УТВЕРЖДЕНО

BY.РТНК.41002-01 34 03-ЛУ

Программный продукт «Клиент безопасности Bel VPN Client-P 4.1»

Подготовительные процедуры

BY.РТНК.41002-01 34 03

Листов 11

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

2017

Содержание

1 Требования на базовые платформы и совместимость

Программный продукт «Клиент безопасности Bel VPN Client-P 4.1» (далее – Bel VPN Client-P, Клиент-П) работает под управлением следующих операционных систем:

- 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 Pro (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 продукт «Клиент безопасности Bel VPN Client-P 4.1» может функционировать в виртуальной среде, под управлением вышеперечисленных ОС.

Bel VPN Client-P совместим со следующими продуктами компании «С-Терра Бел»:

- Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1»
- Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1»
- Программный комплекс «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1»
- Программный комплекс «Bel VPN КР 4.1»

В части реализации протоколов IPsec/IKE и их расширений Bel VPN Client-P совместим с Cisco IOS v.12.4 и v.15.x.x.

2 Подготовка рабочего места администратора безопасности

Администратор безопасности получает административный пакет программного продукта «Клиент безопасности Bel VPN Client-P 4.1», предназначенный для подготовки персонализированных дистрибутивов (содержащих конфигурацию для конкретного пользователя) программного продукта «Клиент безопасности Bel VPN Client-P 4.1».

Административный пакет размещается на компакт-диске, входящем в комплект поставки.

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**, которая входит в программный продукт, и поставляется вместе с его дистрибутивом.

Данная утилита выполняет проверку контрольных характеристик (хэш-сумм) по алгоритму СТБ 34.101.31-2011 (п.6.9).

Утилита **AvVerify** размещается в каталоге `utils` на компакт-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

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

Эталонные значения хэш-сумм приведены в файле **hashes** (размещается в каталоге с дистрибутивом программного продукта), в строках следующего вида:

<hash> <file name>

Пример:

```
E:\util>AvVerify.exe -h e:\Soft\Bel VPN Client-P 4.1\setup.exe
157B41A50895BFDCE0BC652EC988C70AE40E40C3BCB50D5955EC6D0E5B08A64B
```

Далее приведены сообщения, которые могут возникнуть при использовании утилиты AvVerify (таблица 1).

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.

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

3 Подготовка рабочего места пользователя

ВНИМАНИЕ !

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

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

Перед установкой персонифицированного дистрибутива Bel VPN Client-P на компьютере пользователя необходимо временно отключить все антивирусные программы.

3.1 Рекомендации по ручной настройке Брандмауэра Windows

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

Действия, описываемые в данном разделе, выполняются в процессе установки автоматически (инсталлятором); однако, 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 иной персональный межсетевой экран, то в нем следует вручную внести настройки, аналогичные описываемым в этом разделе.

3.1.1 Ручная настройка Брандмауэра Windows на Windows XP

1. Открыть **Панель управления → Брандмауэр Windows**;
2. Перейти во вкладку **Исключения** и нажмите кнопку **Добавить программу...**;
3. В появившемся окне Добавление программы в поле **Путь** необходимо **задать полный путь к файлу vpnsvc.exe**, который располагается в каталоге продукта (по умолчанию – *C:\Program Files\Bel VPN Client-P*);
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-P);

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-P);

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 персонализированного дистрибутива пользователя

Персонализированный дистрибутив программного продукта «Клиент безопасности Bel VPN Client-P 4.1» должен быть установлен пользователем или администратором безопасности в соответствии с руководством пользователя программного продукта «Клиент безопасности Bel VPN Client-P 4.1» (раздел 6 «Инсталляция Bel VPN Client-P»).

4 Требования к внешним мерам безопасности

4.1 Физические меры безопасности

Помещения предприятия должны удовлетворять следующим требованиям:

- 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 руководителя организации либо лица, его замещающего.

4.2 Процедурные меры безопасности

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

- на предприятии должна быть разработана политика информационной безопасности;
- для администрирования Bel VPN Client-P должен быть назначен сотрудник, обладающий навыками администрирования компьютерных систем;
- при приеме на работу сотрудники подписывают Обязательство о неразглашении сведений, составляющих служебную информацию ограниченного доступа;
- перечень сведений, составляющих служебную информацию ограниченного доступа, утверждается в установленном порядке;
- на предприятии должна быть разработана Инструкция по обращению с сертифицированными средствами криптографической защиты информации, включающая перечень действий по реагированию на компрометацию[1] СКЗИ;
- должен вестись Журнал учета СКЗИ, тестовых ключей, эталонных дисков с программными СКЗИ.

