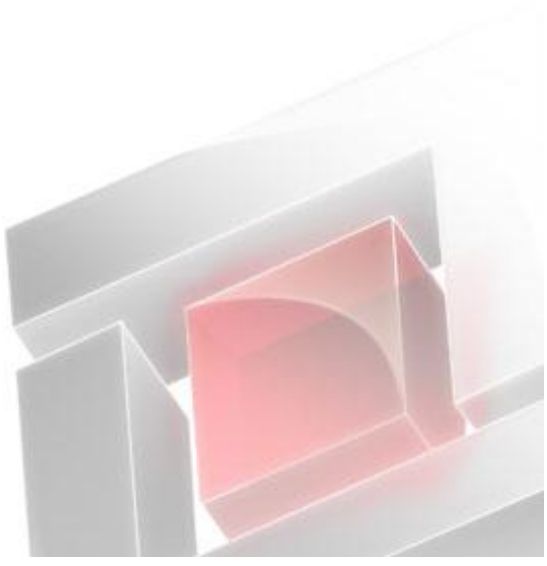
ALTELL
IT Innovations & Security

Altell VPN Client

Руководство администратора

Версия 4.56



Санкт-Петербург 2015

1 Назначение

Altell VPN Client представляет собой программный клиент OpenVPN со встроенной поддержкой отечественных криптографических алгоритмов, который предоставляет графический пользовательский интерфейс для настройки и управления подключениями OpenVPN.

2 Функциональные возможности

Основные функции Altell VPN Client:

— поддержка российских криптографических алгоритмов ГОСТ 28147—89, ГОСТ 34.10—2001;

— создание и редактирование параметров настройки подключения OpenVPN при помощи графического пользовательского интерфейса;

— возможность использования аппаратных идентификаторов «Рутокен ЭЦП» для аутентификации;

— установка, разрыв и перезапуск подключения OpenVPN;

— отображение пиктограммы приложения в области уведомлений;

— поддержка нескольких одновременных подключений;

— отображение статуса подключения OpenVPN в области уведомлений.

— просмотр файлов регистрации;

— настройка параметров подключения к серверу LDAP.

3 Сведения о технических и программных средствах, обеспечивающих выполнение программы

Приложение Altell VPN Client может быть установлено в следующих операционных системах: Windows XP (SP3) / Windows Vista / Windows 7.

Для аутентификации с использованием аппаратных электронных идентификаторов поддерживаются только идентификаторы «Рутокен ЭЦП».

4 Описание действий по настройке программы

4.1 Установка

Для установки Altell VPN Client необходимо выполнить следующие шаги:

1. Запустите программу установки. Программа установки находится на компакт-диске, поставляемом в комплекте с МЭ Altell NEO, в каталоге «Межсетевой экран Altell NEO/Клиентское ПО/Windows».

2. В открывшемся окне (рис. 1) нажмите кнопку «Далее».

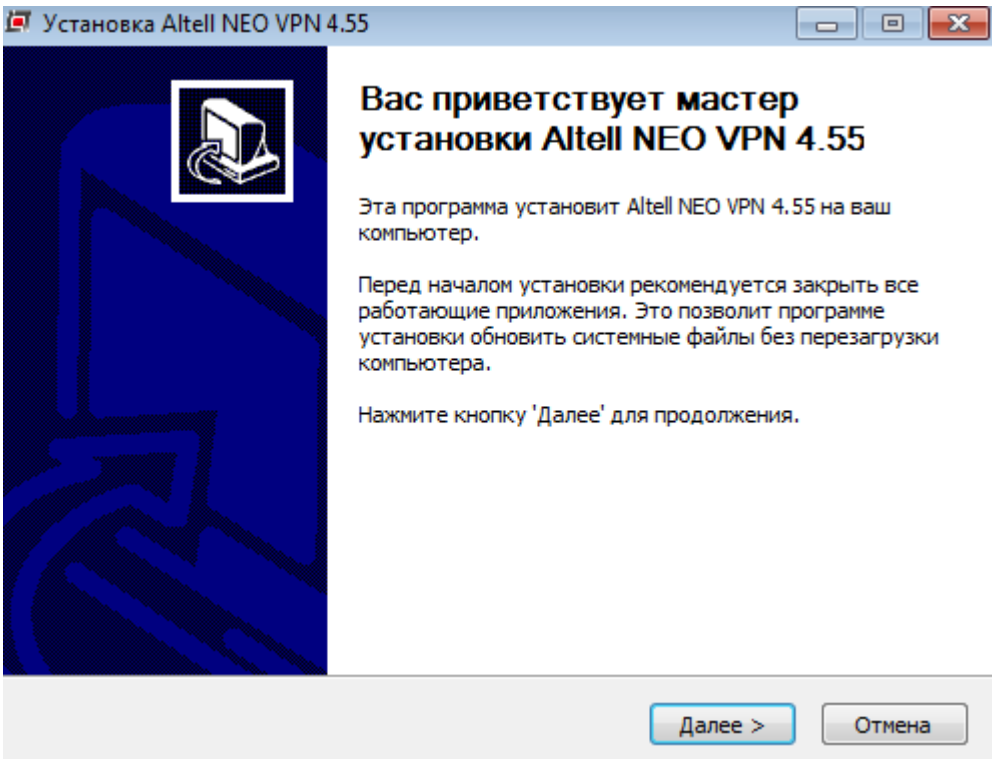


Рис. 1: Мастер установки Altell VPN Client

3. В окне «Компоненты устанавливаемой программы» (рис. 2) можно выбрать модули для установки. В том случае если флажок, связанный с модулем, не активен, модуль устанавливается в обязательном порядке. При первоначальной установке приложения все модули устанавливаются в обязательном порядке. После этого нажмите кнопку «Далее».

4. В окне «Выбор папки установки» (рис. 3) необходимо указать путь к каталогу, в который будет установлено приложение. Этот каталог должен быть доступен всем пользователям ОС Windows, те пользователи, для которых данный каталог будет не доступен, не смогут запустить Altell VPN Client. После указания каталога установки нажмите кнопку «Далее».

5. В том случае для установки был выбран модуль «OpenSSL Gost», автоматически откроется окно программы установки библиотеки OpenSSL Gost (рис. 4). Нажмите кнопку «Далее».

6. В окне «Выбор папки установки» (рис. 5) необходимо указать путь к каталогу, в который будет установлена библиотека OpenSSL Gost. После указания каталога нажмите кнопку «Далее».

7. После окончания установки библиотеки OpenSSL Gost, нажмите кнопку «Закрыть» (рис. 6).

8. В том случае если был установлен компонент OpenSSL Gost, то после завершения установки всех компонентов Altell VPN Client потребуется перезагрузка ОС (рис. 7). При отказе от немедленной перезагрузки выдается сообщение с предупреждением (рис. 8).

9. После завершения установки Altell VPN Client нажмите кнопку «Далее».

