

# **Инструкция по установке и настройке средства криптографической защиты информации «Континент-АП» версии 3.7**

## **ОГЛАВЛЕНИЕ**

1. Общие положения.....	2
2. Установка «Континент-АП».....	3
3. Создание сертификата пользователя.....	8
3.1. Генерация закрытого ключа, формирование запроса и заявки на издание сертификата абонентского пункта .....	8
3.2. Установка сертификата.....	13
4. Подключение к серверу доступа.....	18

## **1. Общие положения**

Данная инструкция предназначена для пользователей средства криптографической защиты информации «Континент-АП» версии 3.7 (далее – «Континент-АП»).

«Континент-АП» предназначен для безопасной передачи данных через общедоступные (незащищенные) сети. Эта технология называется «виртуальная частная сеть» (VPN). Защита данных обеспечивается криптографическими методами, вследствие чего через общедоступную сеть данные передаются в зашифрованном виде.

«Континент-АП» обеспечивает доступ пользователей к ресурсам защищенной системы удаленного финансового документооборота (далее – СУФД) с компьютеров, не входящих в защищаемый сегмент сети. На этих компьютерах устанавливается «Континент-АП», который для передачи данных соединяется с компьютером – сервером доступа, проверяющим полномочия на доступ и разрешающим доступ к ресурсам защищенной сети СУФД.

Для взаимодействия «Континент-АП» и сервера доступа используются следующие сертификаты:

- сертификат пользователя – для аутентификации пользователя на сервер доступа;
- сертификат сервера доступа – для аутентификации сервера доступа;
- сертификат корневого центра сертификации – для подтверждения подлинности сертификатов пользователя и сервера доступа.

«Континент-АП» устанавливается в соответствии с одним из трех вариантов, обеспечивающим необходимый уровень безопасности:

- низкий – соответствует классу КС1;
- средний – соответствует классу КС2;
- высокий – соответствует классу КС3.

### **Что необходимо иметь**

Перед тем как начать работу с ресурсами защищенной сети СУФД:

- необходимо иметь установочный комплект «Континент АП»;
- перед установкой Абонентского пункта необходимо убедиться, что на компьютере установлен криптопровайдер «КриптоПро CSP» версии 4.0 или другой версии, имеющей действующий сертификат соответствия, выданный Федеральной службой безопасности Российской Федерации.

### **Что нужно сделать**

1. установите «Континент-АП»;
2. получите сертификаты, необходимые для работы. Для получения сертификата пользователя потребуется создать файл запроса и предоставить его вместе с бумажной формой запроса в УФК по Алтайскому краю (или Отделение УФК по Алтайскому краю);
3. зарегистрируйте полученные сертификаты;
4. установите соединение с сервером доступа;
5. проверьте связь с сервером СУФД Федерального казначейства.

Если пробное соединение с сервером установлено успешно и подключение к СУФД возможно, значит, все подготовительные действия выполнены правильно. С этого момента «Континент-АП» готово к работе.

Если вы уже являетесь обладателями действующих сертификатов абонентского пункта, перед установкой «Континент-АП» необходимо обеспечить сохранность этих **сертификатов** и соответствующих им **закрытых ключей** на съемном USB Flash-накопителе.

## **2. Установка «Континент-АП»**

1. Войдите в систему с правами администратора компьютера.
2. Завершите работу всех приложений выполняемых на компьютере.
3. Запустите на исполнение файл «**ts\_setup.exe**», находящийся в каталоге «setup» дистрибутива «Континент-АП». Программа установки начнет выполнять подготовительные действия, и на экране появится сообщение об этом. После завершения подготовительных действий на экране будет выведен стартовый диалог мастера установки.

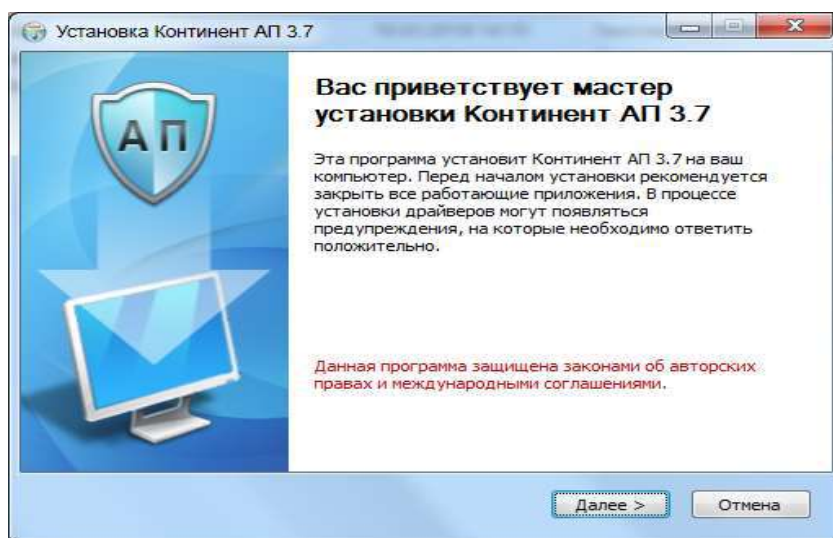


Рис. 1. Стартовый диалог мастера установки.

4. Нажмите кнопку «Далее >» для продолжения установки. На экране появится диалог, содержащий лицензионное соглашение на использование программного продукта.

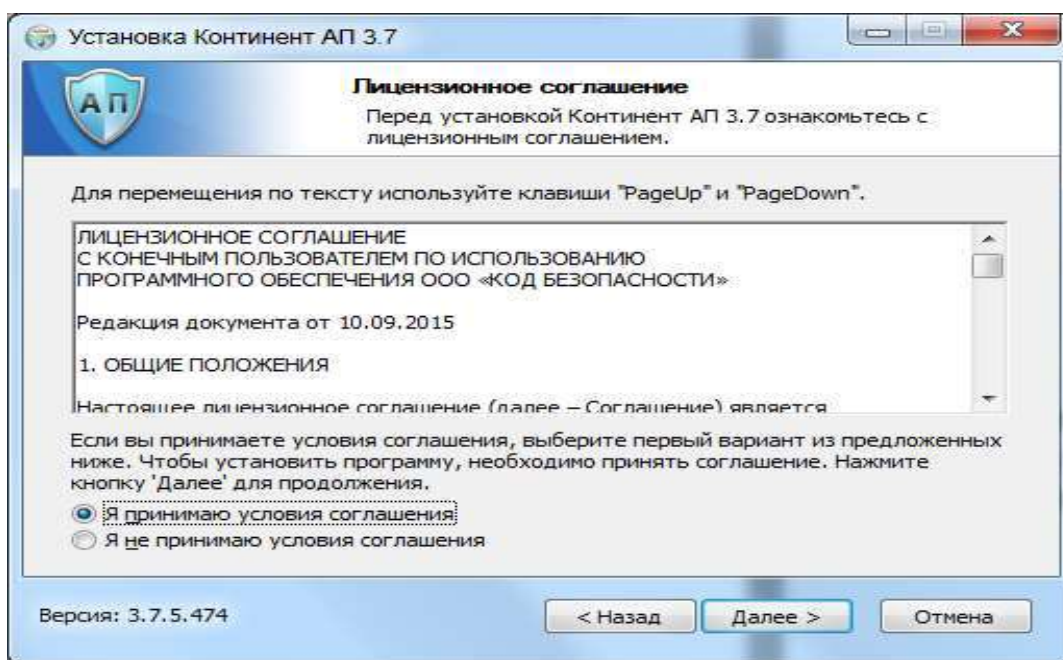


Рис. 2. Принятие лицензионного соглашения

5. Прочтите лицензионное соглашение, и, если вы принимаете его условия, поставьте отметку в поле «Я принимаю условия лицензионного соглашения» и нажмите кнопку «Далее >».

