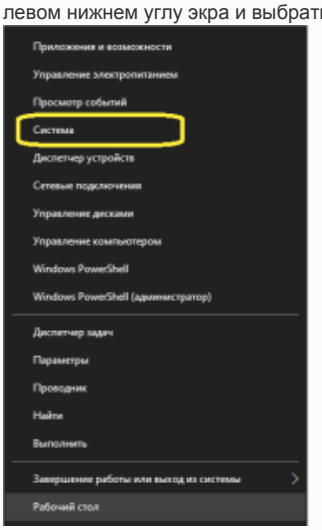
Подключение пользователя к cert.1cfresh.com (доступ к vpn). Инструкция для пользователя

I. Установка СКЗИ Континент-АП для создания защищённого соединения

1. Проверить, что компьютер пользователя отвечает системным требованиям:
   https://www.securitycode.ru/products/skzi-kontinent-ap/?tab=system
   Важно:
   Windows 10 x86/x64 (кроме выпусков Education Edition, Home Edition и Insider Preview)
   Windows 7 SP1 x86/x64 (кроме всех выпусков Starter и Home Edition)

   Где посмотреть параметры компьютера

   В Windows для просмотра параметров компьютера и версии ОС нужно кликнуть правой кнопкой мыши на иконке "Пуск" в левом нижнем углу экра и выбрать пункт "Система"

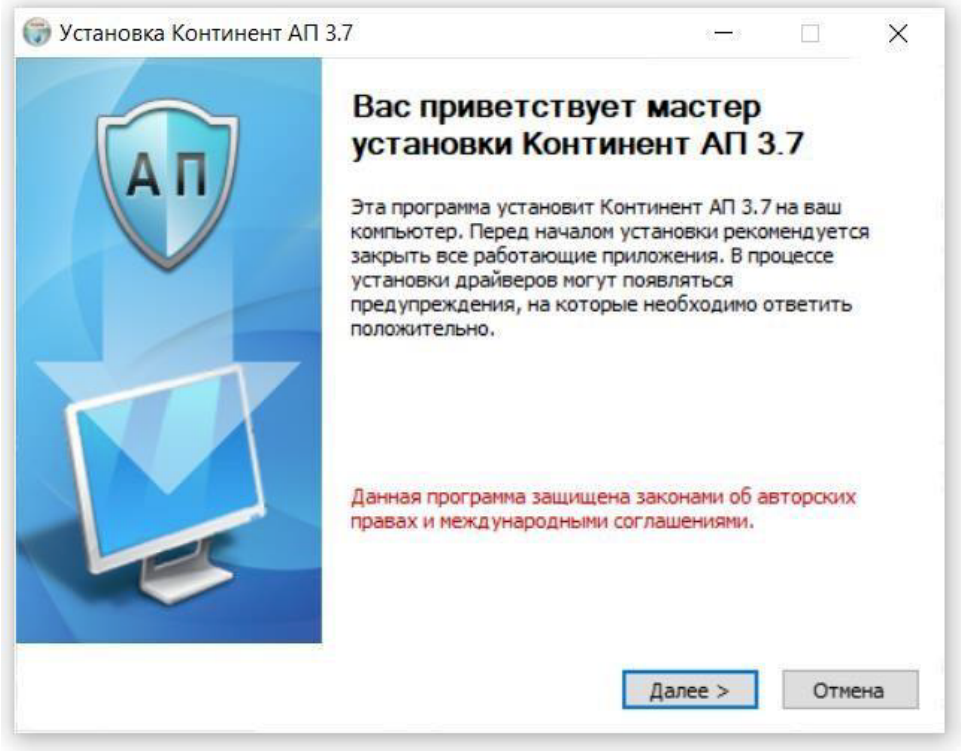
2. Скачать дистрибутив СКЗИ Континент-АП

   Windows: https://files.1c.ru/1cfresh/setup_SKZI_Continent_AP_windows.zip
   Linux: https://files.1c.ru/1cfresh/setup_SKZI_Continent_AP_linix.zip
3. Подготовка к установке
   a. Сделать точку восстановления системы.
      Как сделать в Windows 10 описано тут: https://support.microsoft.com/ru-ru/windows/создание-точки-восстановления-системы-77e02e2a-3298-c869-9974-ef5658ea3be9
   b. В настройках биоса необходимо отключить Secure Boot (оно же: перевести загрузку в Legacy-режим)

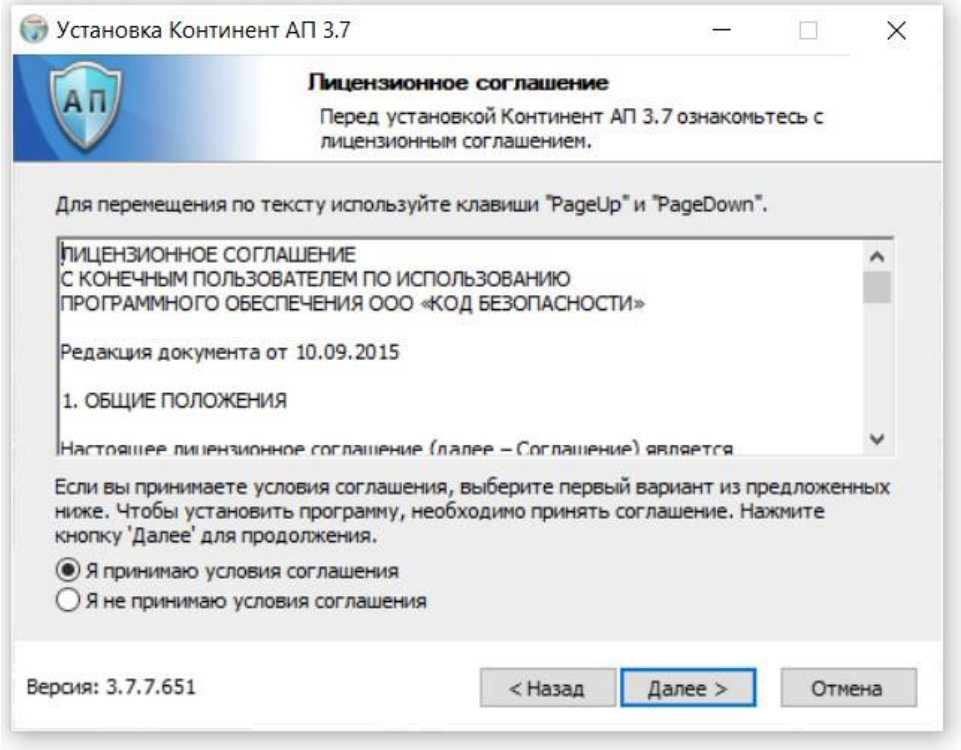
      Без этих действий Вы рискуете потерять доступ к системе при неудачной установке ПО без возможности восстановления, либо вызвать некорректную работу периферийных устройств.
      В некоторых случаях после установки СКЗИ Континент-АП, если в bios не отключена опция Secure Boot, перестаёт работать мышь.
      Восстановить работоспособность можно только удалив СКЗИ Континент-АП (без использования мыши) или отключив Secure Boot в биосе.

