КОД БЕЗОПАСНОСТИ

Средство криптографической защиты информации

Континент-АП
Версия 3.7

Руководство пользователя
Windows

RU.88338853.501430.007 92

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Введение ... **4**

Общие сведения ... **5**
- Что следует знать ... 5
- Что необходимо иметь ... 5
- Что нужно сделать ... 6
- Что важно помнить ... 6

Управление межсетевым экраном ... **7**
- Вызов меню управления МСЭ ... 7
- Включение режима работы пользователя ... 8
- Включение режима ожидания ... 8
- Изменение пароля пользователя ... 8

Управление абонентским пунктом ... **10**
- Вызов меню управления абонентским пунктом ... 10
- Запуск программы управления абонентским пунктом вручную ... 11
- Выход из программы управления ... 11

Управление сертификатами ... **12**
- Общие сведения о сертификатах ... 12
- Получение пользователем сертификатов ... 12
- Создание запроса на получение сертификата пользователя ... 13
- Варианты использования криптопровайдера при формировании закрытого ключа пользователя ... 16
  - КриптоПро CSP ... 16
  - Код Безопасности CSP ... 17
- Регистрация сертификатов ... 18
- Просмотр сведений о сертификатах ... 21
  - Просмотр сертификата пользователя ... 21
  - Просмотр корневого сертификата ... 21
- Использование сертификата пользователя в качестве сертификата компьютера ... 22

Соединение с сервером доступа ... **24**
- Об устанавливаемых соединениях ... 24
- Создание нового соединения с использованием конфигурационного файла ... 24
- Установление соединения с сервером доступа ... 25
- Разрыв соединения с сервером доступа ... 27
- Удаление соединения ... 27

Приложение ... **29**
- Разделение прав пользователей и администраторов АП ... 29

Документация ... **31**

Введение

Данный документ предназначен для администраторов и пользователей изделия "Средство криптографической защиты информации "Континент-АП". Версия 3.7" (далее — абонентский пункт, комплекс). В нем содержатся сведения, необходимые пользователю для эксплуатации программного обеспечения абонентского пункта на платформе Windows.

Сайт в интернете. Вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-495-982-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": http://www.securitycode.ru/products/technical-support/.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Общие сведения

Что следует знать

Комплекс предназначен для организации удаленного доступа к корпоративным ресурсам, а также защиты компьютера пользователя от несанкционированного доступа извне.

Комплекс состоит из следующих компонентов:

- абонентский пункт;
- межсетевой экран.

Абонентский пункт подключается к корпоративным ресурсам и обеспечивает обмен информацией в зашифрованном виде.

Поддерживается работа с криптопровайдерами "Код Безопасности CSP" версии 3.7 (входит в состав программного обеспечения абонентского пункта) и "КриптоПро CSP" версии 4.0 (устанавливается отдельно).

Для подключения к корпоративным ресурсам абонентский пункт устанавливает соединение с сервером доступа, расположенным в корпоративной сети. Сервер доступа определяет права пользователя на доступ к корпоративным ресурсам. Аутентификация пользователя выполняется с помощью метода асимметричного шифрования. Для взаимодействия абонентского пункта и сервера доступа используют следующие сертификаты открытых ключей:

- сертификат пользователя — для аутентификации пользователя на сервере доступа;
- сертификат сервера доступа — для аутентификации сервера доступа;
- сертификат корневого центра сертификации — для подтверждения подлинности сертификата пользователя и сертификата сервера доступа.

Программное обеспечение комплекса устанавливается в соответствии с одним из трех вариантов, обеспечивающим необходимый уровень безопасности:

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

В зависимости от установленного уровня безопасности некоторые функциональные возможности комплекса могут быть пользователю недоступны.

Межсетевой экран (далее — МСЭ) обеспечивает фильтрацию IP-пакетов сетевого трафика компьютера, на котором установлен абонентский пункт.

Предусмотрены два режима работы МСЭ:

- режим ожидания;
- режим работы пользователя.

В режиме ожидания сетевая активность компьютера минимальна. Для перехода к режиму работы необходимо предъявить пароль пользователя.