6. На экране появится список устанавливаемых компонентов программы.

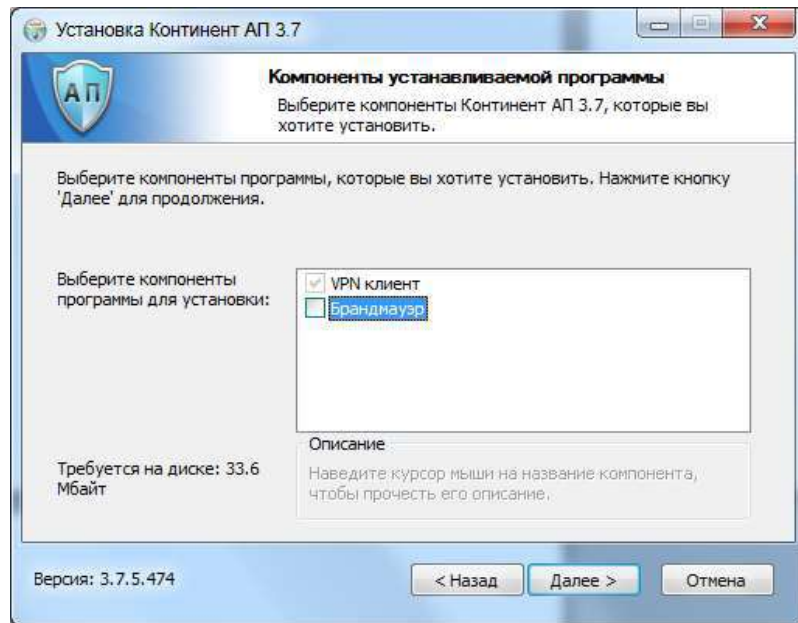


Рис.3. Список устанавливаемых компонентов

Необходимо снять галочку с компонента «Брандмауэр» и нажать кнопку «Далее >>».

7. На экране появится папка установки «Континент-АП».

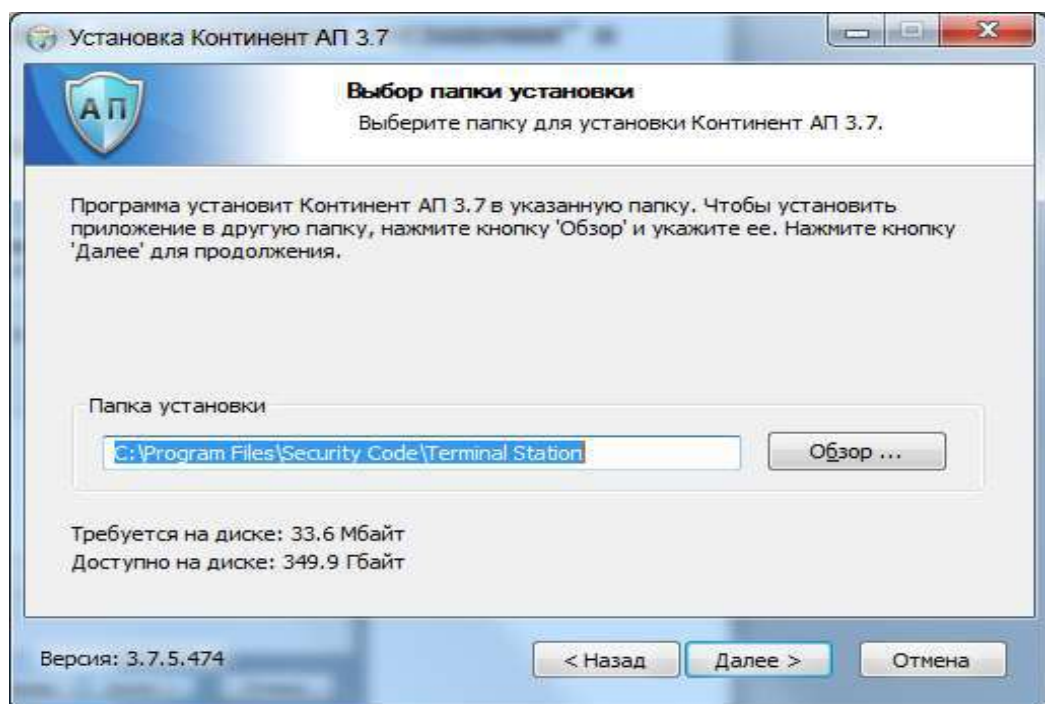


Рис. 4. Путь установки

Выберите папку установки и нажмите кнопку «Далее >>».

8. На экране появится диалоговое окно ввода имени RAS соединения, адреса сервера доступа и выбора уровня безопасности.

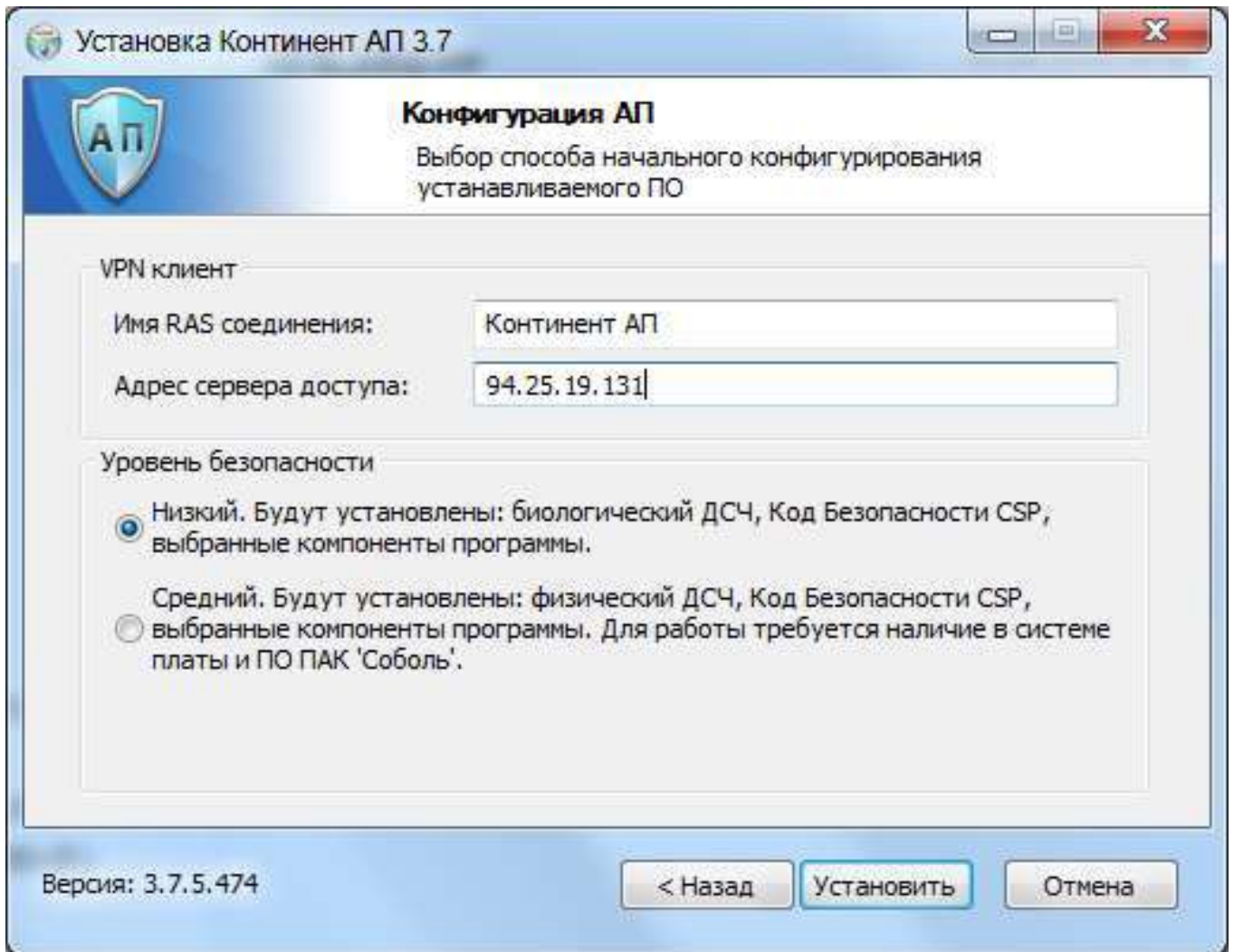


Рис. 5. Ввод параметров соединения и установки

Введите название сетевого подключения для континента в поле «имя RAS соединения» (например – «Континент АП»).