4. Если установлен КриптоПро
   Для совместной работы с Континент-АП с КриптоПРО, требуется чтобы КриптоПРО был установлен после Континент-АП и версия КриптоПРО была не ниже 4.0.9944.
   Если КриптоПРО уже установлен, то возможно его потребуется переустановить. Перед переустановкой требуется обязательно сделать точку восстановления системы, резервные копии личных сертификатов и копию серийного номера лицензии КриптоПРО.
5. Установка СКЗИ Континет-АП

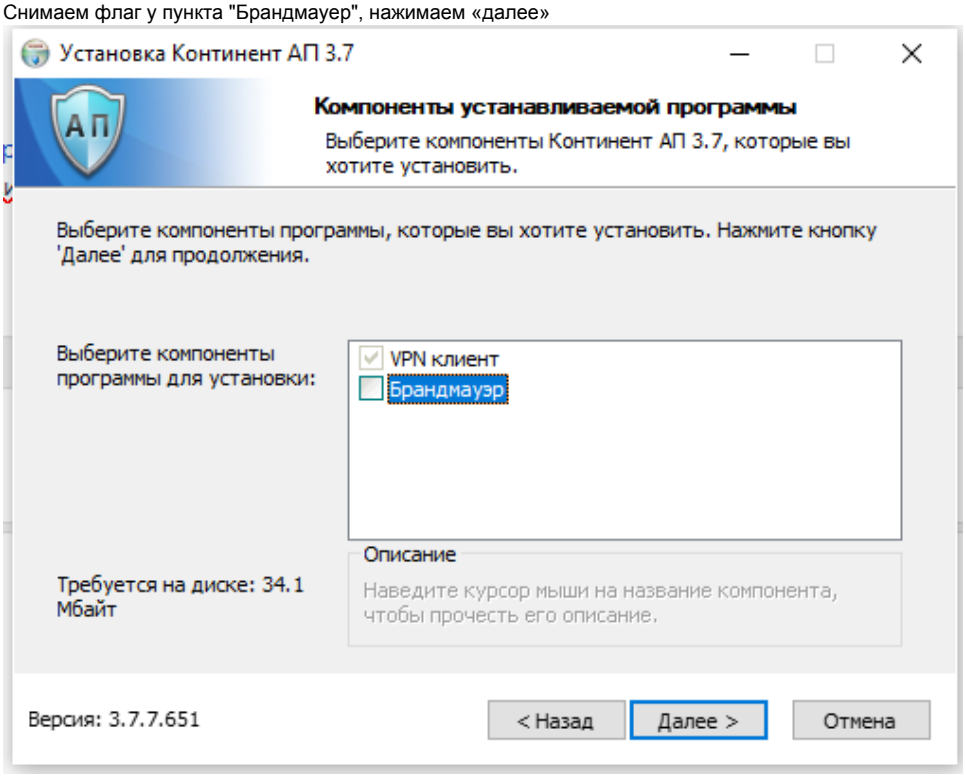
   a. Запускаем скачанный в п.1 **ts_setup**, нажимаем "Далее".



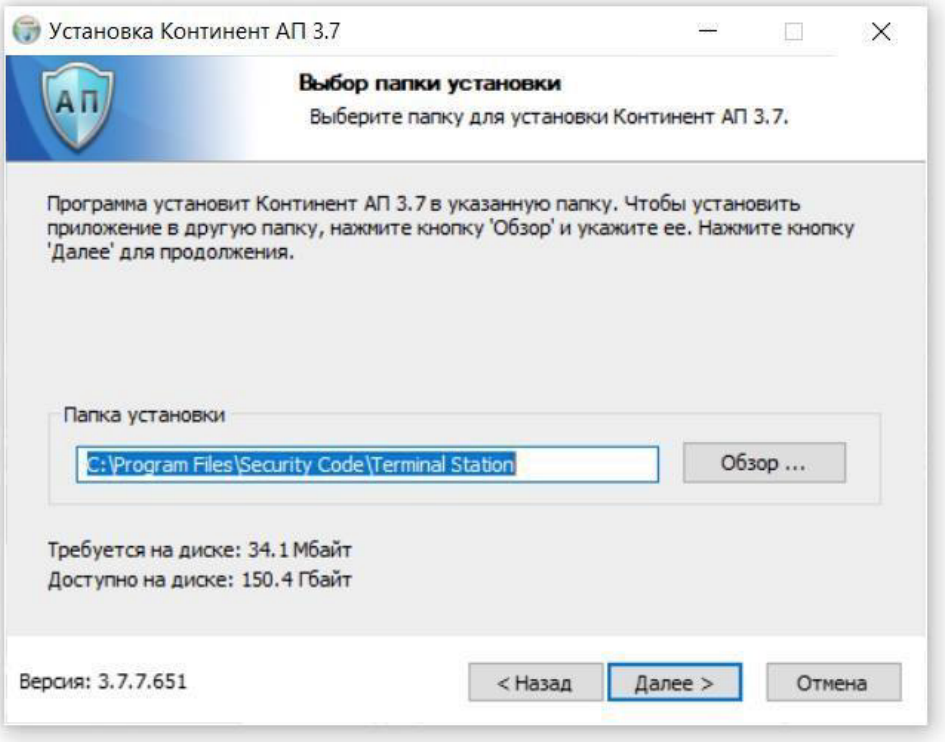
   b. Принимаем лицензионное соглашение, нажимаем «далее».



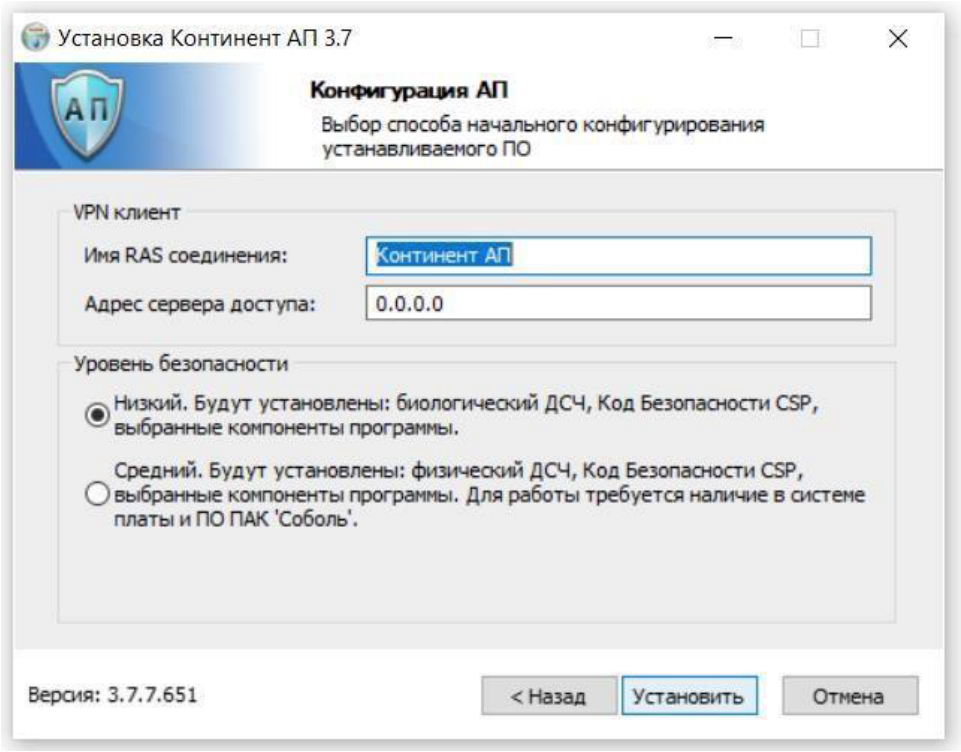
c. Снимаем флаг у пункта "Брандмауер", нажимаем «далее»