Что необходимо иметь

Перед тем как начать работу с ресурсами защищенной корпоративной сети:

1. Необходимо получить у администратора безопасности сертификат пользователя и корневой сертификат.

   Внимание! Если при регистрации в системе администратор не потребовал от вас сформировать запрос на получение сертификата пользователя, необходимо получить у администратора кроме сертификатов еще и носитель с закрытым ключом пользователя.

2. Необходимо выяснить, какие права на доступ к ресурсам корпоративной сети предоставлены вам администратором.

3. Необходимо иметь установочный комплект программного обеспечения абонентского пункта.
4. Если предусмотрена настройка подключения к серверу доступа с использованием конфигурационного файла, получите конфигурационный файл у администратора.

Что нужно сделать

Для ввода в эксплуатацию комплекса:

1. В зависимости от требований, предъявляемых к уровню безопасности, установите и настройте дополнительное программное обеспечение "КриптоПро CSP".
2. Установите программное обеспечение абонентского пункта. Процедура установки подробно рассматривается в [**1**].
3. Включите у межсетевого экрана (если компонент МСЭ установлен) режим работы пользователя (см. стр.**8**).
4. Получите у администратора безопасности сертификаты, необходимые для работы. Для получения сертификата пользователя, возможно, потребуется создать файл запроса (см. стр.**13**) и передать его администратору.
5. Зарегистрируйте полученные сертификаты. Процедуру см. стр.**18**.
6. Если для соединения с сервером доступа должно использоваться подключение, настроенное с помощью конфигурационного файла, передайте конфигурационный файл администратору абонентского пункта и попросите его настроить подключение.
7. Установите соединение с сервером доступа (см. стр. **25**) и попробуйте подключиться к какому- либо доступному ресурсу, находящемуся в защищенном сегменте корпоративной сети.

   Если пробное соединение с сервером установлено успешно и подключение к ресурсу корпоративной сети возможно — значит, все подготовительные действия выполнены правильно. С этого момента абонентский пункт готов к работе.

Что важно помнить

1. Никому не передавайте полученные у администратора ключевые носители с закрытыми ключами.
2. После того как выполнена установка абонентского пункта и включена защита устройств доступа к сети, запрещается вносить любые изменения в свойства сетевого окружения, например, корректировать списки сетевых адаптеров, сервисов, протоколов и т. д.
3. Во всех сложных ситуациях, связанных с работой комплекса, которые вы сами не в состоянии разрешить, обращайтесь к администратору. В частности, если имеющихся прав доступа к ресурсам корпоративной сети недостаточно для эффективного выполнения должностных обязанностей, обратитесь к администратору безопасности или другому должностному лицу, отвечающему за распределение прав доступа к ресурсам.

Управление межсетевым экраном

Вызов меню управления МСЭ

Управление МСЭ выполняется с помощью специального меню.

Для вызова меню управления МСЭ:

- Наведите указатель мыши на пиктограмму МСЭ, расположенную на панели задач Windows, и нажмите правую кнопку мыши.

  Цвет пиктограммы МСЭ указывает на режим его работы:

Пиктограмма	Цвет	Пояснение
	Зеленый	Режим работы пользователя. Для снятия ограничения доступа к сети при работе абонентского пункта режим должен быть включен
	Желтый	Режим ожидания или ошибка в работе

  На экране появится меню управления абонентским пунктом.

Табл.1 Команды меню управления МСЭ

Пункт меню	Описание
Начать сеанс работы…	Вызывает на экран окно для ввода пароля пользователя. После авторизации включается режим работы пользователя
Завершить сеанс работы	Выключает режим работы пользователя и включает режим ожидания
Изменить пароль…	Вызывает на экран окно для изменения пароля пользователя
Входить автоматически	При наличии отметки режим работы пользователя включается автоматически сразу после загрузки операционной системы без запроса пароля
Войти в режим настройки…	Вызывает на экран окно для ввода пароля администратора. После ввода пароля становятся доступными команды управления правилами фильтрации
Выйти из режима настройки	Завершает сеанс работы администратора. Команды управления правилами фильтрации становятся недоступными
Изменить данные администратора…	Вызывает на экран окно для изменения логина и пароля администратора
Изменить расписание…	Открывает окно для формирования расписаний работы правил фильтрации
Изменить правила фильтрации…	Открывает окно для формирования списка правил сетевой фильтрации, действующих в режиме работы пользователя
Изменить правила прикладной фильтрации…	Открывает окно для формирования списка правил прикладной фильтрации. Эти правила действуют в режиме работы пользователя
Изменить правила фильтрации до авторизации…	Открывает окно для формирования списка правил фильтрации, действующих в режиме ожидания
Включить оповещение	При наличии отметки на экран выводятся сообщения о срабатывании правил фильтрации с флагом alert
Журналы	Вызывает на экран выбранный в подменю регистрационный журнал. В комплексе, соответствующем высокому уровню безопасности, пользователю данная команда недоступна

