сертификата можно указать дополнительные параметры:

<code>-certpwd PWD</code>	пароль, которым защищен файл с сертификатом.
<code>-certnum NUM</code>	порядковый номер сертификата (нужен, если файл содержит несколько сертификатов).
<code>-certkey KEY_CONT</code>	имя контейнера с секретным ключом сертификата (сам контейнер – у клиента).
<code>-certkeypwd KEY_PWD</code>	пароль, защищающий ключевой контейнер.
<code>-trust</code>	этот флаг должен выставляться у CA-сертификатов, которым мы доверяем.
<code>-ifdesc IF_FILE</code>	<p>полный путь к текстовому файлу с описанием виртуального адреса и роутинга. Параметр может быть только для Bel VPN Gate 4.5/4.1 on token (СПДС «ПОСТ»). Пример файла:</p> <pre>VirtualDeviceAddress=23.24.24.24 [ExtendedDeviceRoutes] Route_0=10.0.2.0/24 192.168.5.1 Route_1=23.45.55.0/24 1.2.3.4 Route_2=24.0.0.0/16 DGA Route_3=25.0.0.0/16 VDA DGA - default gateway address VDA - virtual device address !Description eth0 [IF_eth0] STATE=UP Address_0=40.0.0.17/24 MTU=1400 !Description eth1 [IF_eth1] STATE=UP Address_0=192.168.1.1/24 MTU=1400</pre>
<code>-ifaliases IF_FILE</code>	<p>полный путь к текстовому файлу с описанием алиасов интерфейсов. Пример файла:</p> <pre>FastEthernet1/0 = eth1 FastEthernet1/1 = eth2,eth3 default = *</pre> <p>По этой информации формируется файл <code>ifaliases.cf</code> (для продуктов версии 4.X) или информация сохраняется в базе продукта (для версий 3.X). Если не определен алиас <code>default</code>, он автоматически добавляется в виде <code>default = *</code></p>

Параметры режима `make_template`

В режиме работы `make_template` создается новый проект-шаблон, в котором есть только сертификаты. Они используются во внутренних тестах.

<code>-fo OUT_FILE</code>	полный путь к файлу с новым проектом. Расширение <code>.exe</code> или <code>.vpd</code> .
<code>-cert LOCAL_CERT_FILE</code>	полный путь к файлу с сертификатом
<code>-cp CPVENDOR</code>	криптопровайдер (AV)

15. Настройки Сервера управления

Администратор Сервера управления может задать некоторые настройки в файле:

C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt или
C:\ProgramData\UPServer\ssettings.txt

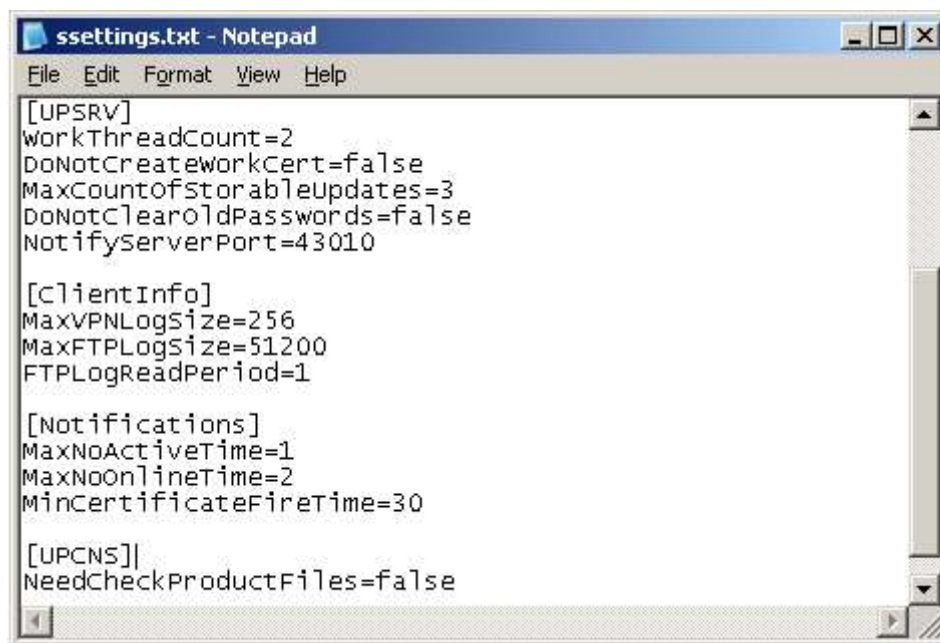


Рисунок 160

В файле ssettings.txt настройки распределены между секциями – Log, UPSRV, FTPServer, ClientInfo, Notifications, UPCNS. Описание переменных в каждой секции представлено ниже. Несколько настроек задается в реестре HKEY_LOCAL_MACHINE\SOFTWARE\UPServer или HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\UPServer.

Администратор может управлять следующими настройками.

Секция	Описание
Log	<p>Флаг включения syslog протоколирования Переменная SyslogEnable Значение: true – включено протоколирование false – выключено (значение по умолчанию – false).</p> <hr/> <p>Адрес Syslog-сервера Переменная SyslogSrvAddr Значение: любой корректный IP-адрес (значение по умолчанию – 127.0.0.1).</p> <hr/> <p>Адрес источника сообщений Переменная SyslogFacility Значение: строка. Возможные значения: log_kern, log_user, log_mail, log_daemon, log_auth, log_syslog, log_lpr, log_news, log_uucp, log_cron, log_authpriv, log_ftp, log_ntp, log_audit, log_alert, log_cron2, log_local0, log_local1, log_local2, log_local3, log_local4, log_local5, log_local6, Значение по умолчанию – log_local7)</p> <hr/> <p>Размер файла протоколирования событий Переменная FileMaxSize Значение: от 10 килобайт (значение по умолчанию – 10200 килобайт, если строка отсутствует или некорректна).</p>

	<p>Имя файла протоколирования: C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log.</p> <p>При достижении заданного значения данные копируются в файл upserver.log.bak, а файл upserver.log очищается. Пример файла с сообщениями.</p>
UPSRV	<p>Количество рабочих ниток в сервисе подготовки обновлений</p> <p>Переменная WorkThreadCount</p> <p>Значение: десятичное число от 1 до 10 (значение по умолчанию 2). Рекомендуемое значение - количество процессоров на компьютере + 1.</p> <hr/> <p>Количество рабочих ниток в сервисе записи статистических данных в базу данных статистики</p> <p>Переменная StatThreadCount</p> <p>Значение: десятичное число от 1 до 10 (значение по умолчанию 1).</p> <hr/> <p>Флаг отключения автоматического пересоздания рабочего сертификата</p> <p>Переменная DoNotCreateWorkCert</p> <p>Значение: false – отключено автоматическое пересоздание (значение по умолчанию)</p> <p>true – включено автоматическое пересоздание</p> <hr/> <p>Максимальное количество хранимых примененных обновлений для каждого клиента</p> <p>Переменная MaxCountOfStorableUpdates</p> <p>Значение: десятичное число от 0 до 4294967295, значение 0 – обновления не удаляются (значение по умолчанию 0).</p> <hr/> <p>Флаг удаления старых паролей к клиентским ключевым контейнерам</p> <p>Переменная DoNotClearOldPasswords</p> <p>Значение: false – удаляются автоматически старые пароли (значение по умолчанию)</p> <p>true – не удаляются автоматически старые пароли</p> <hr/> <p>UDP порт, который используется для обмена нотификациями с Клиентами управления</p> <p>Нотификации используются для отслеживания Клиентов управления, находящихся на связи, и оповещения их о существовании подготовленных обновлений.</p> <p>Переменная NotifyServerPort</p> <p>Значение: десятичное число от 0 до 65535 (значение по умолчанию 43010), значение 0 отключает механизм обмена нотификациями.</p>
FTPServer	<p>Сетевой адрес для взаимодействия с сервисом продукта FileZilla Server</p> <p>Переменная Address</p> <p>Значение: локальный IP-адрес сервера FileZilla Server (значение по умолчанию 127.0.0.1).</p> <hr/> <p>Сетевой порт для взаимодействия с сервисом продукта FileZilla Server</p> <p>Переменная Port</p> <p>Значение: порт сервиса FileZilla Server (значение по умолчанию 14147).</p> <hr/> <p>Пароль для взаимодействия с сервисом продукта FileZilla Server</p> <p>Переменная Password</p> <p>Значение: строка, представляющая из себя пароль сервиса FileZilla Server (значение по умолчанию <пустая строка>).</p>
ClientInfo	<p>Максимальный размер лог сообщений VPN-продукта, хранящихся для каждого Клиента управления</p> <p>Переменная MaxVPNLogSize</p>

	<p>Значение: десятичное число от 1 до 102400 килобайт (значение по умолчанию 256).</p> <p>Максимальный размер лог сообщений FTP-сервера</p> <p>Переменная MaxFTPLogSize</p> <p>Значение: десятичное число от 1024 до 921600 килобайт (значение по умолчанию 51200).</p>
	<p>Период анализа сообщений FTP-сервера</p> <p>Переменная FTPLogReadPeriod</p> <p>Значение: целое число от 1 до 60 минут (значение по умолчанию 5).</p>
Notifications	<p>Максимальное время неактивности клиента</p> <p>Переменная MaxNoActiveTime</p> <p>Значение: десятичное число от 0 до 4294967295 часов, значение 0 – отключает отслеживание максимального времени неактивности клиентов (значение по умолчанию 24).</p> <p>Максимальное время неактивности клиента для признания его находящимся не на связи</p> <p>Переменная MaxNoOnlineTime</p> <p>Значение: десятичное число от 1 до 60 минут (значение по умолчанию 2).</p> <p>Минимальное время перед окончанием срока действия сертификата управляемого устройства</p> <p>Переменная MinCertificateFireTime</p> <p>Значение: десятичное число от 0 до 4294967295 суток, значение 0 – отключает отслеживание минимального времени перед окончанием срока действия сертификатов управляемых устройств (значение по умолчанию 30). При наступлении этого времени дата окончания срока действия сертификата выделена красным цветом в таблице клиентов Сервера управления.</p>
UPCNS	<p>Флаг проверки целостности файлов продукта при старте приложения VPN UPServer console</p> <p>Переменная NeedCheckProductFiles</p> <p>Значение: true – выполняется проверка целостности при каждом старте приложения false – проверка целостности не выполняется (значение по умолчанию)</p>
DBServer	<p>Сетевой адрес для взаимодействия с сервисом продукта PostgreSQL Server</p> <p>Переменная Address</p> <p>Значение: IP-адрес сервиса PostgreSQL Server (значение по умолчанию 127.0.0.1).</p> <p>Сетевой порт для взаимодействия с сервисом продукта PostgreSQL Server</p> <p>Переменная Password</p> <p>Значение: порт сервиса PostgreSQL Server (значение по умолчанию 5432).</p> <p>Пароль для взаимодействия с сервисом продукта PostgreSQL Server</p> <p>Переменная Port</p> <p>Значение: строка, представляющая из себя пароль сервиса PostgreSQL Server (значение по умолчанию 1234567890).</p>

HKEY_LOCAL_MACHINE \ SOFTWARE\ UPServer	Режим работы создаваемых Клиентов управления Переменная ClientMode Значение: windowless – безоконный режим работы Клиента управления (значение по умолчанию) <пустая строка> – оконный режим работы Клиента управления (для отладки и тестирования).
HKEY_LOCAL_MACHINE \ SOFTWARE\ Wow6432Node\ UPServer	Запрос подтверждения у пользователя о начале обновления, устанавливаемый в пакете Клиента управления Переменная ClientUserAskMode Значение: auto – необходимость запроса определяется на основе типа VPN-продукта (если установлен продукт Bel VPN Client - подтверждение запрашивается) (значение по умолчанию) never – подтверждение никогда не запрашивается, не смотря на тип VPN-продукта always – подтверждение запрашивается всегда, не смотря на тип VPN-продукта. Если значение другое, то оно трактуется как auto.
	Проверка исполняемых модулей при получении обновления Переменная ClientUpdateCheckMode Значение: <пустая строка> – исполняемые модули не проверяются none – исполняемые модули не проверяются full – проверяются присланные в обновлении расширенные обновления и бинарные коды нового Клиента управления Если значение отсутствует, то оно приравнивается к значению none. Если значение другое, то оно приравнивается к full. Исполняемые модули подписываются ЭЦП, для которой используется секретный ключ сертификата, изданного компанией С-Терра. Проверка гарантирует, что исполняемые модули были созданы с использованием скриптов, созданных компанией С-Терра. Если администратор управляемых устройств использует свои скрипты, то такую проверку следует отключить.

Пример файла протоколирования:

```

Fri Feb 10 23:18:44 2012 INFO      upsrv 00001744 Log file name:
C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log
Fri Feb 10 23:18:44 2012 INFO      upsrv 00001744 Log setting FileMaxSize: 5120
Fri Feb 10 23:18:44 2012 INFO      upsrv 00001744 Log setting SyslogEnable: false
Fri Feb 10 23:18:44 2012 INFO      upsrv 00001744 Log setting SyslogSrvAddr:
127.0.0.1
Fri Feb 10 23:18:44 2012 INFO      upsrv 00001744 Log setting SyslogFacility:
log_local7
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 Settings is read from file
C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log

Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 UPSRV:WorkThreadCount: 2
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 UPSRV:MaxCountOfStorableUpdates:
1000
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 UPSRV:DoNotCreateWorkCert: false
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 UPSRV:DoNotClearOldPasswords: false
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 UPSRV:NotifyServerPort: 43010
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 ClientInfo:MaxVPNLogSize: 256 KB
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 ClientInfo:MaxFTPLogSize: 51200 KB
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 ClientInfo:FTPLogReadPeriod: 5 min
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 Notifications:MaxNoOnlineTime: 1
min
Fri Feb 10 23:18:53 2012 INFO      upsrv 00001744 00002150 Server notify socket is
opened (any:43010)
Fri Feb 10 23:18:53 2012 NOTICE   upsrv 00001744 Module 4.0.12437 is started
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Log file name:

```

```
C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Log setting FileMaxSize: 5120
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Log setting SyslogEnable: false
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Log setting SyslogSrvAddr:
127.0.0.1
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Log setting SyslogFacility:
log_local7
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Settings is read from file
C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec Notifications:MaxNoActiveTime: 24
hours
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec
Notifications:MinCertificateFireTime: 30 days
Fri Feb 10 23:19:21 2012 INFO      upcns 00000aec UPCNS:NeedCheckProductFiles: false
Fri Feb 10 23:19:21 2012 NOTICE   upcns 00000aec Module 4.0.12437 is started
Fri Feb 10 23:19:24 2012 NOTICE   upcns 00000aec Module is stopped
```

16. Настройки Клиента управления

Настройки по умолчанию Клиента управления записаны на Сервере управления в файле:

C:\Documents and Settings\All Users\Application Data\UPServer\csettings.txt или

C:\ProgramData\UPServer\csettings.txt

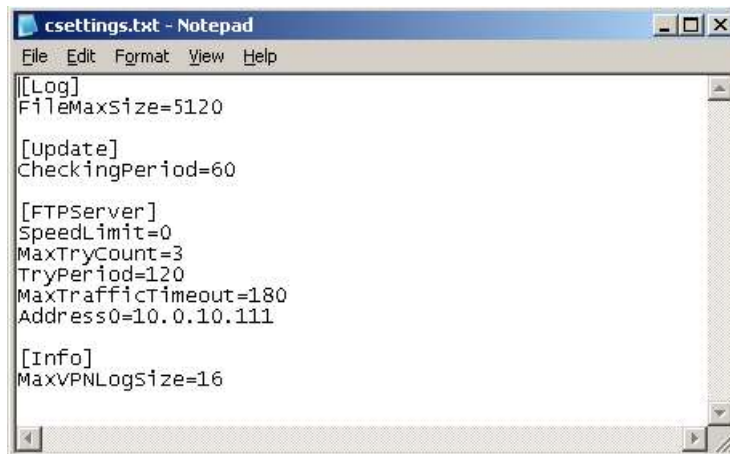


Рисунок 161

Для каждого клиента настройки Клиента управления можно изменить и сохранить в другом файле, а затем указать его в поле **UPAgent settings** (Рисунок 54) окна **Create new client** при создании клиента.