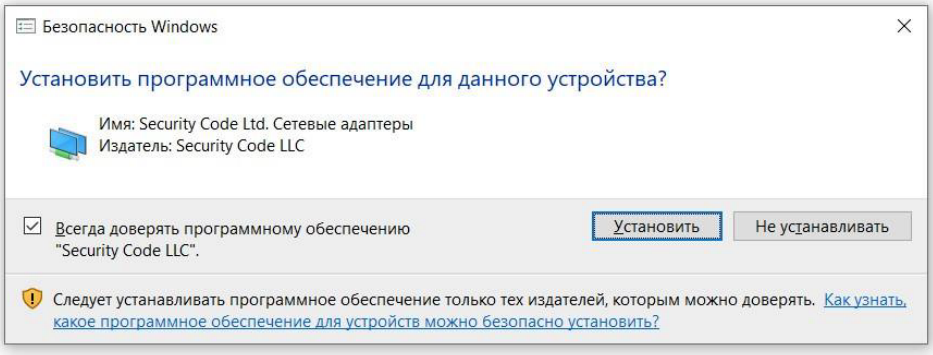
d. Путь по умолчанию НЕ меняем, нажимаем «далее»



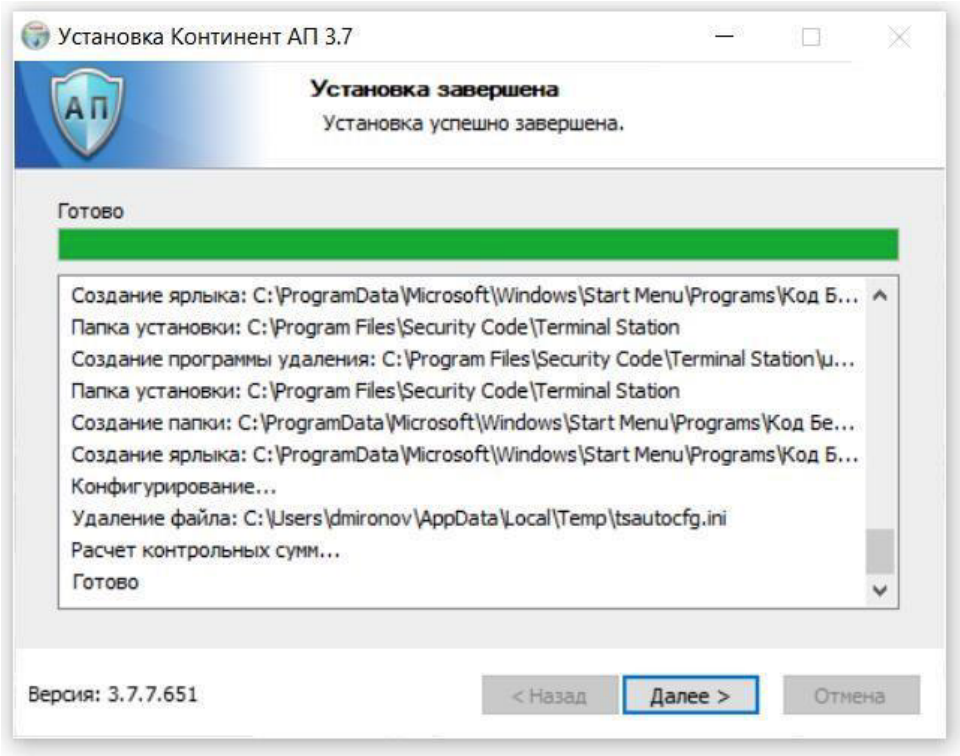
e. Поля не изменяем, уровень безопасности – низкий, нажимаем «установить»

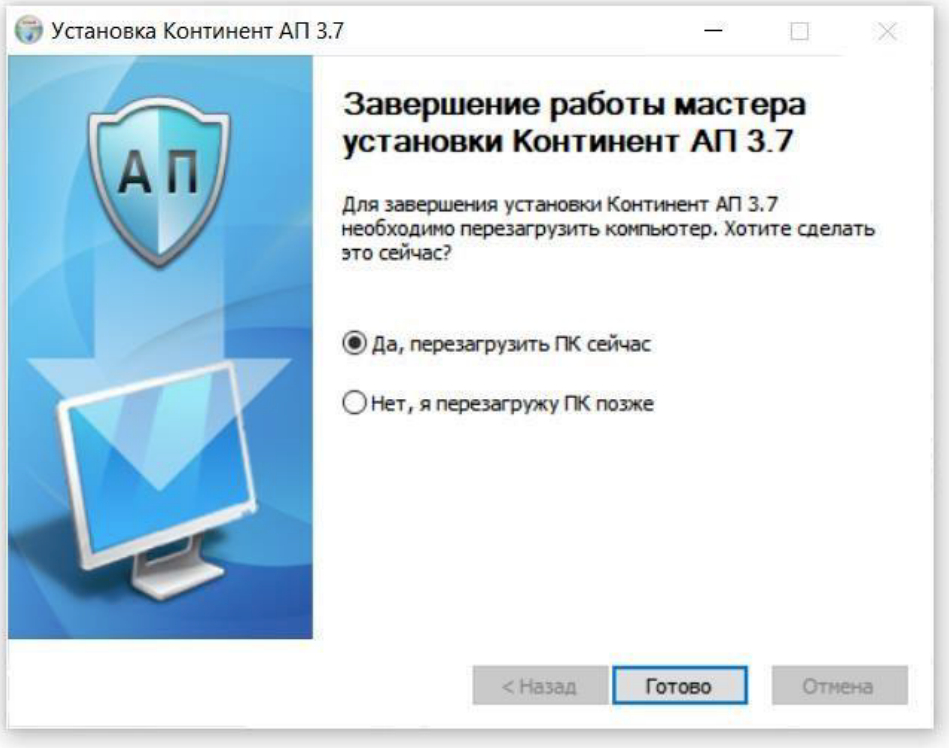


f. В ходе установке соглашаемся с установкой программного обеспечения:

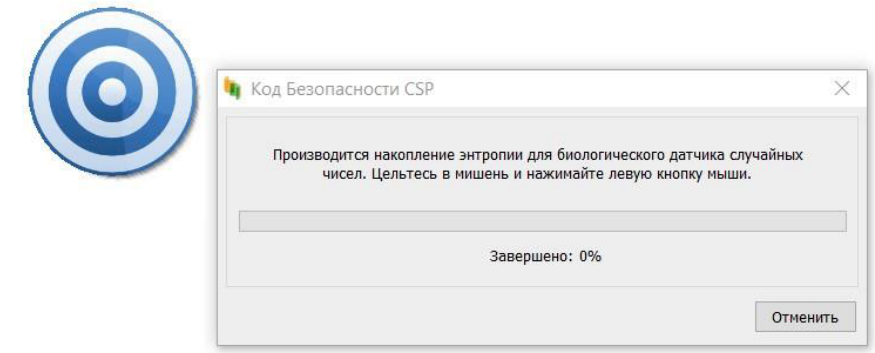


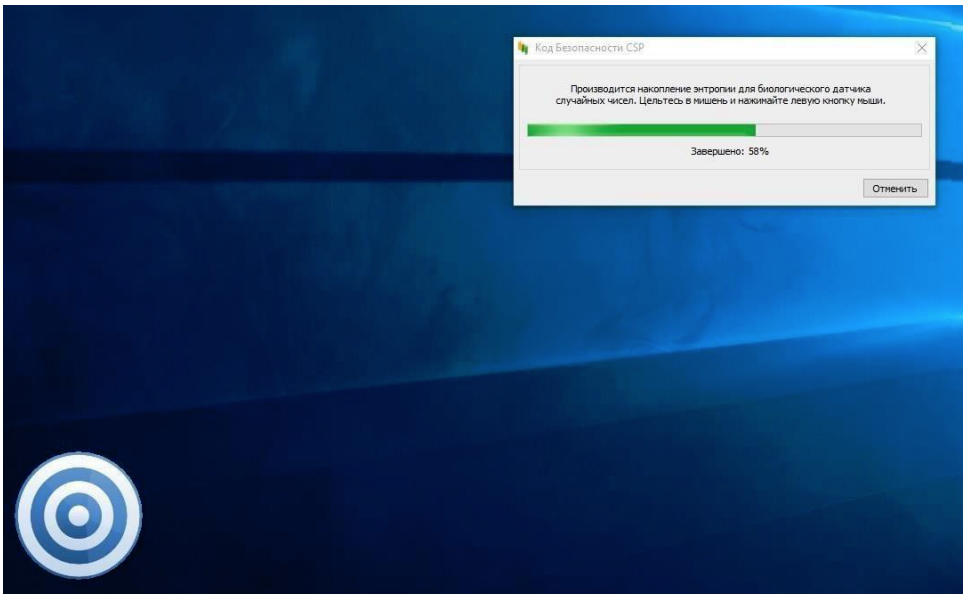
g. Для завершения установки нажимаем «далее» и перезагружаем ПК.