Справка	Вызывает на экран окно справочной системы МСЭ
О программе…	Вызывает на экран окно с информацией об установленной на компьютере версии программного обеспечения МСЭ
Выход	Удаляет значок МСЭ из системной области панели задач

Так как настройку параметров МСЭ может выполнить лишь пользователь, наделенный правами администратора, часть команд контекстного меню доступна для активации только после ввода пароля администратора (см. [**1**]).

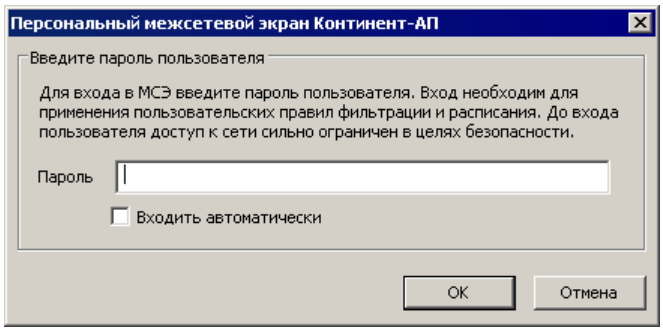
Включение режима работы пользователя

Для включения режима работы пользователя необходимо ввести пароль пользователя. По умолчанию пароль пользователя МСЭ имеет значение "111111", если не был изменен во время установки абонентского пункта.

Для включения режима работы:

1. Активируйте в контекстном меню пиктограммы МСЭ команду "Начать сеанс работы…".

   На экране появится диалог для ввода пароля.



2. Введите пароль и нажмите кнопку "OK".

Примечание. Для автоматического включения режима работы пользователя сразу после загрузки операционной системы установите отметку в поле "Входить автоматически".

Включение режима ожидания

Для включения режима ожидания:

- Активируйте в контекстном меню пиктограммы МСЭ команду "Завершить сеанс работы".

Изменение пароля пользователя

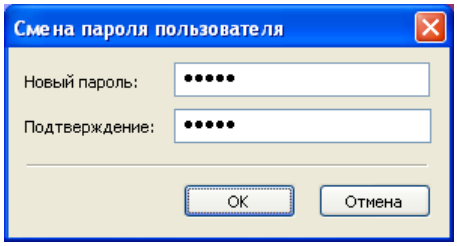
После установки программного обеспечения пароль пользователя МСЭ имеет значение "111111", если не был изменен во время установки абонентского пункта. В дальнейшем этот пароль необходимо изменить.

Внимание! Пароль пользователя можно изменить только после ввода текущего пароля пользователя или администратора.

Для изменения пароля пользователя:

1. Активируйте в контекстном меню пиктограммы МСЭ команду "Изменить пароль…".

   На экране появится диалог для ввода пароля.



2. Заполните поля диалога и нажмите кнопку "OK":
   - в поле "Пароль" введите новый пароль (длина пароля должна быть не менее 5 символов);
   - в поле "Подтверждение" укажите тот же пароль еще раз.

Управление абонентским пунктом

Вызов меню управления абонентским пунктом

Управление абонентским пунктом выполняется с помощью специального меню.

Для вызова меню управления абонентским пунктом:

- Наведите указатель мыши на пиктограмму абонентского пункта, расположенную на панели задач Windows, и нажмите правую кнопку мыши.

  На экране появится меню управления абонентским пунктом.