В файле настройки распределены между секциями – Log, Update, FTPServer, Info. Описание переменных в каждой секции представлено ниже. Несколько настроек выставляется при инсталляции (инициализации) Клиента управления в реестре

HKEY_LOCAL_MACHINE\SOFTWARE\UPAgent либо

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\UPAgent.

Секция	Описание
Log	Флаг включения syslog протоколирования Переменная SyslogEnable Значение: true – включено протоколирование false – выключено (значение по умолчанию – false).
	Адрес Syslog-сервера Переменная SyslogSrvAddr Значение: любой корректный IP-адрес (значение по умолчанию – 127.0.0.1)
	Адрес источника сообщений Переменная SyslogFacility Значение: log_kern, log_user, log_mail, log_daemon, log_auth, log_syslog, log_lpr, log_news, log_uucp, log_cron, log_authpriv, log_ftp, log_ntp, log_audit, log_alert, log_cron2, log_local0, log_local1, log_local2, log_local3, log_local4, log_local5, log_local6, log_local7 (значение по умолчанию)
	Размер файла протоколирования событий Переменная FileMaxSize Значение: от 10 килобайт (значение по умолчанию – 5120 килобайт, если строка отсутствует или некорректна). Имя файла протоколирования событий: для ОС Windows - C:\Program Files\UPAgent\upagent.log

Секция	Описание
	<p>для ОС Unix – /var/log/upagent/upagent.log</p> <p>При достижении заданного значения данные копируются в файл upagent.log.bak, а файл upagent.log очищается.</p>
Update	<p>Период проверки новых обновлений на Сервере управления</p> <p>Переменная CheckingPeriod</p> <p>Значение: от 60 до 86400 секунд (значение по умолчанию – 3600).</p>
	<p>Период между посылками нотификаций Серверу управления</p> <p>Переменная NotifySendPeriod</p> <p>Значение: целое число от 1 до 3600 секунд (значение по умолчанию 60).</p>
	<p>Количество неудачных попыток соединения с Сервером управления перед тем, как заново попытаться подобрать параметры соединения (например, использовать другой IP-адрес Сервера управления).</p> <p>Переменная MaxFailedConnCount</p> <p>Значение: десятичное число от 0 до 200 секунд (значение по умолчанию 0);</p> <p>значение 0 – не подбирать параметры соединения с Сервером управления при любом количестве неудачных попыток.</p>
	<p>UDP порт Клиента управления для обмена нотификациями с Сервером управления</p> <p>Переменная NotifyClientPort</p> <p>Значение: целое число от 0 до 65535,</p> <p>значение 0 – отключает механизм обмена нотификациями (значение по умолчанию 43011).</p> <p>Нотификации используются для механизма отслеживания нахождения Клиента управления на связи и оповещения его о существовании для них подготовленных обновлений.</p>
	<p>UDP порт Сервера управления для получения нотификаций от Клиента управления</p> <p>Переменная NotifyServerPort</p> <p>Значение: целое число от 0 до 65535 (значение по умолчанию 43010),</p> <p>значение 0 – отключает механизм отсылки нотификаций.</p>
FTPServer	<p>Адрес FTP сервера</p> <p>Переменная AddressX, где X любое десятичное число (0,1,2..)</p> <p>Количество таких переменных может быть больше одного, они будут использоваться в том порядке, в котором заданы. Числа должны быть уникальные в пределах секции.</p> <p>Значение: IP-адрес или DNS-имя, которое будет транслироваться в IP-адрес в момент создания соединения.</p>
	<p>Максимальное время ожидания соединения с FTP сервером</p> <p>Переменная MaxConnectTimeout</p> <p>Значение: десятичное число от 0 до 300 секунд (значение по умолчанию 0, т.е. время ожидания определяется настройками ОС, под управлением которой работает Клиент управления).</p>
	<p>Максимальная скорость скачивания обновлений с Сервера управления</p> <p>Переменная SpeedLimit</p> <p>Значение: от 512 до 4294967295 байт/секунду или 0</p> <p>(значение 0 – ограничения нет, значение по умолчанию).</p>

Секция	Описание
	<p>Максимальное количество попыток скачать/получить данные с/на FTP сервер(а) Переменная MaxTryCount Значение: целое число от 1 до 30 (значение по умолчанию 3).</p>
	<p>Период между попытками скачать/получить данные с/на FTP сервер(а) Переменная TryPeriod Значение: целое число от 0 до 300 секунд (значение по умолчанию 120).</p>
	<p>Максимальное время отсутствия трафика между Клиентом управления и FTP-сервером, по истечении которого соединение считается разорванным Переменная MaxTrafficTimeout Значение: целое число от 30 до 3600 секунд (значение по умолчанию 180).</p>
Info	<p>Максимальный размер сообщений продукта Bel VPN Gate/Client, пересылаемых на Сервер управления Переменная MaxVPNLogSize Значение: десятичное число от 1 до 102400 килобайт (значение по умолчанию 16).</p>
	<p>Период между сбором статистической информации на управляемом устройстве Переменная StatCollectPeriod Значение: десятичное число от 0 до 600 секунд (значение по умолчанию 5), значение 0 – сбор статистической информации не производится.</p>
	<p>Максимальный размер памяти на управляемом устройстве для сбора статистической информации. При достижении этого размера собранная статистическая информация пересылается на Сервер управления Переменная StatBufSize Значение: десятичное число от 1 до 2048 килобайт (значение по умолчанию 100).</p>
	<p>Период между посылками собранной статистической информации на Сервер управления Переменная StatSendPeriod Значение: десятичное число от 0 до 7200 минут (значение по умолчанию 10), значение 0 – отключает отслеживание по времени, действует только ограничение по размеру собранной статистической информации.</p>
	<p>Адрес и порт источника SNMP статистики Переменная StatSNMPAddr Значение: корректный IP-адрес и корректный порт, разделенные двоеточием (значение по умолчанию 127.0.0.1:161).</p>
	<p>Community-строка источника SNMP статистики Переменная StatSNMPCommunity Значение: строка, содержащая community (значение по умолчанию - public). Community-строка играет роль пароля при аутентификации сообщений SNMP.</p>
	<p>Период между перепосылками запросов к источнику SNMP статистики Переменная StatSNMPTimeout</p>

Секция	Описание
	<p>Значение: десятичное число от 1 до 100 сотых долей секунды (значение по умолчанию 10).</p> <p>Количество перепосылок запросов к источнику SNMP статистики</p> <p>Переменная StatSNMPRetries</p> <p>Значение: десятичное число от 0 до 5 раз (значение по умолчанию 0), значение 0 – статистика запрашивается только один раз (если в отведенное время ответ не приходит – повторных запросов не производится).</p>
StatVariables	<p>Флаг активности сбора статистики по загрузке процессора</p> <p>Переменная CPUUsage</p> <p>Значение:</p> <p>on – на Сервер управления будет посылаться параметр CPUUsage – средняя загрузка процессоров в процентах за время StatCollectPeriod (значение по умолчанию)</p> <p>off – статистика не собирается.</p> <p>Флаг активности сбора статистики по используемой памяти</p> <p>Переменная MemUsage</p> <p>Значение:</p> <p>on – на Сервер управления будут посылаться значения двух параметров и во вкладке Статистика UPWeb они будут отображены с именами:</p> <p>MemUsage – количество занятых байт в памяти</p> <p>MemFree - количество свободных байт в памяти (значение по умолчанию)</p> <p>off – статистика не собирается.</p> <p>Флаг активности сбора статистики по используемому дисковому пространству (диск, на котором установлен Клиент управления. Обычно для Windows - это диск C, для UNIX – примонтированный диск как /)</p> <p>Переменная DiskUsage</p> <p>Значение:</p> <p>on – на Сервер управления будут посылаться значения двух параметров:</p> <p>DiskUsage – количество занятых байт на диске</p> <p>DiskFree - количество свободных байт на диске (значение по умолчанию)</p> <p>off – статистика не собирается.</p> <p>Флаг активности сбора статистики по используемым сетевым интерфейсам</p> <p>Переменная NetUsage</p> <p>Значение:</p> <p>on – на Сервер управления будут посылаться значения двух параметров:</p> <p>NetInSpeed – среднее количество байт в секунду, полученных всеми интерфейсами, в период между замерами</p> <p>NetOutSpeed - среднее количество байт в секунду, отправленных со всех интерфейсов, в период между замерами (значение по умолчанию)</p>

Секция	Описание
	<p>off – статистика не собирается.</p> <p>Добавление переменной для сбора статистики</p> <p>Запрос составляется в виде:</p> <pre>SNMP:<ID_SNMP>=STATE [-n DISPLAYNAME] [-p COLLECTPERIOD] [-a SNMPADDR] [-c SNMPCOMMUNITY] [-t SNMPTIMEOUT] [-r SNMPRETRIES] [-ev ERROR_VALUE],</pre> <p>где</p> <ul style="list-style-type: none"> <ID_SNMP> – идентификатор запрашиваемой переменной (можно посмотреть в разделе «Мониторинг» пользовательской документации) STATE – флаг активности, значение on, off DISPLAYNAME – имя, под которым данная статистика будет посылаться на Сервер управления COLLECTPERIOD – период сбора статистики в секундах, если не задан, то используется значение StatCollectPeriod SNMPADDR – адрес и порт источника SNMP статистики, если не задан, то используется значение StatSNMPAddr SNMPCOMMUNITY – community-строка источника SNMP статистики, если не задана, используется значение StatSNMPCommunity SNMPTIMEOUT – период между перепосылками запросов к источнику SNMP статистики, если не задан, то используется StatSNMPTimeout SNMPRETRIES – количество перепосылок запросов к источнику SNMP статистики, если не задано, то используется значение StatSNMPRetries ERROR_VALUE – строка, которая будет использоваться в качестве значения статистики при ее неудачном сборе. <p>Пример:</p> <pre>SNMP:1.3.6.1.4.1.9.9.171.1.3.1.1.0 =on -n ActiveTunCount -ev 0</pre>
HKEY_LOCAL_MACHINE\SOFTWARE\UPAgent HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\UPAgent	<p>Режим работы Клиента управления</p> <p>При инсталляции Клиента управления на управляемое устройство в ключе реестра HKEY_LOCAL_MACHINE\SOFTWARE\UPAgent или HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\UPAgent выставляется режим работы, заданный по умолчанию. После инсталляции значение можно изменить.</p> <p>Переменная Mode</p> <p>Значение:</p> <ul style="list-style-type: none"> windowless – безоконный режим работы Клиента управления (значение по умолчанию) <пустая строка> – оконный режим работы Клиента управления (для отладки и тестирования). <p>Запрос подтверждения у пользователя о начале обновления</p> <p>Переменная UserAskMode</p> <p>Значение:</p> <ul style="list-style-type: none"> auto – необходимость запроса определяется на основе типа VPN-продукта (подтверждение запрашивается, если на компьютере установлен продукт Bel VPN Client) (значение по умолчанию) never – подтверждение никогда не запрашивается, не смотря на тип VPN-продукта always – подтверждение запрашивается всегда, не смотря на тип VPN-продукта.

Секция	Описание
	Если значение другое, то оно трактуется как <code>auto</code> .
	<p>Проверка исполняемых модулей при получении обновления</p> <p>Переменная <code>UpdateCheckMode</code></p> <p>Значение:</p> <p><code><пустая строка></code> – исполняемые модули не проверяются</p> <p><code>none</code> – исполняемые модули не проверяются</p> <p><code>full</code> – проверяются присланные в обновлении расширенные обновления и бинарные коды нового Клиента управления</p> <p>Если значение отсутствует, то оно приравнивается к значению <code>none</code>.</p> <p>Если значение другое, то оно приравнивается к <code>full</code>.</p> <p>Исполняемые модули подписываются ЭЦП, для которой используется секретный ключ сертификата, изданного компанией С-Терра. Проверка гарантирует, что исполняемые модули были созданы с использованием скриптов, созданных компанией С-Терра. Если администратор управляемых устройств использует свои скрипты, то такую проверку следует отключить.</p>

17. Описание интерфейса Сервера управления

Графический интерфейс приложения **VPN UPServer console** содержит следующие элементы.

17.1. Вкладка Клиенты

На Сервере управления во вкладке **Клиенты** отражается информация обо всех управляемых устройствах. Эта вкладка предназначена для создания, удаления учетных записей клиентов управляемых устройств, создания для них Клиентов управления, обновлений, приостановки работы с клиентом и т.д. Клиенты могут быть объединены в группы.

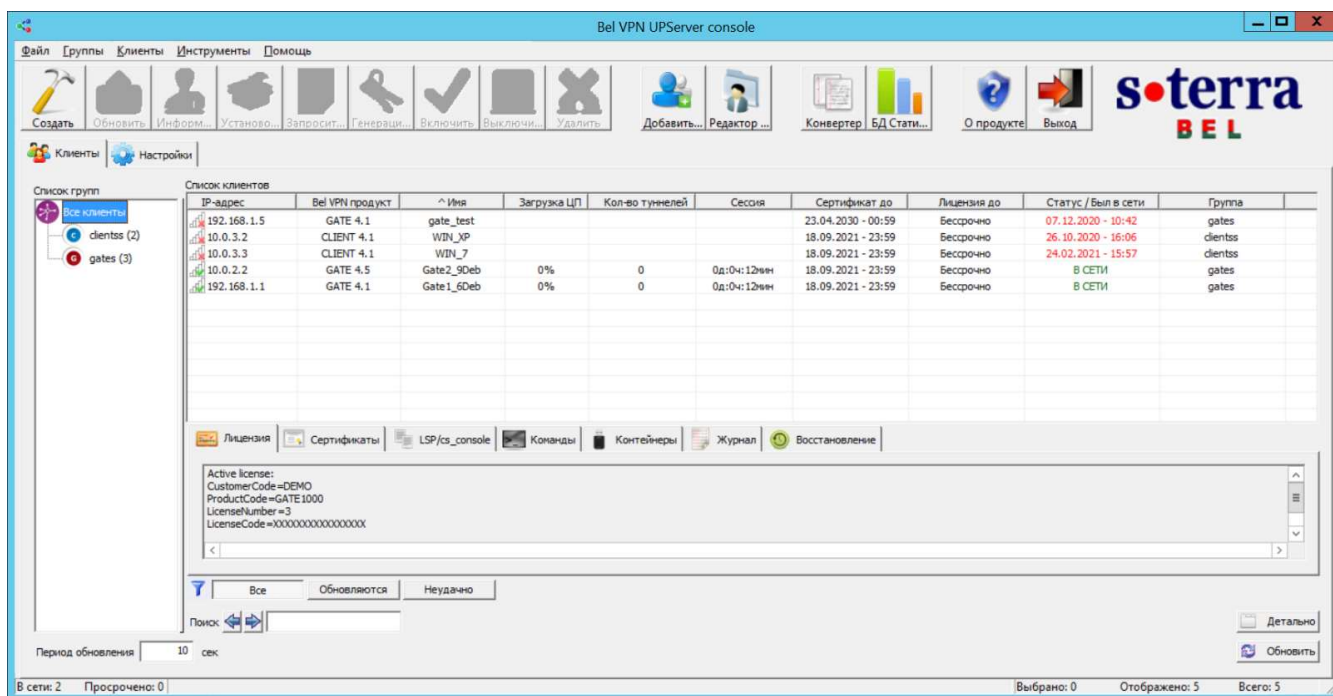


Рисунок 162

Описание вкладки **Клиенты**.