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;
- в операционной системе, на которой эксплуатируется Bel VPN Client-P, должны быть настроены отдельные учетные записи Администратора и Пользователя. Учетная запись Администратора должна использоваться только для установки прикладного/системного ПК и его конфигурирования;
- создание инсталляционного пакета для каждого пользователя и управление политикой безопасности пользователя осуществляется только уполномоченным администратором в соответствии с политикой информационной безопасности предприятия;
- доставка контейнера с криптографическим ключом сертификата пользователя должна осуществляться только по доверенному каналу связи;
- на персональных компьютерах с установленными компонентами Bel VPN Client-P должны использоваться сертифицированные антивирусные средства.

[1] Компрометация – факт несанкционированного доступа к защищаемой информации (данные пользователя; ключевые данные и др.), а также подозрение на него

5 Управление криптографическими ключами

5.1 Перечень криптографических операций и протоколов

В программном продукте «Клиент безопасности Bel VPN Client-P 4.1» реализованы и применяются следующие криптографические операции и протоколы:

- ЭЦП – для аутентификации устройств при установлении защищенного канала связи, (с применением технологического сертификата открытого ключа, далее – ТСОК).
- протокол формирования общего ключа – для формирования общего ключа при установлении защищенного канала связи.
- шифрование и имитозащита данных – для защиты следующих данных:
  - служебных данных – в процессе установлении защищенного канала связи, и в процессе его работы;
  - пользовательских данных – в процессе работы защищенного канала связи.

Далее по тексту под взаимодействующими Продуктами Bel VPN понимается взаимодействующие Клиент-П и Шлюз безопасности (программно-аппаратный или программный), между которыми устанавливается защищенное соединение.

5.1.1 ЭЦП для аутентификации устройств

При установлении защищенного соединения (IPsec VPN) взаимодействующие Продукты Bel VPN выполняют взаимную аутентификацию, для чего используется электронная цифровая подпись (СТБ 34.101.45-2013 либо СТБ 1176.2-99) с применением ТСОК (СТБ 34.101.19-2012 (раздел 6)).

Доверие при аутентификации устанавливается на основании доверия Удостоверяющему центру, а также на основании перечня атрибутов ТСОК (общие данные, организация, и т.д.).

5.1.1.1 Генерация ключей

Личный ключ ЭЦП генерируется в соответствии с:

- СТБ 34.101.45-2013 (подраздел 6.2 раздела 6) с применением СТБ 34.101.47-2012 (подраздел 6.2 раздела 6);
- СТБ 1176.2-99 (пункт 5.1 раздела 5) с применением СТБ 34.101.47-2012 (подраздел 6.2 раздела 6).

Генерация криптографического контейнера, содержащего личный ключ ЭЦП Клиент-П выполняется средствами Клиент-П по команде Администратора безопасности.

Открытый ключ ЭЦП генерируется из личного ключа ЭЦП по СТБ 34.101.45-2013 (подраздел 6.2 раздела 6) либо СТБ 1176.2-99 (пункт 6.1 раздела 6).

Генерация открытого ключа ЭЦП выполняется средствами Продукта Bel VPN в процессе формирования Администратором безопасности запроса на ТСОК. При формировании запроса на ТСОК Администратор указывает атрибуты, позволяющие идентифицировать Продукт Bel VPN.

Запрос на выпуск ТСОК вручную передается в Удостоверяющий центр, обслуживающий систему защиты информации, в которой применяется Клиент-П.

Выпущенный ТСОК импортируется Администратором безопасности в Клиент-П при формировании персонализированного пользовательского дистрибутива.

5.1.1.2 Хранение и доступ

Личный ключ ЭЦП является долговременным и размещается в криптографическом контейнере на файловой системе ПЭВМ либо носителе ключевой информации (AvPass либо AvBign,

в зависимости от комплектации и типа Продукта), подключенном к ПЭВМ. Криптографический контейнер обеспечивает защиту личного ключа от несанкционированного доступа.

Доступ к криптографическому контейнеру (личному ключу) осуществляется по паролю, который задается Администратором безопасности вручную на этапе создания криптографического контейнера (либо инициализации носителя ключевой информации, в случае его применения).