h. После перезагрузки ПК автоматически запустится ПО «Код Безопасности CSP».
Будет производиться накопление энтропии для биологического датчика случайных чисел.
Для этого необходимо с помощью мыши целиться в мишень, появляющуюся в различных частях экрана.
При наведении курсора на мишень необходимо нажать левую кнопку мыши.
Данный процесс необходимо повторять до тех пор, пока шкала накопления энтропии не заполнится до 100%.

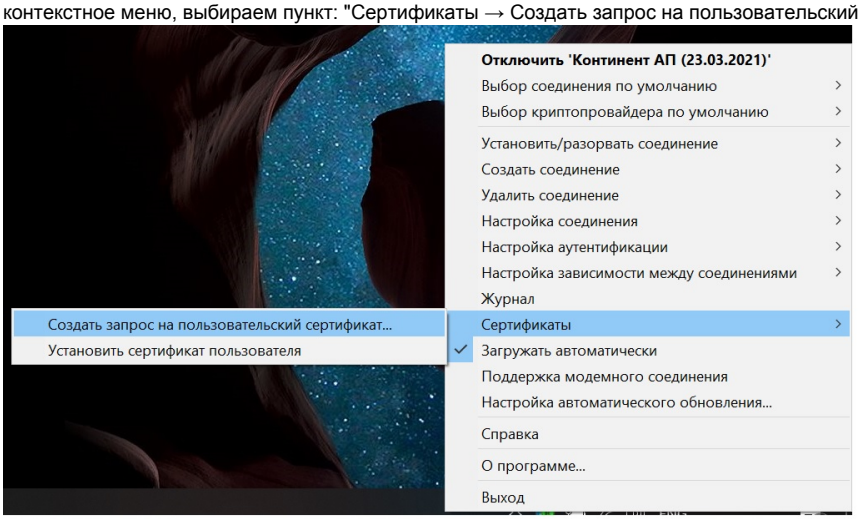




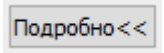
После завершения накопления энтропии установка ПО «Континент-АП» будет завершена. Теперь необходимо перейти к настройке параметров сетевого подключения.

II. Запрос на подключение нового пользователя к сервису cert.1cfresh.com

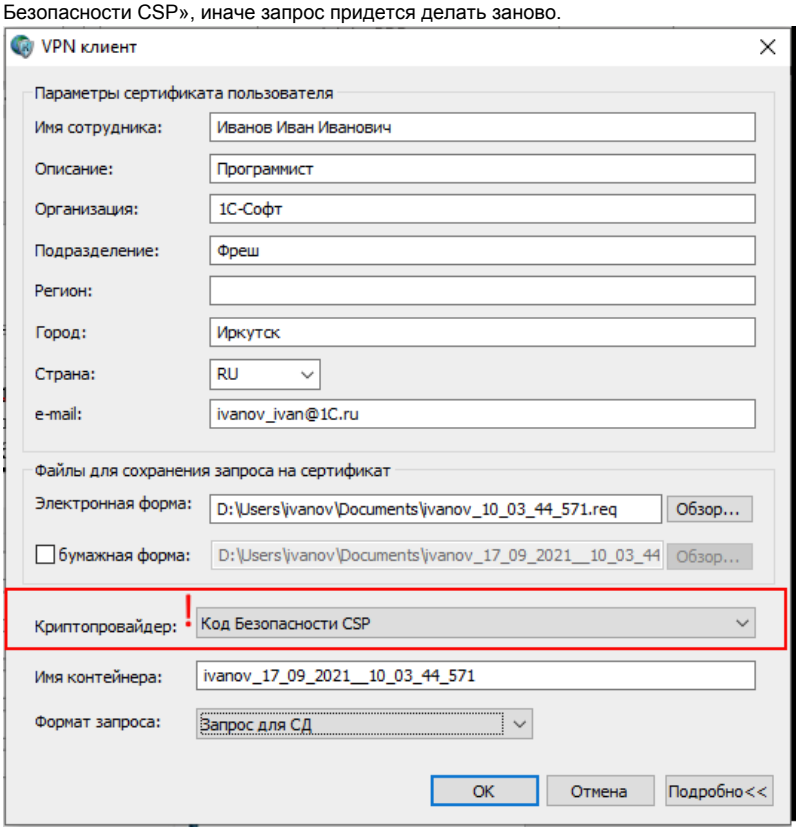
1. В системном трее (правый нижний угол) нажатием правой кнопкой мыши на ярлык VPN-клиенте Континент-АП  , открываем контекстное меню, выбираем пункт: "Сертификаты → Создать запрос на пользовательский сертификат"



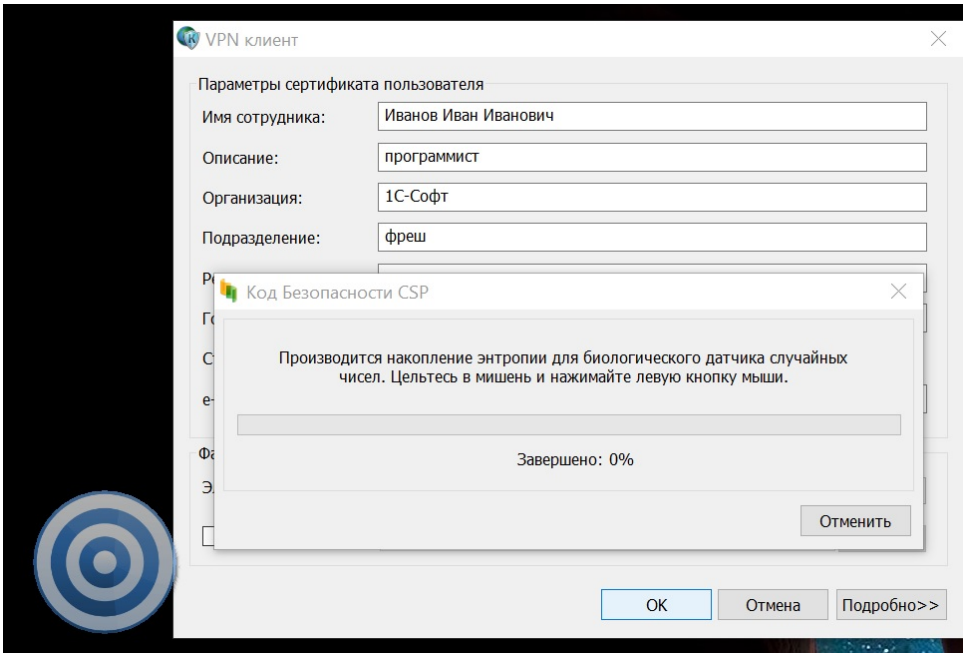
2. Заполняем все поля (Имя сотрудника, Описание, Организация, Город, Страна, e-mail).
   Имя сотрудника должно быть в виде **Фамилия Имя Отчество**

