

**АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА
«РЕСПУБЛИКАНСКАЯ ПЛАТФОРМА, ДЕЙСТВУЮЩАЯ НА ОСНОВЕ
ТЕХНОЛОГИЙ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ»**

ИНСТРУКЦИЯ ПО ПОДКЛЮЧЕНИЮ К СРЕДЕ ВИРТУАЛИЗАЦИИ

Минск, 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 ОБЩИЙ ПОРЯДОК ПОДКЛЮЧЕНИЯ К СРЕДЕ ВИРТУАЛИЗАЦИИ	4
2 ПОЛУЧЕНИЕ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА	4
3 УСТАНОВКА ПО BEL VPN CLIENT	8
4 СООБЩЕНИЯ В ПРОЦЕССЕ УСТАНОВКИ	12
5 ИНФОРМАЦИЯ ДЛЯ СИСТЕМНОГО АДМИНИСТРАТОРА ПОЛЬЗОВАТЕЛЯ	14
5.1 Проверка маршрутов после установки ПО Bel VPN Client-P.....	14
5.2 Добавление исключений прокси-сервера в настройках веб-браузера	14
5.3 Добавление разрешений на межсетевом экране	14
6 ОТОБРАЖЕНИЕ ТЕКУЩЕГО СТАТУСА BEL VPN CLIENT	16

ВВЕДЕНИЕ

Настоящая инструкция описывает процесс подключения к среде виртуализации пользователей услуг облачных вычислений, для чего необходима установка и запуск программного обеспечения Bel VPN Client-P в операционных системах, отличной от Linux.

Порядок установки Bel VPN Client-P в операционных системах, отличных от Linux, подробно отражен в технической документации на Bel VPN Client-P, поставляемой компанией-разработчиком («С-Терра Бел») (<https://s-terra.by/support-pages/documentation/>).

1 ОБЩИЙ ПОРЯДОК ПОДКЛЮЧЕНИЯ К СРЕДЕ ВИРТУАЛИЗАЦИИ

В настоящем разделе кратко описан процесс подключения к среде виртуализации. Более подробная информация по каждому этапу приведена далее в настоящей инструкции.

Пользователь среды виртуализации (Пользователь) – уполномоченное лицо организации, получающей услуги облачных вычислений на основании договора на оказание услуг.

Администратор ИБ – работник ООО «Белорусские облачные технологии», отвечающий за обеспечение информационной безопасности при подключении к порталам самообслуживания услуг облачных вычислений.

Общий порядок подключения к среде виртуализации следующий:

1) Пользователь передает сведения о себе и своей организации Администратору ИБ (см. п. «ПОЛУЧЕНИЕ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА»);

2) Пользователь получает от Администратора ИБ программную утилиту для формирования файла, содержащего криптоконтейнер, и запроса на выпуск сертификата открытого ключа (см. п. «ПОЛУЧЕНИЕ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА»), высыпает его Администратору ИБ для проверки корректности формирования файла запроса и последующей отправки в организацию, ответственную за выпуск сертификатов открытого ключа (в соответствии с требованиями к ГосСУОК);

3) Администратор ИБ получает сертификат открытого ключа для потребителя услуг облачных вычислений, обеспечивает настройку доступа Пользователя, формирует файл с установочным пакетом ПО Bel VPN Client-P, передает пользователю установочный файл с ПО Bel VPN Client-P, содержащий все необходимые настройки для установления безопасного соединения со средой виртуализации;

4) Пользователь устанавливает ПО Bel VPN Client-P из полученного от Администратора ИБ установочного файла, включающего настройки доступа к среде виртуализации и технологический сертификат открытого ключа для установки защищенного соединения (см. п. «УСТАНОВКА ПО BEL VPN CLIENT»).