  Внимание! Состав меню, отображаемого на экране, зависит от прав пользователя, вошедшего в систему, и от уровня безопасности, выбранного при установке абонентского пункта (см. стр.**29**).

  Цвет пиктограммы абонентского пункта указывает на наличие или отсутствие соединения с сервером доступа:

Пиктограмма	Цвет	Пояснение
	Серый	Соединение не установлено
	Зеленый	Соединение установлено

Табл.2 Команды меню управления абонентским пунктом

Команда	Описание
Подключить "<имя подключения>"	Запускает процедуру установки или разрыва подключения абонентского пункта с сервером доступа, определенного как подключение по умолчанию
Выбор соединения по умолчанию	Определяет выбранное в подменю подключение как подключение по умолчанию. В списке отображаются все доступные подключения, зарегистрированные на компьютере
Выбор криптопровайдера по умолчанию	Определяет выбранный в подменю криптопровайдер как криптопровайдер, используемый по умолчанию. В списке отображаются все доступные криптопровайдеры, установленные на компьютере
Установить/разорвать соединение	Запускает процедуру установки или разрыва выбранного в подменю подключения абонентского пункта с сервером доступа
Создать новое соединение	Запускает процедуру создания нового соединения. Параметры подключения могут быть настроены вручную или с применением конфигурационного файла
Удалить соединение	Запускает процедуру удаления выбранного соединения
Настройка соединения	Устанавливает способ подключения к СД (по HTTP-туннелю, через прокси или по UDP). Предоставляет возможность изменить адрес СД и в случае необходимости указать настройки прокси-сервера
Настройка аутентификации	Вызывает на экран диалог свойств протокола проверки подлинности для выбранного в подменю подключения абонентского пункта
Настройка зависимости между соединениями	Включает/выключает режим автоматического запуска процедуры подключения компьютера к сети провайдера
Журнал	Вызывает на экран стандартное приложение просмотра событий ОС Windows. Зарегистрированные события хранятся в разделе "Terminal Station"

Команда	Описание
Сертификаты > Создать запрос на пользовательский сертификат…	Запускает процедуру создания запроса на получение сертификата пользователя
Сертификаты > Установить сертификат пользователя	Вызывает на экран стандартный диалог Windows для выбора файла сертификата
Загружать автоматически	Включает/выключает режим автоматического запуска программы управления абонентским пунктом при запуске Windows
Поддержка модемного соединения	Включает/выключает режим работы МСЭ с внешними 3G/4G-модемами
Настройка автоматического обновления	Вызывает на экран диалог настройки автоматической проверки обновления программного обеспечения абонентского пункта
Справка	Вызывает на экран окно оперативной справочной системы
О программе…	Вызывает на экран диалог со сведениями о номере версии программы и авторских правах
Выход	Завершает работу программы управления абонентским пунктом

Запуск программы управления абонентским пунктом вручную

Для запуска программы управления абонентским пунктом вручную:

- В главном меню Windows активируйте команду "Все Программы\Код Безопасности\Континент-АП 3.7\VPN клиент".

  Программа управления абонентским пунктом будет запущена. На панели задач Windows появится пиктограмма абонентского пункта.

Выход из программы управления

При завершении работы программы управления абонентский пункт продолжает свою работу.

Для выхода из программы:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. Активируйте команду "Выход".

   Работа программы управления абонентским пунктом будет завершена. Пиктограмма этой программы исчезнет с панели Windows.

Управление сертификатами

Общие сведения о сертификатах

Сертификат — это цифровой документ, содержащий информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т. д. Сертификат заверяется электронной цифровой подписью удостоверяющего центра сертификации.

В зависимости от используемого стандарта существуют различные форматы сертификатов. Абонентский пункт может работать со следующими форматами:

- сертификаты в кодировках Distinguished Encoding Rules (DER) и Base-64 (перевод двоичных данных в читаемый текст). Файл, содержащий один сертификат, обычно имеет расширение *.cer. В файлах с таким расширением хранятся сертификаты пользователя (как правило) и реже — сертификаты корневого центра сертификации;
- сертификаты в формате PKCS 7 (обычно с расширением *.p7b). Могут содержать несколько сертификатов, например, цепочку подтверждающих друг друга сертификатов. В таком формате хранятся сертификаты корневого центра сертификации.