   ВАЖНО! Необходимо нажать кнопку 

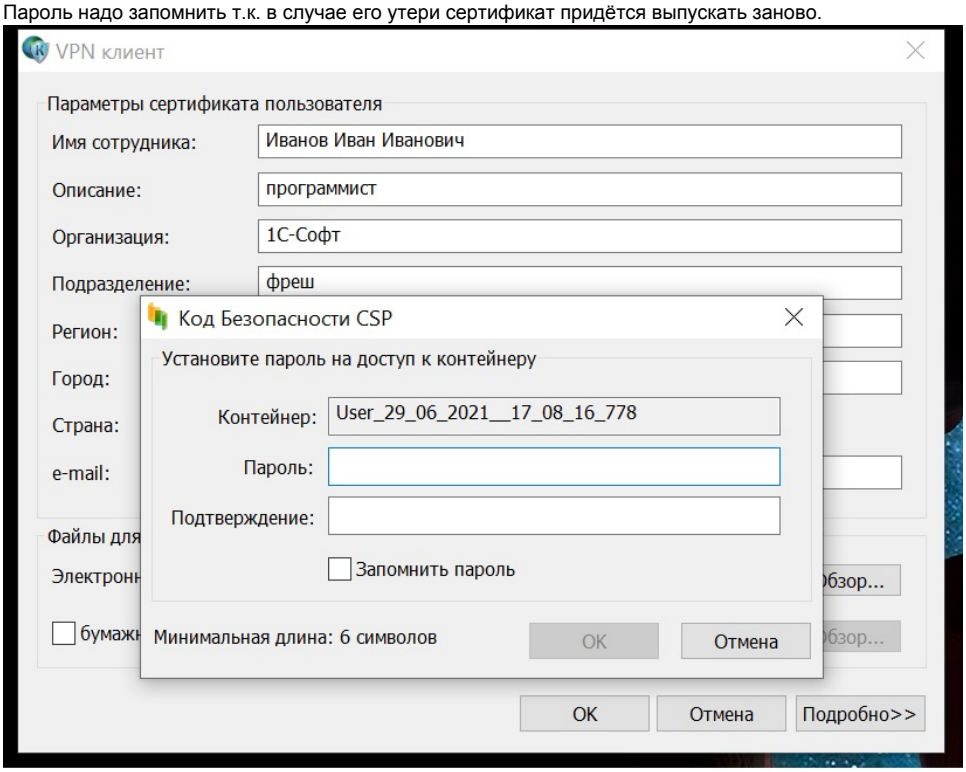
и убедиться что поле "Криптопровайдер" установлено в значение «Код Безопасности CSP», иначе запрос придется делать заново.



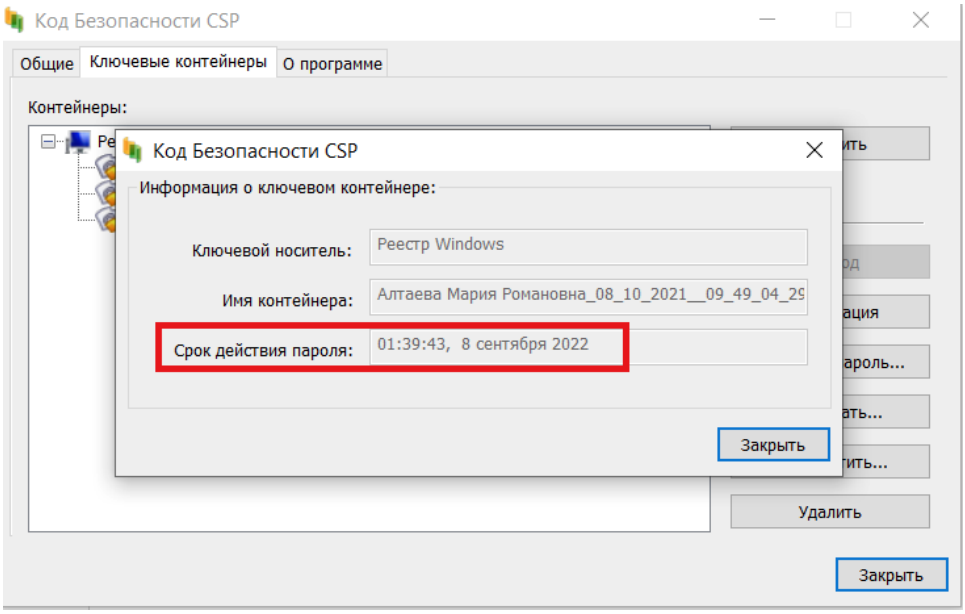
   Далее нужно запомнить куда сохранился файл с сертификатом (поле "электронная форма"). Этот файл далее нужно будет отправить администраторам сервиса.
   По окончанию заполнения и проверки всех полей нажимаем «Ок».
3. Теперь нужно повторить накопление энтропии, для этого кликаем по появляющийся мишеням, пока процесс генерации не будет завершен.



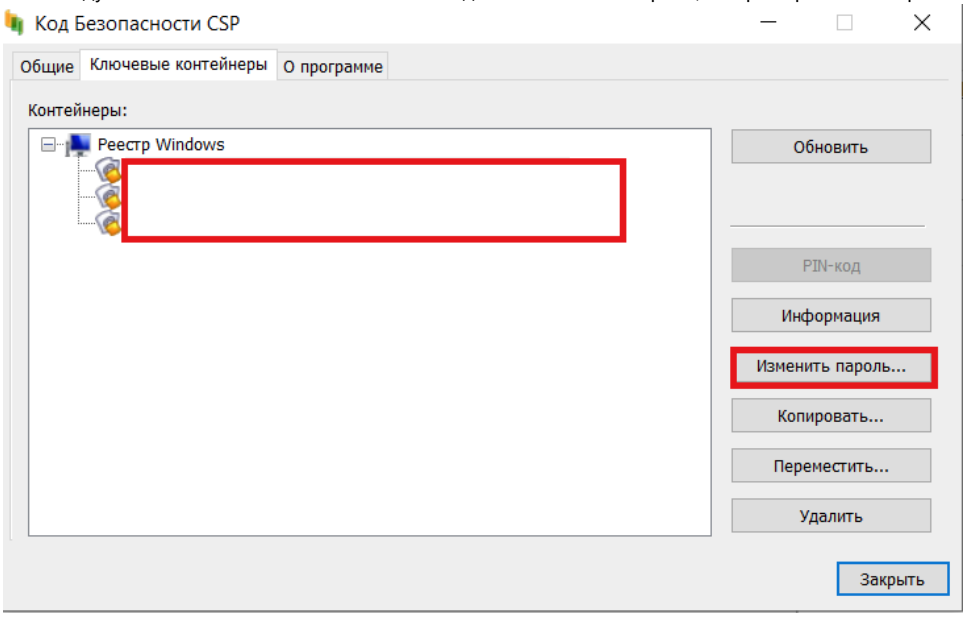
4. После успешного формирования запроса необходимо ввести пароль от будущего сертификата и его подтверждение.
Пароль надо запомнить т.к. в случае его утери сертификат придётся выпускать заново.