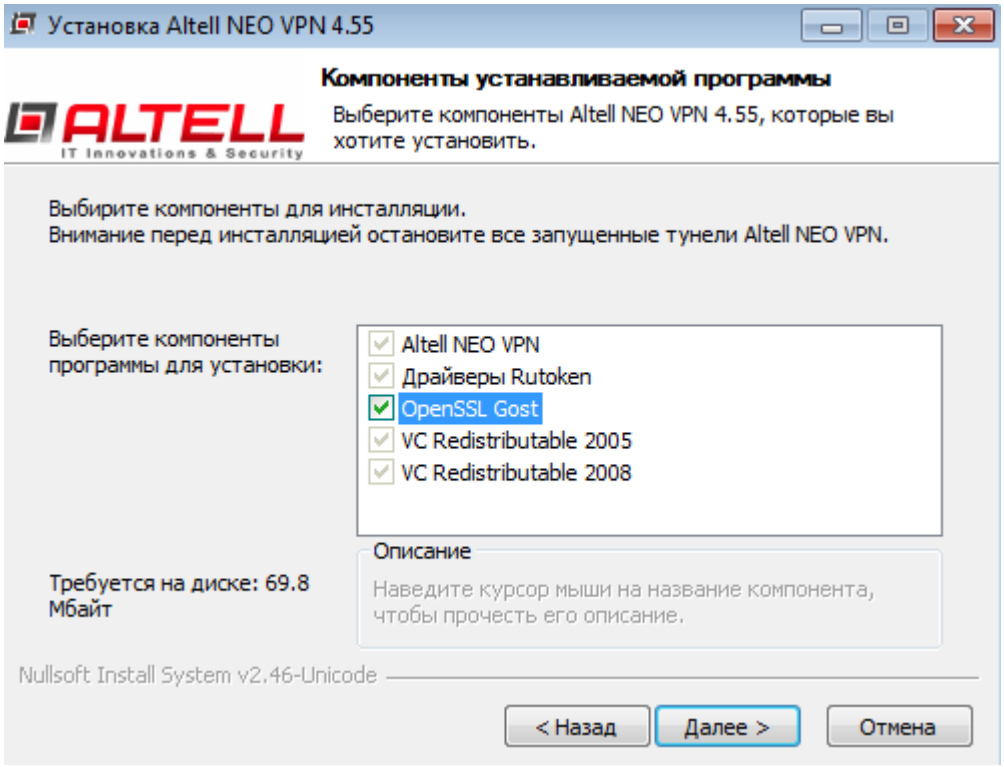


Рис. 2: Компоненты устанавливаемой программы

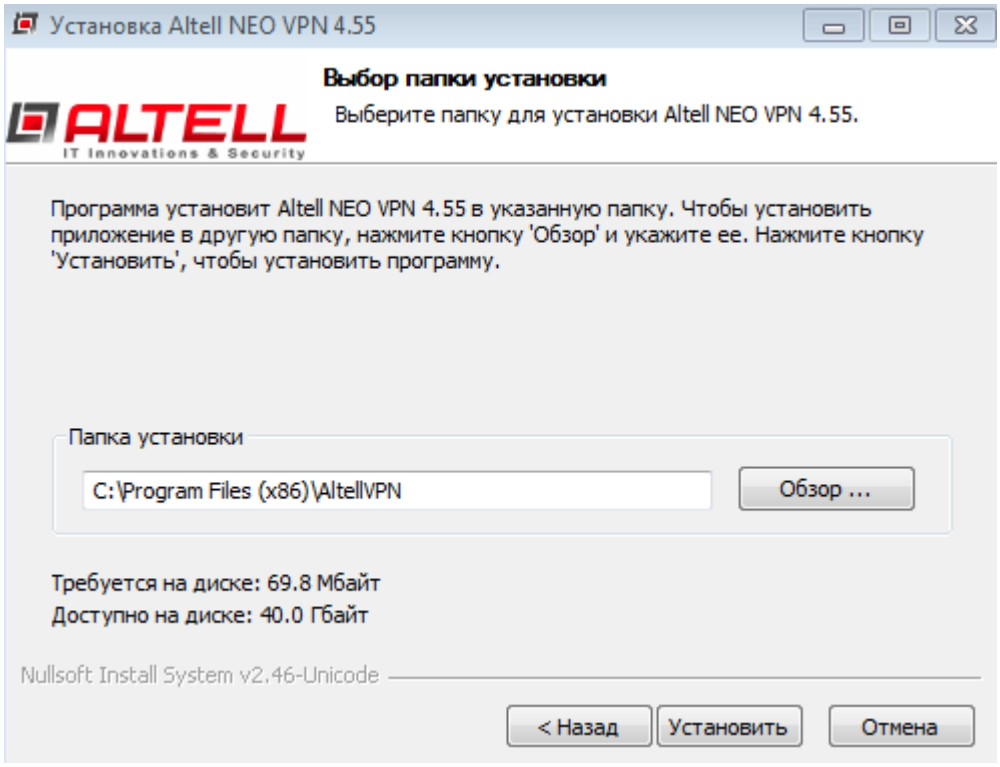


Рис. 3: Выбор каталога для установки

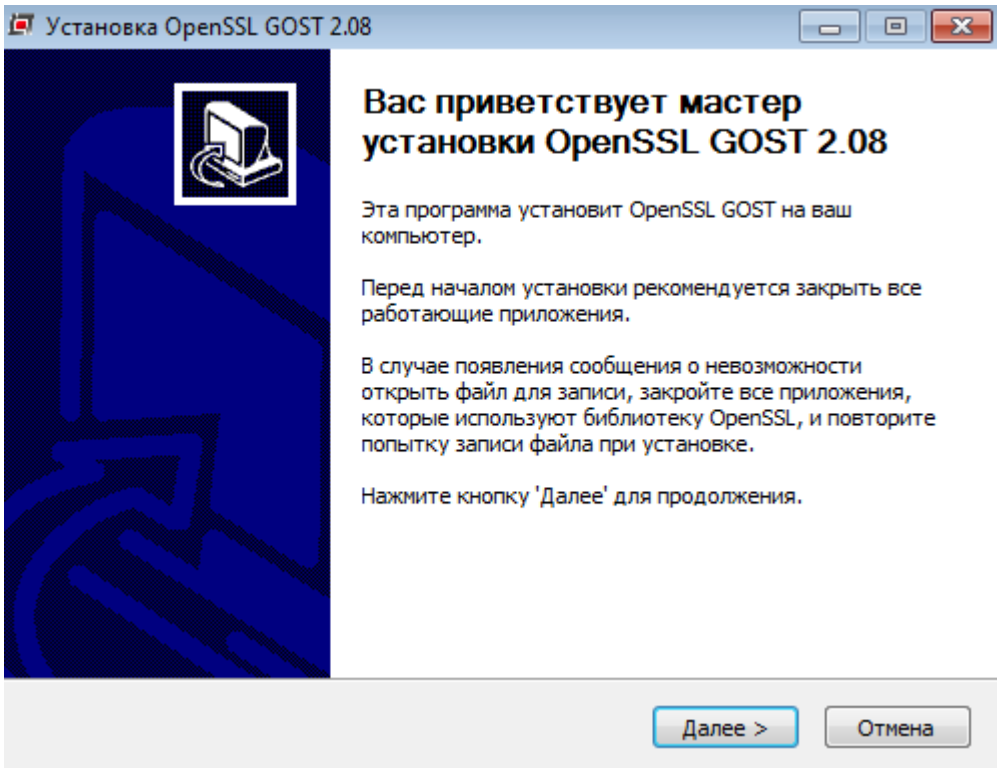


Рис. 4: Мастер установки OpenSSL Gost

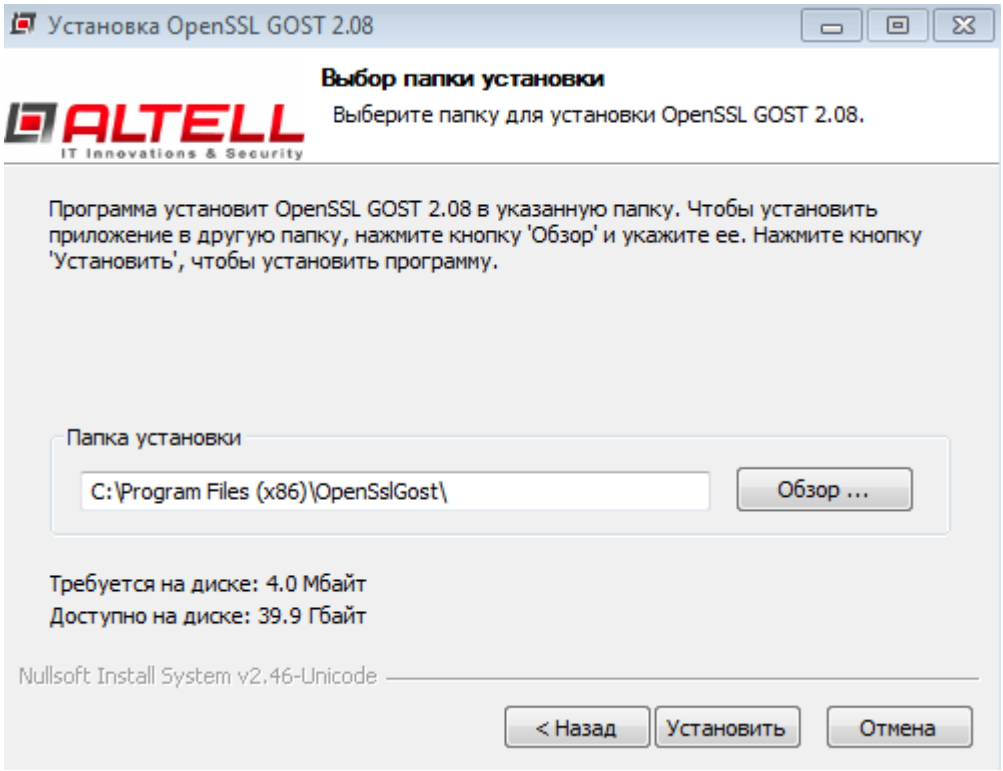


Рис. 5: Выбор каталога для установки OpenSSL Gost

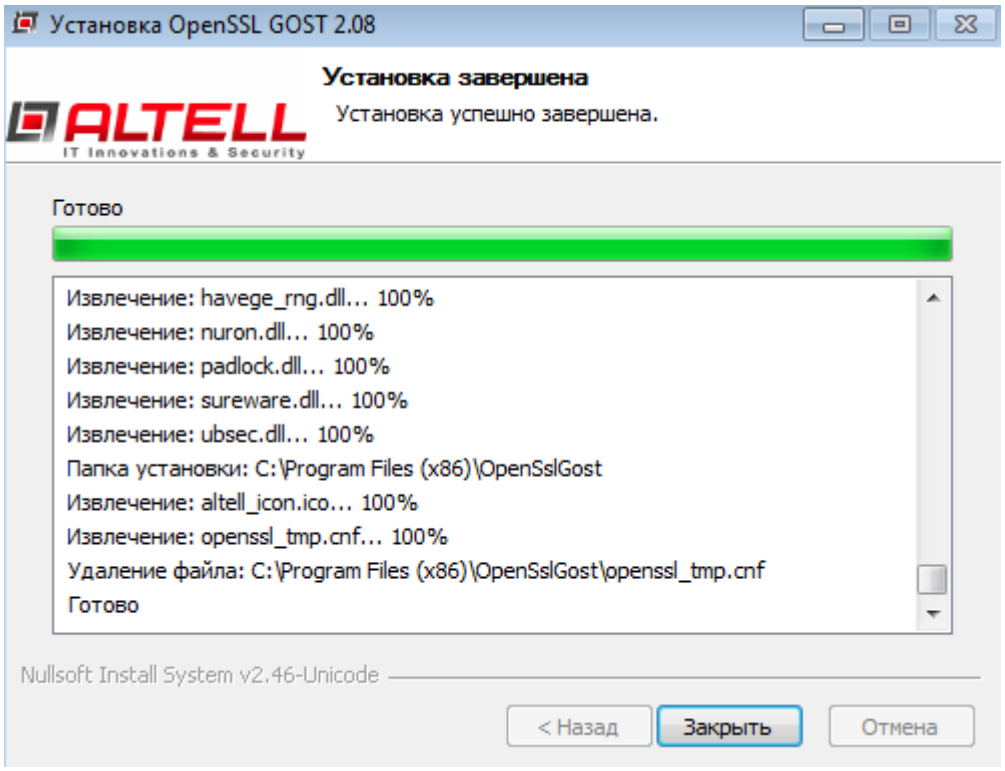


Рис. 6: Завершение установки OpenSSL Gost

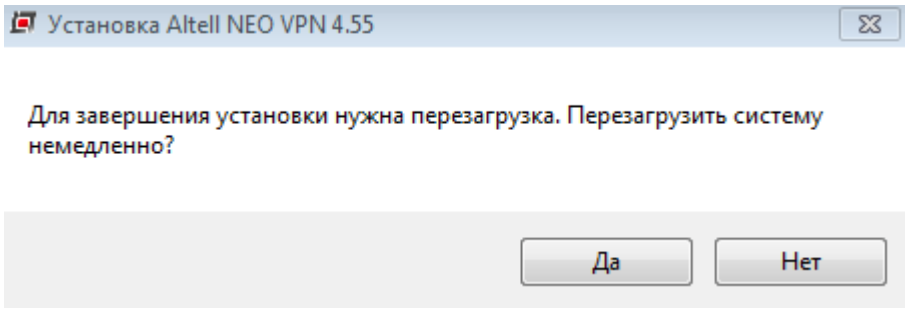


Рис. 7: Перезагрузка после установки OpenSSL Gost

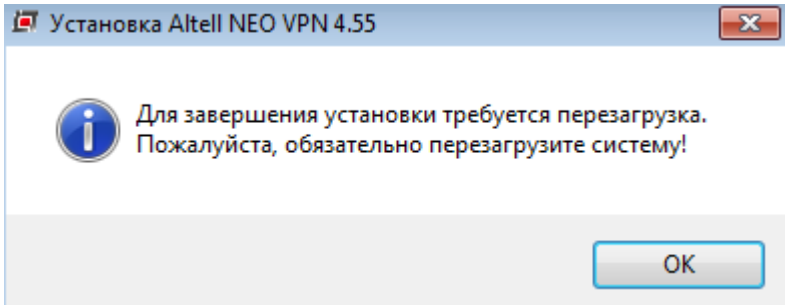


Рис. 8: Перезагрузка после установки OpenSSL Gost

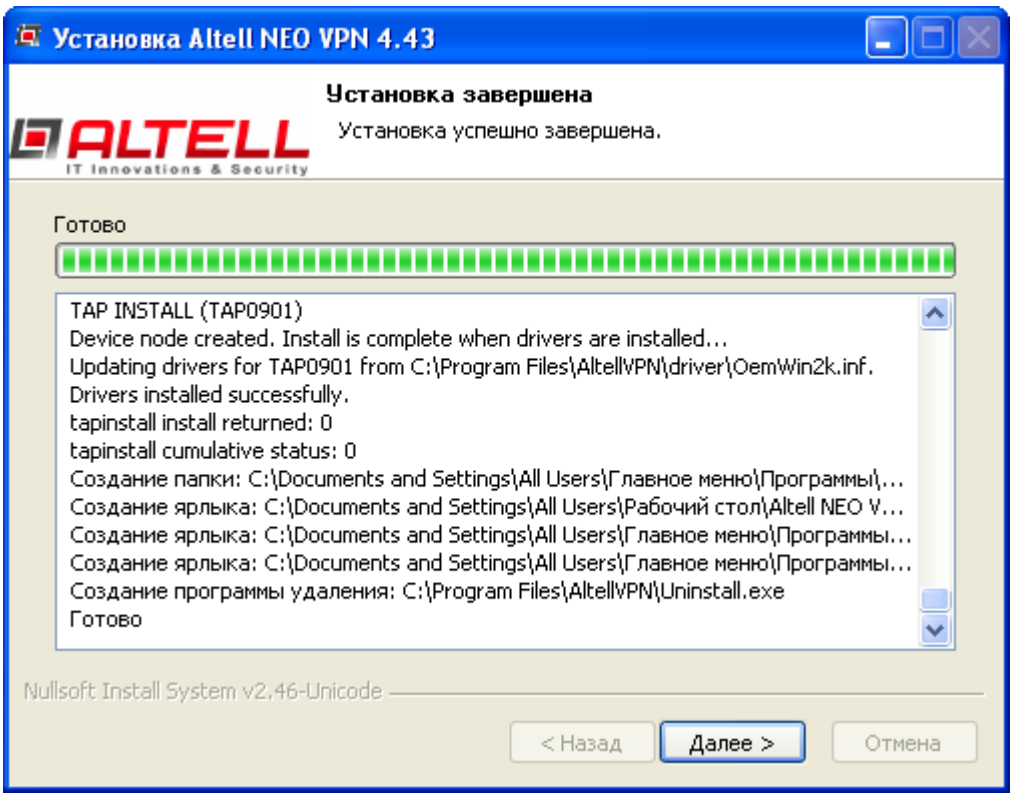


Рис. 9: Завершение установки Altell VPN Client

4.2 Действия, производимые в процессе установки Altell VPN Client

В процессе установки Altell VPN Client производятся следующие действия:

1. Создание каталога, в который будет установлен Altell VPN Client. Копирование в указанный каталог исполняемых, а также других файлов, которые используются приложением Altell VPN Client:
   - Основные файлы:
     - altellvpn.exe — исполняемый файл для запуска ALtell VPN Client с интерфейсом командной строки;
     - altellvpn-gui.exe — исполняемый файл для запуска Altell VPN Client с графическим интерфейсом пользователя;
     - AltellVPNProfile.dll — библиотека для настройки конфигураций;
     - QtCore4.dll, QtNetwork4.dll, QtGUI4.dll — файлы библиотеки QT, которые необходимы для работы приложения с графическим интерфейсом пользователя;