2 ПОЛУЧЕНИЕ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА

Для обеспечения возможности подключения к среде виртуализации Пользователь должен сформировать запрос на выпуск сертификата открытого ключа и прислать файл с запросом Администратору ИБ на адрес электронной почты support_infosec@becloud.by для последующего выпуска сертификата открытого ключа и формирования установочного пакета ПО Bel VPN Client-P. Администратору ИБ:

- ФИО Пользователя;
- УНП организации;
- наименование организации;
- юридический адрес;
- E-mail Пользователя;
- контактный телефон;

1) Пользователь получает от Администратора ИБ по электронной почте программную утилиту CRYPTOCONT, предназначенную для формирования криптоконтейнера для хранения ключевой информации и создания файла запроса на выпуск сертификата открытого ключа (получает архив cryptocont.rar, содержащий исполняемый файл cryptocont.exe и необходимые для работы утилиты cryptocont библиотеки);

2) Следует распаковать файлы из архива CRYPTOCONT в один каталог на жестком диске автоматизированного рабочего места Пользователя;

3) Необходимо создать криптоконтейнер на жестком диске автоматизированного рабочего места Пользователя для хранения ключевой пары.

Для этого следует:

- запустить командную строку (cmd.exe);
 - в командной строке перейти в каталог, в котором расположен распакованный файл cryptocont.exe и необходимые для работы утилиты cryptocont библиотеки;
 - запустить в командной строке утилиту cryptocont.exe со следующими параметрами:

cryptocont.exe n -n=ContainerName -p=Password -key_alg=bign

где

ContainerName - название создаваемого криптоконтейнера на жестком диске автоматизированного рабочего места пользователя в следующем формате: УНП организации_Фамилия пользователя (например: 191772685_Ivanov);

Password - пароль к криптоконтейнеру - необходимо ввести следующий пароль: 12345678;

key_alg=bign - алгоритм создания личного ключа ЭЦП по СТБ 34.101.45-2013.

- нажатием клавиш на клавиатуре случайным образом заполнить требуемое значение для инициализации датчика случайных чисел (Рисунок 1).

```
C:\WINDOWS\system32\cmd.exe - cryptocont.exe n -n=TestCont -p=12345678 -key_alg=bign  
c:\cryptocont>  
c:\cryptocont>cryptocont.exe n -n=TestCont -p=12345678 -key_alg=bign  
creating container TestCont...  
Collecting random data, please press any keys:  
[.....]
```

Рисунок 1

Созданный файл криптоконтейнера с ключевой парой будет размещаться в скрытом системном каталоге C:\ProgramData\Avest\Container\

4) Необходимо сформировать запрос на выпуск сертификата открытого ключа.

Для этого следует запустить в командной строке утилиту cryptocont.exe со следующими параметрами:

**cryptocont.exe r -f=Filename -n=ContainerName -p=Password
cn=CommonName -c=Country -o=Organization -g=StateOrProvince
a=StreetAddress -t=OrganizationalUnit -e=EmailAddress**

где

Filename - имя создаваемого файла запроса с указанием каталога для сохранения (рекомендуется указывать расширение файла «*.req», например: C:\Temp\ContainerName.req);

ContainerName - название криптоконтейнера, созданного на предыдущем шаге;

Password - пароль к криптоконтейнеру, заданный на предыдущем шаге;

CommonName - значение поля CommonName будущего сертификата (следует указать ФИО Пользователя), для которого создается сертификат открытого ключа);

Country - код страны (следует указать значение BY);

Organization - наименование организации-потребителя услуг облачных вычислений (следует ввести наименование организации на английском языке);

StateOrProvince - область, в которой находится организация - потребитель услуг облачных вычислений (Минская, Брестская, Витебская, Гомельская, Гродненская, Могилевская, г. Минск - следует ввести значение на английском языке, например Minskaya);

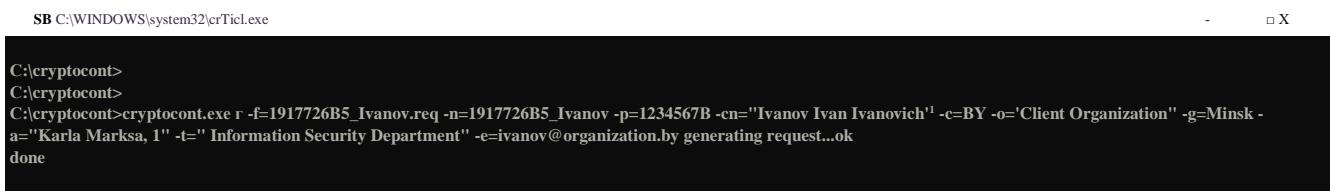
StreetAddress - адрес организации-потребителя услуг облачных вычислений (следует ввести адрес организации (улица, дом) на английском языке без пробелов);