Параметр	Описание
Список групп	дерево групп клиентов, объединенных администратором по территориальному или организационному признаку расположения управляемых устройств
Список клиентов	таблица со списком клиентов, входящих в выделенную группу. Столбцы таблицы имеют следующие значения:
Bel VPN продукт	тип VPN-продукта, установленного на клиенте управления
Загрузка ЦП	усредненное значение загрузки ядер процессора на управляемом устройстве
Кол-во туннелей	количество IPsec соединений на управляемом устройстве
Сессия	длительность текущей сессии (время проведенное управляемым устройством "В СЕТИ")
Имя	уникальный идентификатор клиента
Состояние	состояние Клиента управления, может принимать следующие значения: <p>Новый – Клиент управления зарегистрирован на Сервере управления и еще ни разу не выходил на связь по сети</p> <p>Активен – Клиент управления готов к приему обновлений</p> <p>Ожидает – обновление для клиента создано и выложено на FTP-сервер и ожидается, что Клиент управления начнет его скачивание</p>

	<p>Обновляется – Клиент управления применяет обновление (в данном состоянии Клиент управления находится с момента, когда он обнаружил обновление на Сервере управления и до момента, когда он его применил или отвергнул)</p> <p>Неудачно – Клиент управления не смог применить очередное обновление (в этом состоянии клиент продолжает работу на предыдущем комплекте обновления, попытки по применению обновления не предпринимаются, пока администратор не изменит это состояние на active, отменив неуспешное обновление). Ошибка детектируется на основании невозможности скачать то же обновление с Сервера управления при примененном обновлении</p>
Активные обновления	количество еще непримененных обновлений
Примененные обновления	количество успешно примененных обновлений
Администрирование	<p>административное состояние обслуживания Клиента управления, может принимать следующие значения:</p> <p>Включен – Клиент управления обслуживается</p> <p>Выключен – Клиент управления не обслуживается (все его обращения к серверу игнорируются)</p>
Сертификат до	ближайшая дата и время истечения срока действия одного из сертификатов, размещенных в базе продукта Bel VPN Gate/Client 4.1
Статус / Был в сети	<p>время последнего выхода в сеть, может принимать следующие значения:</p> <p>дата и время последнего удачного FTP-соединения клиента (когда клиент удачно аутентифицировался на FTP-сервере)</p> <p>В СЕТИ – в данный момент клиент находится на связи</p>
IP-адрес	IP-адрес клиента, с которого было осуществлено последнее удачное FTP-соединение
Группа	имя группы, к которой принадлежит клиент
Описание	произвольная строка, вносимая администратором, для описания клиента

Допускается **сортировка по столбцам** таблицы клиентов. Значком **^** метится столбец, по которому сортируются данные, если данные в таком столбце одинаковые, то они сортируются по **Имя**. Поддерживается сортировка по убыванию и возрастанию. При первом нажатии на заголовок столбца сортировка проводится по возрастанию, при втором – по убыванию, третье нажатие – отмена действия.

Для изменения порядка расположения столбцов друг относительно друга выберите нужный столбец, с зажатой левой кнопкой мыши на заголовке столбца, перетащите его на новое расположение.

Для отображения/скрытия столбца в таблице клиентов, нажмите правой кнопкой на панель, содержащую заголовки столбцов. Из выпадающего списка выберите имя столбца для отображения/скрытия.

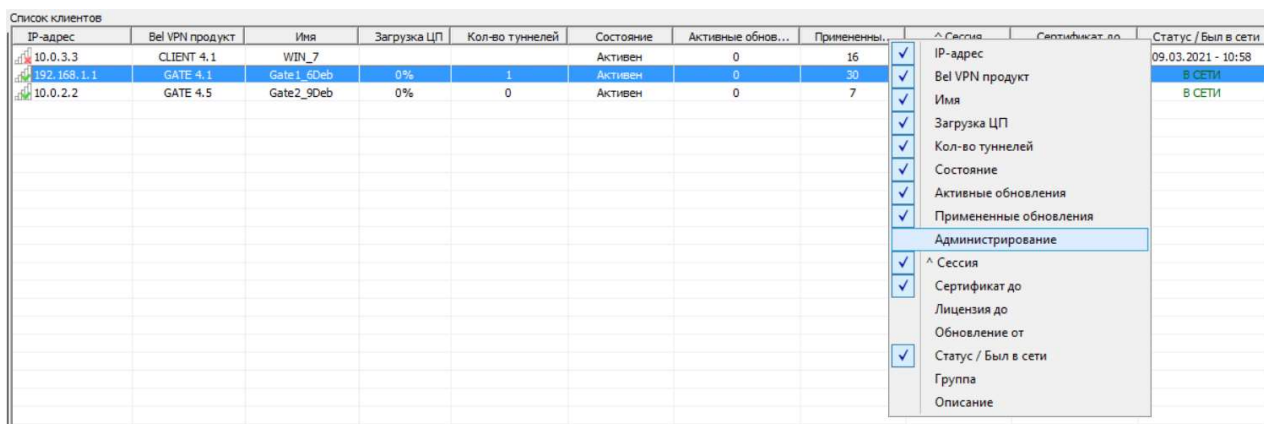


Рисунок 194

Вкладка **Clients** имеет следующие кнопки управления:

Кнопка, поле	Описание
Все	в таблице отображаются все клиенты группы
Обновляются	в таблице отображаются только те клиенты, которые имеют хотя бы одно неприменное обновление или находятся в состоянии не active
Неудачно	в таблице отображаются клиенты в состоянии failed (не смогли применить очередное обновление)
Поиск	поле для ввода строки, по которой будет происходить поиск клиентов в таблице, содержащих данную строку в любом поле. Если такой клиент найден - он выделяется в списке клиентов.
->	кнопка запуска поиска следующего клиента, относительно выделенного, удовлетворяющего заданной строке в поле Find. Аналогично нажатию клавиши F3
<-	кнопка запуска поиска предыдущего клиента, относительно выделенного, удовлетворяющего заданной строке в поле Find. Аналогично нажатию клавиш Shift-F3
Период обновления	поле, в котором задается период времени в секундах обновления информации в таблице клиентов
Обновить	кнопка для принудительного обновления информации в таблице клиентов. Нажатие кнопки дает команду для сбора информации обо всех существующих клиентах. Так как процесс сбора информации может быть долговременным, то ожидание по кнопке Refresh производится только для выделенных на данный момент клиентов. Отображение обновленной информации для всех остальных клиентов будет произведено позднее, по мере получения полной информации. Аналогично нажатию клавиши F5
Детально	разворачивает/сворачивает информационную панель со следующими вкладками:
Лицензия	отображает информацию о лицензии установленного VPN-продукта на выбранном управляемом устройстве
Сертификаты	отображает все зарегистрированные в установленном на выбранном управляемом устройстве VPN-продукте сертификаты и их статус
LSP/cs_console	отображает загруженную политику безопасности на управляемом устройстве в виде текстового файла и в виде cisco-like конфигурации
Команды	отображает список команд для управляемых устройств. Позволяет создавать, удалять, редактировать и отправлять на выполнение команды клиенту управления
Контейнеры	отображает созданные на управляемом устройстве запросы на сертификаты, используемые и неиспользуемые контейнеры с ключевыми парами
Журнал	отображает журналы протоколируемых событий на управляемом устройстве: VPN log (журнал VPN-продукта), UPLog (журнал клиента управления)
Восстановление	отображает список резервных копий в хронологическом порядке. Позволяет просматривать, удалять, открывать директории выбранных из списка резервных копий и восстанавливать из выбранной резервной копии управляемое устройство

Нижняя строка вкладки **Клиенты** отражает:

Выбрано – количество выделенных на данный момент клиентов

Отображено – количество отображаемых на данный момент клиентов

Всего – количество всех клиентов на Сервере управления.

В сети: – количество клиентов “В СЕТИ” в выбранной группе.

Просрочено: – количество клиентов с “просроченным” сертификатом/лицензией VPN-продукта в выбранной группе.

17.2. Меню Файл

Меню **Файл** включает одно предложение:

Выход – завершает работу консоли управления (обслуживание клиентов при этом не завершается).

17.3. Меню Группы

Меню **Группы** содержит следующие элементы:

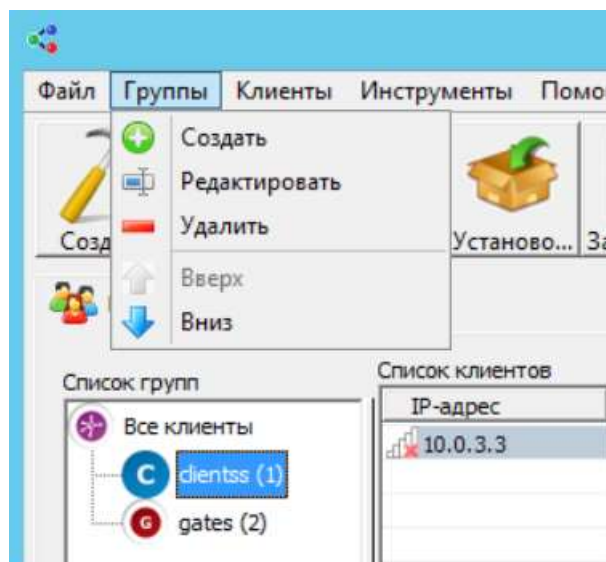


Рисунок 163

Создать - вызывает окно **Новая группа** создания новой группы (группа создается как подгруппа выделенной группы), в котором надо задать имя группы (Рисунок 164).

Имя группы родителя – имя группы, в которой создается подгруппа

Имя группы – имя создаваемой подгруппы.

Иконка группы: – тип отображаемой иконки для группы

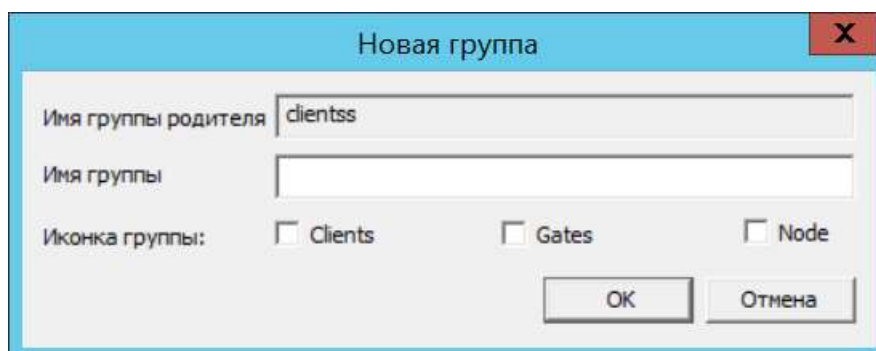


Рисунок 164

Редактировать - вызывает окно переименования выделенной группы, в котором задается новое имя группы (Рисунок 165).

Имя группы родителя – имя группы, в которой переименовывается подгруппа

Имя группы – новое имя подгруппы.

Иконка группы: – тип отображаемой иконки для группы

При переименовании группы все входящие в нее клиенты и группы сохраняются.

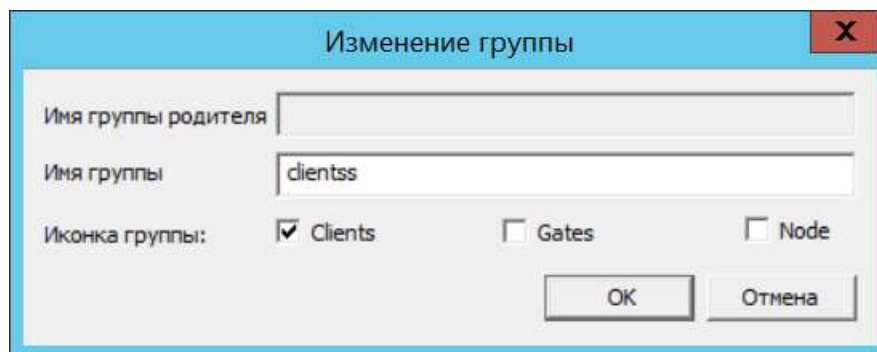


Рисунок 165

Удалить – удаляет выделенную группу; при этом все клиенты и подгруппы, входящие в нее, перемещаются в группу уровнем выше.

Вверх – перемещает выделенную группу в списке вверх, сохраняя уровень группы в дереве

Вниз – перемещает выделенную группу в списке вниз, сохраняя уровень группы в дереве.

17.4. Меню Клиенты

Меню **Клиенты** содержит следующие элементы:

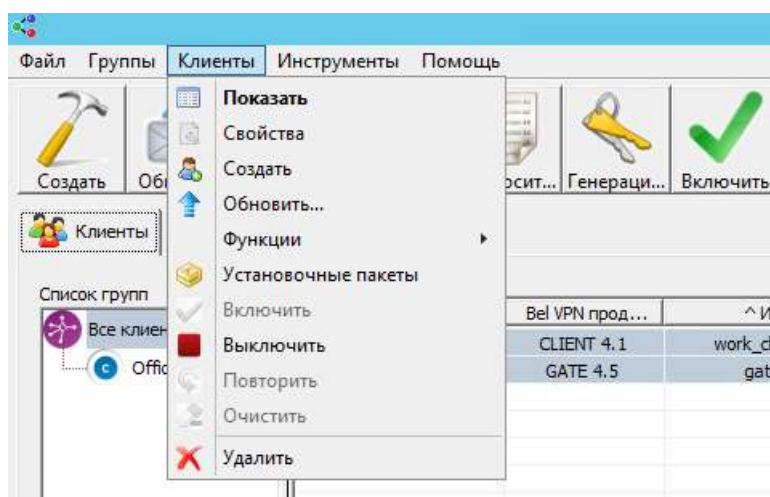


Рисунок 166

Показать – вызывает окно отображения параметров существующего клиента (Рисунок 129)

Свойства - вызывает окно **Свойства клиента** с информацией об управляемом устройстве и следующими полями:

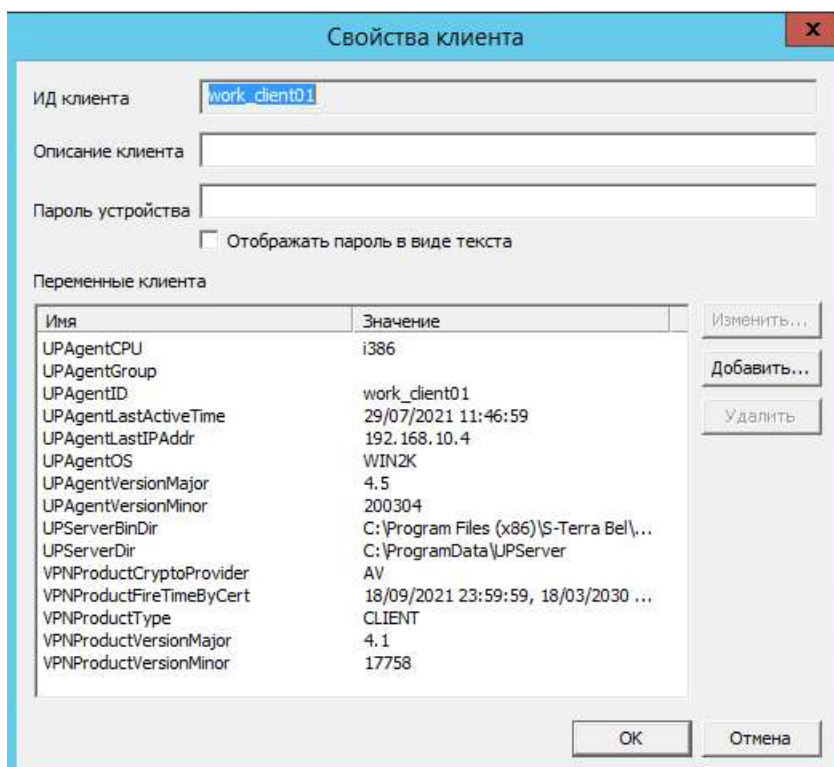


Рисунок 167

ИД клиента - идентификатор клиента

Описание клиента – введенная администратором в это поле информация будет отображена в поле Description вкладки **Clients** (Рисунок 162)

Пароль устройства – в данной версии это поле не используется

Отображать пароль в виде текста – в данной версии этот флаг не используется

Переменные клиента – список переменных, описывающих клиента, которые передаются скрипту `cook.bat` при его запуске в процессе подготовки расширенного обновления. Список переменных может быть дополнен администратором, используя кнопку **Add**. Все добавляемые переменные должны начинаться с префикса `EX_`.