Сертификаты в файлах с расширением *.cer и *.p7b соответствуют стандарту X.509v3 Международного телекоммуникационного союза (ITU-T).

Система автоматически отслеживает статус сертификата: действителен или недействителен. Недействительным сертификат может быть признан по следующим причинам:

- срок действия сертификата не наступил;
- срок действия сертификата истек;
- сертификат отозван удостоверяющим центром;
- отсутствует сертификат удостоверяющего центра.

Необходимо использовать только действительные сертификаты.

Статус сертификатов, выданных внешним удостоверяющим центром, проверяется по списку отозванных сертификатов этого центра (файл с расширением *.crl). Если список отозванных сертификатов на компьютере отсутствует или просрочен, то проверка сертификатов не выполняется.

Внимание! При использовании сертификатов внешнего удостоверяющего центра необходимо средствами Windows установить на компьютере список отозванных сертификатов этого центра и периодически проводить его обновление.

Получение пользователем сертификатов

Для создания защищенного соединения между абонентским пунктом и сервером доступа пользователю абонентского пункта необходимо получить у администратора безопасности и зарегистрировать на своем компьютере следующие сертификаты:

- сертификат пользователя абонентского пункта;
- сертификат корневого центра сертификации, удостоверяющий сертификат пользователя.

Пояснение. Кроме сертификатов пользователь должен иметь ключевой носитель, в котором содержится ключевой контейнер с закрытым ключом сертификата пользователя, и знать пароль доступа к нему. Пароль следует держать в секрете. Передавать ключевой носитель другому лицу нельзя. Перечень ключевых носителей, которые можно использовать при работе с абонентским пунктом, зависит от настроек криптопровайдера, установленного на том же компьютере, что и абонентский пункт. Рекомендуется использовать отчуждаемый ключевой носитель (например, USB-флеш-накопитель).

Предусмотрены следующие варианты получения пользователем сертификатов:

- администратор безопасности передает пользователю абонентского пункта корневой и пользовательский сертификаты вместе с ключевым носителем, на котором хранится закрытый ключ сертификата пользователя. Администратор также сообщает пользователю пароль доступа к ключевому контейнеру, содержащему закрытый ключ сертификата пользователя.

  Примечание. Передача сертификатов, закрытого ключа и пароля от администратора к пользователю осуществляется в соответствии с правилами пользования (см. документ "Средство криптографической защиты информации "Континент-АП". Версия 3.7. Правила пользования" RU.88338853.501430.007 93).

  От пользователя в этом случае не требуется никаких предварительных действий;

- администратор безопасности передает пользователю сертификаты в составе конфигурационного файла. Помимо сертификатов конфигурационный файл содержит настройки, необходимые для создания нового подключения абонентского пункта к серверу доступа;

- по требованию администратора безопасности пользователь абонентского пункта создает на своем компьютере запрос на получение сертификата пользователя. Запрос создается средствами абонентского пункта. Одновременно с запросом будет создан закрытый ключ сертификата пользователя, при этом пользователь самостоятельно назначает пароль доступа к ключевому контейнеру. Созданный запрос на получение сертификата пользователь передает администратору безопасности, а закрытый ключ хранит у себя. На основании полученного от пользователя запроса администратор создает сертификат и передает его пользователю. При необходимости администратор также передает пользователю сертификат корневого центра сертификации.

  Примечание. Передача запроса на получение сертификата от пользователя к администратору, получение сертификата пользователя, а также получение корневого сертификата осуществляются в соответствии с .правилами пользования (см. документ "Средство криптографической защиты информации "Континент-АП". Версия 3.7. Правила пользования" RU.88338853.501430.007 93).

Последний из описанных способов является предпочтительным, так как позволяет пользователю сохранить в тайне закрытый ключ и пароль. Кроме того, при создании запроса на сертификат пользователь самостоятельно указывает информацию о себе, что обеспечивает максимальную точность данных.

Если пользователь должен получить сертификаты на основании запроса, ему предварительно необходимо создать запрос и передать его администратору (см. стр.**13**).