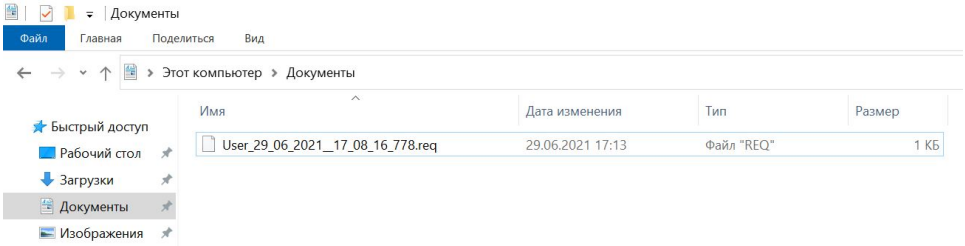
ВАЖНО!
Пароль устанавливается на **5 месяцев**.
Если до истечения срока пароля его не сменить, потребуется перевыпускать сертификат.
Срок действия пароля можно проверить срок действия просьба зайти в **Пуск – Код Безопасности CSP – Выбрать нужный контейнер – Информация**.



Смена пароля производится по кнопке Изменить пароль: вводите старый пароль и вносите новый пароль, который важно **запомнить**. Рекомендуется поставить напоминание о необходимости сменить пароль, которое сработает через 4 - 4,5 месяца.



5. Заходим в каталог, который был указан в п.II.2 данной инструкции, находим "Файл для сохранения запроса на сертификат" (имеет расширение **.req**) и отправляем администратору сервиса на адрес support@cert.1cfresh.com

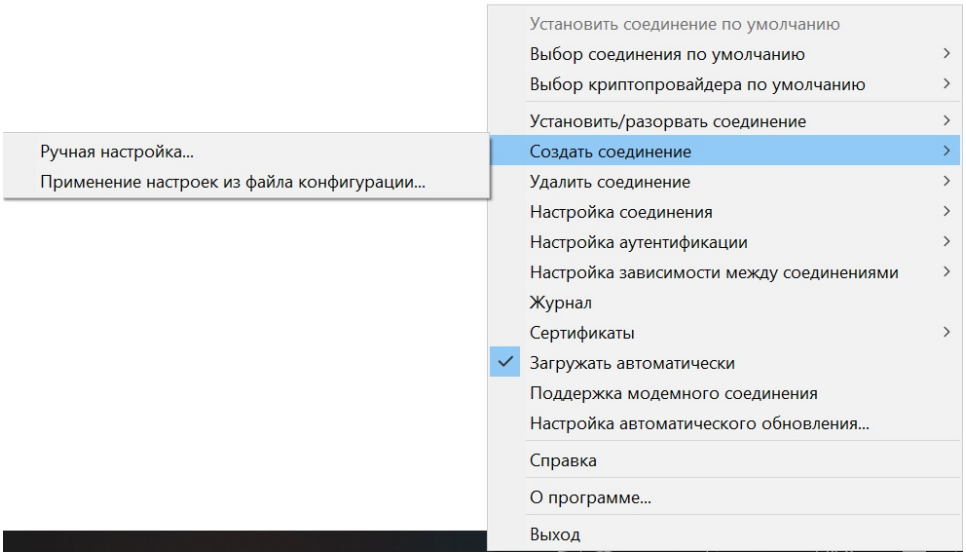


6. Ожидаем ответа от администратора сервиса. Ответ должен прийти в виде файла с расширением .apcfg

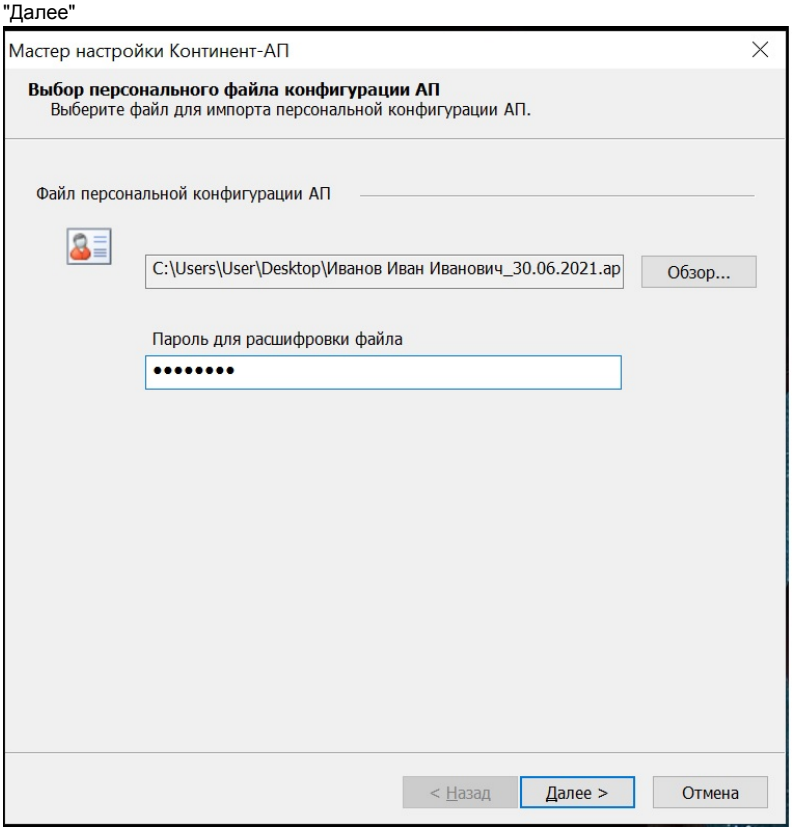
III. Установка сертификата пользователя

1. От администрации сервиса в ответ на запрос придёт файл с расширением ".apcfg"

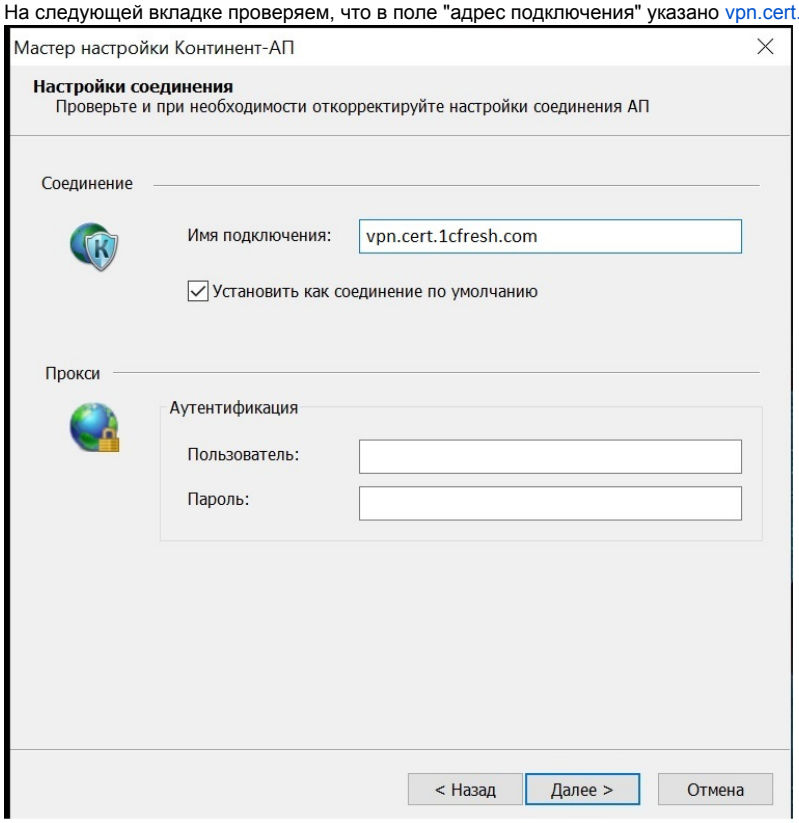
2. Открываем контекстное меню VPN-клиента, выбираем "Создать соединение" → Применение настроек из файла конфигурации



