КОМИТЕТ ПО УПРАВЛЕНИЮ ИМУЩЕСТВОМ КУРСКОЙ ОБЛАСТИ

УТВЕРЖДАЮ

Председатель Комитета
по управлению имуществом
Курской области

_____ И.В. Куцак

«05» декабря 2019 г.

М.П.

РЕГЛАМЕНТ ПОДКЛЮЧЕНИЯ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ К РЕГИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ В СФЕРЕ ЗАКУПОК ДЛЯ ОБЕСПЕЧЕНИЯ НУЖД КУРСКОЙ ОБЛАСТИ «ТОРГИ КУРСКОЙ ОБЛАСТИ»

г. Курск – 2019

Оглавление

Принятые термины и определения

АРМ	-	Автоматизированное рабочее место
ЕИС	-	Единая информационная система в сфере закупок
Региональная информационная система в сфере закупок для обеспечения нужд Курской области «Торги Курской области»	-	Автоматизированная информационная система государственных закупок Курской области, программный комплекс, состоящий из баз данных, содержащих информацию, предусмотренную Законом о контрактной системе и принятыми в соответствии с ним правовыми актами, и обеспечивающих ввод, обработку, представление, передачу и размещение в ЕИС информации и документов, предусмотренных Законом № 44-ФЗ
СКЗИ	-	Средство криптографической защиты информации
СЗИ	-	Средство защиты информации
АПКШ	-	Аппаратно-программный комплекс шифрования
Внешние пользователи	-	Внешние пользователи Региональной информационной системы в сфере закупок Курской области
Оператор	-	Комитет по управлению имуществом Курской области
Учреждения	-	Органы, уполномоченные на осуществление функций по размещению заказов для государственных (муниципальных) заказчиков Финансовые органы, координирующие органы, контролирующие органы, поставщики государственного (муниципального) заказа, главные распорядители бюджетных средств, включая их структурные подразделения, государственные (муниципальные) заказчики, получатели бюджетных средств
Регламент	-	Регламент подключения внешних пользователей к Региональной информационной системы в сфере закупок Курской области

Нормативно-правовые ссылки

Настоящий документ разработан в соответствии со следующими нормативно-правовыми актами Российской Федерации (далее – НПА):

– [1] Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– [2] Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– [3] Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Введение

Настоящий документ разработан в соответствии с НПА [1]-[3] и регламентирует порядок подключения внешних пользователей к защищенной сети Региональной информационной системы в сфере закупок для обеспечения нужд Курской области «Торги Курской области».

1. Требования по обеспечению информационной безопасности при подключении внешних пользователей к защищенной сети Региональной информационной системы в сфере закупок для обеспечения нужд Курской области «Торги Курской области»

1.1 Общие положения

В соответствии с НПА [1]-[3], информационное взаимодействие внешних пользователей с защищенной сетью Региональной информационной системы в сфере закупок для обеспечения нужд Курской области «Торги Курской области» (далее – Система) должно осуществляться по защищенному каналу связи.

В целях реализации требований вышеуказанных НПА, подключение к защищенной сети Системы производится с использованием средства криптографической защиты информации, обеспечивающих безопасное информационное взаимодействие внешних пользователей.

1.2 Основные требования

Для реализации защищенного взаимодействия внешних пользователей с Оператором внешние пользователи, подключающиеся к защищенной сети Системы, должны выполнять следующие требования:

- защита от несанкционированного доступа;
- межсетевое экранирование;
- обеспечение антивирусной защиты;
- обеспечение защиты конфиденциальности и целостности передаваемой по каналам связи информации;
- аттестация информационной системы «Региональная информационная система в сфере закупок для обеспечения нужд Курской области «Торги Курской области» Учреждения на соответствие требованиям по обеспечению безопасности информации не ниже чем по 4 уровню защищенности персональных данных.

Оператор использует защищенную сеть на базе АПКШ «Континент». Для защищенного удаленного доступа внешних пользователей к Системе используется СКЗИ «АПКШ «Континент» 3.7. Сервер Доступа». Учитывая особенность используемого оборудования и технологий, возможны две схемы защищенного взаимодействия:

- защищенного взаимодействия № 1
  - установка и настройка на периметре сети Учреждения АПКШ «Континент» для подключения к защищенным ресурсам Системы;
  - установка и настройка на АРМ внешних пользователей сертифицированного ФСТЭК России по требованиям безопасности средств защиты информации:
    - средства антивирусной защиты;
    - средства защиты от несанкционированного доступа.
- Схема защищенного взаимодействия № 2
  - установка и настройка на АРМ внешних пользователей сертифицированного ФСБ России СКЗИ «Континент-АП» для подключения к защищенным ресурсам Системы;
  - установка и настройка на АРМ внешних пользователей сертифицированного ФСТЭК России по требованиям безопасности средств защиты информации:
    - средства антивирусной защиты;
    - средства защиты от несанкционированного доступа;
    - средства межсетевого экранирования.

Обобщенная схема информационного взаимодействия АРМ внешних пользователей и АРМ Учреждений с Системой представлена на рисунке 1, где:

- ✓ 1 вариант отражает схему защищенного взаимодействия № 1;
- ✓ 2 вариант отражает схему защищенного взаимодействия № 2.