OrganizationalUnit - наименование подразделения Пользователя

(необходимо ввести на английском языке отдел, подразделение, в котором работает Пользователь, подключающийся к среде виртуализации);
EmailAddress – адрес электронной почты Пользователя.

Если поле содержит символ «пробела», то данное поле необходимо указывать в двойных кавычках (например, **-t="IT Department"**)

Далее приведен пример использования утилиты cryptocont.exe для формирования запроса на выпуск сертификата (Рисунок 2).



```
SB C:\WINDOWS\system32\crTcl.exe
C:\cryptocont>
C:\cryptocont>
C:\cryptocont>cryptocont.exe r -f=1917726B5_Ivanov.req -n=1917726B5_Ivanov -p=1234567B -cn="Ivanov Ivan Ivanovich" -c=BY -o='Client Organization' -g=Minsk -a="Karla Marks, 1" -t=" Information Security Department" -e=ivanov@organization.by generating request...ok
done
```

Рисунок 2

После этого в каталоге, в который был распакован файл cryptocont.exe, будет сформирован файл запроса на выпуск сертификата открытого ключа с расширением *.req.

1) Следует отправить сформированный файл запроса на выпуск сертификата открытого ключа Администратору ИБ на адрес электронной почты support_infosec@becloud.by.

Администратор ИБ проверяет корректность сформированного запроса на выпуск сертификата открытого ключа и передает файл запроса в организацию, ответственную за выпуск сертификатов открытого ключа (в соответствии с требованиями к ГосСУОК).

После получения сертификата открытого ключа в формате «*.p7b» или «*.cer» Администратор ИБ формирует файл с установочным пакетом ПО Bel VPN Client-P, содержащий все необходимые настройки для установления безопасного соединения со средой виртуализации.

Файл с установочным пакетом и цепочкой сертификатов «*.p7b» передается Пользователю для установки ПО Bel VPN Client-P на автоматизированном рабочем месте.

3 УСТАНОВКА ПО BEL VPN CLIENT

Перед установкой Bel VPN Client-P рекомендуется закрыть все работающие прикладные программы (приложения), а также либо деактивировать, либо приостановить работающее антивирусное программное обеспечение.

Для установки Bel VPN Client-P необходимо:

- 1) Получить у Администратора ИБ установочный файл.
- 2) Убедиться в наличии подключения АРМ к сети Интернет. При невозможности это проверить, следует обратиться к Администратору ИБ.
- 3) Запустить установочный файл **vPNClient_xxx.exe**, присланный Администратором ИБ (где **xxx** - УНП_ФИО).
- 4) В открывшемся сообщении о начале процесса инсталляции ПО (Рисунок 3) нажать Да.



Рисунок 3

- 5) После нажатия кнопки Да появится окно с приглашением в мастер установки Bel VPN Client (Рисунок 4).