     - libeay32.dll, ssleay32.dll — файлы библиотеки OpenSSL, которые необходимы для работы с криптографическими алгоритмами.
   - Файлы для работы с адаптером TAP:
     - tapinstall.exe — утилита для создания и удаления адаптеров TAP;
     - driver — каталог, который содержит драйвер TAP;
     - addtap.bat — пакетный файл для добавления нового адаптера TAP; для данного файла создан ярлык в разделе меню «Пуск»→«Все программы→«Altell NEO VPN»→«Utilities»→«Add a new TAP virtual ethernet adapter»;

— deltap.bat — пакетный файл для удаления всех адаптеров TAP; для данного файла создан ярлык в разделе меню «Пуск»→«Все программы»→«Altell NEO VPN»→«Utilities»→«Delete ALL TAP virtual ethernet adapters»;

— Файлы для доступа к сертификатам и ключам, которые хранятся на электронных идентификаторах «Рутокен ЭЦП»:

— lib — каталог, который содержит библиотеки для доступа к сертификатам и ключам, хранящимся на электронных идентификаторах «Рутокен ЭЦП», а также консольную программу pkcs11-tool.exe для определения наличия идентификатора, а также чтения метаданных о сертификах и ключах.

2. В реестр ОС Windows добавляются ключи приложения Altell VPN Client. Эти ключи используются при повторной установке, а также при удалении приложения.

   Пути в реестре Windows:

   — `HKLM\SOFTWARE\Altell\AltellVPN`;

   — `HKLM\SOFTWARE\Microsoft Windows\CurrentVersion\Uninstall\AltellVPN`.