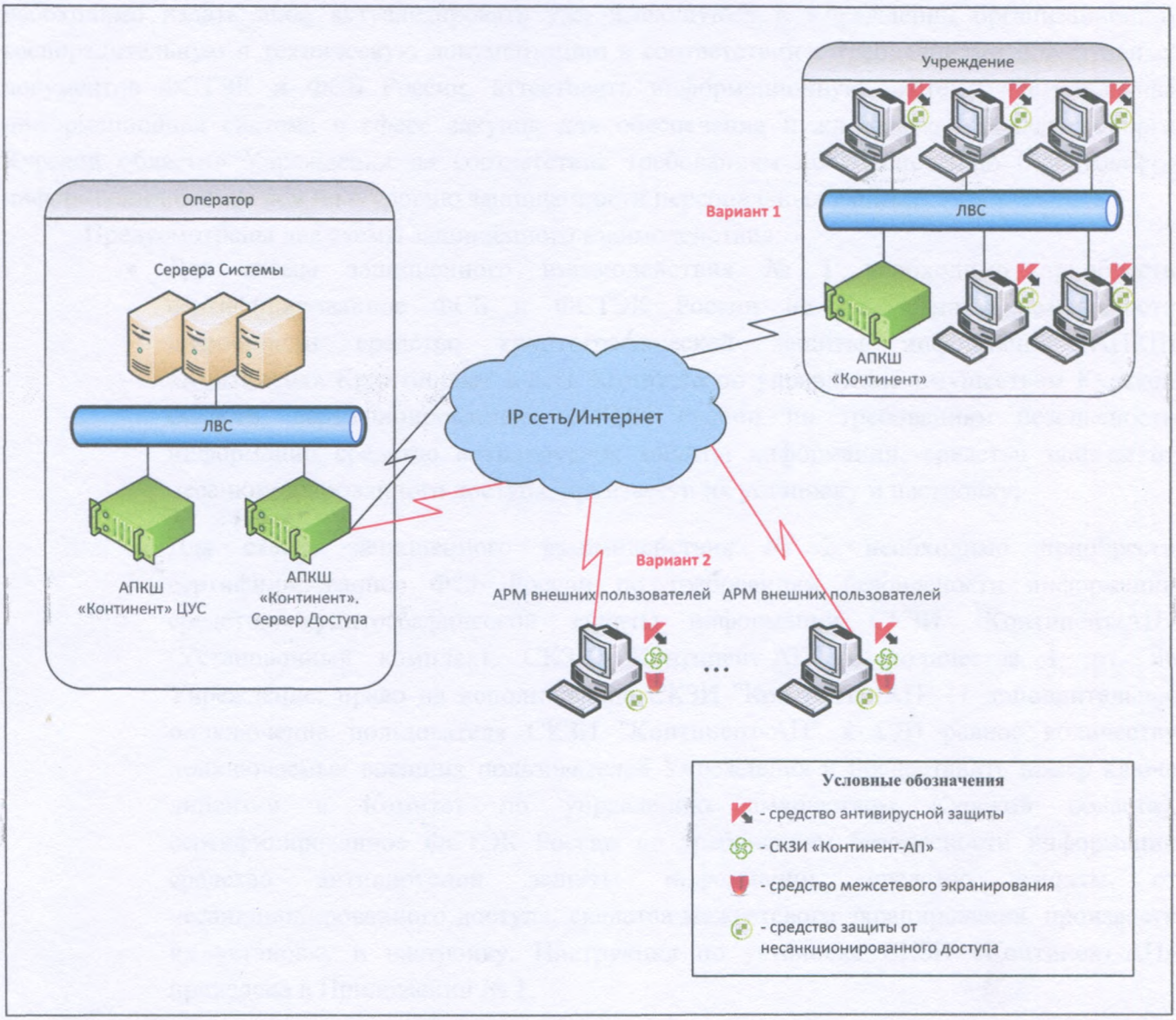

Рисунок 1. Обобщенная схема информационного взаимодействия АРМ внешних пользователей и АРМ Учреждений с Системой

2. Порядок подключения внешних пользователей к защищенной сети Региональной информационной системы в сфере закупок для обеспечения нужд Курской области «Торги Курской области»

Для подключения внешнего пользователя к защищенной сети Системы Учреждению необходимо издать либо актуализировать уже имеющуюся в Учреждении организационно-распорядительную и техническую документацию в соответствии с требованиями нормативных документов ФСТЭК и ФСБ России, аттестовать информационную систему «Региональная информационная система в сфере закупок для обеспечения нужд Курской области «Торги Курской области» Учреждения на соответствие требованиям по обеспечению безопасности информации не ниже чем по 4 уровню защищенности персональных данных.

Предусмотрены две схемы защищенного взаимодействия:

- Для схемы защищенного взаимодействия № 1 необходимо приобрести сертифицированное ФСБ и ФСТЭК России по требованиям безопасности информации средство криптографической защиты информации АПКШ «Континент» Криптошлюз в сеть Комитета по управлению имуществом Курской области, сертифицированное ФСТЭК России по требованиям безопасности информации средство антивирусной защиты информации, средство защиты от несанкционированного доступа, произвести их установку и настройку;

- Для схемы защищенного взаимодействия № 2 необходимо приобрести сертифицированное ФСБ России по требованиям безопасности информации средство криптографической защиты информации СКЗИ «Континент-АП» (Установочный комплект. СКЗИ "Континент-АП" в количестве 1 шт. на Учреждение; право на использование СКЗИ "Континент-АП" (1 дополнительное подключение пользователя СКЗИ "Континент-АП" к СД) равное количеству подключаемых внешних пользователей Учреждения и предоставить номер ключа лицензии в Комитет по управлению имуществом Курской области), сертифицированное ФСТЭК России по требованиям безопасности информации средство антивирусной защиты информации, средство защиты от несанкционированного доступа, средства межсетевого экранирования, произвести их установку и настройку. Инструкция по установке СКЗИ «Континент-АП» приведена в Приложении № 1.

По итогу установки СЗИ составляется и подписывается Акт установки и ввода в эксплуатацию средств защиты информации (средств криптографической защиты информации).

По результатам установки и настройки средств защиты информации, актуализации (оформления) организационно-распорядительной документации в соответствии с требованиями нормативных документов ФСТЭК и ФСБ России, аттестации информационной системы «Региональная информационная система в сфере закупок для обеспечения нужд Курской области «Торги Курской области» Учреждения, Учреждение предоставляет копию аттестата соответствия информационной системы «Региональная информационная система в сфере закупок для обеспечения нужд Курской области «Торги Курской области» Учреждения в Комитет по управлению имуществом Курской области на адрес эл. почты: obl_im@imkursk.ru.

