УТВЕРЖДЕНО

BY.РТНК.00002-04.1 34 01-3-ЛУ

Программно-аппаратное устройство «Клиент безопасности Bel VPN Client 4.1»

Подготовительные процедуры

BY.РТНК.00002-04.1 34 01-3

Листов 8

Подп. и дата	
Инв. № дубл.	
Взам. инд. №	
Подп. и дата	
Инд. № подл.	

2016

Содержание

1 Требования на базовые платформы и совместимость

Продукт Bel VPN Client работает под управлением следующих ОС:

- MS Windows XP SP3 Russian Edition;
- MS Windows Vista SP2 Russian Edition (32-bit, 64-bit);
- MS Windows 7 Russian Edition (32-bit, 64-bit);
- MS Windows 8 Russian Edition (32-bit, 64-bit);
- MS Windows 8.1 Russian Edition (32-bit, 64-bit);
- MS Windows 10 (32-bit, 64-bit);
- MS Windows Server 2003 Edition 32-bit;
- MS Windows Server 2008 Edition (32-bit, 64-bit);
- MS Windows Server 2008R2 Edition 64-bit;
- MS Windows Server 2012 Edition 64-bit.

Программный комплекс Bel VPN Client может функционировать в виртуальной среде (VMWare).

Клиент безопасности Bel VPN Client 4.1 совместим со следующими продуктами компании «С-Терра Бел»:

- Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1»;
- Программно-аппаратный комлпекс «Шлюз безопасности Bel VPN Gate 4.1»;
- Программный комплекс «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1»;
- Программный комплекс «Bel VPN KP 4.1».

В части реализации протоколов IPsec/IKE и их расширений Продукт совместим с Cisco IOS v.12.4 и v.15.x.x.

2 Подготовка рабочего места администратора безопасности

Администратор безопасности получает административный пакет программного-аппаратного устройства «Клиент безопасности Bel VPN Client 4.1», предназначенный для подготовки персонифицированных дистрибутивов (содержащих конфигурацию для конкретного пользователя) программно-аппаратного устройства «Клиент безопасности Bel VPN Client 4.1». Административный пакет размещается на поставляемом компакт-диске.

Перед установкой административного пакета необходимо убедиться в целостности поставляемого дистрибутива.

2.1 Контроль целостности дистрибутива

Проверка целостности дистрибутива административного пакета осуществляется с использованием утилиты AvVerify, разработанной ЗАО «Авест». Данная утилита выполняет проверку контрольных характеристик (хэш-сумм) по алгоритму СТБ 34.101.31-2011 (п.6.9).

Утилита AvVerify размещена в каталоге utils на поставляемом CD диске. Для вычисления хэш-суммы и сравнения ее с эталонной по каждому файлу дистрибутива и выдачи результата на экран выполните команду:

```
avverify –h <full_name_with_path_of_file> <hash>
```

где:

<hash> – эталонное значение хэш-суммы, которое необходимо скопировать из файла hashes из состава дистрибутива. Файл hashes содежит строки вида
<hash> <file name>

<full_name_with_path_of_file> – полный путь и имя файла, для которого подсчитана хэш-сумма.

Пример:

```
E:\util>AvVerify.exe -h e:\Soft\setup.exe
157B41A50895BFDCE0BC652EC988C70AE40E40C3BCB50D5955EC6D0E5B08A64B
```

Таблица 1

Сообщение об ошибке	Описание проблемы
Verification COMPLETED	Успешное окончание проверки.
USAGE: avverify -h <full_name_with_path_of_file> <hash> or avverify -e <full_name_with_path_of_file> <EDS>	Недостаточное количество параметров в командной строке вызывает вывод подсказки в использовании.
ERROR: Hash initialization fault	Внутренняя ошибка инициализации системы вычисления хеша.
ERROR: Invalid check value	Отсутствует или имеет неверный формат значение контрольной информации для проверки.
ERROR Open file is fault. <далее строка описания ошибки в формате операционной системы>	Ошибка открытия проверяемого файла.
ERROR: Read file is fault. <далее строка описания ошибки в формате операционной системы>	Ошибка чтения содержимого проверяемого файла.
ERROR: Verification unsuccessfull.	Проверка выявила несоответствие предложенного значения контрольной информации и вычисленного значения. Возможно проверяемый файл поврежден.