3. Создается адаптер TAP;

4. Для установки драйверов «Рутокен ЭЦП» используется программа установки с сайта
   www.rutoken.ru;

5. Устанавливается библиотека OpenSSL Gost. В реестр ОС Windows добавляются ключи библиотеки OpenSSL Gost. Создается переменная среды окружения OPENSSL_CONF. Для работы Altell VPN Client необходимо перезагрузить ОС Windows, чтобы новая переменная среды окружения OPENSSL_CONF стала доступна программам.

   Пути в реестре ОС Windows:

   — `HKLM\SOFTWARE\Altell\OpenSSL`;

   — `HKLM\SOFTWARE\Microsoft Windows\CurrentVersion\Uninstall\OpenSSL`.

6. Вызов программы установки VC Redistributable 2005 и VC Redistributable 2008.

4.3 Использование программы

После установки приложения Altell VPN Client в меню «Пуск» будет создан новый раздел («Пуск»→«Все программы»→«Altell NEO VPN»). В этом разделе находятся:

— «Altell VPN GUI» — программа для запуска Altell VPN Client с графическим интерфейсом пользователя;

— «Uninstall Altell NEO VPN» — программа для удаления Altell VPN Client;

— «Utilities» — подраздел, в котором находятся:

— «Add a new TAP virtual ethernet adapter» — программа для добавления виртуального адаптера TAP;

— «Delete all TAP virtual ethernet adapters» — программа для удаления всех виртуальных адаптеров TAP.

Рис. 10: Пиктограмма в области уведомления

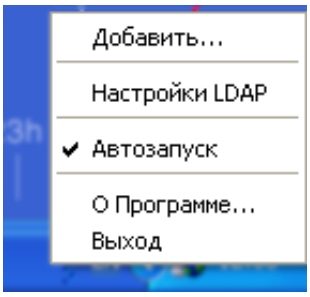


Рис. 11: Контекстное меню

Также ярлык «Altell VPN GUI» будет создан на рабочем столе пользователя.