Приложение № 1

Инструкция по установке и настройке средств криптографической защиты информации Континент-АП для подключения к защищенным ресурсам Региональной информационной системы в сфере закупок для обеспечения нужд Курской области «Торги Курской области»

1. Общие положения

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

«Континент-АП» обеспечивает доступ пользователей к ресурсам Региональной информационной системы в сфере закупок для обеспечения нужд Курской области «Торги Курской области» (далее – Система) с компьютеров, не входящих в защищаемый сегмент Системы. На этих компьютерах устанавливается «Континент-АП», который для передачи данных соединяется с СКЗИ «АПКШ «Континент». Сервер Доступа», проверяющим полномочия на доступ и разрешающим доступ к ресурсам защищенной сети Системы.

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 сертификата пользователя.

Установка, настройка и использование СКЗИ Континент-АП подробно описаны в документе «Средство криптографической защиты информации Континент-АП. Руководство администратора». Руководство администратора содержится в комплекте с дистрибутивом на СКЗИ Континент-АП.

Что необходимо иметь

Перед тем как начать работу с ресурсами защищенной сети Системы:

- необходимо иметь сертифицированный 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 Комитет по управлению имуществом Курской области;
3. зарегистрируйте получение сертификаты;
4. установите соединение с сервером доступа;
5. проверьте связь с сервером Системы.

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

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.

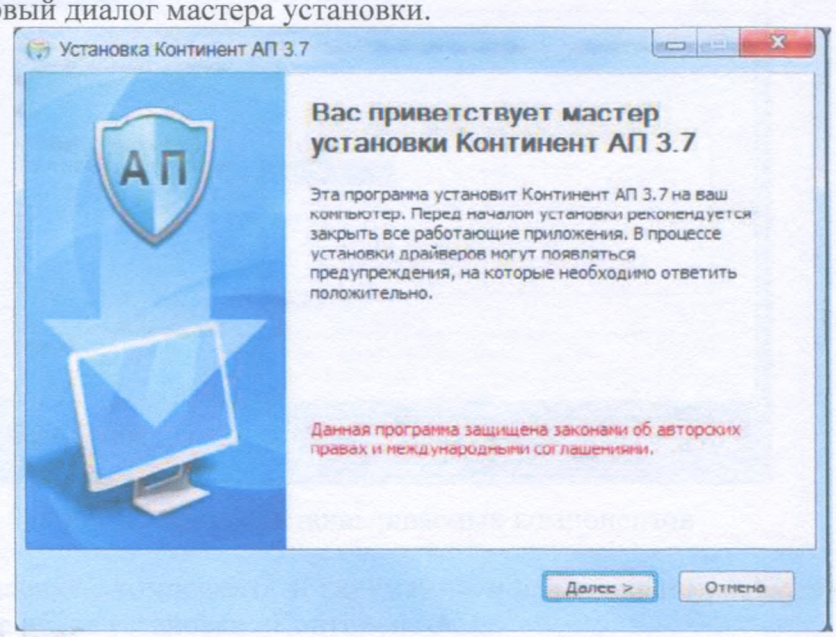

Рис. 1. Стартовый диалог мастера установки

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

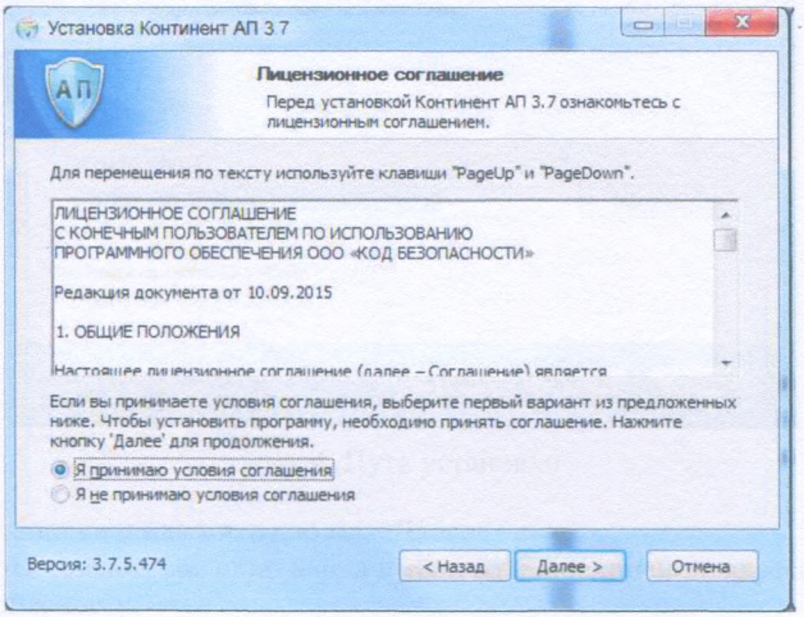

Рис. 2. Принятие лицензионного соглашения

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.