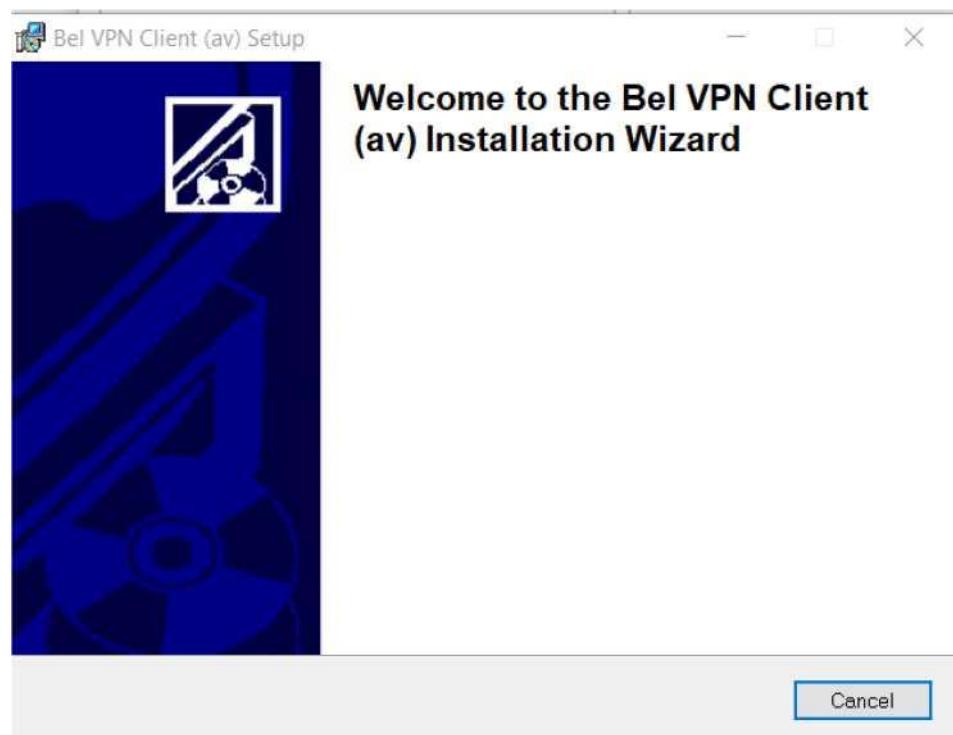


Рисунок 4

- 6) При появлении предупреждения о деактивации средств антивирусной защиты во время процесса установки, необходимо убедиться, что средства

антивирусной защиты деактивированы/приостановлены и нажать OK (Рисунок 5).

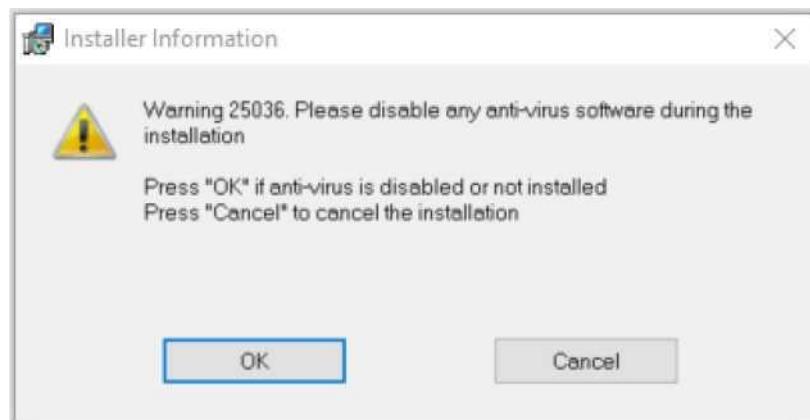


Рисунок 5

- 7) После этого будет отражен процесс установки и обновления системы.
- 8) В процессе установки будет проинициализирован датчик случайных чисел (Рисунок 6).