Примечание. *Для корректной работы приложения, пользователь, от имени которого запущено приложение, должен иметь привилегии администратора, либо должен состоять в группе «Операторы настройки сети» (Networks Configuration Operators Group). Это связано с тем, что сервер VPN при определенных настройках может сообщать клиенту VPN дополнительные маршруты сети. Эти маршруты должны быть добавлены в таблицу маршрутизации операционной системы, в которой запущен Altell VPN Client.*

После запуска приложения Altell VPN Client в области уведомлений появляется пиктограмма приложения (рис. 10).

Управление программой осуществляется при помощи контекстного меню, которое вызывается нажатием правой кнопки мыши на пиктограмме приложения в области уведомлений (рис. 11).

В контекстном меню доступны следующие элементы:

— «Добавить…» — добавить новую конфигурацию клиента VPN;

— «Настройка LDAP» — настройка параметров подключения к серверу LDAP;

— «Автозапуск» — настройка автоматического запуска приложения при запуске ОС Windows;

— «О программе» — вызов окна, содержащего сведения о программе;

— «Выход» — завершение работы приложения.

4.3.1 Создание конфигурации подключения VPN

Файлы конфигурации клиентского узла VPN могут быть созданы на сервере VPN Altell NEO и экспортированы на рабочие станции под управлением ОС Windows (описание процедуры экспорта приведено в пользовательской документации на МЭ Altell NEO).

Кроме этого Altell VPN Client позволяет при помощи графического интерфейса пользователя создать новую конфигурацию клиентского узла VPN, а также изменить параметры существующего подключения.

Для того чтобы создать новое подключение VPN, выберите элемент контекстного меню «Добавить», после чего откроется окно «Создание новой конфигурации» (рис. 12).

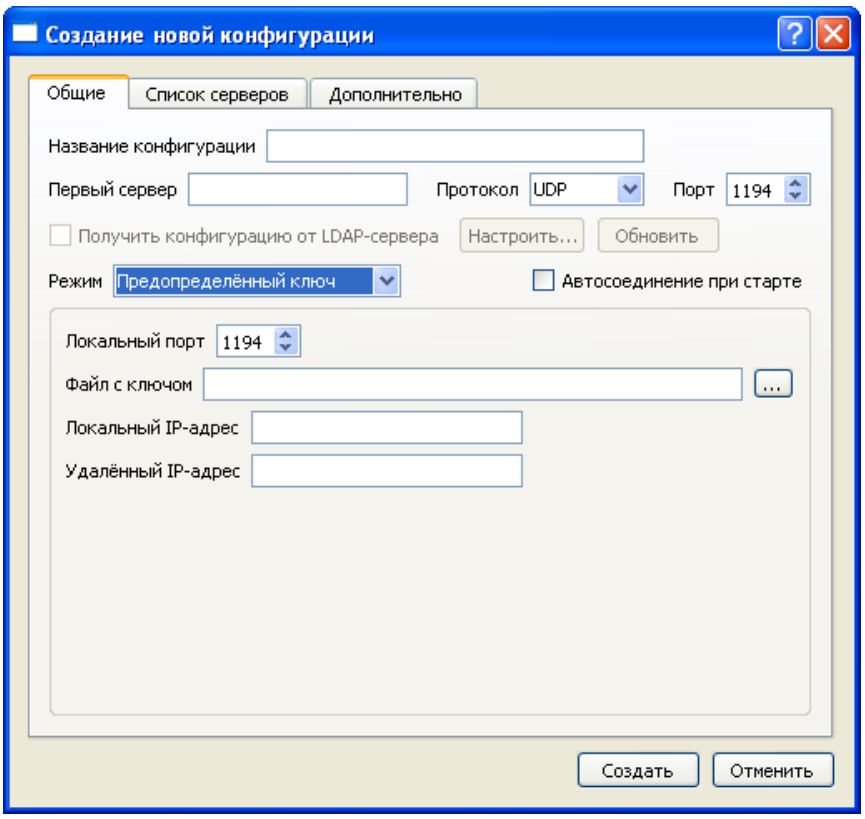


Рис. 12: Параметры режима аутентификации на основе предопределенного ключа

При настройке следует учитывать то, что параметры конфигурации клиента VPN должны быть настроены соответственно параметрам конфигурации сервера VPN. Подробное описание настройки сервера VPN приведено в пользовательской документации на МЭ Altell NEO.

Во вкладке «Общие» приведены основные параметры конфигурации клиентского узла VPN:

- «Название конфигурации» — название подключения, которое будет использоваться для управления подключением из контекстного меню;
- «Первый сервер» — IP-адрес или символьное имя сервера VPN, к которому будет осуществляться подключение;
- «Протокол» — используемый протокол транспортного уровня;
- «Порт» — номер удаленного порта, на котором сервер VPN ожидает входящие подключения;
- «Автосоединение при старте» — при установлении данной опции подключение будет осуществляться автоматически при запуске приложения Altell VPN Client;
- «Режим» — используемый режим аутентификации:
  - «Предопределенный ключ» — аутентификация на основе разделяемого секретного ключа;
  - «Имя пользователя и пароль» — аутентификация на основе учетной записи пользователя и пароля;
  - «Файлы сертификатов X.509» — аутентификация на основе инфраструктуры открытых ключей;

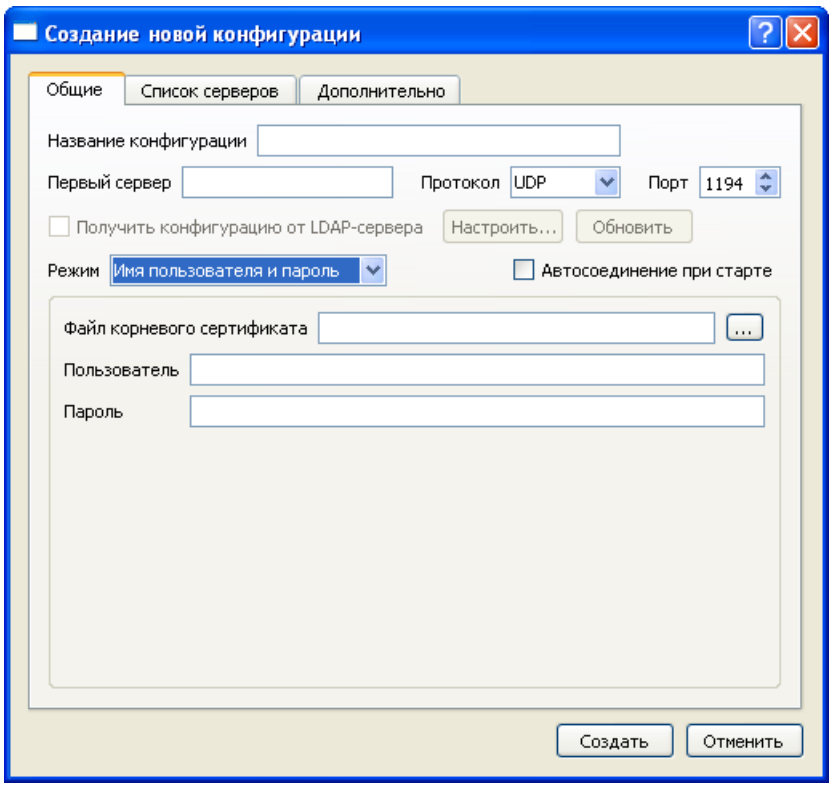


Рис. 13: Параметры режима аутентификации на основе учетной записи пользователя и пароля

— «Токен с сертификатами X.509» — аутентификация на основе инфраструктуры открытых ключей с использованием электронных идентификаторов «Рутокен ЭЦП».