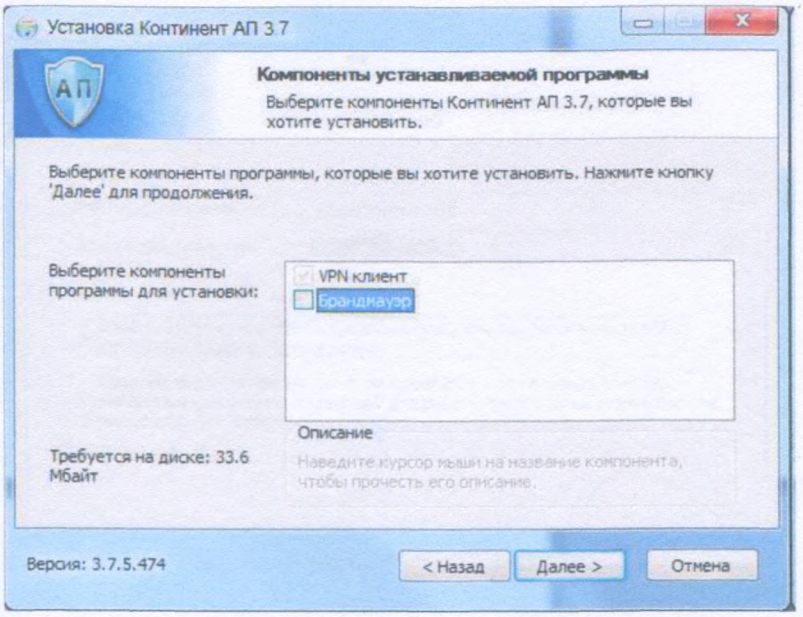

Рис.3. Список устанавливаемых компонентов

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

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

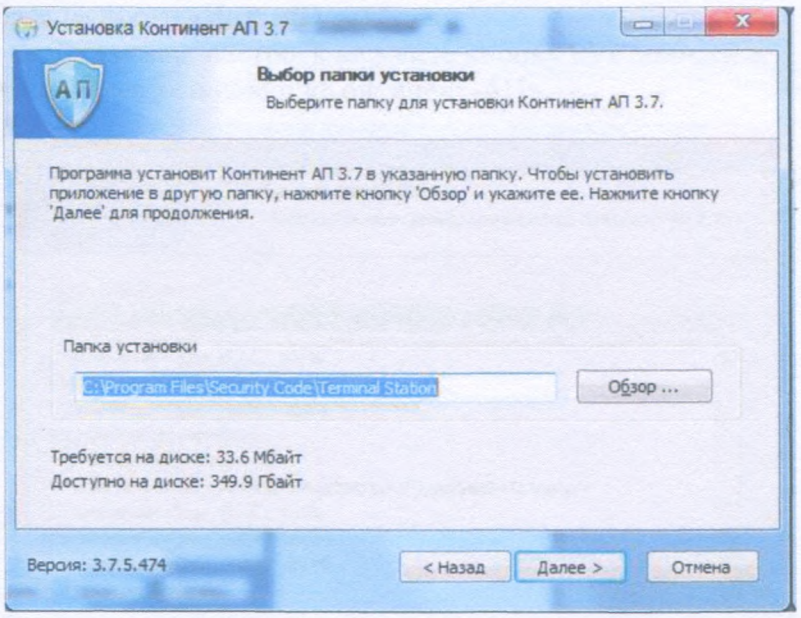

Рис. 4. Путь установки

Выберите папку установки и нажмите кнопку «Далее».

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

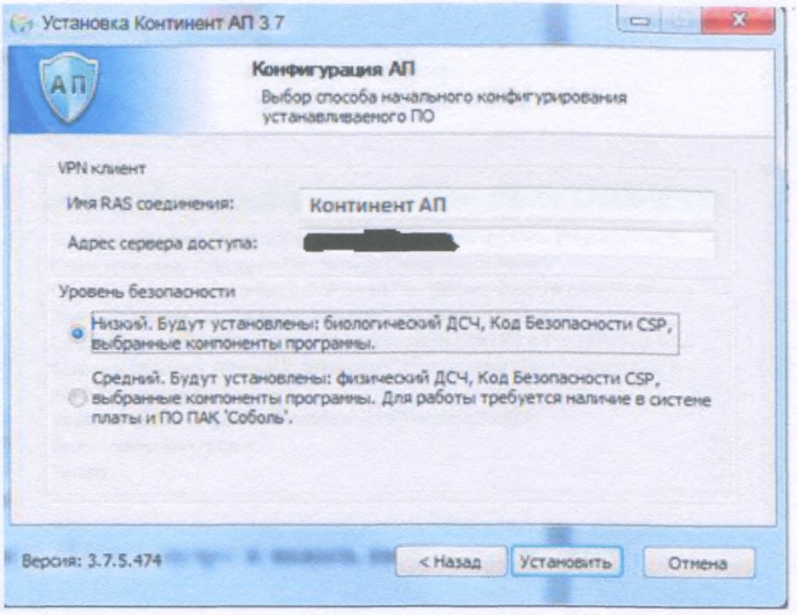

Рис. 5. Ввод параметров соединения и установки

Введите название сетевого подключения для континента в поле «имя RAS соединения».
Введите адрес сервера доступа
Выберите уровень безопасности «Низкий уровень».
После задания всех необходимых настроек нажмите кнопку «Установить».
После этого начнется процесс установки «Континент-АП».

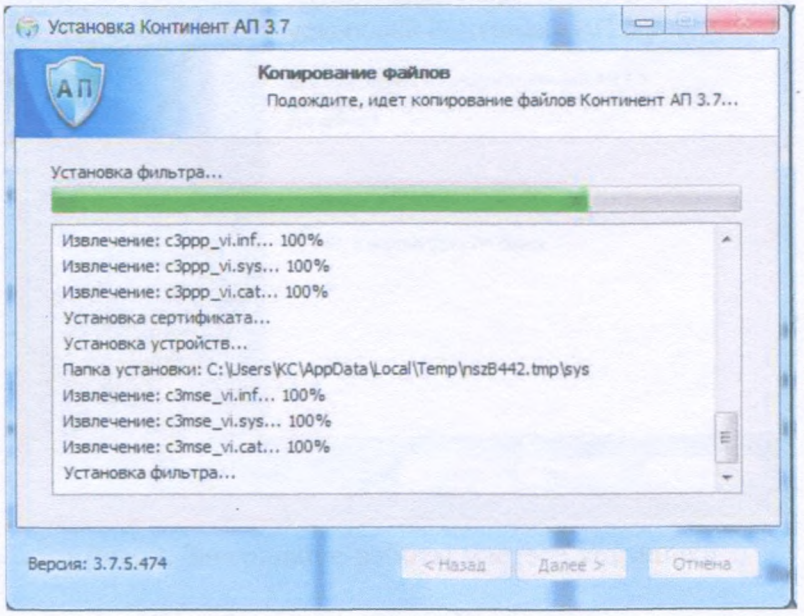

Рис. 6. Процесс установки

После завершения процесса установки нажмите кнопку «Далее».