Создать – вызывает окно **Создание нового клиента** создания нового клиента (Рисунок 78)

Обновить... – вызывает окно **Обновление для клиента** создания обновления для существующего клиента (Рисунок 168) со следующими полями:

ИД клиента – идентификатор клиента

Время создания – дата и время, когда создаваемое обновление будет доступно для скачивания Клиентом управления

Пакет продукта – имя инсталляционного файла Bel VPN Gate 4.5/4.1/Client-P 4.1 (который был создан с помощью продукта Bel VPN Client-P 4.1 AdminTool) или имя файла с данными продукта Bel VPN Gate 4.5/4.1/Client-P 4.1, созданного с помощью окна **VPN data maker**, вызываемого кнопкой **E**

Кнопка **E** – вызывает окно **VPN data maker** (Рисунок 55) для задания политики безопасности и настроек продукта Bel VPN Gate 4.5/4.1/Client-P 4.1

UPAgent директория – имя каталога, в котором расположен инсталляционный файл Клиента управления (заполняется, если надо установить новую версию Клиента управления)

UPAgent настройки – имя файла с настройками Клиента управления (заполняется, если надо обновить настройки Клиента управления) (см. главу «[Настройки Клиента управления](#)»)

Расширенные данные - путь к каталогу, в котором расположены расширенные данные и скрипты обновления

Отправить список текущих UPServer УЦ сертификатов клиенту – установка флажка для пересылки клиенту вместе с обновлением актуального списка СА сертификатов Сервера управления.

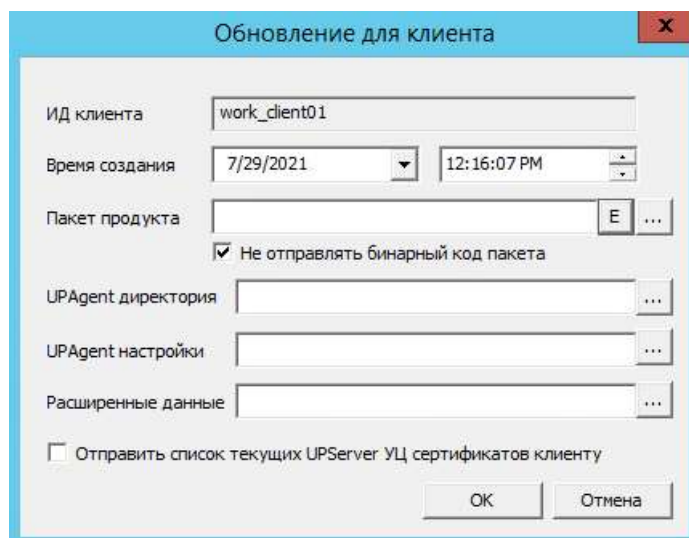


Рисунок 168

Функции – вызывает подменю (Рисунок 169):

Ключевая пара – позволяет задать действия с ключевой парой на управляемом устройстве:

Генерация – создать ключевую пару на управляемом устройстве. При выборе этого предложения появляется окно **Создание ключевой пары** (Рисунок 101) для задания параметров ключевой пары и запроса на сертификат.

Удалить – удалить ключевую пару с управляемого устройства, при этом появляется окно **Удаление контейнера** (Рисунок 170) для задания параметров удаляемой ключевой пары:

Время создания – дата и время, когда Сервер управления сделает доступным для скачивания Клиентом управления пакет обновления, содержащий данные для удаления ключевой пары на управляемом устройстве. Если указанное время уже прошло, то пакет обновления будет открыт для скачивания сразу после его создания

Имя контейнера – имя контейнера на управляемом устройстве, который будет удален. Поле является обязательным для заполнения. В выпадающем списке присутствуют имена существующих, но не используемых VPN-продуктом контейнеров

Пароль контейнера – пароль контейнера, который будет использоваться при удалении. Если это поле не задано, то пароль считается пустым.

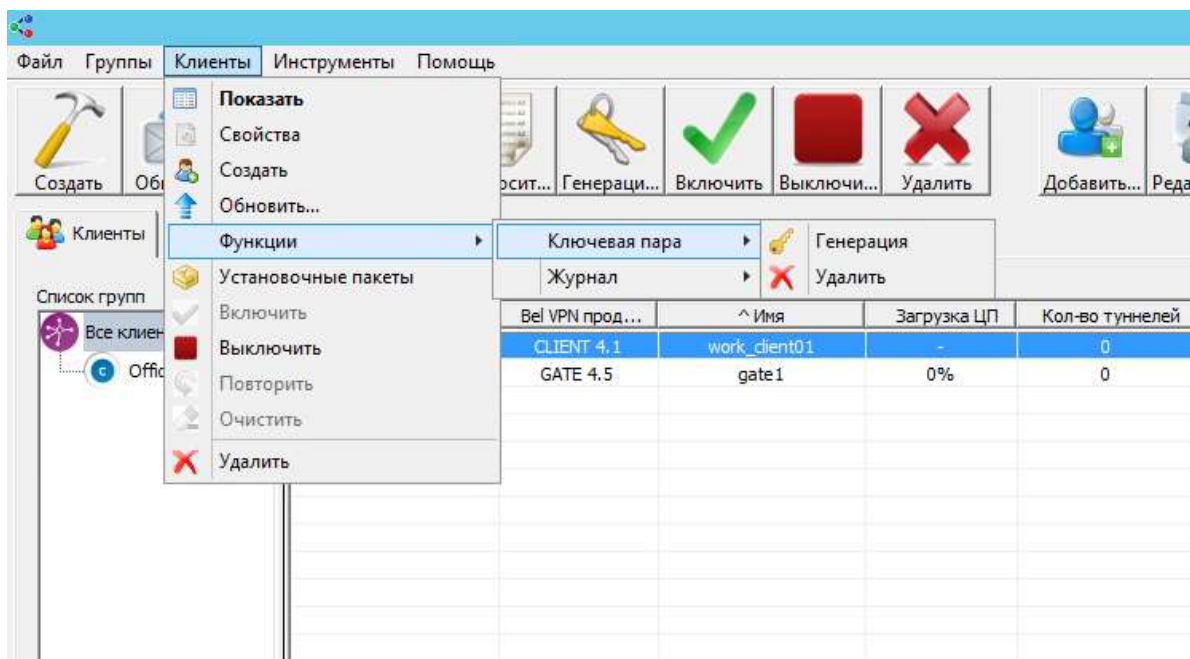


Рисунок 169

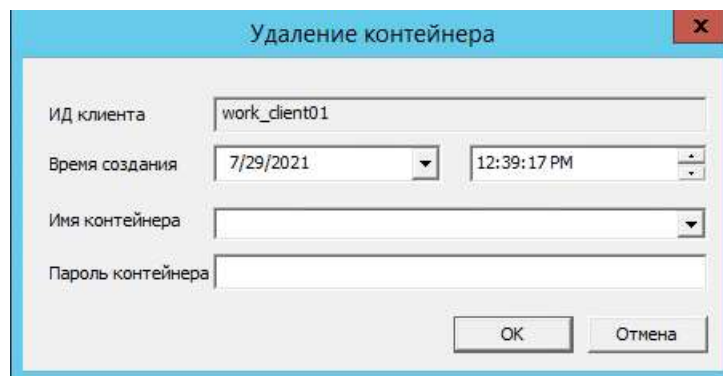


Рисунок 170

Журнал – позволяет задать настройки протоколирования событий на управляемом устройстве, при этом возможны два действия (Рисунок 171):

Установить – задать параметры протоколирования в окне **Установка журнала** (Рисунок 172):

Время создания – дата и время, когда пакет обновления с настройками протоколирования на управляемом устройстве, будет доступен для скачивания. Если указанное время уже прошло, то пакет обновления будет открыт для скачивания сразу после его создания

Состояние – состояние системы протоколирования:

- ON – включить пересылку syslog сообщений в стандартную систему протоколирования операционной системы Windows
- OFF – выключить пересылку syslog сообщений в стандартную систему протоколирования операционной системы Windows

Эта настройка работает только для управляемых устройств с ОС Windows. Для устройств с ОС Unix эта настройка не применяется, журналирование на таких устройствах включено по умолчанию и не может быть отключено.

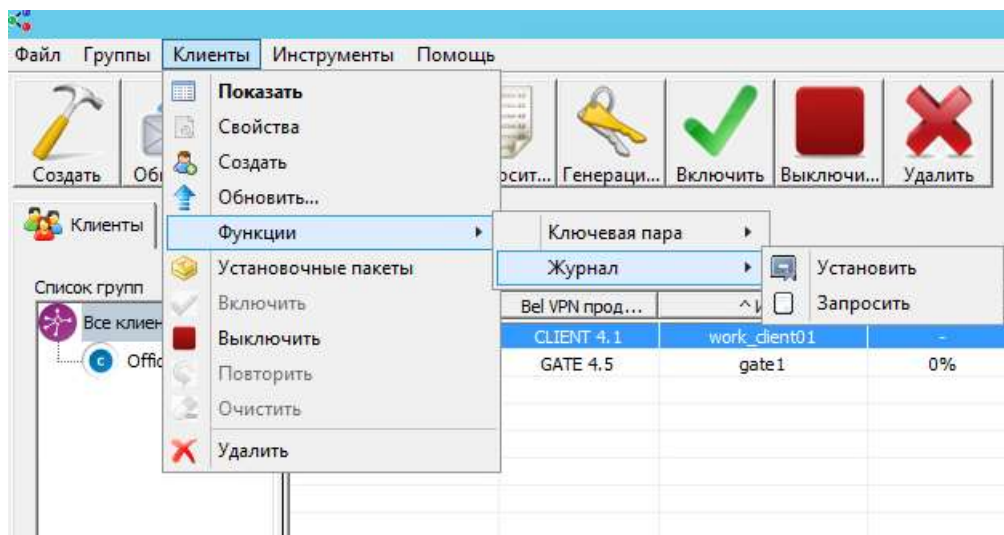


Рисунок 171

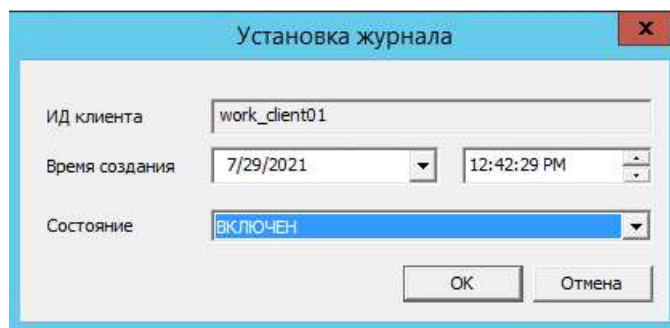


Рисунок 172

Запросить – запросить данные из системы протоколирования на управляемом устройстве, заполнив в окне **Запрос журнала** (Рисунок 173) поле:

Время создания – дата и время, когда пакет обновления с запросом данных протоколирования syslog канала, будет доступен для скачивания. Если указанное время уже прошло, то пакет обновления будет открыт для скачивания сразу после его создания.

Установочные пакеты – вызывает окно запроса каталога, в который будут сохранены инициализационные дистрибутивы для управляемого устройства

Включить – включает механизм обмена данными с клиентом

Выключить – выключает механизм обмена данными с клиентом

Повторить – снимает признак неудачного обновления, вследствие чего обновление будет скачено Клиентом управления еще раз, без каких либо изменений

Очистить – удаляет все непримененные обновления для клиента (предназначено для отмены неудачных обновлений)

Удалить – удаляет информацию о клиенте с Сервера управления.

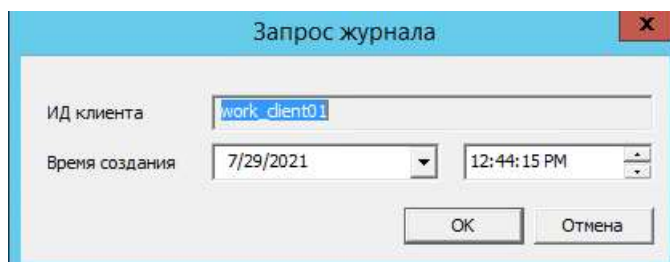


Рисунок 173

17.5. Меню Инструменты

Меню **Инструменты** содержит предложения [VPN data maker](#), [VPN data converter](#), [UPFlash creator](#), [User edition](#), [Statistic DB editor](#) (Рисунок 174):

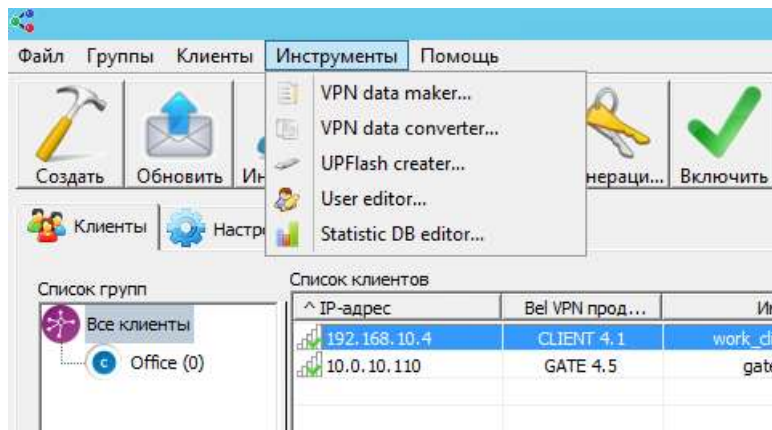


Рисунок 174

Предложение **VPN data maker** вызывает одноименное окно **VPN data maker** для задания настроек продукта Bel VPN Gate 4.5/4.1/Client-P 4.1 для нового проекта (Рисунок 175). Сделать это можно с использованием:

- [вкладок данного окна](#)
- или [окон мастера](#), вызываемого кнопкой [Запуск Мастера](#).

Созданный проект можно [сохранить в файл](#) и использовать при создании обновления для клиента (указать созданный файл в поле **Пакет продукта** окна **Обновление для клиента**).