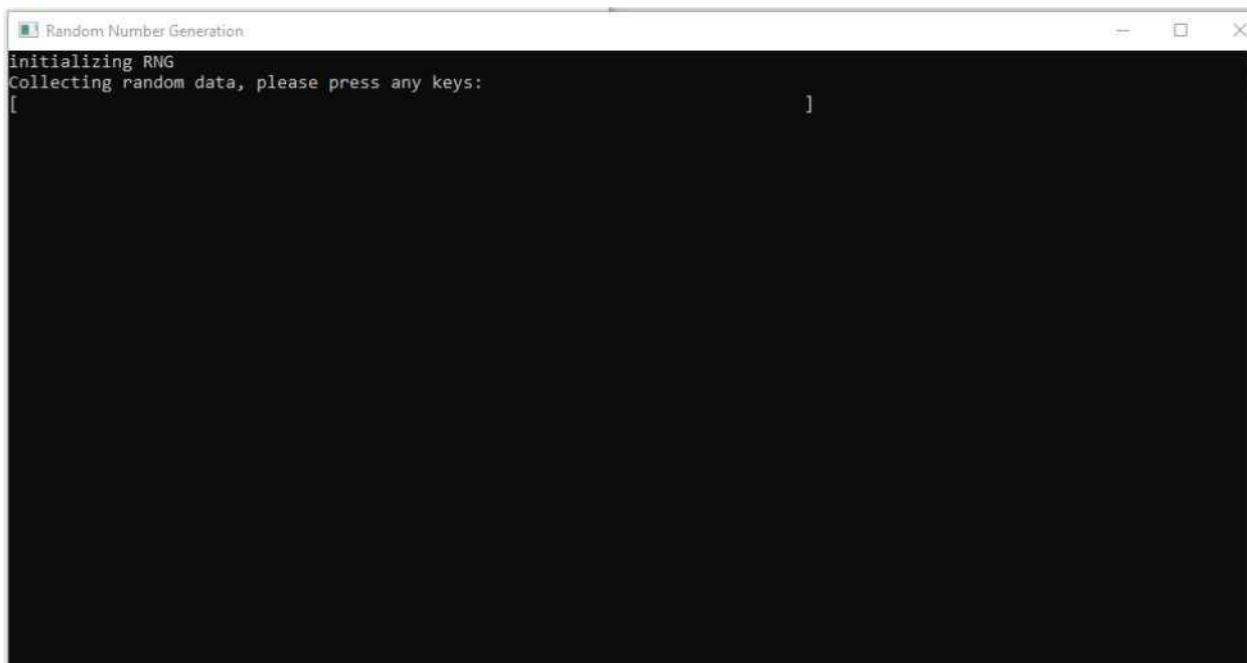


Рисунок 6

Необходимо нажимать на любые клавиши клавиатуры до тех пор, пока не завершится процесс инициализации (Рисунок 7).

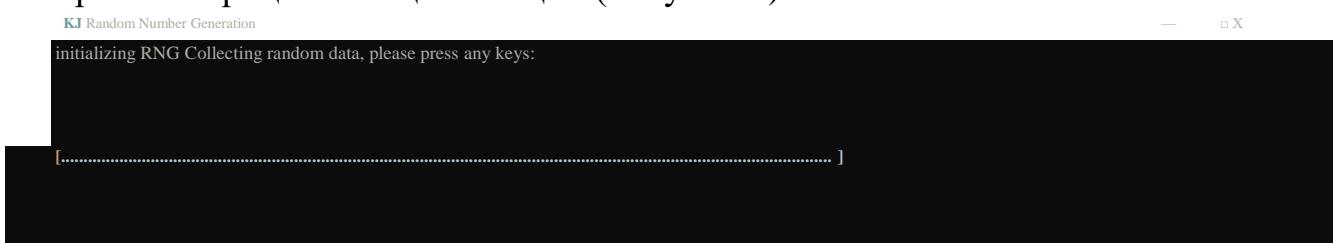


Рисунок 7

- 9) После окончания сбора случайных данных появится окно (Рисунок 8), в котором отображается продолжение процесса установки и обновления системы.