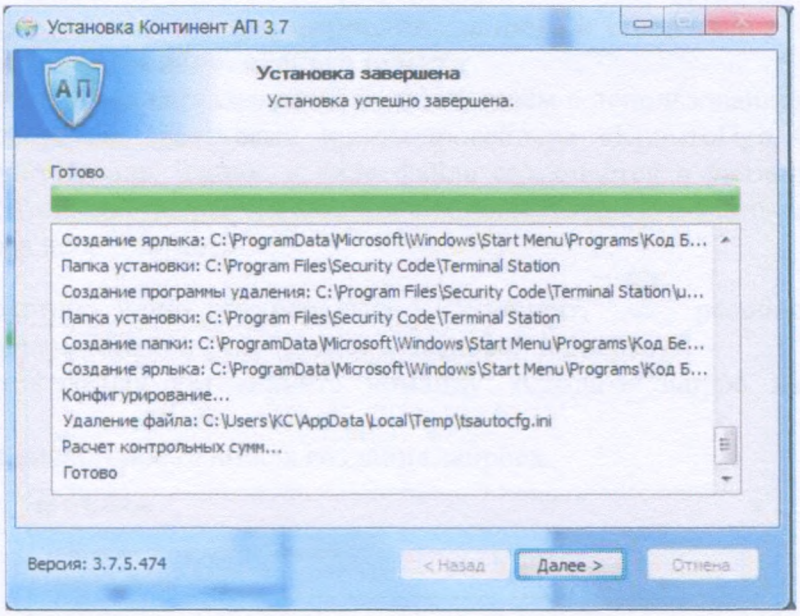

Рис. 7. Завершение установки

В конце программа установки попросит вас перезагрузить компьютер.

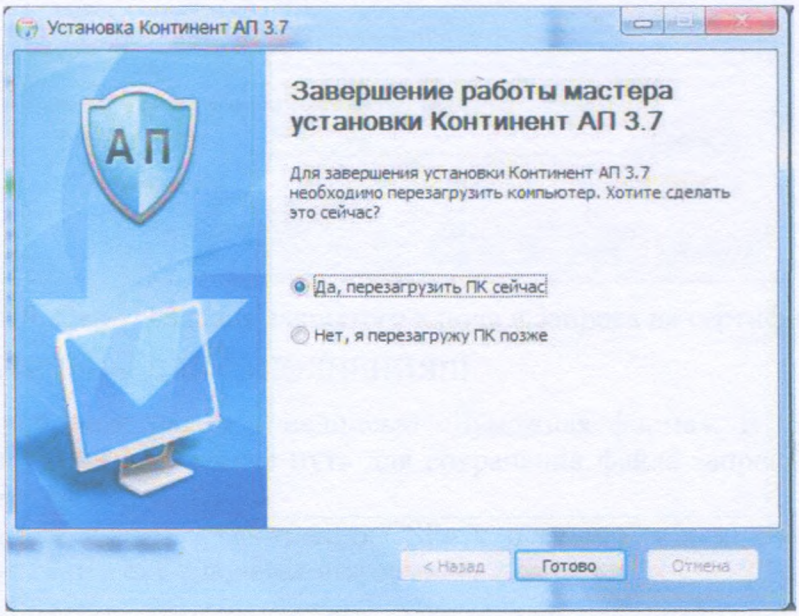

Рис. 8. Завершение работы мастера установки

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.xsl» (предоставляется Оператором Системы), 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.

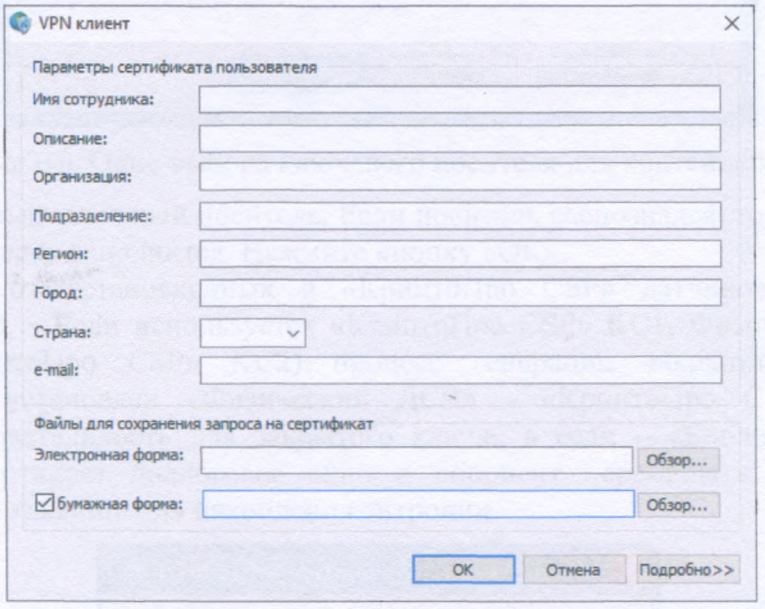

Рис. 9. Окно создания закрытого ключа и запроса на сертификат

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 «OK».

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

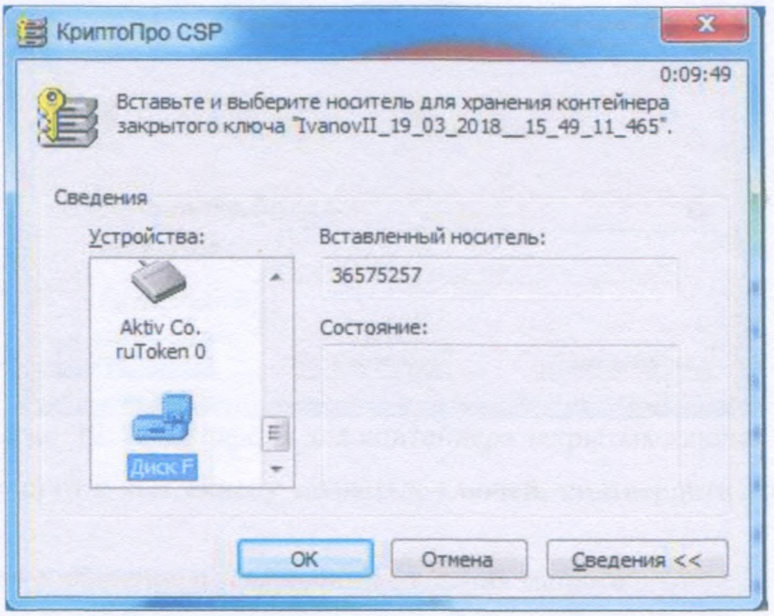

Рис. 10. Окно выбора ключевого носителя для контейнера

Выберите необходимый ключевой носитель. Если носитель распознался, 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» КС1, Физический ДСЧ – Если используется «КриптоПро CSP» КС2) 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.