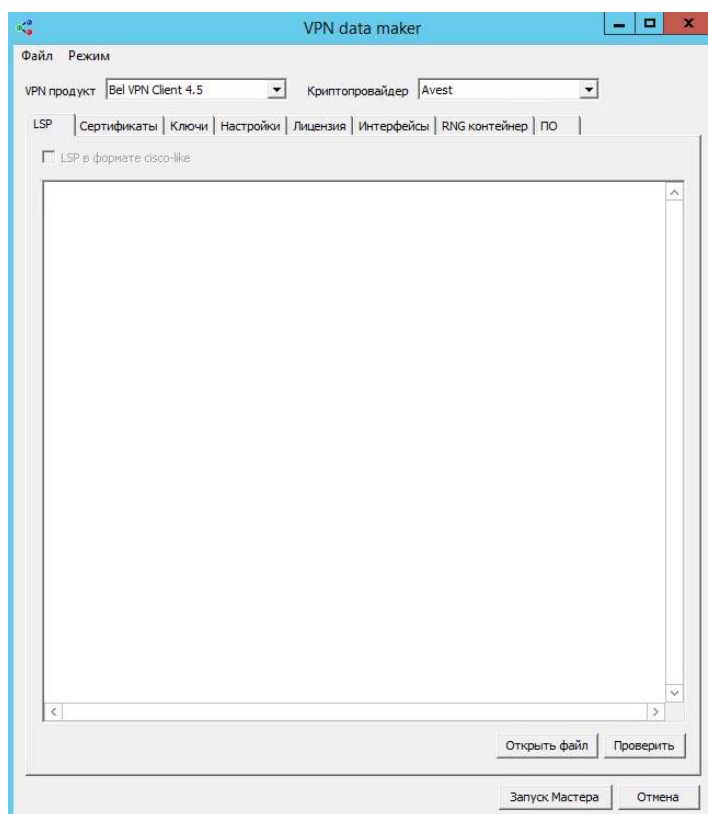


Рисунок 175

17.5.1. Задание политики и настроек с использованием вкладок

VPN продукт только в режиме шаблона проекта – выпадающий список, из которого выбирается продукт, для которого далее задаются все настройки во вкладках:

Bel VPN Client 4.1
 Bel VPN Gate 4.1
 Bel VPN Client 4.5
 Bel VPN Gate 4.5

Криптопровайдер – выпадающий список с используемым криптопровайдером в продукте:

Avest – криптопровайдер ЗАО «Авест»

LSP – вкладка для задания локальной политики безопасности продукта Bel VPN Gate/Client, предписанной управляемому устройству (Рисунок 175):

LSP в формате cisco-like – установка этого флажка говорит о том, что локальная политика безопасности задана в формате cisco-like

Открыть файл - нажатие этой кнопки вызывает окно для загрузки LSP из файла

Проверить – запускает процесс проверки синтаксиса LSP. В этой версии продукта проверка синтаксиса LSP в виде cisco-like формата не производится

Запуск Мастера – вызывает **окно мастера** задания настроек.

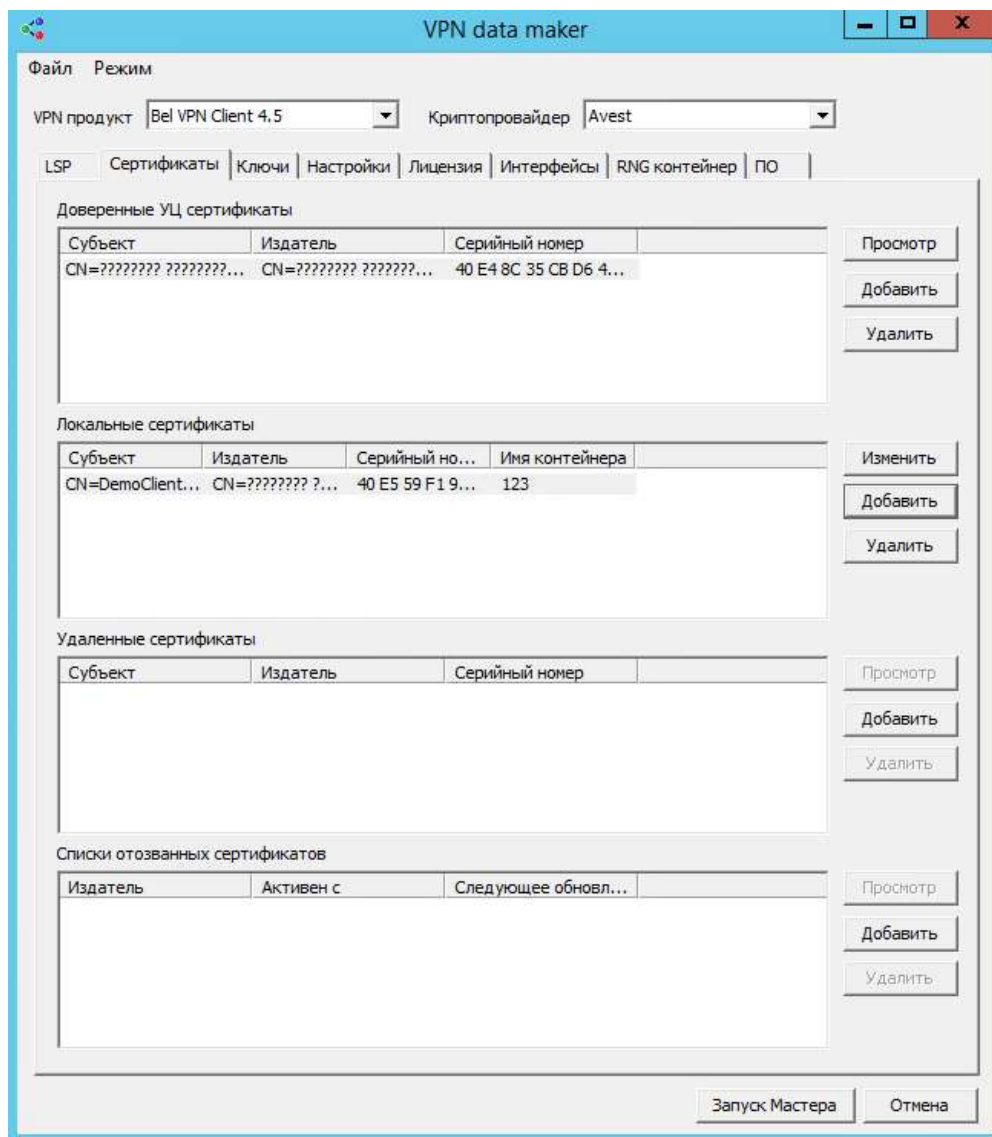


Рисунок 176

Сертификаты – вкладка для задания CA, локальных, партнерских и списков отозванных сертификатов для продукта Bel VPN Gate 4.5/4.1/Client-P 4.1 (Рисунок 176).

Keys – вкладка для задания предопределенных ключей для работы продукта Bel VPN Gate 4.5/4.1/Client-P 4.1 с партнерами (Рисунок 177).

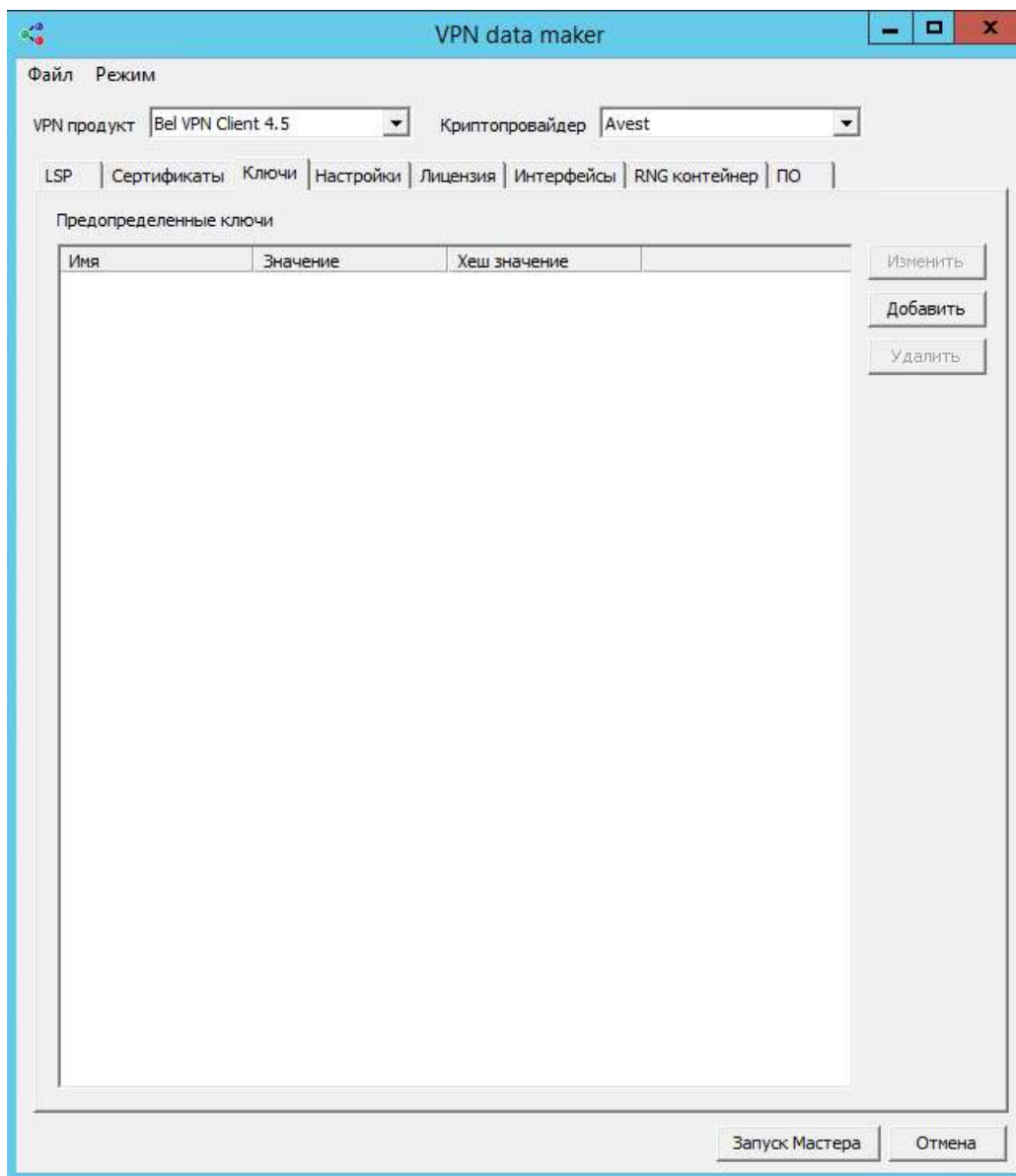


Рисунок 177

Настройки – вкладка для задания настроек управляемого устройства.

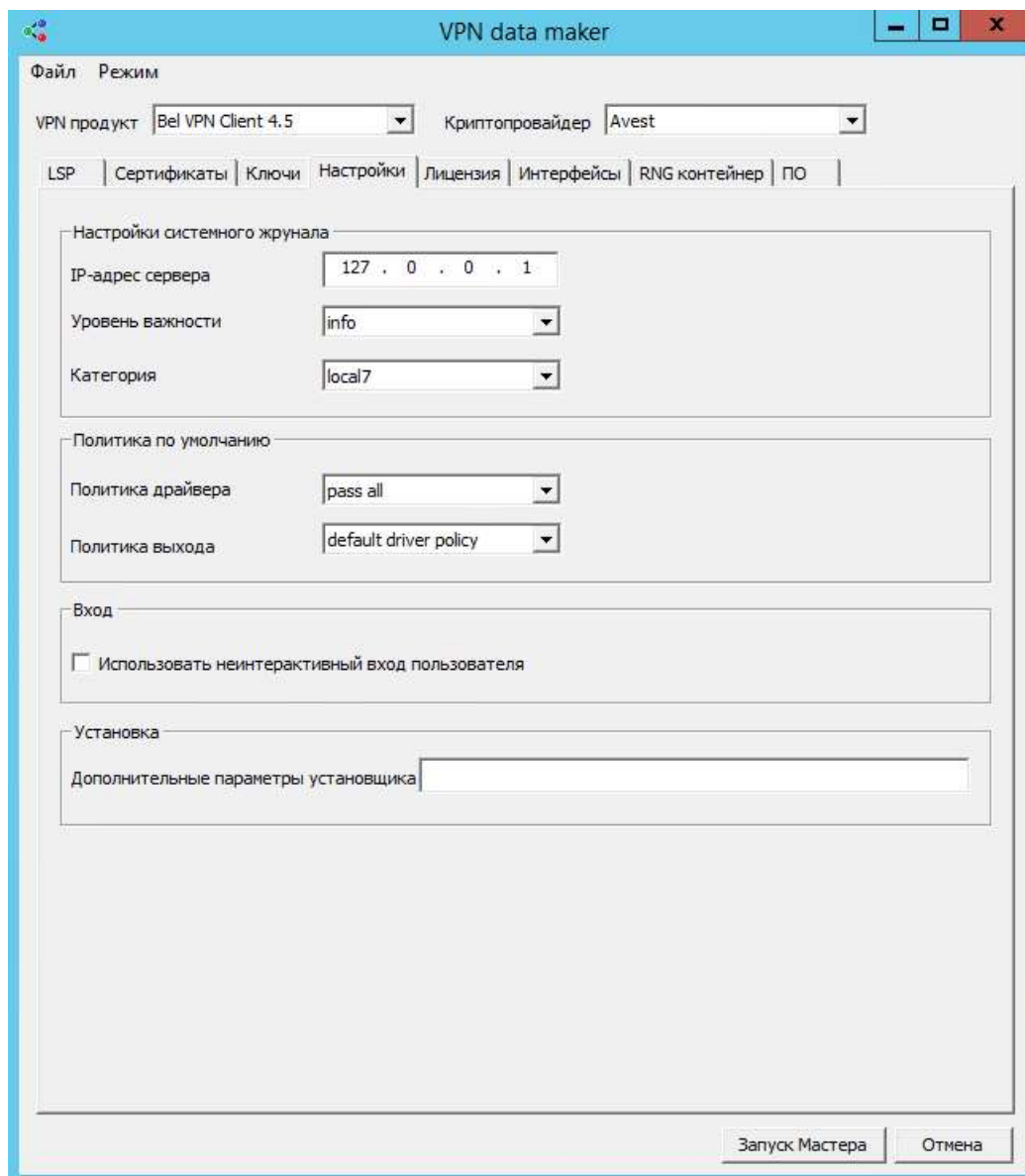


Рисунок 178

Лицензия – вкладка для ввода данных лицензии на продукт Bel VPN Gate 4.5/4.1/Client-P 4.1.

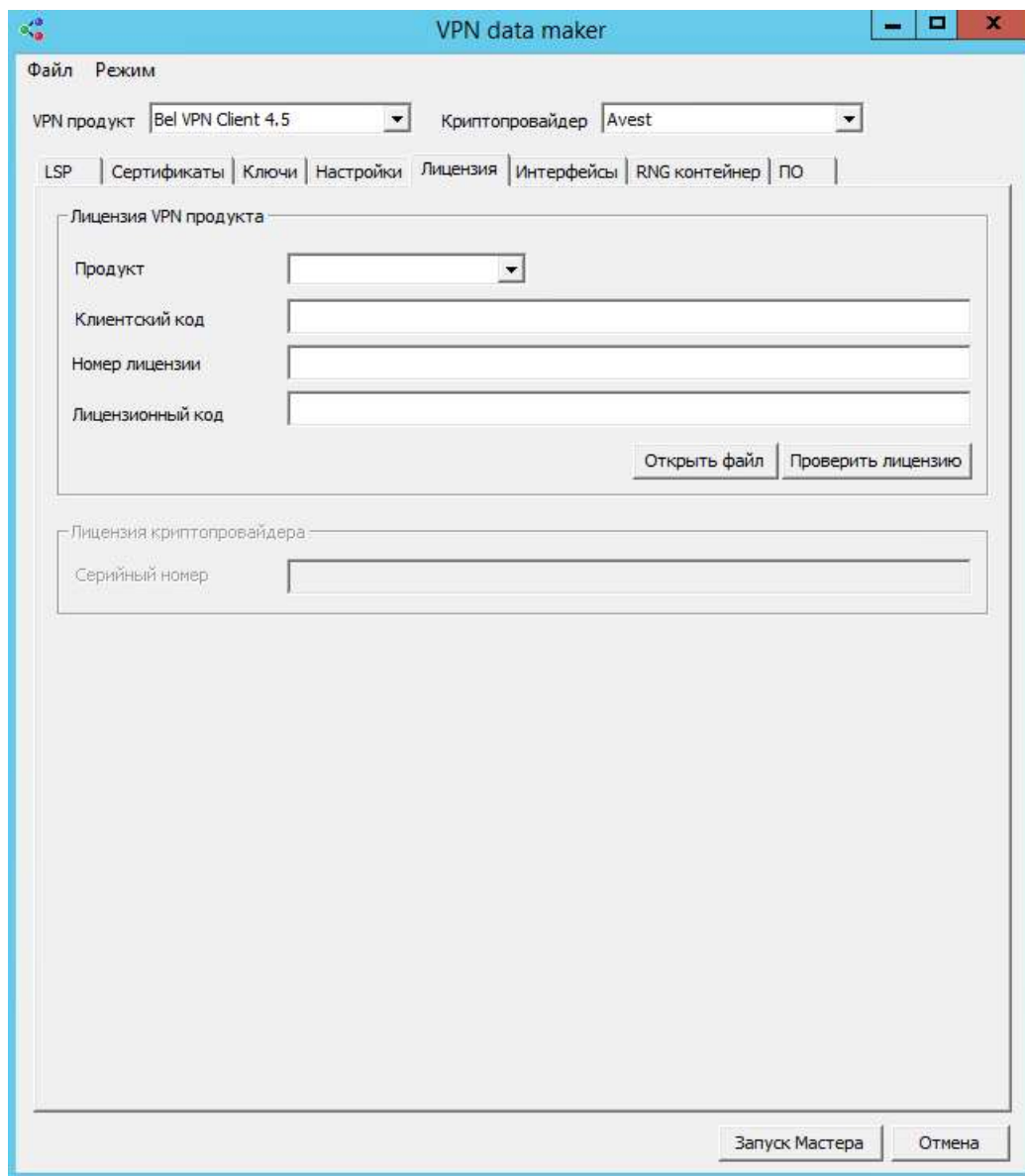


Рисунок 179

Интерфейсы — вкладка для задания настроек сетевых интерфейсов управляемого устройства.