После получения сертификатов пользователь должен выполнить процедуру регистрации сертификатов на компьютере (см. стр.**18**).

Создание запроса на получение сертификата пользователя

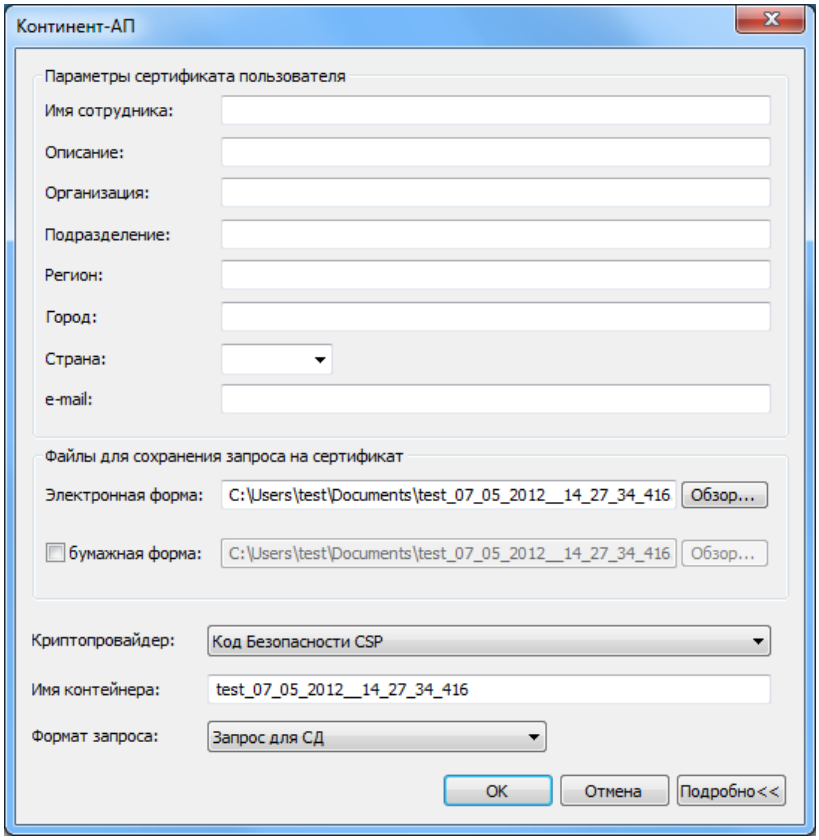
Запрос на получение сертификата создается пользователем средствами абонентского пункта по требованию администратора безопасности. Одновременно с запросом средствами криптопровайдера генерируется закрытый ключ пользователя. Запрос в виде файла сохраняется в указанную пользователем папку, ключевой контейнер с закрытым ключом сохраняется на ключевом носителе, указанном в настройках.

Совет. Перед тем как приступить к созданию запроса, приготовьте чистый отформатированный ключевой носитель для записи ключевого контейнера.

Для создания запроса на получение сертификата:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. В меню "Сертификаты" активируйте команду "Создать запрос на пользовательский сертификат".

   На экране появится диалоговое окно для создания запроса.



3. Укажите достоверные сведения о себе в полях группы "Параметры сертификата пользователя".

   Внимание! Текстовые поля "Имя сотрудника", "Организация" и "Подразделение" для заполнения обязательны. При отсутствии этих сведений создание сертификата пользователя невозможно. Рекомендуется заполнять все поля данного диалога.

4. В группе "Файлы для сохранения запроса на сертификат" укажите значения следующих параметров:

   - в поле "Электронная форма" при необходимости измените путь и имя файла с электронной формой запроса;

     Примечание. По умолчанию запрос сохраняется в файле с расширением *.req и именем, содержащим имя текущего пользователя Windows, а также текущие время и дату.

   - в поле "Бумажная форма" установите отметку, если необходимо сохранить версию запроса для печати.

     Примечание. По умолчанию запрос сохраняется в файле с расширением *.html и именем, содержащим имя текущего пользователя Windows, а также текущие время и дату.