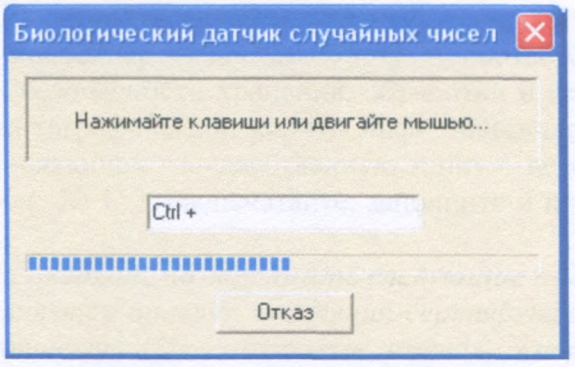

Рис. 11. Для «Биологического ДСЧ»

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

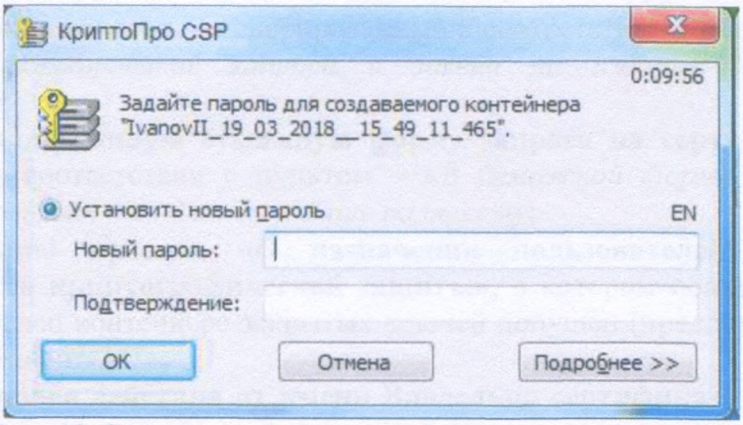

Рис. 12. Ввод пароля для контейнера закрытых ключей

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

6) На экране появится сообщение о завершении создания запроса.

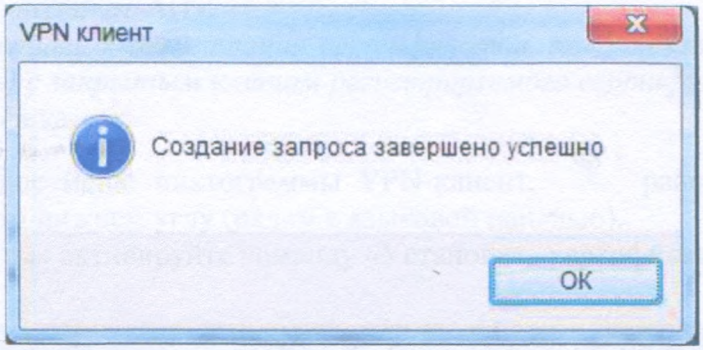

Рис. 13. Завершение создания контейнера закрытых ключей

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» веденной в действие приказом ФАПСИ от 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 Комитета по управлению имуществом Курской области 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», 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 Комитета по управлению имуществом Курской области 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».