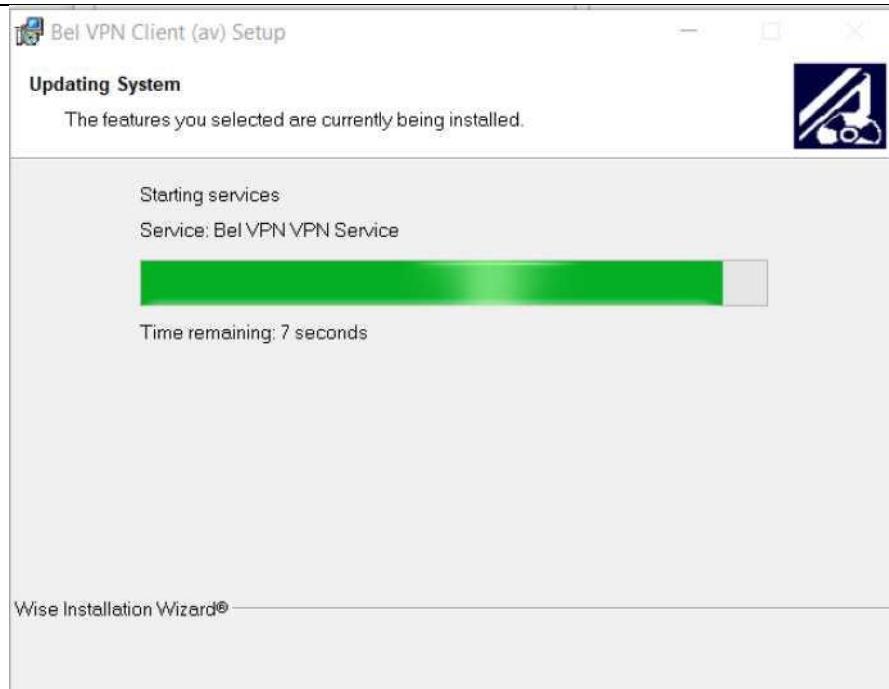


Рисунок 8

10) При инсталляции Bel VPN Client-P в ОС Windows 10 (версия 1803 и старше), будет выведено окно с ошибкой о невозможности запуска службы *Bel VPN Service* (Рисунок 9).

Для решения указанной проблемы, не закрывая окно с предупреждением, необходимо запустить в командной строке от имени администратора скрипт *win10_1803_UI0Detect_dependency_off.bat* (присыпается в архиве вместе с установочным пакетом). После этого в окне (Рисунок 9) следует нажать кнопку *Retry*.



Рисунок 9

11) При успешном завершении процесса установки и обновления системы появится окно с запросом на ввод и смену пароля к Bel VPN Client-P (Рисунок 10). По умолчанию пароль отсутствует (необходимо нажать кнопку OK для пропуска этапа смены пароля).



Рисунок 10

Для смены пароля необходимо нажать Change Password (Рисунок 10).

Далее поле Old Password: оставить пустым, так как первоначальный пароль не задан; в строке New Password: следует ввести новый пароль; в строке Confirm New Password: повторно ввести новый пароль и нажать OK (Рисунок 11).



Рисунок 11

Примечание:

Необходимо запомнить пароль после смены. Запрещается передавать персональный пароль иным лицам.

12) Необходимо перезагрузить АРМ.

После перезагрузки ОС Windows или при последующем включении компьютера/ноутбука необходимо ввести пароль к Bel VPN Client-P перед входом в ОС Windows (см. Рисунок 8).

После загрузки ОС Windows происходит автоматический запуск установленного клиентского ПО Bel VPN Client-P и в панели задач (системном



трее) появится иконка клиентского ПО или в зависимости от того, прошел пользователь аутентификацию или нет.

13) Для подключения к сети администрирования (создания VPN-соединения) необходимо в панели задач выбрать иконку Bel VPN Client-P и в контекстном меню выбрать Login. После создания подключения (VPN-туннеля) в панели задач появится иконка Bel VPN Client-P (Рисунок 12).



Рисунок 12

14) Для подключения к среде виртуализации необходимо в Интернет-браузере в строке ввода адреса ввести следующий адрес (Рисунок 13):



Рисунок 13

15) В случае успешного подключения к среде виртуализации в Интернет-браузере отразится страница авторизации в среде виртуализации.

16) При этом в панели задач на АРМ Пользователя иконка Bel VPN Client-P примет следующий вид (Рисунок 14):



Рисунок 14

Примечание:

В случае отсутствия подключения к среде виртуализации обратитесь к Администратору ИБ.

4 СООБЩЕНИЯ В ПРОЦЕССЕ УСТАНОВКИ

В процессе установки ПО «Клиент безопасности Bel VPN Client-P 4.1» могут появляться ошибки и предупреждения мастера установки при возникновении нештатных ситуаций при обновлении системы.

Наиболее частые ошибки и предупреждения:

1) В случае, если Bel VPN Client-P 4.1 устанавливается на АРМ повторно, то в процессе инсталляции может возникнуть ошибка 25021 (Рисунок 15).