5.1.1.3 Распределение

В процессе аутентификации взаимодействующие Продукты Bel VPN обмениваются собственными ТСОК автоматически.

5.1.1.4 Уничтожение

Уничтожение личного ключа ЭЦП выполняется Администратором безопасности вручную, средствами программного обеспечения Клиент-П, с указанием криптографического контейнера и пароля доступа к криптографическому контейнеру / носителю ключевой информации.

Уничтожение ТСОК (отзыв ТСОК) выполняется Администратором безопасности в соответствии с регламентом Удостоверяющего центра, выпустившего ТСОК.

5.1.2 Формирование общего ключа

При установлении защищенного соединения (IPsec VPN) взаимодействующие Продукты Bel VPN формируют общий ключ, на котором осуществляется защита канала передачи ключевых данных.

5.1.2.1 Генерация

Общий ключ защиты ключевой информации генерируется сессионно (на ограниченное время, устанавливаемое Администратором безопасности; по умолчанию – 1 сутки либо до завершения сесии) для каждой пары взаимодействующих Продуктов Bel VPN, по протоколу Диффи-Хеллмана, в соответствии с СТБ 34.101.66-2014 (приложение А) с параметрами из СТБ 34.101.45-2013 (таблица Б1, приложение Б, приложение Д).

5.1.2.2 Распределение

Общий ключ защиты ключевой информации распределяется между взаимодействующими Продуктами Bel VPN автоматически, в процессе работы протокола формирования общего ключа, в соответствии с СТБ 34.101.66-2014 (приложение А).

5.1.2.3 Хранение и доступ

Общий ключ защиты ключевой информации размещается в оперативной памяти ПЭВМ, на которой установлен Клиент-П. Ограничение доступа к общему ключу защиты ключевой информации в оперативной памяти ПЭВМ осуществляется средствами операционной системы в соответствии с моделью защиты доступа к оперативной (виртуальной) памяти процесса, принятой в операционной системе семейства Windows.

5.1.2.4 Уничтожение

Уничтожение общего ключа защиты ключевой информации осуществляется автоматически при завершении защищенного соединения, либо при выключении Клиента-П либо ПЭВМ, на которой установлен Клиент-П, путем очистки соответствующих участков оперативной памяти, выделенной для программных процессов Клиент-П.

5.1.3 Шифрование и имитозащита данных

При установлении защищенного соединения (IPsec VPN) Продукты Bel VPN формируют симметричные ключи шифрования и имитозащиты данных для защиты служебных и пользовательских данных. Данные ключи распределяются между взаимодействующими

Продуктами Bel VPN автоматически, в рамках соединения, защищаемого на общем ключе, сформированном на этапе формирования общего ключа.

5.1.3.1 Генерация ключей

Защита служебных и пользовательских данных осуществляется с применением:

- шифрования по СТБ 34.101.31-2011 (подраздел 6.4 раздела 6) и имитозащиты по СТБ 34.101.31-2011 (подраздел 6.6 раздела 6);
- шифрования по ГОСТ 28147-89 (пункт 4) и имитозащиты по ГОСТ 28147-89 (пункт 5).

Ключи шифрования и имитозащиты данных генерируются сессионно (на ограниченное время, устанавливаемое Администратором безопасности; по умолчанию – 1 час или ~4,39 Гбайт переданных данных, либо до завершения сессии) для каждой пары взаимодействующих Продуктов Bel VPN, с использованием СТБ 34.101.47-2012 (п.6.2) и при передаче защищаются на общем ключе (см.п.2).

5.1.3.2 Хранение и доступ

Ключи шифрования и имитозащиты данных размещается в оперативной памяти ПЭВМ, на которой применяется Клиент-П. Ограничение доступа к общему ключу защиты ключевой информации в оперативной памяти ПЭВМ осуществляется средствами операционной системы в соответствии с моделью защиты доступа к оперативной (виртуальной) памяти процесса, принятой в операционной системе семейства Windows.

5.1.3.3 Распределение

Ключи шифрования и имитозащиты данных распределяются между взаимодействующими Продуктами Bel VPN автоматически, в процессе работы протокола установления защищенного соединения.

5.1.3.4 Уничтожение

Уничтожение ключей шифрования и имитозащиты осуществляется автоматически при завершении защищенного соединения, либо при выключении Продукта Bel VPN, путем очистки соответствующих участков оперативной памяти, выделенной для программных процессов Клиент-П.