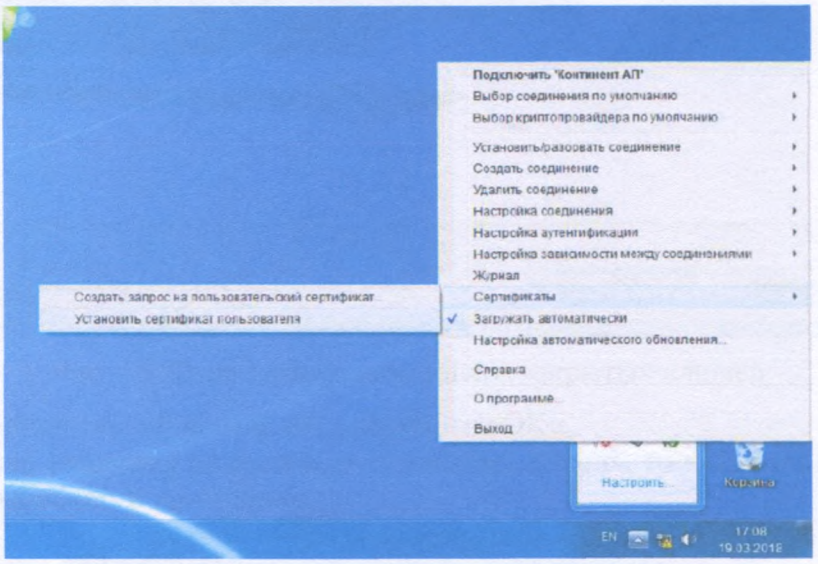

Рис. 14. Открытие окна для установки сертификата пользователя

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

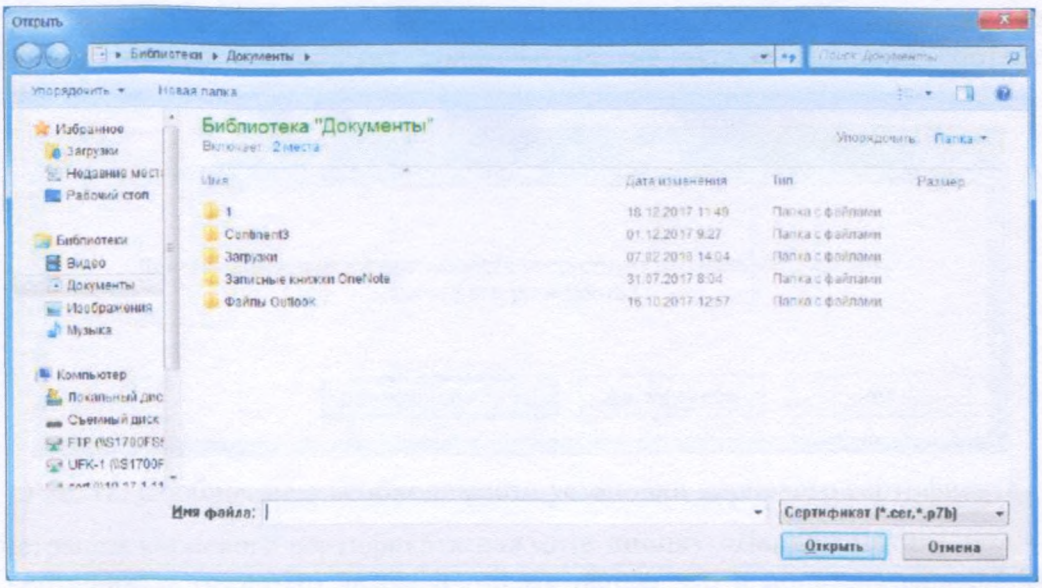

Рис. 15. Окно выбора сертификата

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.

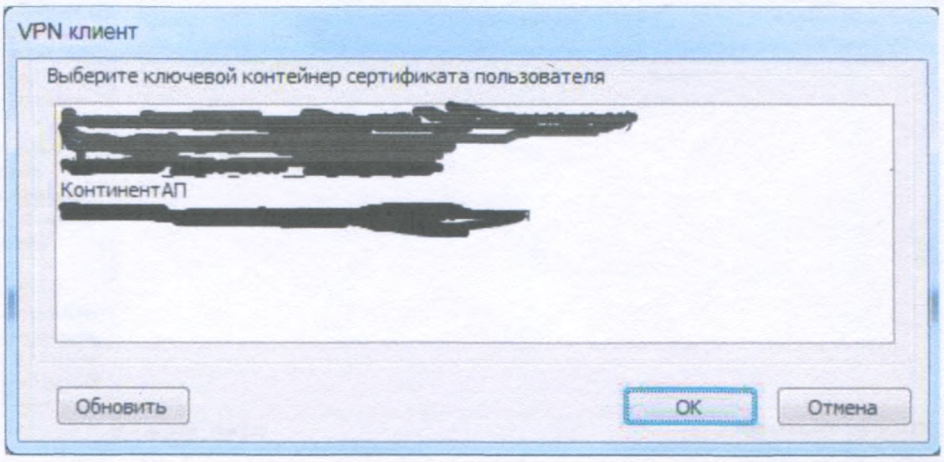

Рис. 16. Окно выбора контейнера закрытых ключей

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.