Введите адрес сервера доступа – **94.25.19.131** (адрес основного сервера доступа), также можно воспользоваться адресом – **94.25.19.132** (адрес резервного сервера доступа).

Выберите уровень безопасности. **Низкий уровень** – при отсутствии программно-аппаратного комплекса «Соболь» на используемой рабочей станции. **Средний уровень** – при наличии программно-аппаратного комплекса «Соболь» на используемой рабочей станции.

После задания всех необходимых настроек нажмите кнопку «**Установить**».

После этого начнется процесс установки «Континент-АП».



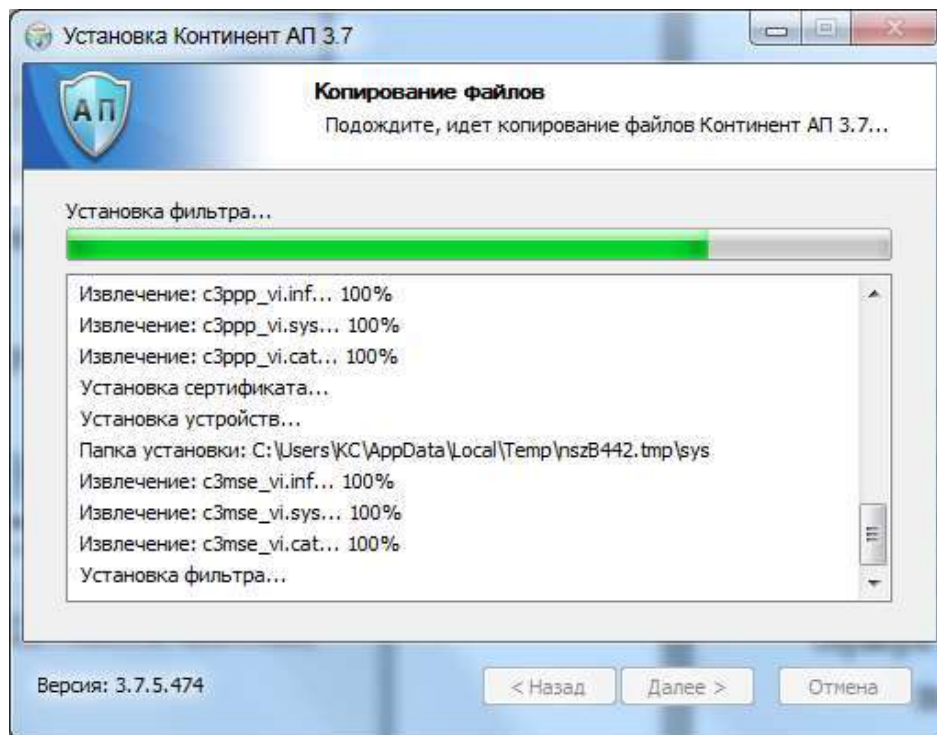


Рис. 6. Процесс установки

После завершения процесса установки нажмите кнопку «Далее >».

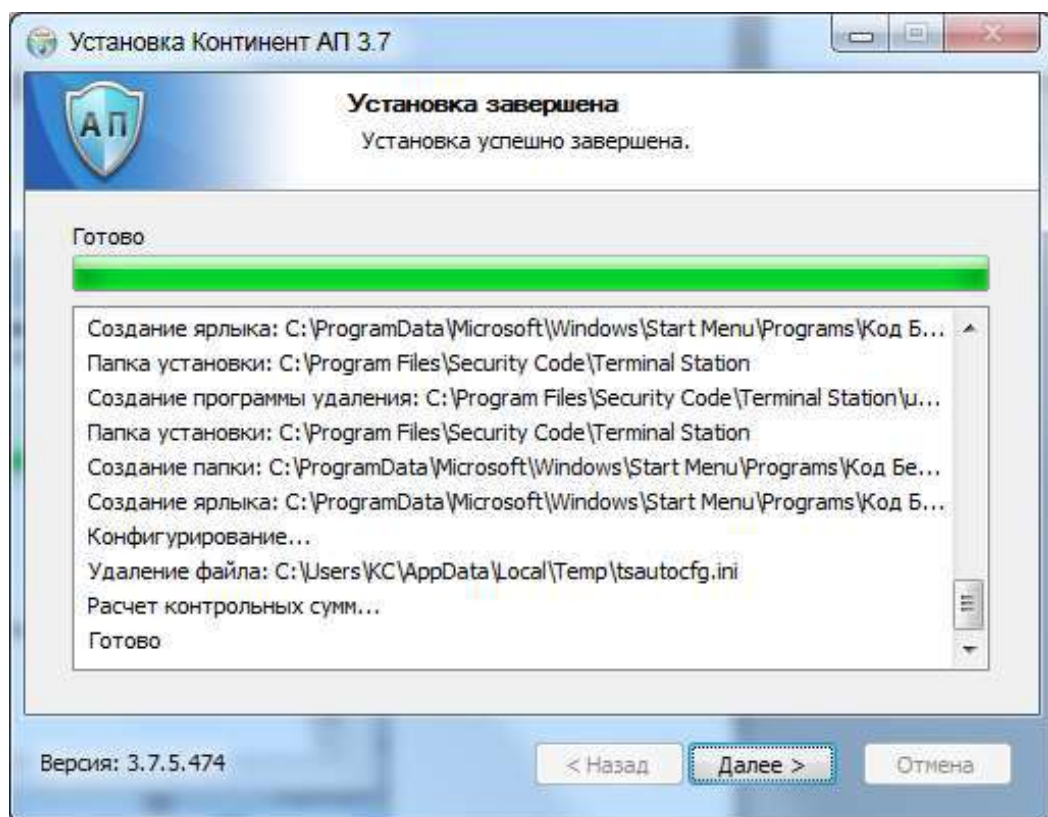


Рис. 7. Завершение установки

В конце программа установки попросит вас перезагрузить компьютер.