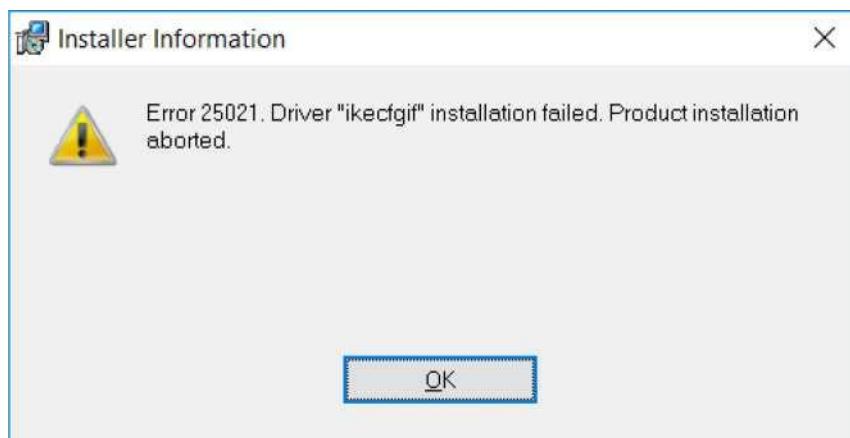


Рисунок 15

Для ее устранения необходимо проделать следующее:

- прервать установку Bel VPN Client-P 4.1, нажав кнопку OK;
- произвести удаление Bel VPN Client-P 4.1 через Панель управления;
- перезагрузить АРМ;

- очистить операционную систему от компонентов, не удалившихся через Панель управления: для этого следует запустить из командной строки от имени администратора утилиту *bel_vpn_install_cleaner.exe* с ключом *clean* (утилита присыпается в архиве вместе с установочным пакетом);

- перезагрузить АРМ;

- зайти в свойства сетевых адаптеров и проверить наличие компонента ***IP Security Module - Lightweight Filter***;

В случае, если указанный компонент присутствует на интерфейсе, то следует удалить его, нажав кнопку Удалить;

В случае, если удалить указанный компонент не удалось - запустить от имени администратора операционной системы скрипт *bel_vpn_cleaner_10.bat* (присыпается в архиве вместе с установочным пакетом);

- перезагрузить АРМ;

- установить Bel VPN Client-P 4.1 заново.

2) Если Bel VPN Client-P 4.1 устанавливается на АРМ, на котором уже либо был установлен и удален клиент безопасности Bel VPN Client-P 4.1, либо по каким-то причинам установка Bel VPN Client-P 4.1 не была проведена до успешного завершения, то в процессе повторной установки может появиться предупреждение о том, что при импорте криптоконтейнера с криптографическими ключами на компьютере/ноутбуке уже имеется криптоконтейнер с таким именем, и будет предложено удалить имеющийся криптоконтейнер и произвести импорт (Рисунок 16). Следует нажать No для последующего успешного продолжения процесса установки Bel VPN Client-P 4.1.

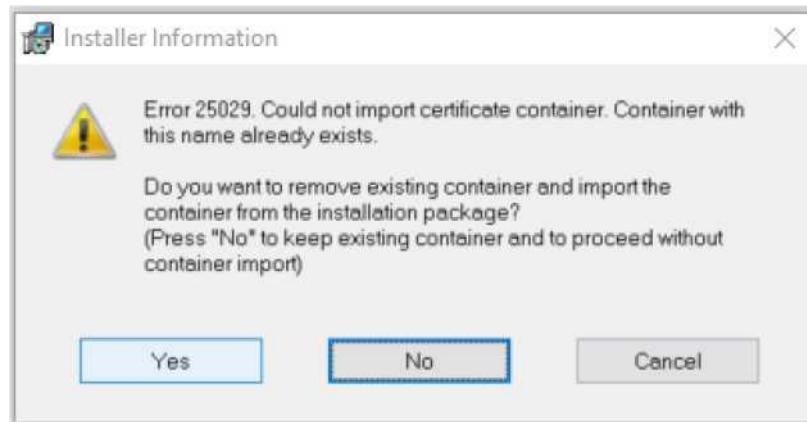


Рисунок 16

При выборе Yes произойдет импорт этого же криптоконтейнера из установочного пакета с удалением аналогичного имеющегося в системе.