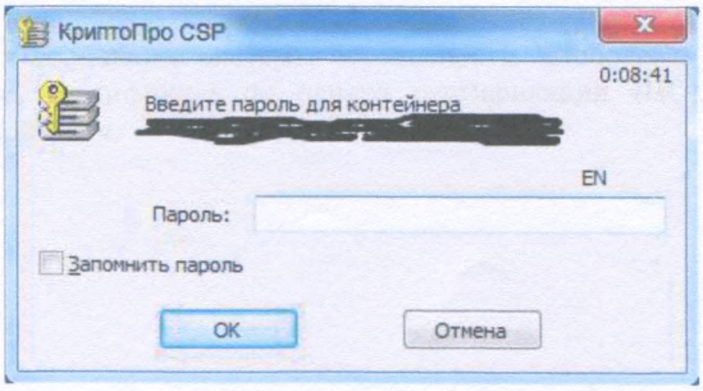

Рис. 17. Окно ввода пароля от контейнера

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

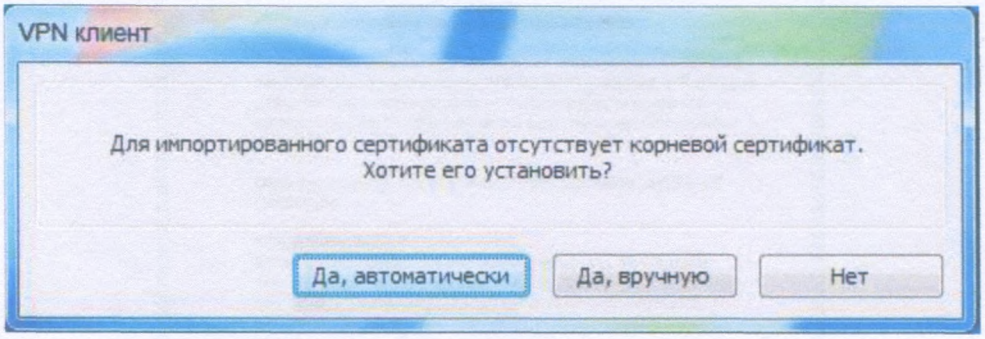

Рис. 18. Сообщение о необходимости установки корневого сертификата

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».*

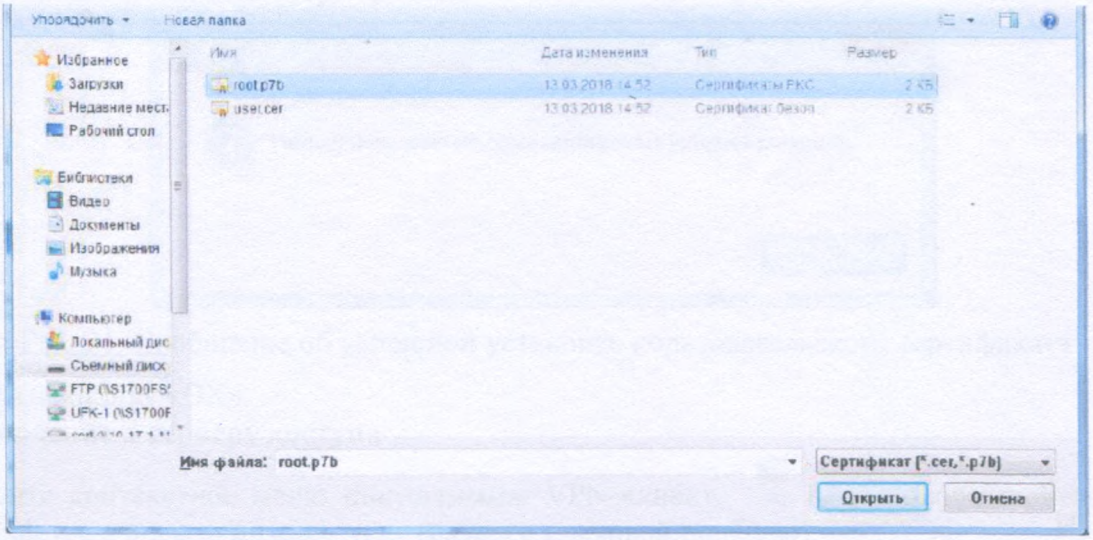

Рис. 19. Выбор корневого сертификата для кнопки «Да, вручную»

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.

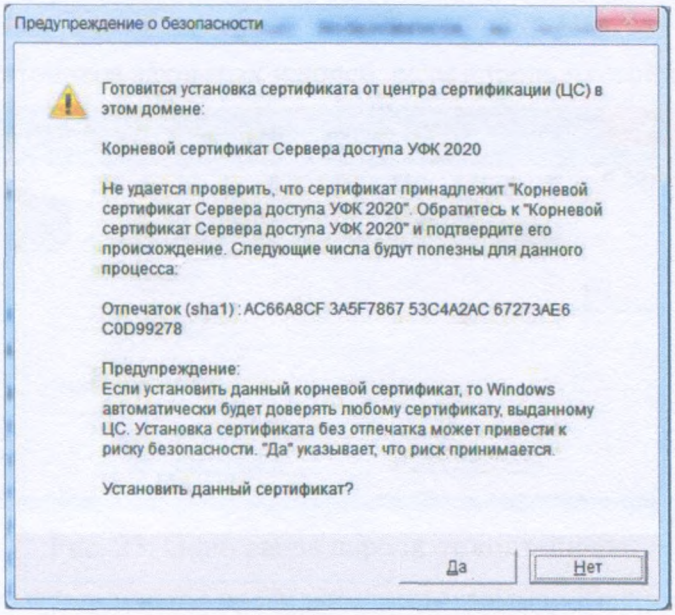

Рис. 20. Предупреждение о безопасности

Нажмите кнопку «Да».

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

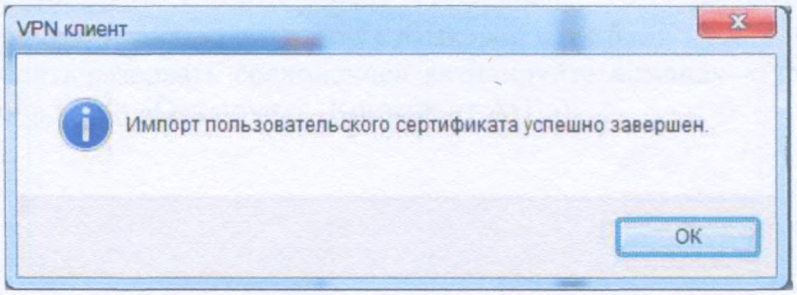

Рис. 21. Сообщение об успешной установке пользовательского сертификата

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».

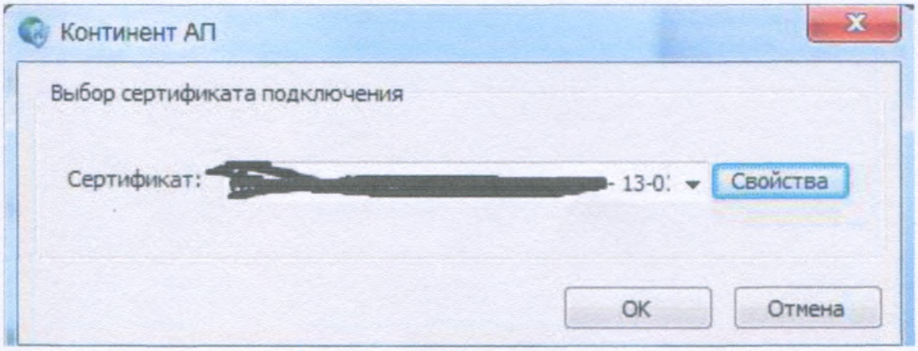

Рис. 22. Окно выбора сертификата пользователя

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

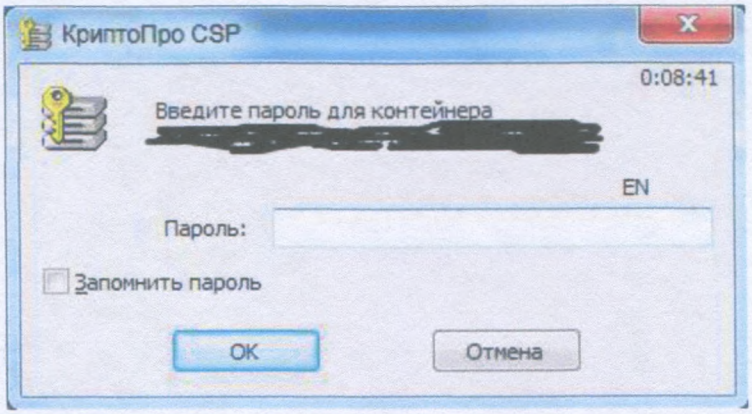

Рис. 23. Окно ввода пароля от контейнера

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’»).