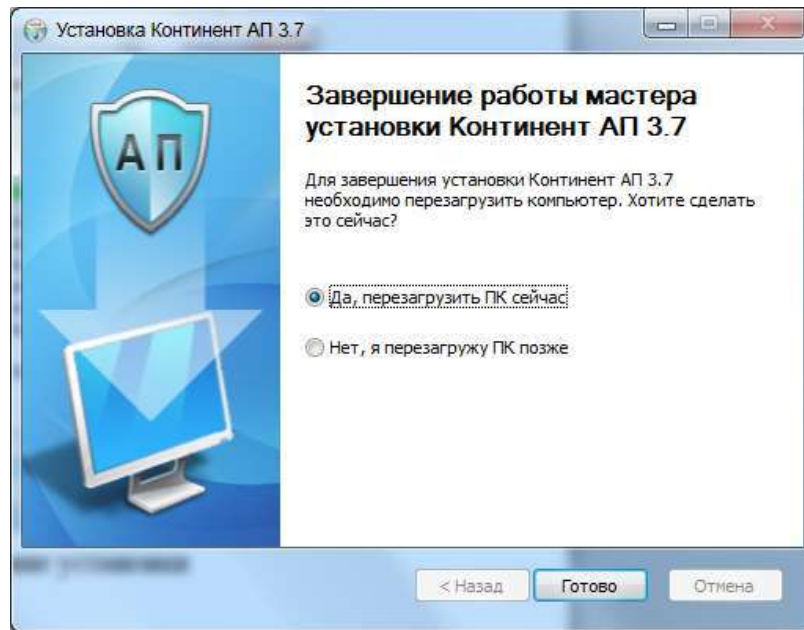


Рис. 8. Завершение работы мастера установки

Нажмите «Да, перезагрузить ПК сейчас» и кнопку «Готово».

На этом процесс установки «Континент-АП» закончен.

9. Для формирования правильной формы заявки на сертификат абонентского пункта, необходимо файл с названием «**request.xml**» (скачивается с сайта [altay.roskazna.ru](http://altay.roskazna.ru) из раздела *ГИС/Удостоверяющий центр/Доступ через Континент АП (для СУФД)/Организация защищённого канала для обмена данными в СУФД пункта 2. бумажную форму запроса....*), копировать с заменой в папку расположения (установки) «Континент-АП» (например: «C:\Program Files\Security Code\Terminal Station\vpn») (путь может отличаться, в зависимости от версии операционной системы). **Операция копирования производится под пользователем, обладающим правами администратора.**

### 3. Создание сертификата пользователя

#### 3.1. Генерация закрытого ключа, формирование запроса и заявки на издание сертификата ключа абонентского пункта

Запрос на получение сертификата создается пользователем с использованием «Континент-АП». Одновременно с запросом средствами криптопровайдера «КриптоПро CSP» генерируется закрытый ключ пользователя. Запрос в виде файла



сохраняется в указанную пользователем папку, ключевой контейнер с закрытым ключом сохраняется на USB Flash-накопитель.

Для создания запроса необходимо:

1) Вызовите контекстное меню пиктограммы VPN-клиент, расположенной на панели задач Windows, в правом нижнем углу (рядом с языковой панелью).



2) В меню «Сертификаты» активируйте команду «Создать запрос на пользовательский сертификат...».

На экране появится диалоговое окно для создания запроса.

Владелец сертификата

Код ТОФК, в который Обращается пользователь

Последние 5 символов лицевого счета в Казначействе

Населенный пункт

Корректный адрес электронной почты

Место сохранения запроса

Место сохранения Бумажной заявки

Только КриптоПро

Имя контейнера, пригодится при создании связки: контейнер-сертификат

Обязательно для сервера доступа

Открыть все параметр

Рис. 9. Окно создания закрытого ключа и запроса на сертификат  
**ВСЕ ПОЛЯ ОБЯЗАТЕЛЬНЫ ДЛЯ ЗАПОЛНЕНИЯ!!!!!!!!!!!!!!!!!!!!!!**

3) Отметьте галочкой поле рядом с надписью «Бумажная форма». В полях «Электронная форма» и «Бумажная форма» укажите путь для сохранения файла запроса и файла заявки на сертификат.

Нажмите кнопку «ОК».

4) На экране появится диалог «КриптоПро CSP» с перечнем тех ключевых носителей, на которых может быть сохранена ключевая информация.

Список устройств для записи ключевого контейнера (зависит от настроек «КриптоПро CSP»)

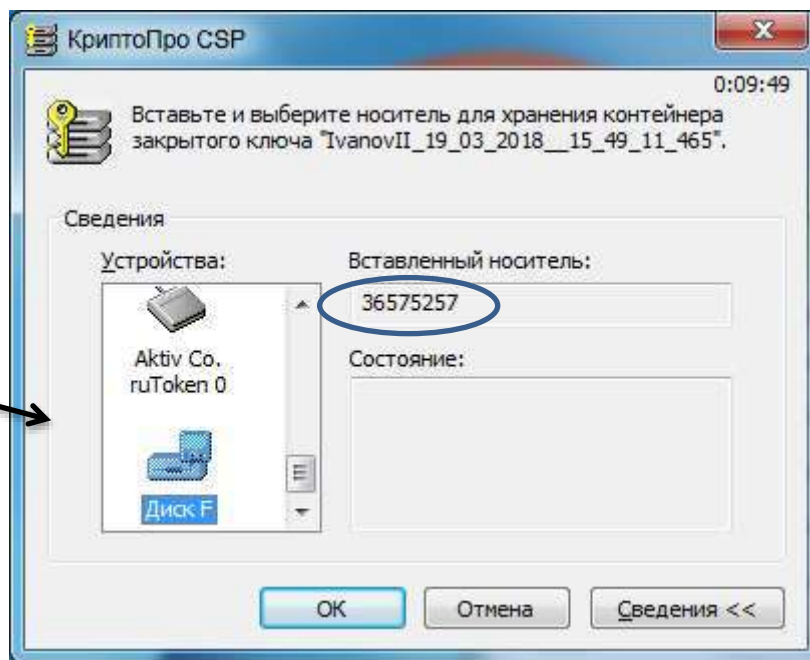


Рис. 10. Окно выбора ключевого носителя для контейнера

Выберите необходимый ключевой носитель. Если носитель распознал, то поле «Вставленный носитель» автоматически заполнится.

Нажмите кнопку «ОК».

5) В зависимости от установленных в «КриптоПро CSP» датчиков случайных чисел (Биологический ДСЧ – Если используется «КриптоПро CSP» KC1, Физический ДСЧ – Если используется «КриптоПро CSP» KC2) процесс генерации закрытого ключа немного различается. Если установлен «Физический ДСЧ» - «КриптоПро CSP» автоматически сгенерирует последовательность для закрытого ключа, а если – «Биологический ДСЧ», то «КриптоПро CSP» откроет диалоговое окно и попросит перемещать указатель мыши и нажимать различные клавиши для накопления энтропии.

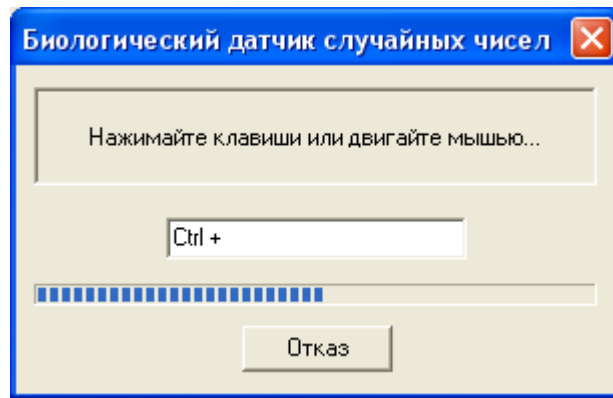


Рис. 11. Для «Биологического ДСЧ»

После успешного создания ключей и записи закрытого ключа на ключевой носитель на экране появится диалог для назначения пароля доступа к ключевому контейнеру.