VPN data maker

Файл Режим

VPN продукт: Bel VPN Client 4.5 Криптопровайдер: Avest

LSP | Сертификаты | Ключи | **Настройки** | Лицензия | Интерфейсы | RNG контейнер | ПО

Адрес виртуального устройства: . . .

☐ Описание сетевых интерфейсов

Имя	Описание
-----	----------

Изменить
Добавить
Удалить
Вверх
Вниз
Открыть
Сохранить

Расширенная маршрутизация

Назначение	Шлюз
------------	------

Изменить
Добавить
Удалить

☐ Псевдонимы сетевых интерфейсов

Логическое имя	Физическое имя
----------------	----------------

Изменить
Добавить
Удалить

☐ Настройки драйвера

Переменная	Значение
------------	----------

Изменить
Добавить
Удалить

Запуск Мастера Отмена

Рисунок 180

Адрес виртуального устройства – поле зарезервировано для будущего применения

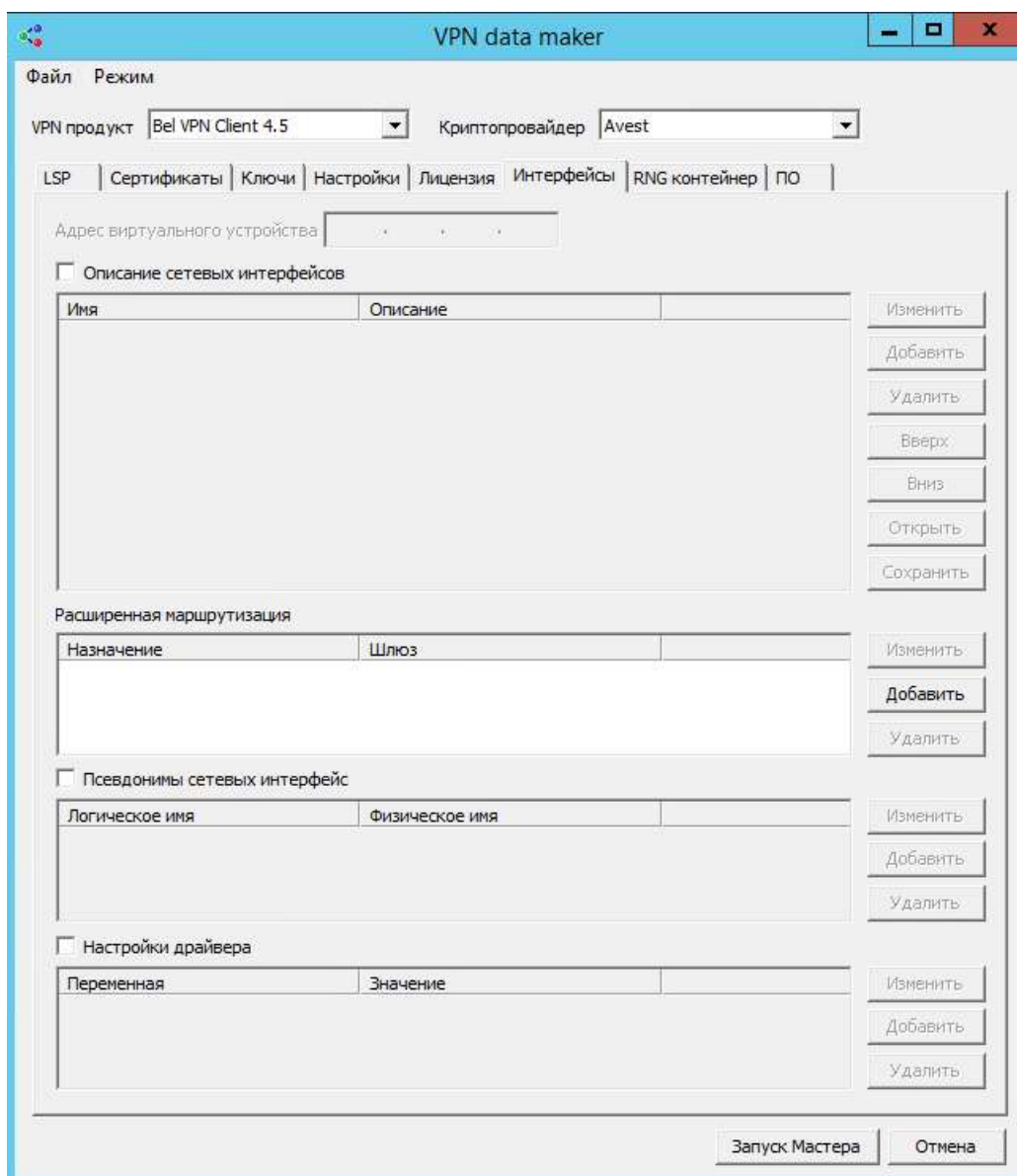


Рисунок 181

Псевдонимы сетевых интрерфейсов – установка этого флажка позволяет добавлять, модифицировать, удалять логические и физические имена сетевых интерфейсов

Настройки драйвера – установка флажка позволяет изменить настройки IPsec драйвера, установленные по умолчанию (Рисунок 182). Эти настройки имеются только у продукта Bel VPN Gate 4.5/4.1. Описание этих настроек (утилита drv_mgr) см. в документе «Специализированные команды», входящем в состав продукта.

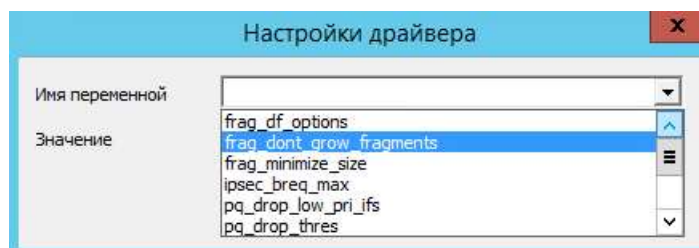


Рисунок 182

RNG контейнер – вкладка задания местоположения криптографического (RNG) контейнера, содержащего инициализационные данные для датчика случайных чисел (ДСЧ). Зарезервирован для будущего применения.

ПО – вкладка для задания настроек дополнительных продуктов, установленных на управляемом устройстве. Зарезервировано для будущего применения.

Сохранение и загрузка настроек продукта

Меню **Файл** окна **VPN data maker** содержит два предложения (Рисунок 183):

Открыть – загружает настройки из файла данных продукта Bel VPN Gate 4.5/4.1/Client-P 4.1.

Сохранить как – сохраняет в файл данные продукта Bel VPN Gate 4.5/4.1/Client-P 4.1, отраженные во вкладках окна **VPN data maker**.

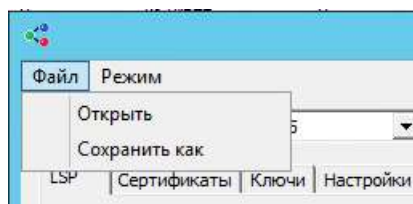


Рисунок 183

17.5.2. Задание политики и настроек с использованием мастера

При нажатии кнопки **Запуск Мастера** в окне **VPN data maker** появляется первое окно мастера для задания сертификатов и предопределенных ключей (Рисунок 184).

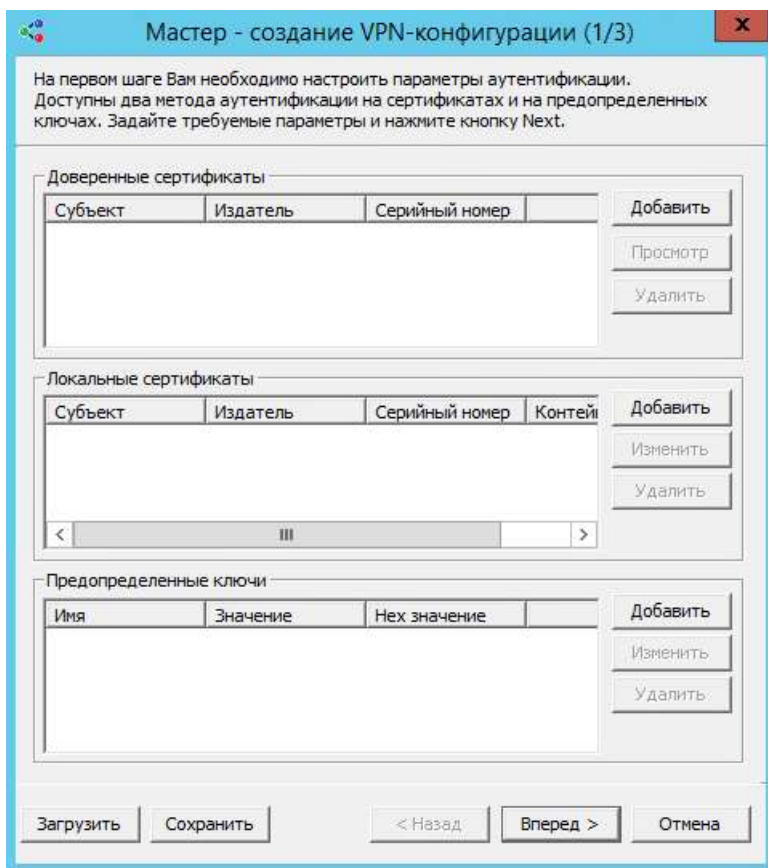


Рисунок 184

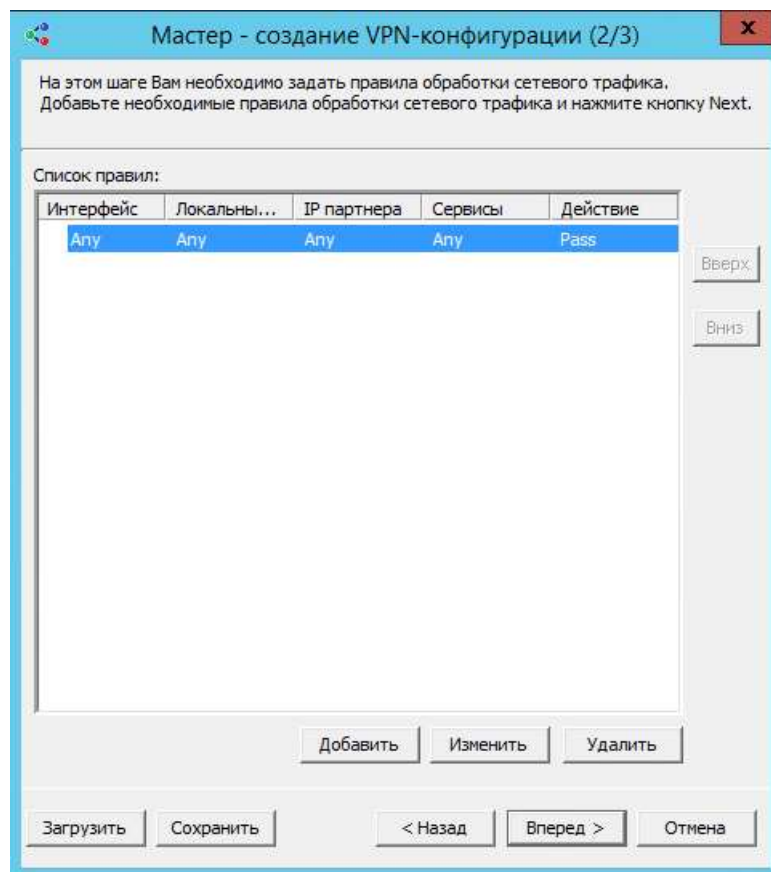


Рисунок 186

В окне задания правила в разделе **Действие** кнопка [Расширенные настройки](#) предназначена для задания расширенных настроек правила (Рисунок 187).

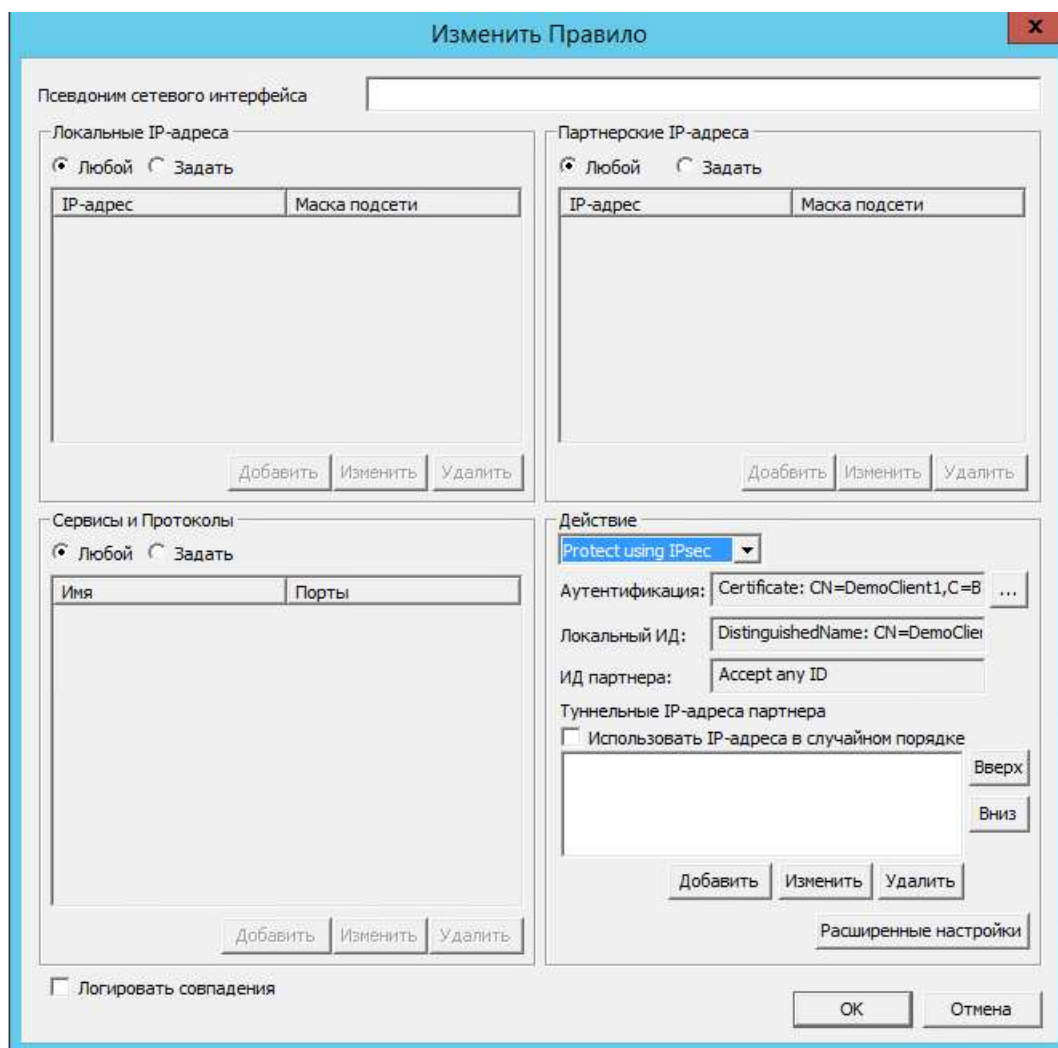


Рисунок 187

В первой вкладке **IKE настройки** расширенных настроек представлен упорядоченный список алгоритмов, который предлагается партнеру для согласования, который может использоваться для защиты трафика при создании ISAKMP соединения (Рисунок 188).