Сообщение об ошибке	Описание проблемы
ERROR: Calculation unsuccessfull..	Ошибка вычисления контрольной информации

2.2 Установка административного пакета

Установка администратративного пакета программно-аппаратного устройства «Клиент безопасности Bel VPN Client 4.1» должна выполняться администратором безопасности в соответствии с руководством администратора программно-аппаратного устройства «Клиент безопасности Bel VPN Client 4.1» (раздел 5.2 «Инсталляция административного пакета»).

2.3 Подготовка персонифицированного дистрибутива пользователя

Подготовка персонифицированного дистрибутива пользователя программно-аппаратного устройства «Клиент безопасности Bel VPN Client 4.1» должна выполняться администратором безопасности в соответствии с руководством администратора программно-аппаратного устройства «Клиент безопасности Bel VPN Client 4.1» (раздел 4 «Процесс подготовки персонального инсталляционного пакета пользователя»).

Для передачи персонифицированного дистрибутива пользователю должен использоваться доверенный канал связи, обеспечивающий защиту от модификации и подмены.

3 Подготовка рабочего места пользователя

Для операционных систем Windows Vista, Windows 7, Windows 2008 должно быть установлено обновление KB3033929.

Перед установкой Продукта Bel VPN Client на компьютере пользователя необходимо отключить все антивирусные программы.

3.1 Рекомендации по ручной настройке Брандмауэра Windows

Данные рекомендации описывают ручную настройку Брандмауэра Windows для обеспечения работоспособности VPN сервиса.

Обычно действия, описываемые в данном разделе, выполняются автоматически инсталлятором. Но если на момент инсталляции служба Брандмауэра Windows была отключена, никаких действий с Брандмауэром Windows на этапе инсталляции не производится. Это может привести к частичной неработоспособности Продукта после запуска службы Брандмауэра Windows.

Если вместо Брандмауэра Windows используется другой персональный firewall, в нем следует вручную внести настройки, аналогичные описываемым в этом разделе.

3.1.1 Ручная настройка Брандмауэра Windows на Windows XP

1. Войти в Панель управления -> Брандмауэр Windows.
2. Перейти во вкладку Исключения и нажмите кнопку Добавить программу...
3. В появившемся окне Добавление программы в поле Путь необходимо задайть полный путь к файлу vpnsvc.exe, который располагается в каталоге продукта (по умолчанию – C:\Program Files\Bel VPN Client).
4. Нажать кнопку «Изменить область...» и убедиться, что выбрано значение «Любой компьютер (включая из Интернета)». По умолчанию выставляется именно такая настройка.
5. Подтвердить настройку, нажав OK.

3.1.2 Ручная настройка Брандмауэра Windows на Windows Vista

1. Войти в Панель управления -> Система и ее обслуживание → Администрирование → Брандмауэр Windows в режиме повышенной безопасности;
2. Выбрать пункт *Правила для входящих подключений*, выбрать *Действия* → *Новое правило...*;
3. Тип правила – *Настраиваемые*;
4. Для раздела *Программа* указать:
    4.1. Путь программы (задайте полный путь к файлу vpnsvc.exe, который располагается в каталоге продукта (по умолчанию – C:\Program Files\Bel VPN Client);
    4.2. Службы → Настроить → Применять только к службам;
        4.2.1. Тип протокола – *UDP. Все порты*;
        4.2.2. Область – *Любой IP-адрес*;
        4.2.3. Действие – *Разрешить подключение*;
        4.2.4. Профиль – *Все (Домен, Личный, Общий)*;
        4.2.5. Имя – *Bel VPN Service*;
5. Нажать «Готово».