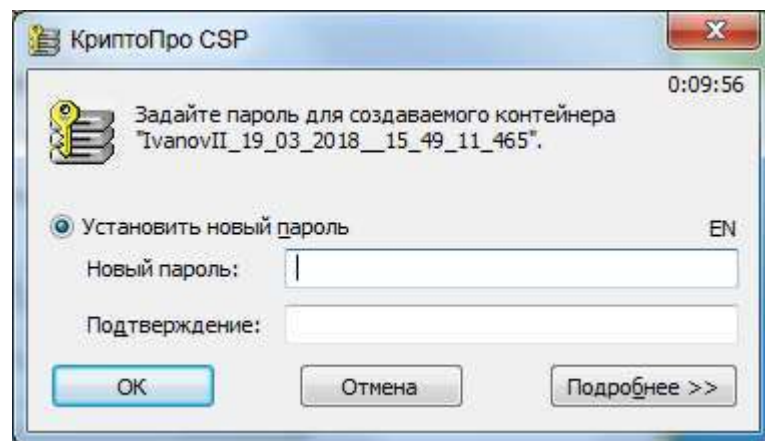


Рис. 12. Ввод пароля для контейнера закрытых ключей

Задайте пароль на доступ к контейнеру закрытых ключей, подтвердите его и нажмите кнопку «ОК».

МОЖНО ЗАДАТЬ ПУСТОЙ ПАРОЛЬ, для этого можно просто нажать кнопку «ОК».

б) На экране появится сообщение о завершении создания запроса.

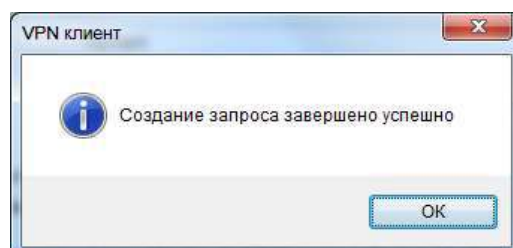


Рис. 13. Завершение создания контейнера закрытых ключей

7) Нажмите кнопку «ОК» в окне сообщения.

**Изготовленный ключевой контейнер подлежит учету в соответствии с «Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», введенной в действие приказом ФАПСИ от 13 июня 2001 г. № 152.**

Распечатайте, заполните и подпишите бумажную форму запроса.

***В бумажной форме запроса необходимо заполнить следующие поля:***

1. в поле «В связи с» заполняется причина получения сертификата («предоставление права использования СКЗИ Континент АП», «плановая смена», «порча ключевого носителя», «изменение реквизитов владельца сертификата» или др.);

2. в поле «Приказом по организации» заполняется название приказа, на основании которого пользователю предоставлены права на эксплуатацию «Континент-АП», а также его дата и номер;

3. в поле «Владелец ключей абонентского пункта, сформировавший запрос» проставляется подпись владельца контейнера закрытых ключей, соответствующих предоставленному запросу на сертификат абонентского пункта, содержащего значение открытого ключа, ниже проставляется дата создания запроса;

4. в поле «Руководитель» заполняется наименование организации, ниже подпись и расшифровка подписи руководителя организации, ниже дата подписания заявки;

5. в поле «МП» ставится печать организации.

Передается в адрес УФК по Алтайскому краю (Отделения УФК по Алтайскому краю) следующие документы:

**1) req-файл на съемном носителе**, сгенерированный в соответствии с разделом 3.1. Генерация закрытого ключа, формирование запроса и заявки на издание сертификата ключа абонентского пункта;

2) заполненную и подписанную бумажную форму запроса на сертификат «Континент-АП», заполненную в соответствии с пунктом – «В бумажной форме запроса необходимо заполнить следующие поля», находящимся выше по тексту;

3) заверенную копию приказа «О назначении пользователей ответственных за эксплуатацию средств криптографической защиты» (Название может быть другое), в котором обязательно должно быть определено, что Владелец контейнера закрытых ключей допущен (предоставлены полномочия) к эксплуатации «Континент-АП»;


4) доверенность на право действия от имени Владельца сертификата (ЕСЛИ сертификат получается уполномоченным лицом).

### 3.2. Установка сертификата

Пользователь «Континент-АП» получает от УФК по Алтайскому краю (или Отделение УФК по Алтайскому краю) сертификат пользователя и сертификат корневого центра сертификации. Эти сертификаты необходимо зарегистрировать в хранилище сертификатов на компьютере, на котором установлен «Континент-АП».

*Перед тем, как приступить к регистрации сертификатов, **предъявите ключевой носитель (USB Flash-накопитель) с закрытым ключом регистрируемого сертификата пользователя.***

Для регистрации сертификатов:

1) Вызовите контекстное меню пиктограммы VPN-клиент,  расположенной на панели задач Windows, в правом нижнем углу (рядом с языковой панелью).

2) В меню «Сертификаты» активируйте команду «Установить сертификат пользователя».

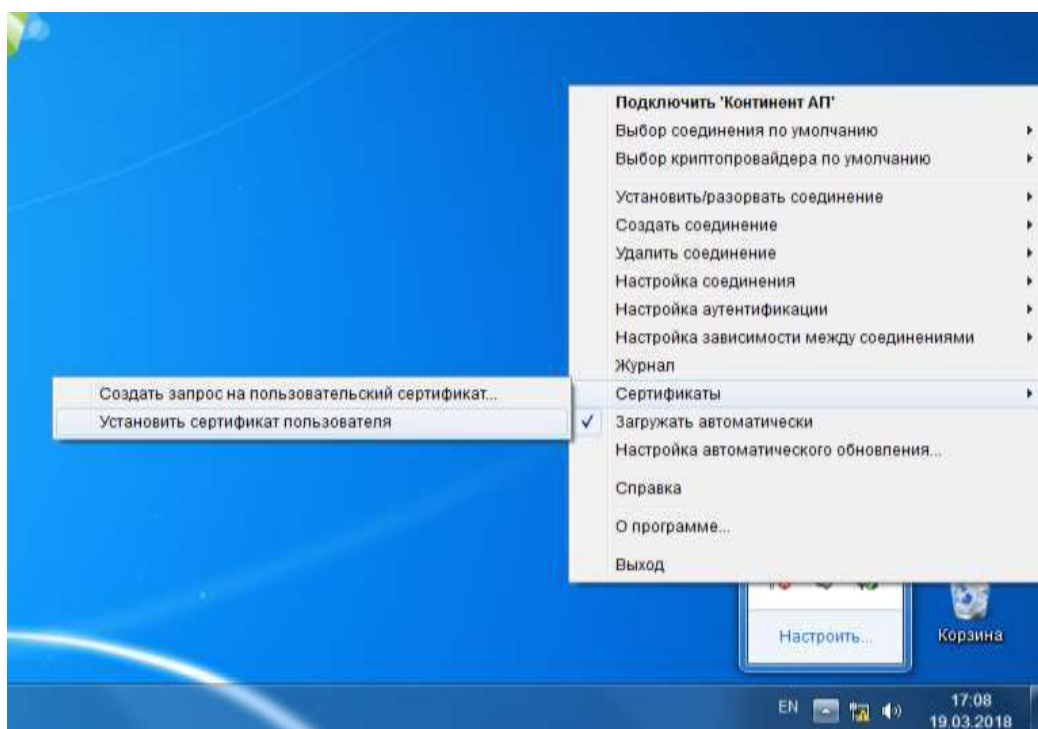


Рис. 14. Открытие окна для установки сертификата пользователя

На экране появится стандартное диалоговое окно Windows для работы с файлами.