IKE наборы – упорядоченный список IKE предложений по приоритету. В верхней строчке находится предложение с наивысшим приоритетом.

Шифрование – предлагаемые алгоритмы шифрования пакетов. Предлагаются следующие белорусские криптографические алгоритмы:

- СТБ 34.101.31-2011

Также есть возможность выбрать международный алгоритм шифрования AES-256.

Целостность – предлагаемые алгоритмы проверки целостности пакетов. Предлагаются следующие белорусские криптографические алгоритмы:

- СТБ 34.101.31-2011

Также есть возможность выбрать международный алгоритм SHA1.

Группа – параметры выработки общего сессионного ключа по алгоритму Диффи-Хеллмана:

BELTDH – протокол формирования общего ключа на основе эллиптических кривых согласно СТБ 34.101.66-2014 (приложение А).

MODP_768 – группа 1 (768-битовый вариант алгоритма Диффи-Хеллмана)

MODP_1024 – группа 2 (1024-битовый вариант алгоритма Диффи-Хеллмана)

MODP_1536 – группа 5 (1536-битовый вариант алгоритма Диффи-Хеллмана).

Включить агрессивный режим – установка этого флажка позволяет использовать агрессивный режим обмена информацией о параметрах защиты и установления ISAKMP SA. В этом режиме партнеру высылается только первая IKE политика из списка, имеющая самый высокий приоритет. При выборе этого режима выдается об этом предупреждение. Если для аутентификации используется предопределенный ключ и выбран тип идентификатора *KeyID*, то должен использоваться только режим Aggressive. При отсутствии этого флажка используется основной режим - партнеру высылаются все IKE политики для выбора и согласования.

Время жизни (sec) – время в секундах, в течение которого ISAKMP SA будет существовать. Возможное значение – целое число из диапазона 0..2147483647. Рекомендуемое значение – 28800, которое выставлено при открытии нового проекта. Значение 0 означает, что время действия SA не ограничено. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

Время жизни (Kb) – указывает объем данных в килобайтах, который могут передать стороны во всех IPsec SA, созданных в рамках одного ISAKMP SA. Возможное значение – целое число из диапазона 0..2147483647. Рекомендуемое значение – 0, которое выставлено при открытии нового проекта. Значение 0 означает, что объем данных в килобайтах не ограничен. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

IPsec SA – количество IPsec SA, созданных в рамках одного ISAKMP SA. Значение 0 означает, что количество IPsec SA не ограничено.

Сертификат – задает логику отсылки локального сертификата на запрос партнера в процессе первой фазы IKE. В своем запросе партнер может указать какому CA сертификату он доверяет. Если такой сертификат не найден, то он не отправляется. Возможные значения:

AUTO – автоматически определяется, когда необходима отсылка локального сертификата партнеру (значение по умолчанию).

NEVER – сертификат не высылается.

ALWAYS – сертификат высылается всегда.

CHAIN – сертификат высылается всегда, причем в составе с цепочкой доверительных CA. Имеется ввиду цепочка сертификатов, построенная от локального сертификата до CA, который удовлетворяет описанию, присланному партнером в запросе. В общем случае это CA, удовлетворяющий запросу партнера, произвольное количество промежуточных CA и локальный сертификат.

Расширенные настройки правил

IKE настройки | IKECFG настройки | IPsec настройки

IKE наборы

Шифрование	Целостность	Группа
GOST 28147-89	STB 1176.1	BELTDH
GOST 28147-89	STB 34.101.31-2011 (6.9)	BELTDH
STB 34.101.31-2011 (6.4)	STB 1176.1	BELTDH
STB 34.101.31-2011 (6.4)	STB 34.101.31-2011 (6.9)	BELTDH
GOST 28147-89	STB 1176.1	MODP_1536
GOST 28147-89	STB 1176.1	MODP_1024
GOST 28147-89	STB 1176.1	MODP_768
GOST 28147-89	STB 34.101.31-2011 (6.4)	MODP_1536

Добавить Изменить Удалить

☐ Включить агрессивный режим

Время жизни: 28800 sec 0 Kb 0 IPsec SA

Сертификат: AUTO отправлять: AUTO

☐ Выключить смену ключей ☐ Выключить DPD

OK Отмена

Рисунок 188

отправлять – задает логику отсылки запроса на сертификат партнера. Возможные значения:

AUTO – запрос высылается, если возможный сертификат партнера отсутствует (значение по умолчанию).

NEVER – запрос не высылается.

ALWAYS – запрос высылается всегда.

Выключить смену ключей – установка этого флажка приводит к тому, что заблаговременная смена ключевого материала (сессионного ключа) не проводится.

Выключить DPD – установка этого флажка отключает использование протокола DPD для проверки IKE соединения.

Во второй вкладке **IKECFG настройки** (Рисунок 189) задаются данные для использования протокола IKECFG.

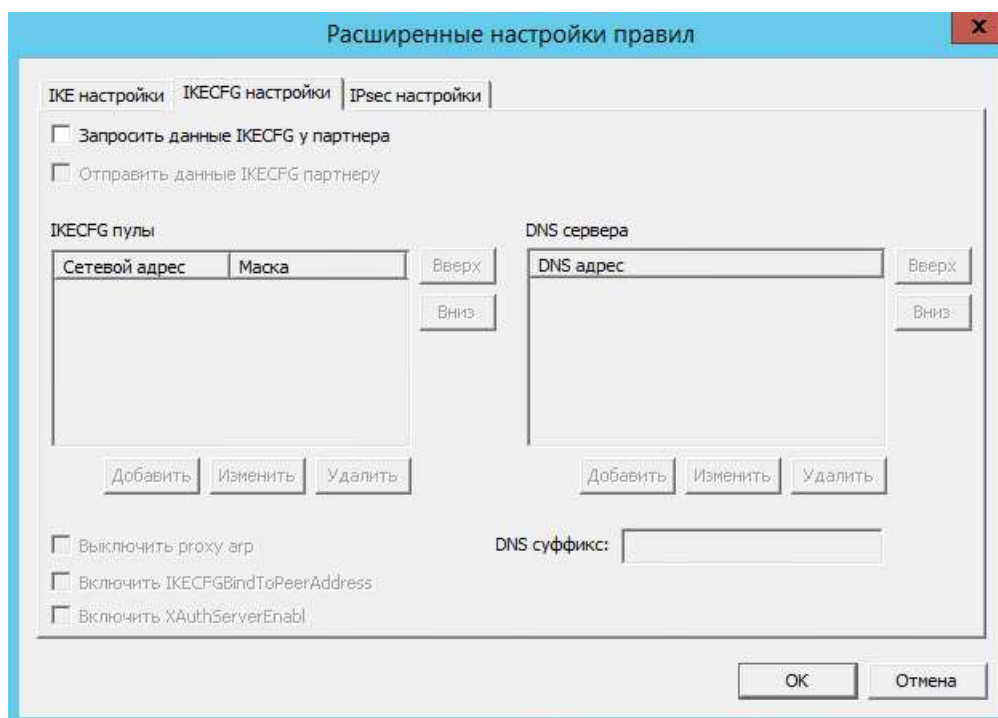


Рисунок 189

Запросить данные IKECFG у партнера – при установке этого флажка у партнера будут запрашиваться данные по протоколу IKECFG – адрес из пула, адреса DNS серверов, DNS суффиксы (для продуктов Bel VPN Client-P 4.1).

Отправить данные IKECFG партнеру – при установке этого флажка партнеру будут передаваться данные по протоколу IKECFG: адрес из пула, адреса DNS серверов, DNS суффиксы (для продуктов Bel VPN Gate 4.5/4.1).

IKECFG пулы – в этом поле следует задать адреса IKECFG пулов (для продуктов Bel VPN Gate 4.1).

DNS сервера – в этом поле следует задать адреса DNS серверов (для продуктов Bel VPN Gate 4.1).

DNS суффикс – в этом поле следует задать DNS суффикс (для продуктов Bel VPN Gate 4.1).

Выключить проху arp –

при установке этого флажка - адреса не проксируются

при снятии флажка - при неустановленном флажке Bel VPN Gate выступает в роли ProхуARP для указанного множества адресов пула. Если IP-адрес не попадает ни в одну

из защищаемых локальных подсетей, проху-агр запись не создается, и это не считается ошибкой

Включить IKECFGBindToPeerAddress –

при установке этого флажка - IKECFG сервер будет идентифицировать клиентов по IP-адресу и порту партнера (видимые гейту, по которым построен ISAKMP SA)

при снятии флажка - идентификация клиентов осуществляется по ID первой фазы IKE).

Включить XauthServerEnable –

при установке этого флажка – Bel VPN Gate выступает в роли XAuth-сервера. Для данного IKE правила шлюз требует поддержку метода аутентификации с использованием XAuth. После успешного построения ISAKMP SA, Bel VPN Gate иницирует XAuth-сессию.

при снятии флажка – Bel VPN Gate работает в обычном режиме, XAuth-обмены не проводятся.

В третьей вкладке **IPsec настройки** (Рисунок 190) задаются параметры, которые используются при защите трафика. Партнеру направляется список наборов преобразований, по протоколу IKE происходит согласование и выбор конкретного набора преобразований, который будет использоваться для защиты трафика одного SA.

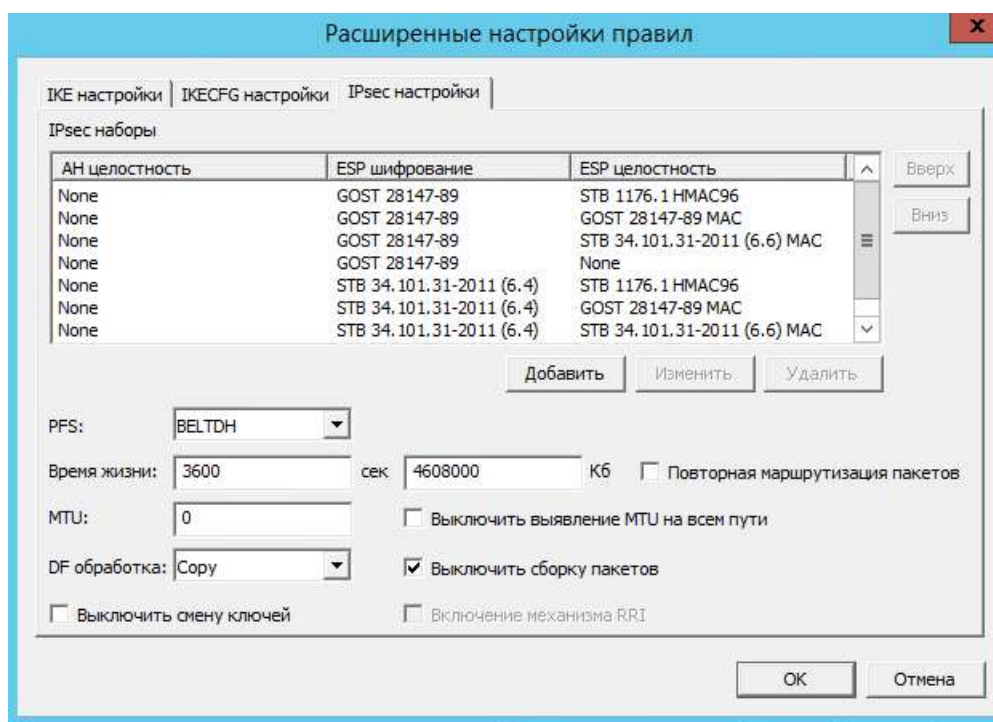


Рисунок 190

IPsec наборы – упорядоченный по приоритету список наборов преобразований, высылаемых партнеру для согласования. При помощи кнопок Up и Down выполняется упорядочивание списка по приоритету. В верхней строчке находится набор преобразований с наивысшим приоритетом.

АН целостность – предлагаемые алгоритмы проверки целостности пакета по протоколу АН. Имеются следующие значения:

- *None* – алгоритм проверки целостности не применяется;
- *СТБ 34.101.31-2011* – белорусский криптографический алгоритм;
- *СТБ 1176.1-99* – белорусский криптографический алгоритм;
- *ГОСТ 28147-89* – белорусский криптографический алгоритм;

- также есть возможность добавить преобразование *SHA1* – международный криптографический алгоритм.

ESP целостность – предлагаемые алгоритмы проверки целостности пакета по протоколу ESP. Имеются следующие значения:

- *None* – алгоритм проверки целостности не применяется;
- *СТБ 34.101.31-2011 (раздел 6.6)* – белорусский криптографический алгоритм;
- *СТБ 1176.1-99* – белорусский криптографический алгоритм;
- *ГОСТ 28147-89* – белорусский криптографический алгоритм;
- также есть возможность добавить преобразование *SHA1* – международный криптографический алгоритм.

ESP шифрование – предлагаемые алгоритмы шифрования пакетов по протоколу ESP:

- *None* – алгоритм шифрования ESP не применяется;
- *Null* – алгоритм применять, но не шифровать;
- *СТБ 34.101.31-2011 (раздел 6.4)* – белорусский криптографический алгоритм;
- *ГОСТ 28147-89* – белорусский криптографический алгоритм;
- Также есть возможность добавить преобразование *AES-256* – международный криптографический алгоритм.

PFS– параметры выработки ключевого материала, высылаемые партнеру для согласования:

No PFS – опция PFS не включена и при согласовании новой SA новый обмен по алгоритму Диффи-Хеллмана для выработки общего сессионного ключа не выполняется. Ключевой материал заимствуется из первой фазы IKE.

Выбранный параметр означает, что при согласовании новой SA выполняется новый обмен ключами по алгоритму Диффи-Хеллмана в рамках IPsec. Может использоваться один из параметров:

BELTDH – используется алгоритм Диффи-Хеллмана на эллиптических кривых по СТБ 34.101.66-2014 (Приложение А).

MODP_768 – группа 1 (768-битовый вариант алгоритма Диффи-Хеллмана).

MODP_1024 – группа 2 (1024-битовый вариант алгоритма Диффи-Хеллмана).

MODP_1536 – группа 5 (1536-битовый вариант алгоритма Диффи-Хеллмана).

Время жизни (sec) – время в секундах, в течение которого IPsec SA будет существовать. Возможное значение – целое число из диапазона 1..2147483647. Рекомендуемое значение – 3600, которое выставлено при открытии нового проекта. Пустая строка и значение 0, которое означает неограниченное время жизни IPsec SA, – недопустимы, при создании инсталляционного файла будет выдано сообщение об ошибке.