При выборе режима «Предопределенный ключ» доступны следующие параметры (рис. 12):

— «Локальный порт» — номер локального сетевого порта источника;
— «Файл с ключом» — файл, который содержит разделяемый секретный ключ;
— «Локальный IP-адрес» — локальный IP-адрес туннеля VPN;
— «Удаленный IP-адрес» — удаленный IP-адрес туннеля VPN.

При выборе режима «Имя пользователя и пароль» доступны следующие параметры (рис. 13):

— «Файл корневого сертификата» — путь к файлу корневого сертификата;
— «Пользователь» — имя учетной записи пользователя, используемой для аутентификации клиента VPN;
— «Пароль» — пароль, используемый для аутентификации.

При выборе режима «Файлы сертификатов X.509» доступны следующие параметры (рис. 14):

— «Файл корневого сертификата» — путь к файлу сертификата удостоверяющего центра;

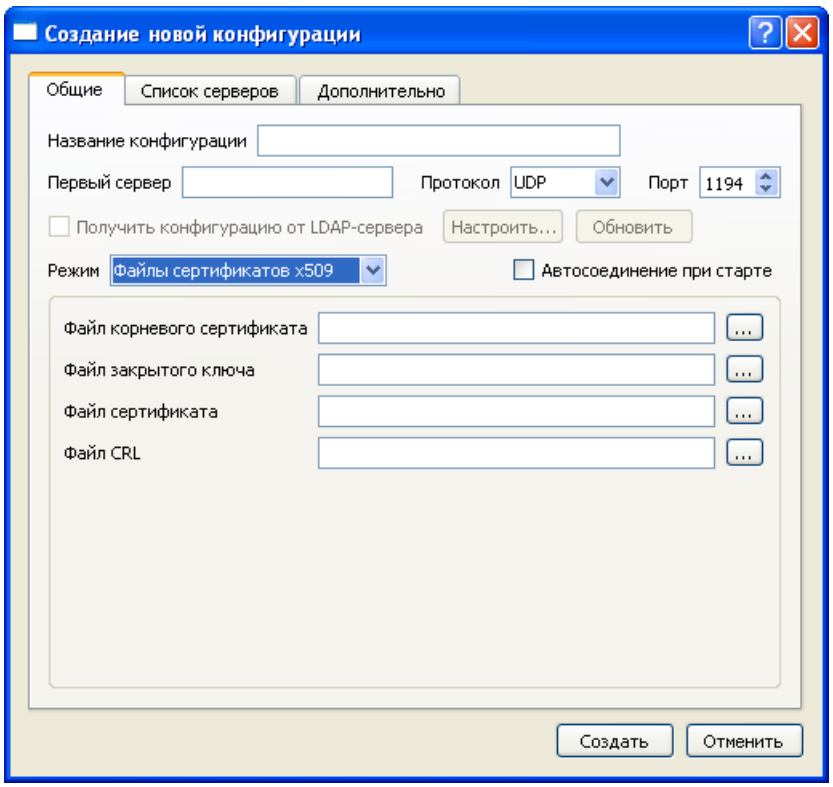


Рис. 14: Параметры режима аутентификации на основе инфраструктуры открытых ключей

— «Файл закрытого ключа» — путь к файлу закрытого ключа клиента VPN;
— «Файл сертификата» — путь к файлу сертификата клиента VPN;
— «Файл CRL» — путь к файлу со списком отозванных сертификатов.

При выборе режима «Токен с сертификатами X.509» доступны следующие параметры:

— «Токен» — идентификатор токена;
— «Объект корневого сертификата» — идентификатор сертификата удостоверяющего центра;
— «Объект закрытого ключа» — идентификатор закрытого ключа;
— «Объект сертификата» — идентификатор сертификата пользователя;
— «Объект CRL» — идентификатор списка отозванных сертификатов;
— «Пин код» — ПИН-код токена.

При необходимости можно указать список серверов VPN. В случае отказа одного из серверов, клиент сможет подключиться к другому. Для этого выберите вкладку «Список серверов» (рис. 16), затем установите флажок параметра «Включить список серверов», после чего укажите список IP-адресов (или символьных имен) серверов VPN, а также номеров портов для подключения.

В случае если не удалось установить подключение к первому серверу из списка, Altell VPN Client будет осуществлять попытки подключения к остальным серверам из списка.

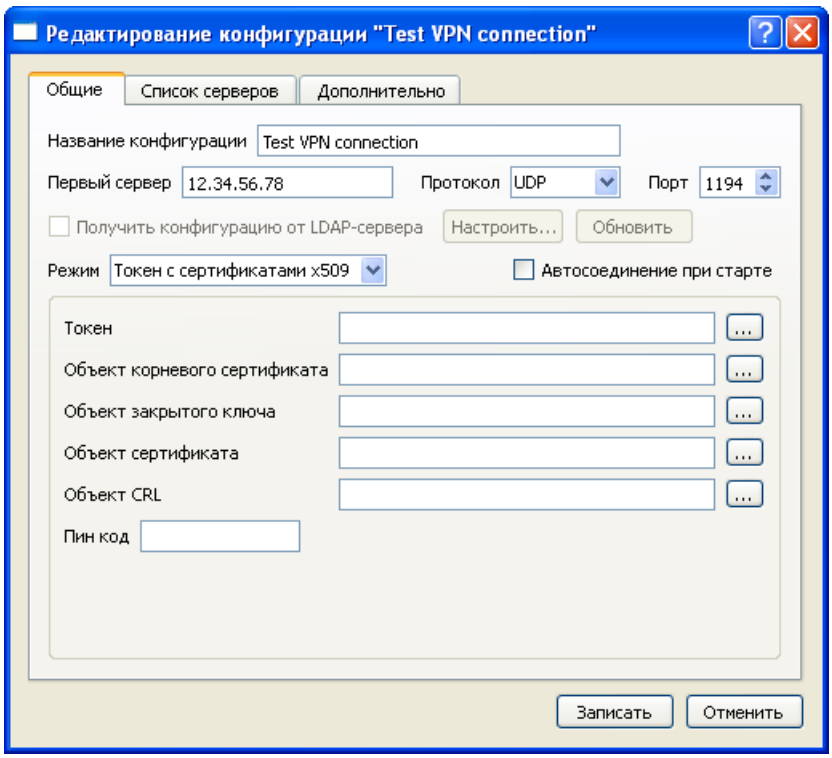


Рис. 15: Параметры режима аутентификации на основе инфраструктуры открытых ключей с использованием электронного идентификатора «Рутокен ЭЦП»

По умолчанию включена опция «Выбрать сервер для подключения случайным образом», в том случае если данную опцию отключить, сервера из списка будут выбираться в порядке очередности.