3) В случае появления иных предупреждений и ошибок в процессе установки Bel VPN Client-P 4.1 и обновлении системы, необходимо сделать скриншот окна ошибки/предупреждения и прислать его на электронную почту support_infosec@becloud.by с темой письма «Ошибка при установке VPN-клиента для подключения к среде виртуализации».

5 ИНФОРМАЦИЯ ДЛЯ СИСТЕМНОГО АДМИНИСТРАТОРА ПОЛЬЗОВАТЕЛЯ

Информация, представленная в данном разделе, предназначена для системного администратора организации - потребителя услуг облачных вычислений.

5.1 Проверка маршрутов после установки ПО Bel VPN Client-P

После установки ПО Bel VPN Client-P и его запуска, в случае неудачного установления VPN-соединения со шлюзом безопасности, необходимо убедиться в наличии маршрута к среде виртуализации.

1) Для этого в командной строке АРМ пользователя необходимо ввести команду:

route print

2) Если в списке маршрутов отсутствует запись вида:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
195.50.4.0	255.255.255.0	On-link	10.220.4.1	2
195.50.4.255	255.255.255.255	On-link	10.220.4.1	257

, то необходимо обратиться в службу технической поддержки.

5.2 Добавление исключений прокси-сервера в настройках веб-браузера

1) В случае использования в организации для выхода в Интернет прокси-сервера необходимо перед подключением к среде виртуализации внести адреса vcloud.becloud.by и vcloudproxy.becloud.by в исключения для прокси-сервера.

5.3 Добавление разрешений на межсетевом экране

1) Если подключение АРМ Пользователя к сети Интернет осуществляется из корпоративной локальной сети через межсетевой экран, то необходимо на межсетевом экране открыть (разрешить) порты UDP 500 и UDP 4500 для подключения к шлюзам безопасности Bel VPN Gate с IP-адресами: 93.125.20.146, 93.125.20.147.

2) Если на АРМ Пользователя используется персональный межсетевой экран, то для установки шифрованного соединения между АРМ и шлюзом безопасности Bel VPN Gate персональный межсетевой экран необходимо настроить в соответствии с п.1).

3) Если для подключения локальной вычислительной сети к сети Интернет применяются управляемые сетевые устройства (модем, маршрутизатор), то следует обратить внимание на настройки на данных устройствах правил сетевого доступа - не должен блокироваться входящий и исходящий трафик на порты UDP 500 и UDP 4500 (например, может блокироваться входящий трафик на порт UDP 500, если на маршрутизаторе опубликован внутренний IPsec сервер - в этом случае

маршрутизатор блокирует все IPSec соединения, создаваемые не на опубликованный IPsec-сервер, в том числе и входящий на порт UDP 500 трафик).

6 ОТОБРАЖЕНИЕ ТЕКУЩЕГО СТАТУСА BEL VPN CLIENT

Текущий статус Bel VPN Client-Р отображает иконка, расположенная в панели задач. Эта иконка появляется при запуске сервиса и удаляется при его остановке.

Если пользователь не аутентифицировался, то иконка имеет вид:



Пользователь аутентифицировался, но Bel VPN Client не имеет ни одного защищенного соединения - иконка примет вид:



Когда появляется хотя бы одно защищенное соединение, но трафик по этим соединениям отсутствует, то на иконке изменяется цвет «соединения» с серого на зеленый:



Если Bel VPN Client имеет хотя бы одно защищенное соединение и обрабатывает трафик по этим соединениям, то на иконке изменяется цвет «монитора» с синего на бирюзовый:



При наведении указателя мыши на иконку всплывает информация о количестве «активных» защищенных соединений (существующих на момент наведения мыши на иконку) и количестве байт обработанного трафика по всем существовавшим и существующим защищенным соединениям с момента загрузки операционной системы:

IPsec connections: 0
Processed bytes: 13104