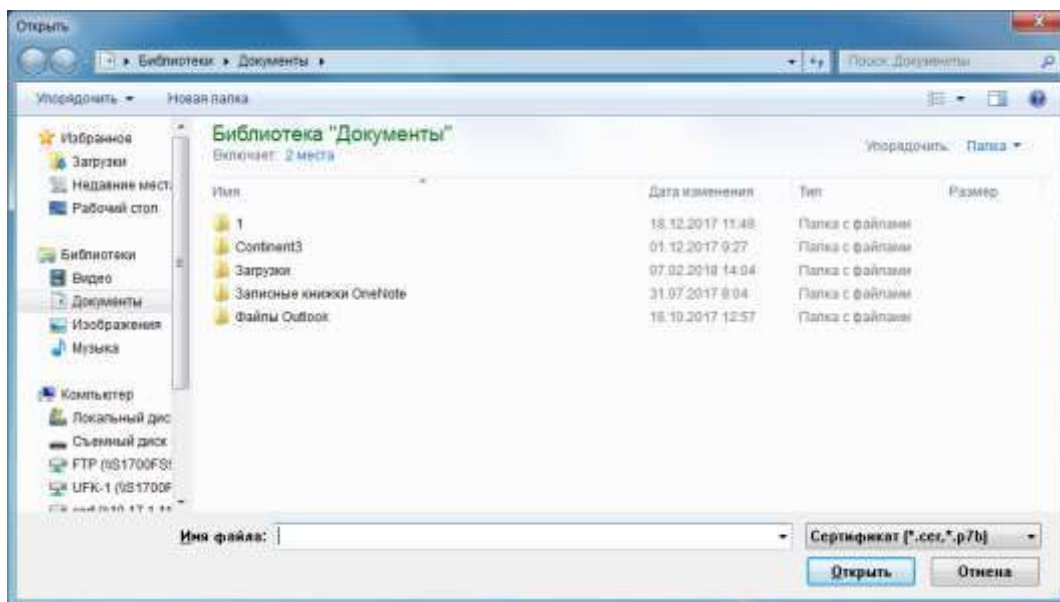


Рис. 15. Окно выбора сертификата

3. Выберите файл сертификата пользователя (имя файла по умолчанию – user.cer) и нажмите кнопку «Открыть» (файл находится на USB Flash-накопителе).

На экране появится диалог выбора ключевого контейнера для чтения закрытого ключа сертификата пользователя.



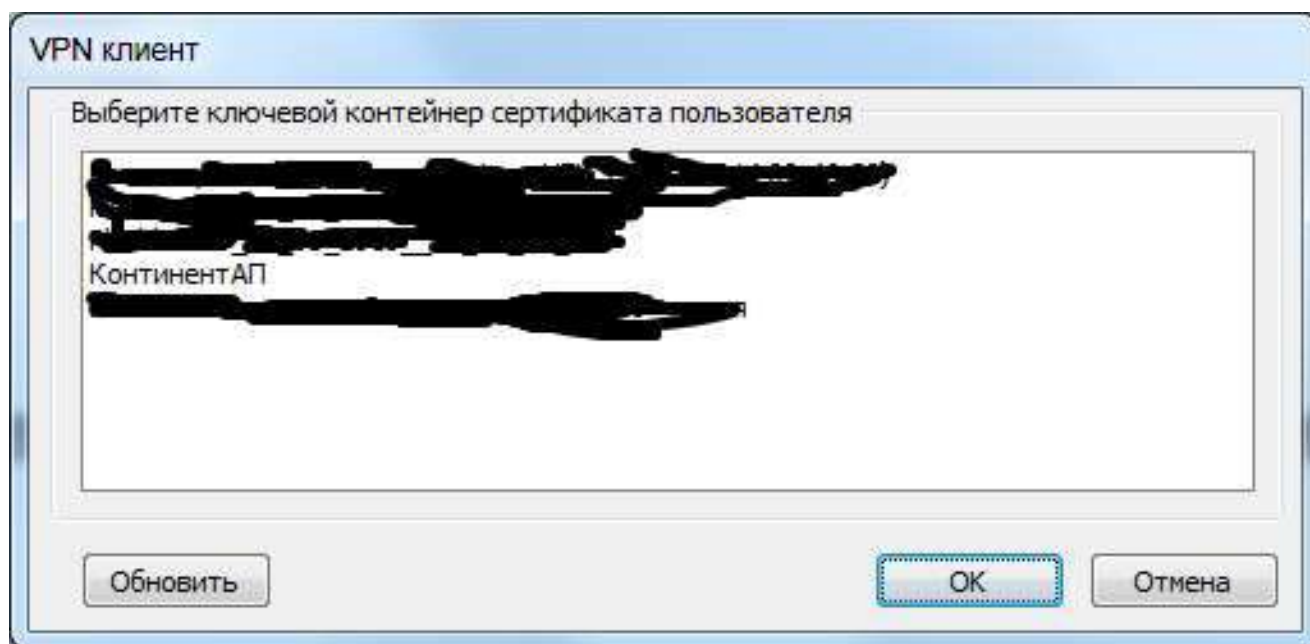


Рис. 16. Окно выбора контейнера закрытых ключей

4. Выберите нужный ключевой контейнер и нажмите «OK».

5. Если на контейнер закрытых ключей был установлен пароль, то «КриптоПро CSP» попросит ввести пароль от выбранного контейнера.

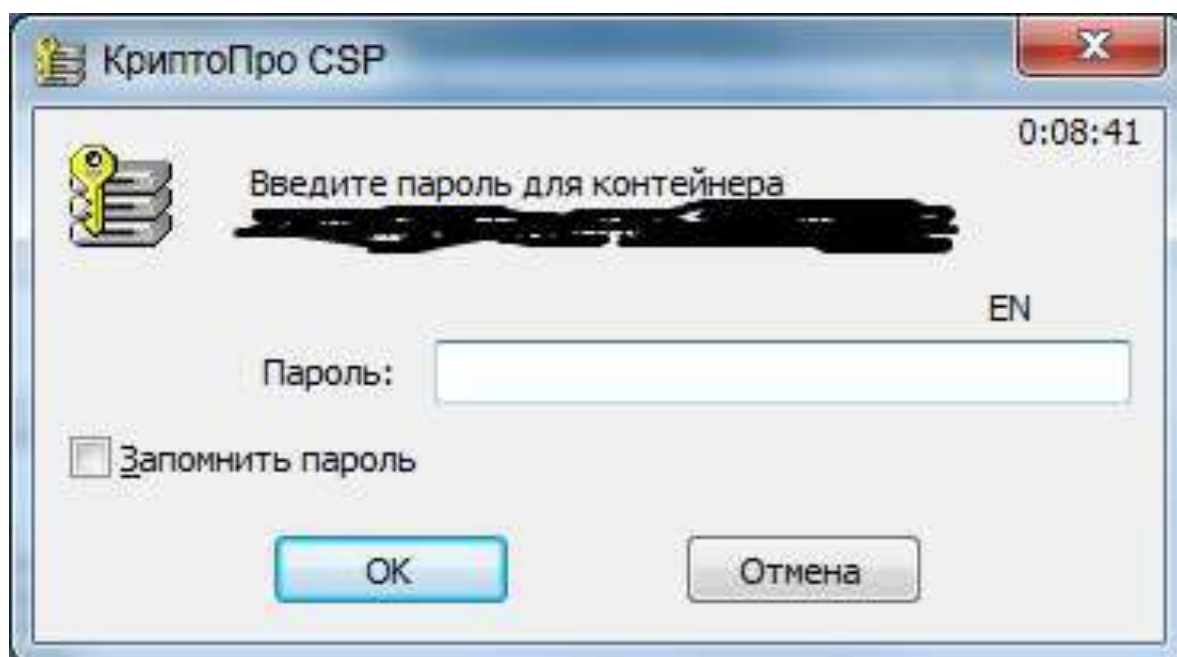


Рис. 17. Окно ввода пароля от контейнера

6. В том случае, если в хранилище сертификатов отсутствует корневой сертификат, подтверждающий данный сертификат пользователя, на экране появится соответствующее сообщение.