Параметр «Таймаут для повторной отправки DNS-запроса» определяет интервал времени, в течении которого Altell VPN Client будет пытаться разрешить символьное имя сервера VPN, перед тем как перейти к следующему серверу в списке.

Если сервер VPN использует в ответных пакетах аутентификации IP-адрес, отличный от IP-адреса, на который был послан запрос на аутентификацию от клиента, и при этом опция «Разрешить получение пакетов аутентификации от любых адресов» выключена, то клиент не будет воспринимать эти ответы как разрешенные. По умолчанию опция «Разрешить получение пакетов аутентификации от любых адресов» выключена.

На вкладке «Дополнительно» доступны следующие параметры:

— «Туннель» — тип соединения: «TUN» — маршрутизируемое соединение, «TAP» — соединение типа «мост»;

— «Шифр» — криптографический алгоритм, используемый для шифрования;

— «Хэш» — криптографический алгоритм, используемый для аутентификации;

— «Топология» — используемая топология подключения;

При установке параметра «Использовать настройки, полученные от сервера», Altell VPN Client автоматически установит значения для данных параметров, полученные от сервера VPN.

Параметр «Уровень сообщений в окне статуса» определяет уровень детализации сообщений, регистрируемых в журнале.

Параметр «Переустанавливать соединение каждые <> секунд» определяет период времени, по истечении которого подключение будет установлено заново.

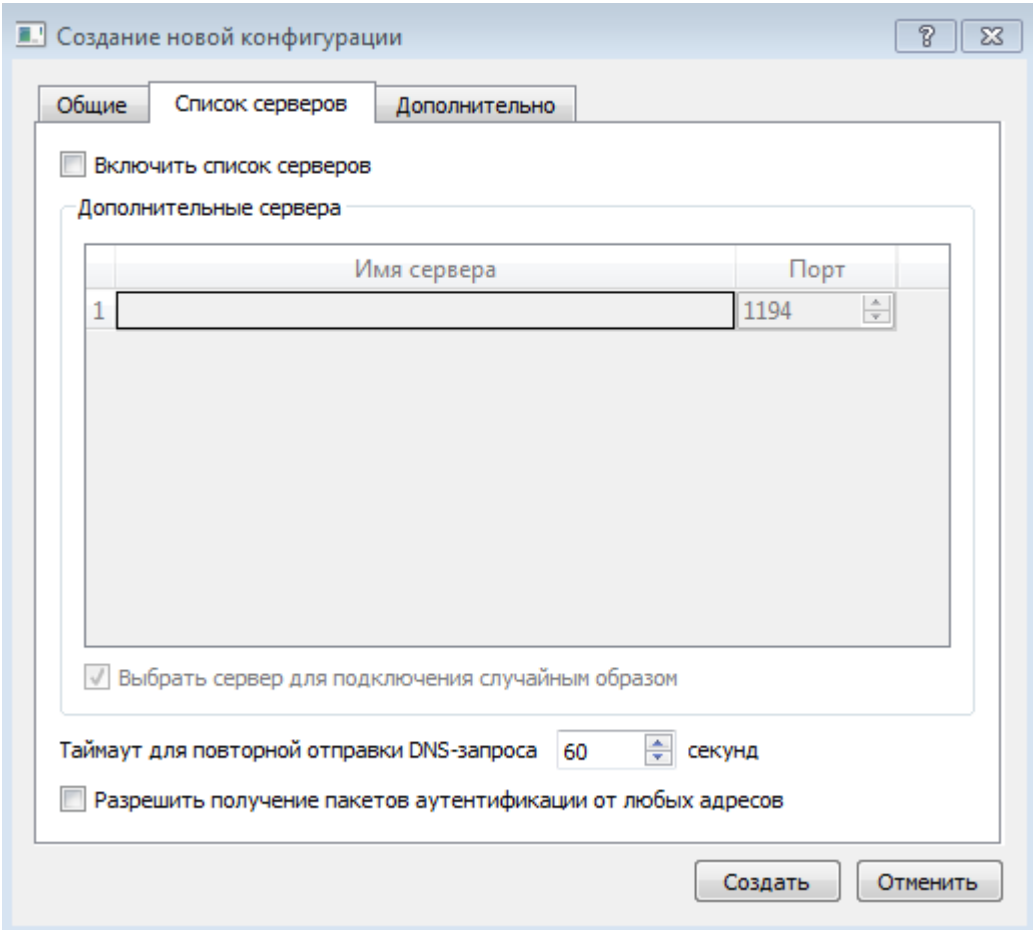


Рис. 16: Список серверов VPN для подключения

4.3.2 Управление подключениями

Управление настроенными подключениями осуществляется из контекстного меню. После добавления новой конфигурации в контекстном меню появляется соответствующий элемент. При нажатии левой кнопкой мыши на названии подключения открывается подменю, представленное на рис. 17. . В этом меню доступны следующие элементы:

— «Соединить» — установить подключение к серверу VPN;

— «Отсоединить» — разорвать подключение с сервером VPN;

— «Показать статус» — отобразить окно с журналом регистрации для данного подключения VPN;

— «Посмотреть лог» — отобразить окно журнала регистрации для данного подключения VPN;

— «Редактировать конфигурацию» — открыть окно с параметрами подключения;

— «Удалить» — удалить конфигурацию.

Цвет пиктограммы Altell VPN Client зависит от состояния подключений:

— красный — ни одно подключение не установлено;

— зеленый — для всех выбранных конфигураций подключения установлены успешно;

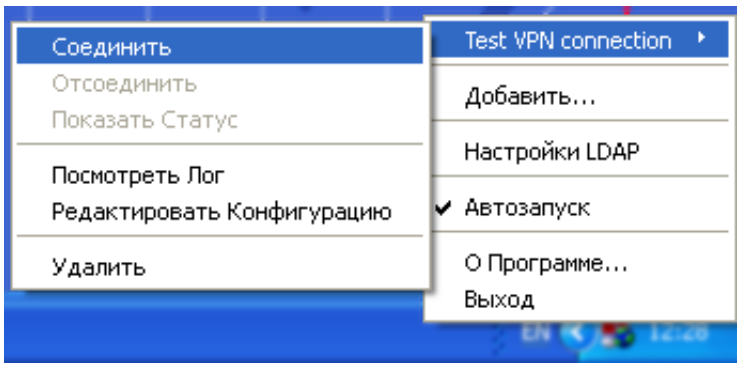


Рис. 17: Управление подключениями из контекстного меню

— желтый — установка подключения для по крайней мере одной конфигурации еще не завершена;
— оранжевый — для одной из конфигураций попытка подключения завершилась неудачей, начат процесс повторного подключения.

Одновременно могут быть настроены несколько подключений. При этом следует учитывать, что для одновременной работы нескольких подключений требуется соответствующее количество адаптеров TAP. Адаптер TAP может быть единовременно использован только одним подключением VPN. Первый адаптер TAP создается автоматически при установке приложения Altell VPN Client. В том случае если требуется более одного адаптера TAP, они могут быть добавлены при помощи пакетного файла addtap.bat, который доступен из каталога Altell NEO VPN в меню («Пуск»→«Все программы»→«ALtell NEO VPN»→«Utilities»→«Add a new TAP virtual ethernet adapter»).