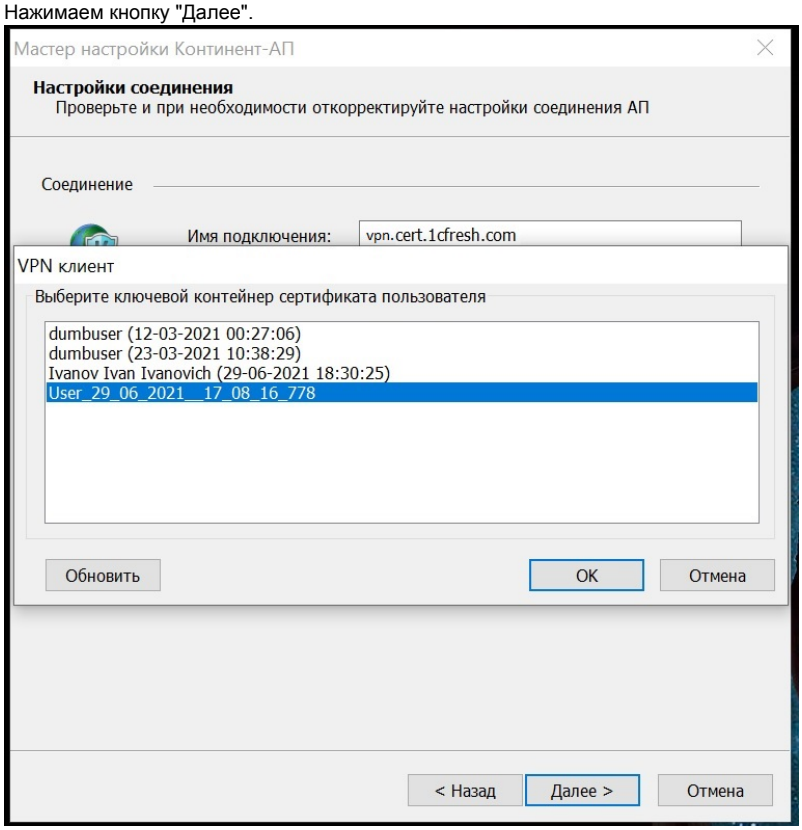
3. Выбираем полученный файл, указываем пароль для расшифровки файла, полученный от администратора сервиса. Нажимаем кнопку "Далее"



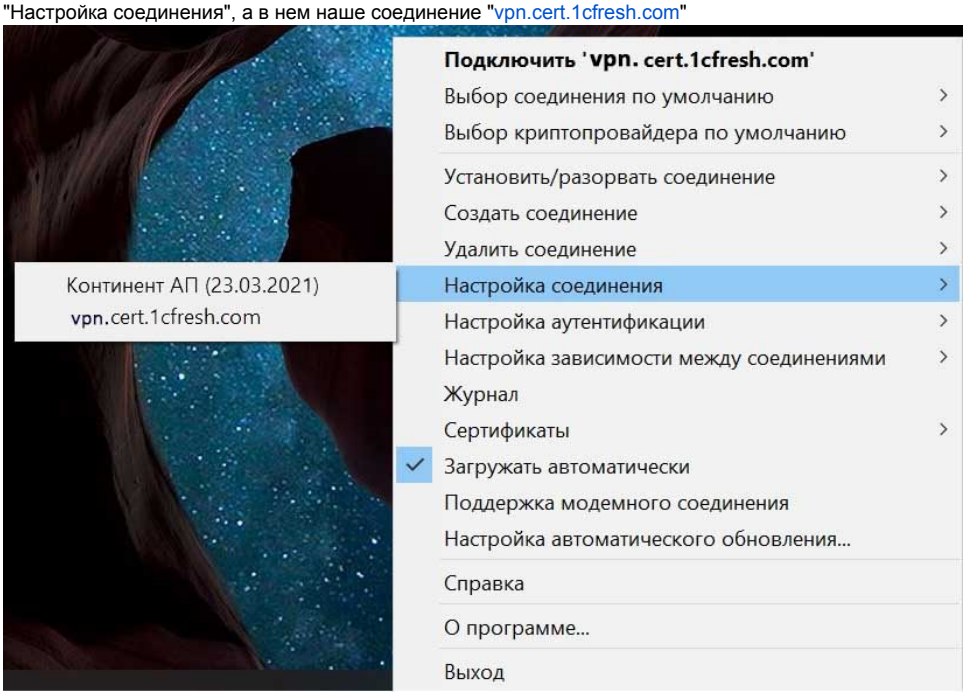
4. На следующей вкладке проверяем, что в поле "адрес подключения" указано vpn.cert.1cfresh.com. Нажимаем кнопку "Далее".



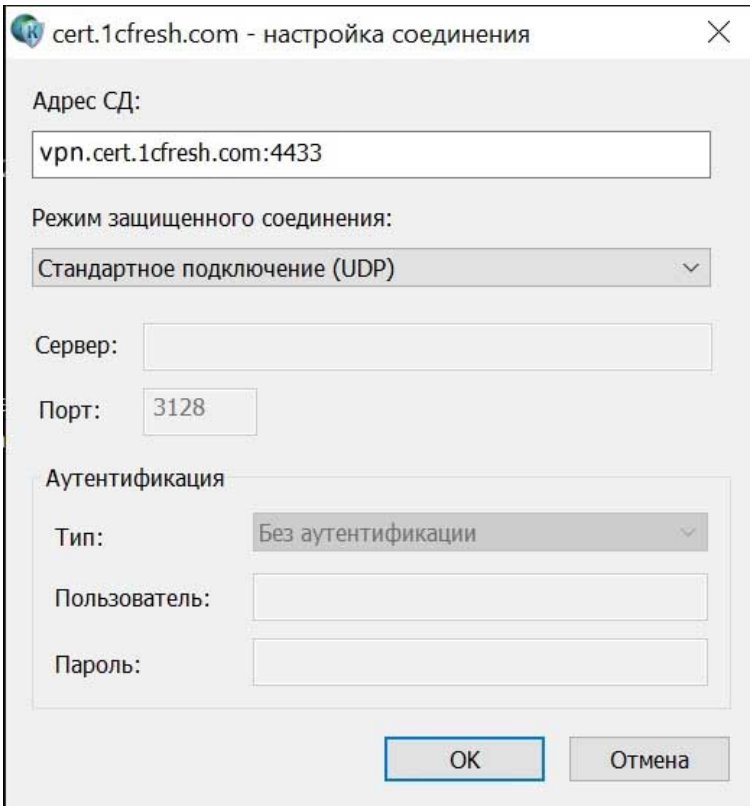
5. (при необходимости) Выбираем ключевой контейнер, который был сформирован для хранения ключа сертификата, если их несколько. Нажимаем кнопку "Далее".