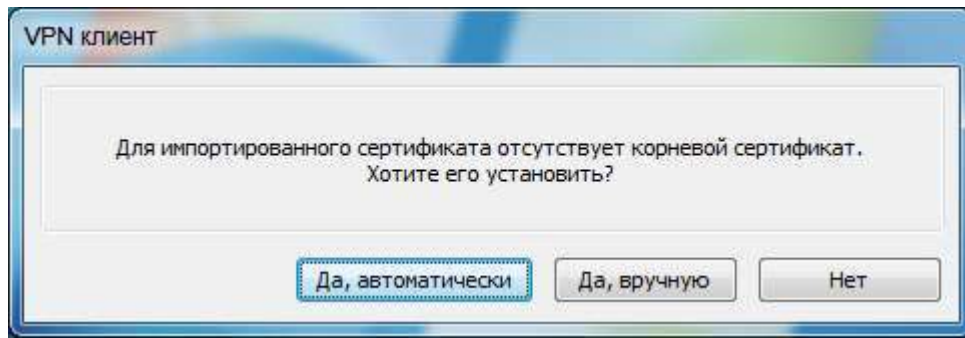


Рис. 18. Сообщение о необходимости установки корневого сертификата

7. Для регистрации корневого сертификата нажмите кнопку «Да, автоматически» - если файл корневого сертификата (root.p7b) лежит в той же папке, что и пользовательский сертификат, или «Да, вручную», если корневой сертификат лежит в другом месте (потребуется в открывшемся окне выбрать корневой сертификат (root.p7b)) в окне сообщения.

*Для того чтобы файл с корневым сертификатом отображался в списке файлов, в поле «Тип файла» в раскрывающемся списке выберите значение «Хранилище PKCS 7(\*.p7b)» - кнопки «Да, вручную».*

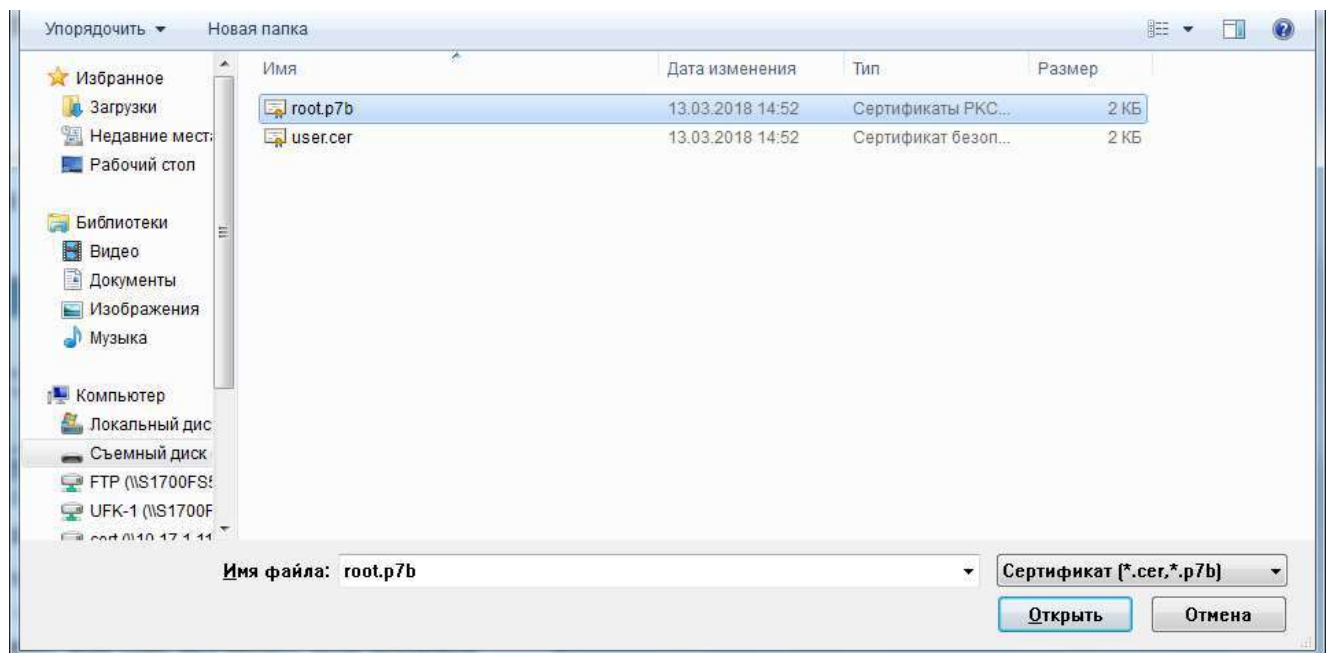


Рис. 19. Выбор корневого сертификата для кнопки «Да, вручную»

Если нажата кнопка «Да, автоматически» Континент-АП сам выберет корневой сертификат. Если нажата кнопка «Да, вручную» выберите корневой сертификат и нажмите кнопку «Открыть».

8. На экране появится сообщение системы безопасности Windows о том, что сейчас будет произведена установка сертификата от центра сертификации (ЦС), в котором описаны последствия данного действия.

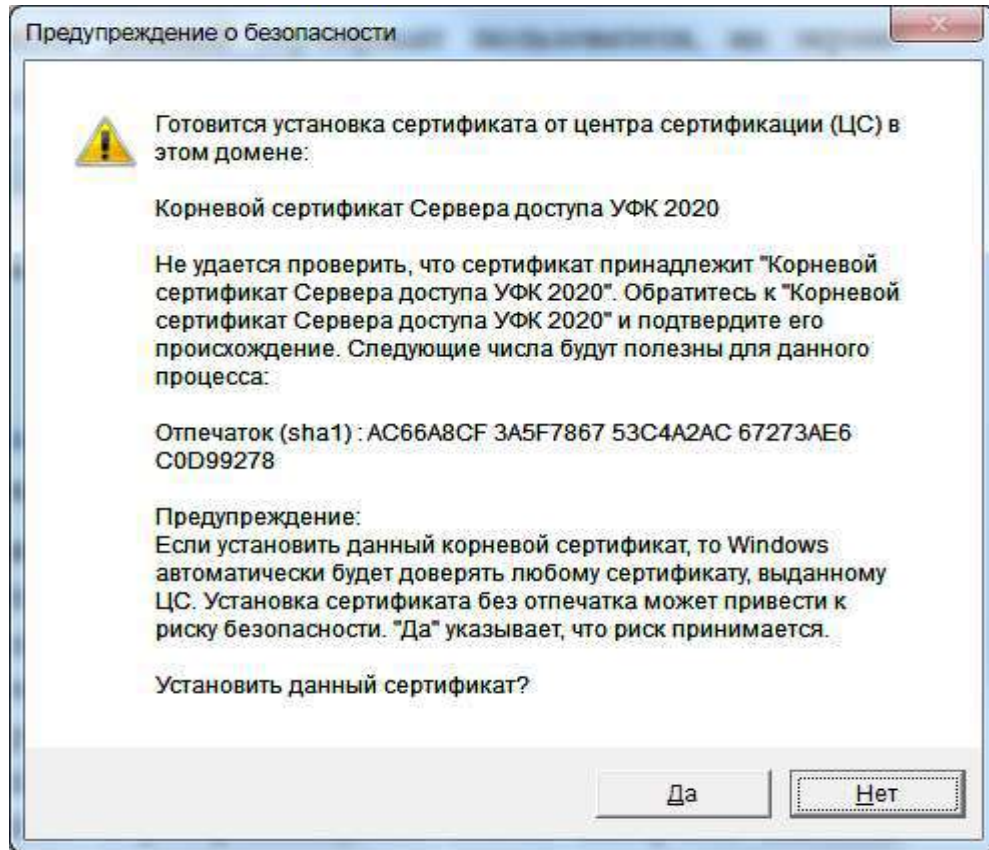


Рис. 20. Предупреждение о безопасности

Нажмите кнопку «Да».