Время жизни (Kb) – указывает объем данных в килобайтах, который могут передать стороны в рамках одной IPsec SA. Возможное значение – целое число из диапазона 0..2147483647. Рекомендуемое значение – 4608000, которое выставлено при открытии вкладки. Значение 0 означает, что объем данных в килобайтах не ограничен. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

Повторная маршрутизация пакета:

при установке этого флажка – исходящий пакет после цикла обработки не отправляется в драйвер сетевого интерфейса, а направляется для повторной маршрутизации. Такой пакет может попасть на повторную обработку IPsec драйвером, так что правила фильтрации должны учитывать и пропускать такие пакеты. Устанавливать данный флажок имеет смысл для SA, заменяющих адрес назначения. Если по ходу обработки пакета адрес назначения не изменился, флаг *reroute packets* игнорируется.

при снятии флажка – пакет не будет подвергаться повторной маршрутизации/

MTU – задает значение MTU для IPsec SA, создаваемых по данному правилу, значение MTU используется только для исходящих пакетов и для последнего SA, примененного к пакету (в случае вложенного IPsec значение MTU для внутреннего SA игнорируется). Значение - целое число из диапазона 1..65535, рекомендуется устанавливать значение MTU не менее 670 байт, значение 0 означает, что MTU определяется автоматически.

Выключить выявление MTU на всем пути

при установке этого флажка - отключается алгоритм "Path MTU Discovery" (выявление максимального размера пакета, проходящего на всем пути от отправителя к получателю без фрагментации) для IPsec SA, создаваемых по данному правилу. ICMP-сообщения не обрабатываются, значение MTU вычисляется только из локальной конфигурации. *при снятии флажка* - обрабатываются ICMP-сообщения типа destination unreachable/fragmentation needed, приходящих в ответ на IPsec-пакеты. На основе этих сообщений вычисляется эффективное значение MTU трассы.

DF обработка – задает алгоритм формирования DF (Don't Fragment) бита внешнего IP-заголовка для туннельного режима IPsec:

COPY – копировать DF бит из внутреннего заголовка во внешний заголовок

SET – всегда устанавливать DF бит внешнего заголовка в 1

CLEAR – всегда сбрасывать DF бит внешнего заголовка в 0.

Выключить сборку пакетов – сборка пакета из IP-фрагментов перед инкапсуляцией в IPsec:

при установке этого флажка – пакет не подвергается сборке

при снятии флажка – пакет будет собран из IP-фрагментов перед инкапсуляцией в IPsec. Рекомендуется устанавливать при работе по защищенному соединению с предыдущими версиями Шлюза безопасности. В транспортном режиме IPsec сборка пакетов перед инкапсуляцией производится всегда.

Выключить смену ключей – задает режим "мягкой" смены ключевого материала:

при установке этого флажка – заблаговременная смена ключевого материала (rekeying) не проводится. При отсутствии подходящего IPsec соединения, новый IPsec SA создаётся только по запросу из ядра – при наличии исходящего IP-пакета, либо по инициативе партнера. В результате, во время создания нового IPsec SA IP-трафик приостанавливается, а при интенсивном трафике возможна потеря пакетов.

при снятии флажка – заблаговременно, незадолго до окончания действия IPsec соединения, на его основе (с теми же параметрами) проводится IKE-сессия (Quick Mode) по созданию нового IPsec SA – rekeying. Rekeying не проводится, если за время существования старого SA под его защитой не было никакого трафика.

Включение механизма RRI:

при установке этого флажка – после установления защищенного соединения с удаленным партнером, при включенном механизме RRI, в системную таблицу маршрутизации автоматически добавляется запись об обратном маршруте

при снятии флажка – механизм RRI выключен, при создании SA по этому IPsec правилу дополнительных действий не предпринимается.

17.5.3. Конвертирование политики

При выборе предложения **vpn data converter** появляется окно **VPN data converter** для преобразования политики безопасности из одной версии продукта в другую, из текстового представления (LSP) в cisco-like формат или наоборот.

При переходе на управляемом устройстве с одной версии продукта на другую и для перевода отлаженной политики безопасности в другую версию, можно использовать окно **VPN data converter**. Конвертирование отлаженной работающей политики применимо и для настройки другого управляемого устройства с другой версией продукта Bel VPN Gate/Client.

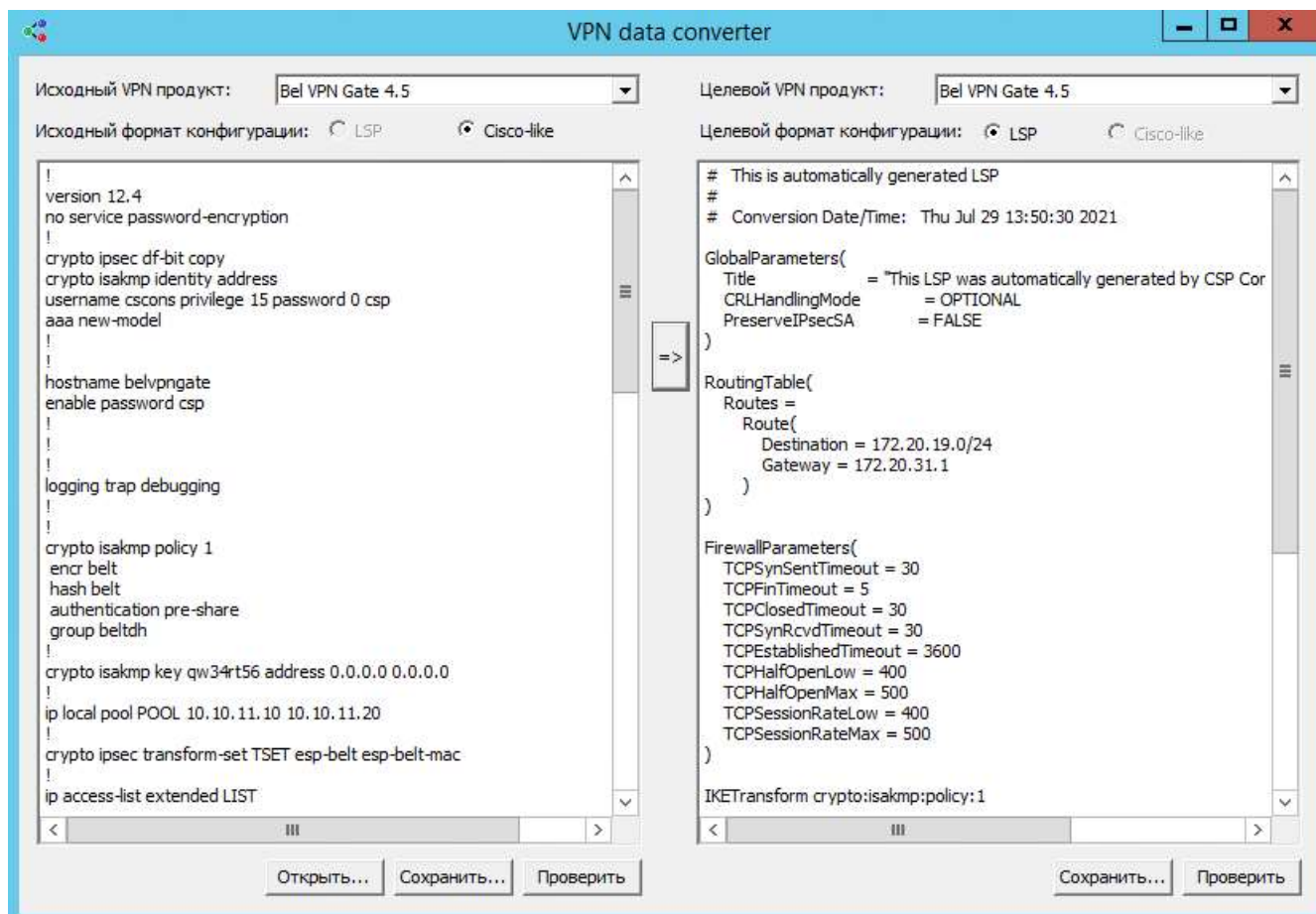


Рисунок 191

17.5.4. Создание носителя с образом диска для восстановления

При выборе предложения **UPFlash creator** появляется окно **UPFlash creator** для создания USB Flash, который можно использовать для восстановления образа Bel VPN Gate 4.5/4.1 на шлюзах или изменения версии образа.

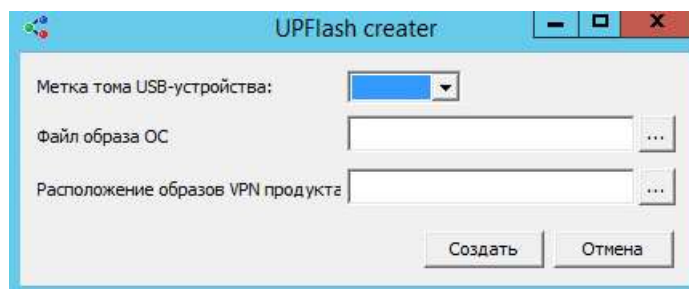


Рисунок 192

Метка тома USB-устройства – имя диска, которым представляется USB Flash носитель. На этот носитель будут записаны данные, позволяющие использовать этот USB Flash носитель как загрузочный для шлюзов.

Файл образа ОС – образ операционной системы, которая будет использоваться как базовая для загрузки с создаваемого USB Flash носителя. Данный файл можно будет скачать с сайта компании или запросить в службе поддержки

Расположение образов VPN продукта – каталог с образами шлюзов. Эти образы будут скопированы на USB Flash носитель и будут использованы для загрузки на шлюзы. Данные файлы можно будет скачать с сайта компании или запросить в службе поддержки.

17.5.5. Редактирование настроек базы данных

При выборе предложения **Statistic DB editor** появляется окно **Statistic DB editor...** для редактирования настроек базы данных, которая используется для хранения статистических данных об управляемых устройствах.

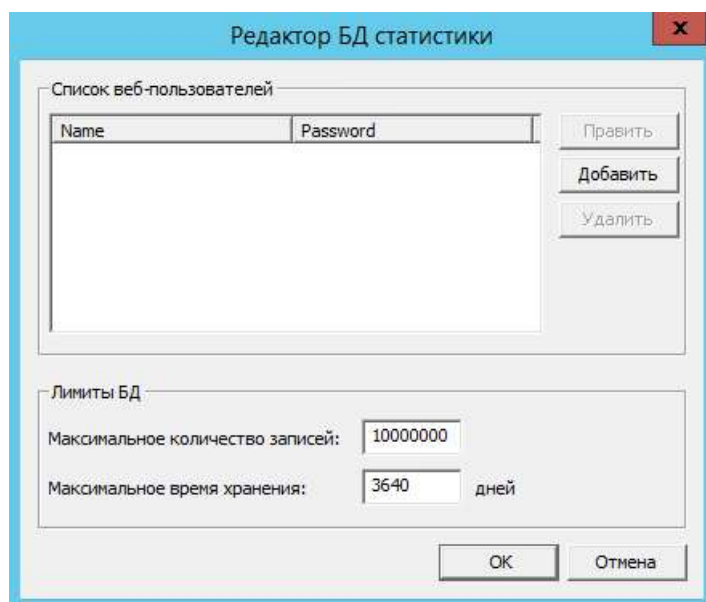


Рисунок 193

Списко веб-пользователей – список пользователей базы данных статистики, которые могут работать с данными базы данных через Web браузер, заходя на сервер под именами и паролями заданными в этом списке. (адрес для доступа к базе данных статистики https://АДРЕС_СЕРВЕРА:8443/)

Максимальное количество записей – максимальное количество записей статистики, полученных от всех управляемых устройств (по умолчанию каждое устройство присылает около 5000 записей в час)

Максимальное значение хранения – максимальное количество дней, которое будет храниться информация о действиях администратора, связанных с изменениями имен клиентов или групп клиентов (добавление/удаление/переименование клиентов или групп клиентов).

17.6. Меню Помощь

В меню **Помощь** предложение **О About VPN UPServer console** выводит информацию о продукте.



Рисунок 194

17.7. Панель инструментов

Под главным меню расположена панель инструментов, дублирующая некоторые из пунктов главного меню и предоставляющая быстрый доступ к ним.

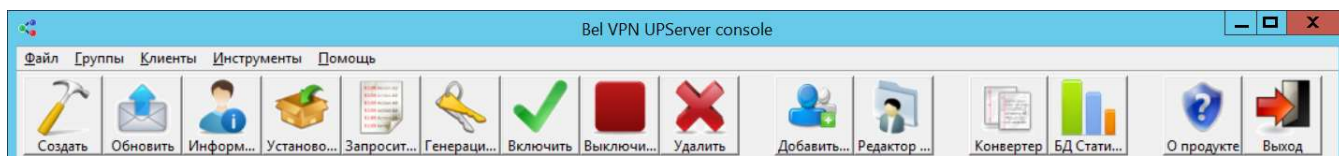


Рисунок 195

Создать – соответствует пункту меню **Клиенты – Создать**;

Обновить – соответствует пункту меню **Клиенты – Обновить**;

Информация – соответствует пункту меню **Клиенты – Показать**;

Установочные пакеты – соответствует пункту меню **Клиенты – Установочные пакеты**;

Запросить журнал – соответствует пункту меню **Клиенты – Функции – Журнал - Запросить**;

Генерация ключевой пары – соответствует пункту меню **Клиенты – Функции – Ключевая пара – Генерация**;

Включить – соответствует пункту меню **Клиенты – Включить**;

Выключить – соответствует пункту меню **Клиенты – Выключить**;

Удалить – соответствует пункту меню **Клиенты – Удалить**;

Добавить группу – соответствует пункту меню **Группы – Создать**;

Редактор пользователей – соответствует пункту меню **Инструменты – User Editor**;

Конвертер – соответствует пункту меню **Инструменты – VPN data converter**;

БД Статистика – соответствует пункту меню **Инструменты – БД Статистика**;

О продукте – соответствует пункту меню **Помощь – О Bel VPN UPServer console**;

Выход – соответствует пункту меню **Файл – Выход**;

18. Протоколирование событий

18.1. Сервер управления

Все сообщения о протоколируемых событиях Сервера управления по умолчанию записываются в файл:

`C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log.`

18.2. Клиент управления

На управляемом устройстве все сообщения о протоколируемых событиях Клиента управления по умолчанию записываются в файл:

для ОС Windows - `C:\Program Files\UPAgent\upagent.log`

для ОС Unix - `/var/log/upagent/upagent.log`

Эти же сообщения передаются на Сервер управления и их можно посмотреть во вкладке **Uplog** окна **Client information**, вызываемом выделением клиента в таблице и предложением **Show** в контекстном меню.

18.3. Продукт Bel VPN Gate 4.5/4.1/Client-P 4.1

На управляемом устройстве все сообщения от продукта **Bel VPN Gate 4.5/4.1/Client-P 4.1** передаются Клиентом управления на Сервер управления и их можно посмотреть во вкладке **VPNlog** окна **Информация о клиенте**, вызываемом выделением клиента в таблице и предложением **Показать** в контекстном меню.

Кроме того, на управляемом устройстве все сообщения о протоколируемых событиях работы продукта **Bel VPN Gate 4.5/4.1** передаются на локальный syslog-сервер:

- в файл **`/var/log/cspvpngate.log`** для аппаратных платформ с жестким диском
- в файл **`/tmp/cspvpngate.log`** для аппаратных платформ с флеш-диск

Протоколирование работы некоторых утилит и сервисов передается в специальные файлы. Все сообщения и настройка syslog-клиента и сервера описаны в документации продукта.

А для продуктов **Bel VPN Client-P 4.1** просмотр сообщений, посылаемых на локальный хост, осуществляется с использованием продукта Kiwi Syslog Daemon.