3.1.3 Ручная настройка Брандмауэра Windows на Windows 7

1. Войти в Панель управления → Система и ее обслуживание → Администрирование → Брандмауэр Windows.
2. Выбрать раздел *Дополнительные параметры*. Должно появитьяс окно *Брандмауэр Windows в режиме повышенной безопасности*;
3. Выбрать пункт «Правила для входящих подключений» выбрать «Действия» → *Создать правило...*;
4. Тип правила – *Настраиваемые*;
5. Для раздела *Программа* указать:
    5.1. Путь программы (задайте полный путь к файлу vpnsvc.exe, который располагается в каталоге продукта (по умолчанию – C:\Program Files\Bel VPN Client);
    5.2. Службы → Настроить → Применять только к службам;
        5.2.1. Тип протокола – *UDP. Все порты*;
        5.2.2. Область – *Любой IP-адрес*;
        5.2.3. Действие – *Разрешить подключение*;
        5.2.4. Профиль – *Все (Доменный, Частный, Публичный)*;
        5.2.5. Имя – *Bel VPN Service*;
6. Нажать «Готово».

3.2 Установка персонифицированного дистрибутива пользователя

Персонифицированный дистрибутив программно-аппаратного устройства «Клиент безопасности Bel VPN Client 4.1» должен быть установлен пользователем или администратором безопасности в соответствии с руководством пользователя программно-аппаратного устройства «Клиент безопасности Bel VPN Client 4.1» (раздел 6 «Инсталляция Bel VPN Client»).

4 Требования к внешним мерам безопасности

4.1 Физические меры безопасности

Помещения предприятия должны удовлетворять следующим требованиям:

- обеспечение круглосуточной охраны корпусов предприятия;
- обеспечение контроля внешнего периметра и внутренних помещений (видеонаблюдение);
- обеспечение пропускного режима;
- рядом с окнами помещений не должно быть пожарных лестниц и водосточных труб;
- двери должны быть прочными и оборудованы надежными механическими замками;
- оборудование помещений системой пожарной сигнализации;
- ведение Журнала выдачи ключей от входных дверей в офисы, в котором регистрируется время сдачи и выдачи ключей, фамилия сотрудника, взявшего или сдавшего ключ дежурному вахтеру по зданию;
- наличие опечатываемого сейфа, оборудованного двумя внутренними замками, для хранения СКЗИ, тестовых ключей, эталонных CD дисков с продуктом, другой конфиденциальной информации. Для сейфа должно быть два ключа – основной ключ хранится у сотрудника, отвечающего за СКЗИ, а дубликат в опечатанном его личной печатью пенале в сейфе Генерального директора.

4.2 Процедурные меры безопасности

К безопасной эксплуатации продукта и обращения с СКЗИ предъявляются следующие требования:

- при приеме на работу сотрудники подписывают Обязательство о неразглашении сведений, составляющих коммерческую тайну организации
- перечень сведений, составляющих служебную информацию ограниченного доступа, коммерческую тайну организации, утверждается в установленном порядке;
- На предприятии должна быть разработана Инструкция по обращению с сертифицированными ОАЦ средствами криптографической защиты информации;
- Ведение Журнала учета СКЗИ, тестовых ключей на предприятии;
- Ведение Журнала учета обращения эталонных CD дисков на предприятии.

4.3 Технические меры безопасности

К техническим мерам безопасности предъявляются следующие требования:

- доступ к персональным компьютерам и средствам вычислительной техники осуществляется на основе логического имени и пароля пользователя в рамках операционных систем;
- создание инсталляционного пакета для каждого пользователя и управление политикой безопасности пользователя осуществляется только администратором в соответствии с политикой безопасности предприятия;
- администратор должен быть аутентифицирован и идентифицирован перед доступом к продукту с целью администрирования. Аутентификация осуществляется на основе пароля, вводимого с клавиатуры, не отображаясь на экране монитора, и выполняется операционной системой;
- доставка контейнера с криптографическим ключом сертификата пользователя должна осуществляться только по доверенному каналу связи;
- должны использоваться антивирусные продукты для защиты от вирусов клиентских компьютеров и серверов.