9. После всех произведенных действий «Континент-АП» выдаст сообщение о результате установки пользовательского сертификата.

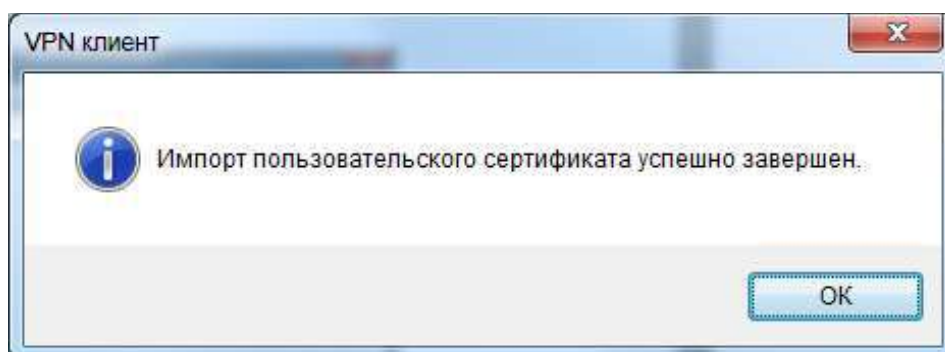


Рис. 21. Сообщение об успешной установке пользовательского сертификата

10. Нажмите кнопку «ОК».

#### 4. Подключение к серверу доступа



1) Вызовите контекстное меню пиктограммы VPN-клиент, расположенной на панели задач Windows, в правом нижнем углу (рядом с языковой панелью).

2) В меню «Установить/разорвать соединение» активируйте команду «Установить соединение Континент АП» (или в меню «Подключить 'Континент АП'»).

3) Выберите сертификат пользователя, который будет использоваться для подключения к серверу доступа.

Для проверки выбранного сертификата воспользуйтесь кнопкой «Свойства».

Нажмите для того, чтобы убедиться в правильном выборе сертификата

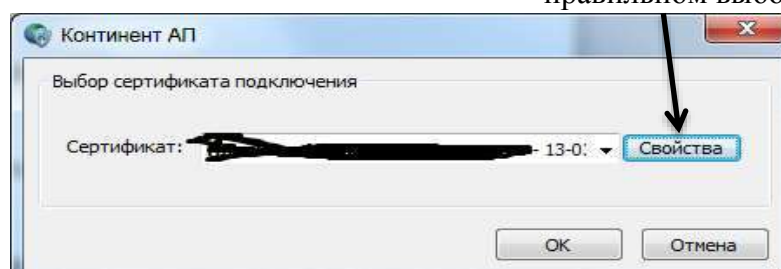


Рис. 22. Окно выбора сертификата пользователя

У сертификата «Континент-АП» поле «Кем выдан» заполнено – «Корневой сертификат Сервера доступа УФК 2020».

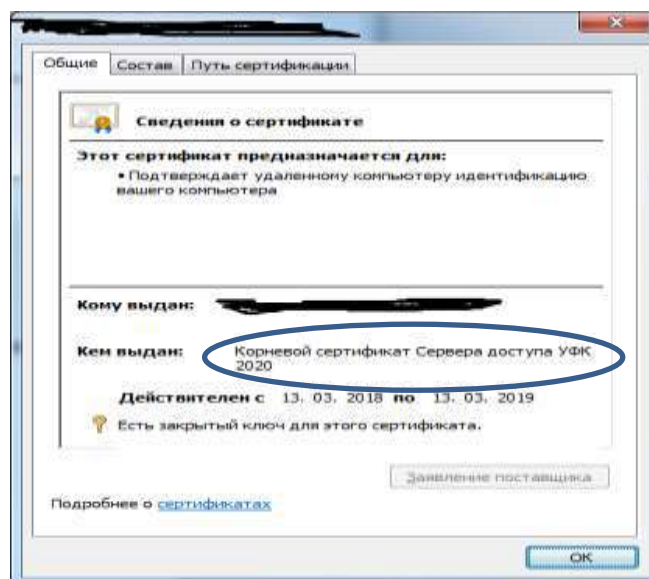


Рис. 23. Сертификат, выданный для «Континент-АП»

Нажмите кнопку «ОК».

4) Введите пароль от контейнера закрытых ключей (если устанавливали), если пароль пустой пропустите этот шаг.

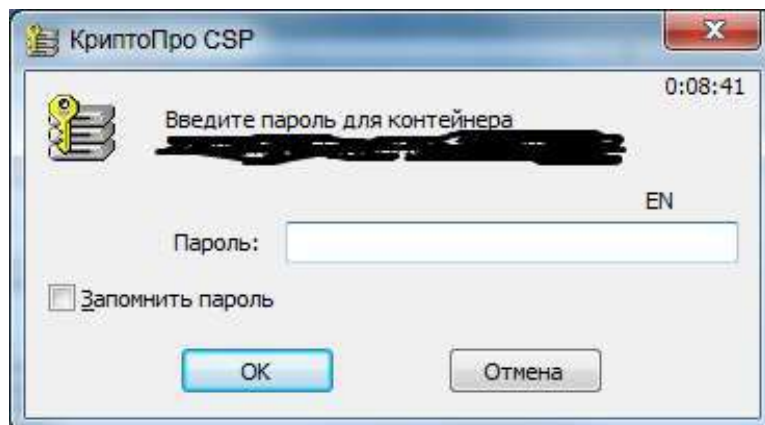


Рис. 23. Окно ввода пароля от контейнера

5) Если подключение производится впервые, то Континент АП выдаст следующее сообщение.

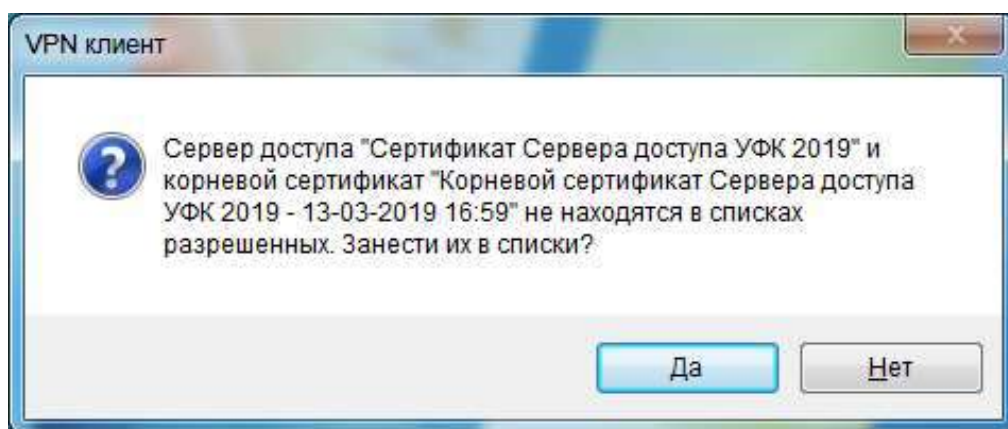


Рис. 24. Разрешение для добавление сертификата Сервера доступа и Корневого сертификата Сервера доступа в списки разрешенных

Нажмите кнопку «Да».

6) Если все действия были выполнены правильно пиктограмма «Континент АП» поменяет свой цвет и будет выглядеть, как показано справа.



После окончания работы в СУФД необходимо разорвать (отключить) активное соединение Континент АП. Для этого необходимо:



- 1) Вызовите контекстное меню пиктограммы VPN-клиент, расположенной на панели задач Windows, в правом нижнем углу (рядом с языковой панелью);
- 2) В меню «Установить/разорвать соединение» активируйте команду «Разорвать соединение Континент АП» (или в меню «Отключить ‘Континент АП’»).