4.3.3 Настройка автозапуска и автосоединения при старте

Параметр «Автозапуск», доступный из контекстного меню, позволяет настроить автоматический запуск приложения Altell VPN Client после авторизации пользователя при запуске ОС Windows.

При этом можно настроить подключение к серверу VPN таким образом, чтобы установление соединения происходило автоматически при запуске Altell VPN Client. Для это нужно в настройках подключения установить флаг «Автосоединение при старте».

В том случае если опции «Автозапуск» и «Автосоединение при старте» используются одновременно, то подключение к серверу VPN будет осуществляться автоматически после авторизации пользователя при запуске ОС Windows.

4.3.4 Получение конфигураций с сервера LDAP

Altell VPN Client может загрузить файлы конфигурации, набор сертификатов и список отозванных сертификатов от сервера LDAP и сохранить их в каталоге пользователя ОС Windows. Для этого необходимо настроить параметры подключения к серверу LDAP. Выберите пункт контекстного меню «Настройки LDAP», откроется окно с параметрами подключения (рис. 18). При настройке подключения к серверу LDAP необходимо указать следующие параметры:

— «LDAP-сервер» — IP-адрес или символьное имя сервера LDAP, к которому будет осуществляться подключение;

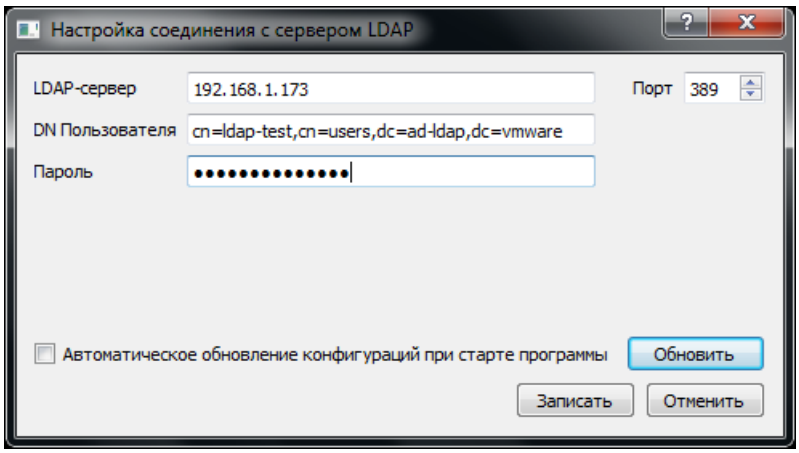


Рис. 18: Параметры подключения к серверу LDAP

— «DN пользователя» — отличительное имя пользователя, используемое для аутентификации на сервере LDAP;

— «Пароль» — пароль пользователя, используемый для аутентификации.

При нажатии на кнопку «Обновить» все доступные конфигурации для пользователя будут загружены с сервера LDAP. Также возможно получение обновленных конфигурации при запуске приложения Altell VPN Client. Для этого нужно установить опцию «Автоматическое обновление конфигураций при старте программы».

Для того чтобы сохранить параметры подключения к серверу LDAP, нажмите кнопку «Записать».

В том случае если конфигурация загружена от сервера LDAP, для в окне редактирования параметров подключения доступны дополнительные элементы, используемые для управления обновлением конфигурации от сервера LDAP (рис. 19).

Кнопка «Обновить» позволяет загрузить новую конфигурацию для данного подключения от сервера LDAP. Загрузка обновлений конфигурации будет отключена при выключении опции «Получить конфигурацию от LDAP-сервера».

При нажатии на кнопку «Настроить» откроется окно с параметрами загрузки сертификатов (рис. 20).

Доступны следующие параметры:

— «Загружать корневой сертификат» — при установке данного параметра сертификат удостоверяющего центра будет загружен с сервера LDAP при обновлении конфигурации подключения;

— «Загружать сертификат пользователя» — при установке данного параметра сертификат пользователя будет загружен с сервера LDAP при обновлении конфигурации подключения;

— «Загружать CRL» — при установке данного параметра список отозванных сертификатов будет загружен с сервера LDAP при обновлении конфигурации подключения.

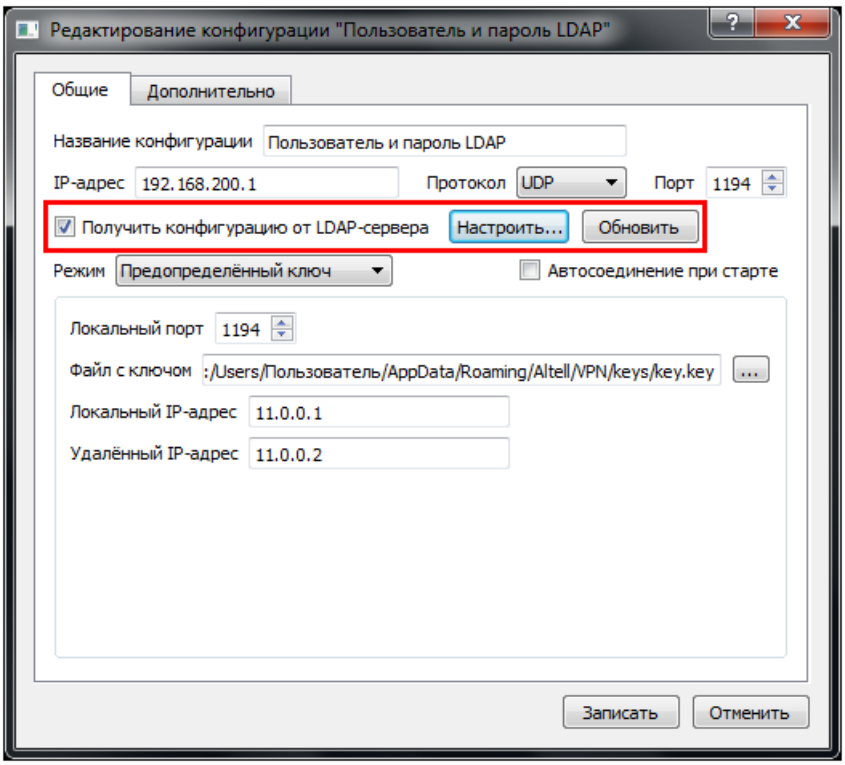


Рис. 19: Редактирование конфигурации, полученной от сервера LDAP

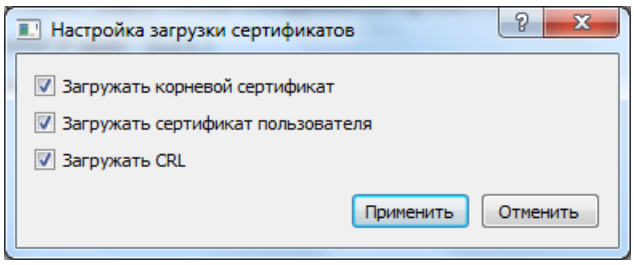


Рис. 20: Параметры загрузки сертификатов