6. Для проверки/изменения параметров подключения к сервису открываем настройку соединения в главном меню Континент АП. Пункт "Настройка соединения", а в нем наше соединение "vpn.cert.1cfresh.com"

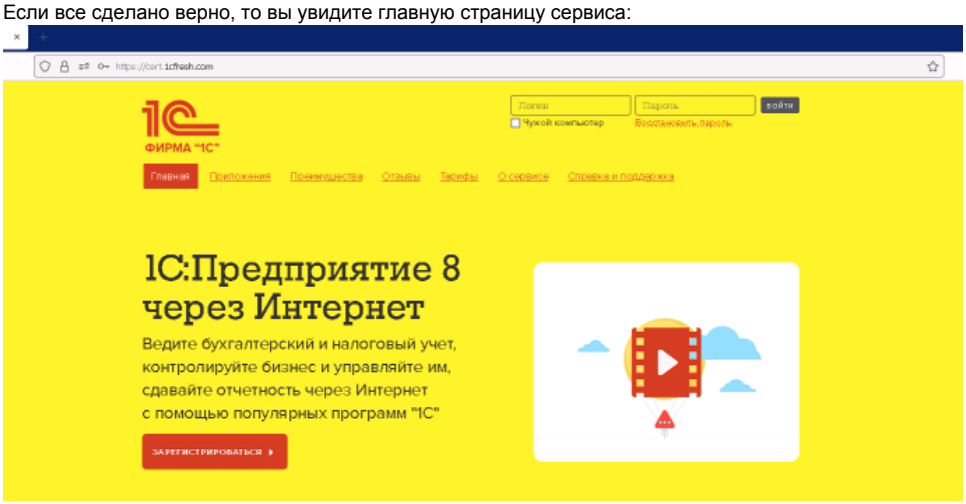


7. В появившемся диалоге подключения проверяем, чтобы правильно были заполнены поля:
Адрес СД: vpn.cert.1cfresh.com:4433 (или vpn.cert.1cfresh.com)
Режим защищенного соединения: Стандартное подключение (UDP)
После успешного заполнения нажать "ОК" для закрытия диалога.



8. Через контекстное меню "Установить\разорвать соединение" → "Установить соединение vpn.cert.1cfresh.com".
Должно появиться окно с запросом пароля, который был задан при формировании сертификата.

Если соединение было успешно установлено - иконка VPN-клиента в системном трее изменится с серой на зелёную 

9. Открываем в браузере сайт cert.1cfresh.com
   Если все сделано верно, то вы увидите главную страницу сервиса:


10. Настройка защищённого соединения завершена. Можно приступать к установке платформы 1С.

IV. Установка тонкого клиента платформы 1С:Предприятие 8

Работа в облачных приложениях можно с помощью Тонкого клиент 1С или веб-браузера.
Рекомендуется установить Тонкий клиент и использовать в качестве основного варианта.
Скачать дистрибутив можно

- по ссылке: https://releases.1c.ru/version_files?nick=Platform83&ver=8.3.17.2306
- Либо перейти в список всех версий платформы 1С и выбрать нужную: https://releases.1c.ru/project/Platform83

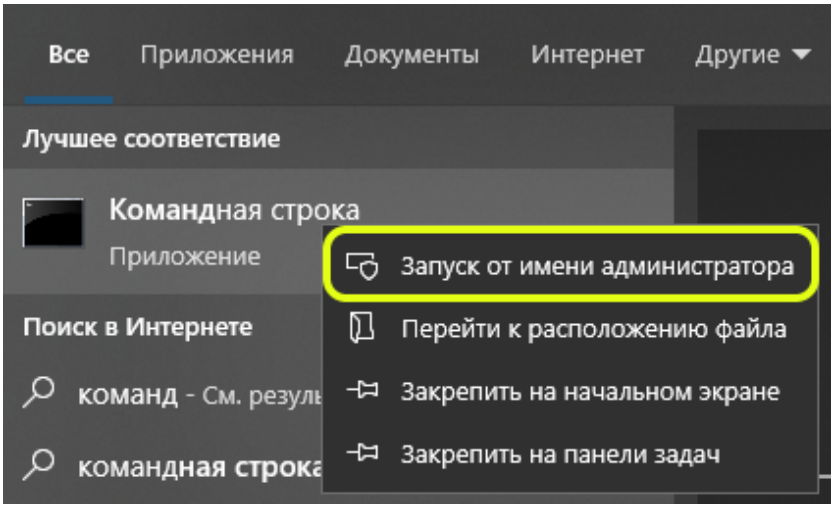
В списке компонентов, вероятнее всего, вам необходим "Тонкий клиент 1С:Предприятие (64-bit) для Windows". Скачиваем его.
Разархивируем скаченный файл и запускаем "setup.exe".

V. Проблемы и их решения

1. ## После установки\переустановки Континент-АП перестала работать мышь\тачпэд ноутбука
   Решение: 8689 - Почему перестает работать мышь/клавиатура после установки/удаления TLSClient/"Континент-АП"? (securitycode.ru)

2. ## При запуске VPN-Клиент Континент-АП ошибка "Тест контроля целостности не пройден"


   Решение:
   a. Нажать кнопку "Пуск", ввести "cmd" или "Командная строка".
      На найденной в списке программе нажать правой кнопкой мыши и выбрать пункт "Запуск от имени администратора"



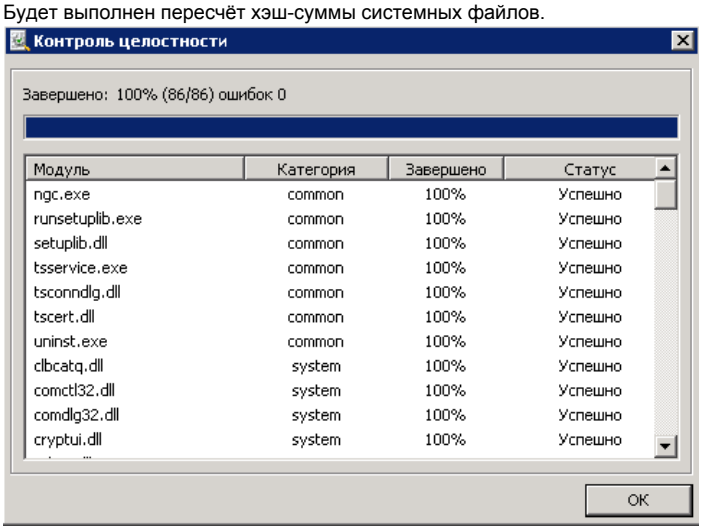
Ввести команду для переход в каталог с установленным VPN-клиентом

```
cd "C:\Program Files\Security Code\Terminal Station\"
```

Далее выполнить комменду

```
ngc.exe /b
```

Будет выполнен пересчёт хэш-суммы системных файлов.



После окончания выполнения процедуры контроля целостности нужно закрыть окно и запустить VPN-клиент Континент-АП: приложение должно запуститься без ошибок.
Важно!
Чтобы эта ошибка больше не появлялась, нужно отредактировать файл Integrity.xml.
Для этого откройте Блокнот от имени администратора, в нем откройте файл C:\Program Files\Security Code\Terminal Station\Integrity.xml. В файле удалите все строки, оставив только:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<integrity><catalog name="common"></catalog></integrity>
```

Сохраните файл и перезапустите VPN клиент.

3. ## После установки\переустановки КАП перестал работать КриптоПро CSP

Решение: Необходимо выполнить настройку совместимости Континент АП и КриптоПро CSP.

a. В ветках реестра:
Для 32х разрядной системы: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\

Для 64х разрядной системы:

• HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\

• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\

Для значения **OID [1.2.643.2.1.3.2.1!1]** переименуйте параметр "**Algid**"=**dword:0000801e** в уникальное, например "**Algid-**"=**dword: 0000801e**

После внесения изменений перезагрузите компьютер.

b. Удалить ветки реестра, если есть:
    i. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 1\CryptDllImportPublicKeyInfoEx\1. 2.643.7.1.1.1.1
    ii. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 1\CryptDllImportPublicKeyInfoEx\1.2.643.7.1.1.1.1
    iii. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 1\CryptDllImportPublicKeyInfoEx\1. 2.643.2.2.19
    iv. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 1\CryptDllImportPublicKeyInfoEx\1.2.643.2.2.19