   Для изменения расположения или имени файла с электронной или бумажной формой запроса нажмите кнопку "Обзор...", расположенную справа от соответствующего поля. В стандартном окне Windows, появившемся на экране, выполните следующие действия:

   - укажите диск (папку) для создания файла;
   - укажите имя файла запроса;
   - нажмите кнопку "Сохранить".

5. Если требуется изменить дополнительные параметры, нажмите кнопку "Подробно>>" и выполните следующие действия:
   - в поле "Криптопровайдер" выберите нужное значение.
   - в поле "Имя контейнера" укажите имя ключевого контейнера, в котором будет сохранен закрытый ключ сертификата пользователя;

     Примечание. По умолчанию имя ключевого контейнера содержит имя текущего пользователя Windows, а также текущие время и дату.

   - в поле "Формат запроса" в раскрывающемся списке выберите формат запроса на сертификат:
     - "Запрос для СД" (по умолчанию) — формат запроса для создания сертификата в программе управления сервером доступа;
     - "Запрос для УЦ КриптоПРО" — формат запроса для дальнейшей обработки в УЦ КриптоПРО;
     - "Запрос для СА" — формат запроса для создания сертификата внешним центром сертификации.
6. Нажмите кнопку "ОК".

   Криптопровайдер приступит к созданию закрытого ключа. Необходимо выполнить следующие операции:
   - сформировать закрытый ключ с помощью датчика случайных чисел;
   - выбрать тип ключевого носителя для записи закрытого ключа;
   - ввести пароль для ограничения доступа к ключевому контейнеру.

     Примечание. При наличии отметки в поле "Запомнить пароль" введенный пароль сохраняется в реестре компьютера. В дальнейшем при обращении к этому ключевому контейнеру запрос пароля на экран не выводится.

   Порядок выполнения операций зависит от используемого криптопровайдера, датчика случайных чисел и ключевого носителя, выбранного для хранения ключевой информации. Следуйте указаниям, появляющимся на экране.

   Более подробно о создании закрытого ключа см. стр.**16**.

   После завершения процедуры на экране появится сообщение о завершении создания запроса на сертификат.
7. Нажмите кнопку "ОК" в окне сообщения для завершения процедуры создания запроса.

   Внимание! Если в качестве ключевого носителя был выбран системный реестр, после создания ключевой информации не рекомендуется выполнять действия, затрагивающие системное программное обеспечение данного компьютера.

Передайте созданный файл запроса администратору безопасности. При этом можно пользоваться общедоступной сетью передачи данных, например, переслать файл как вложение электронной почты.

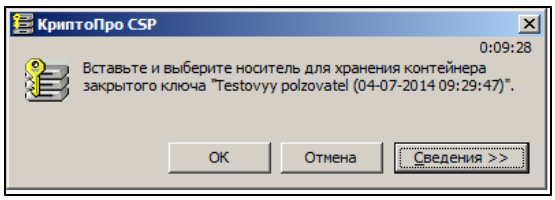
Варианты использования криптопровайдера при формировании закрытого ключа пользователя

Ниже приведены процедуры формирования закрытого ключа пользователя при создании запроса на получение сертификата. Представлены варианты использования криптопровайдеров "КриптоПро CSP" и "Код Безопасности CSP".

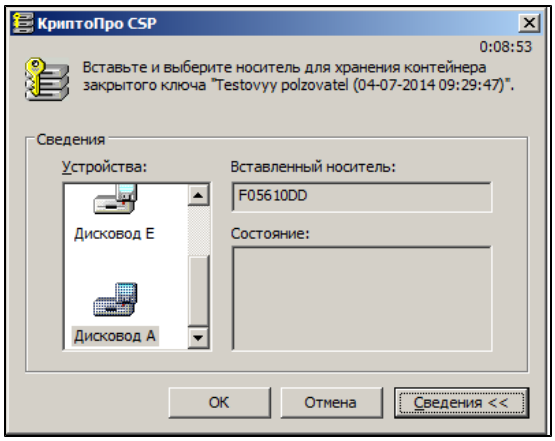
КриптоПро CSP

Для формирования закрытого ключа:

1. После нажатия в окне создания запроса кнопки "OK" на экране появится окно с указанием вставить чистый ключевой носитель.



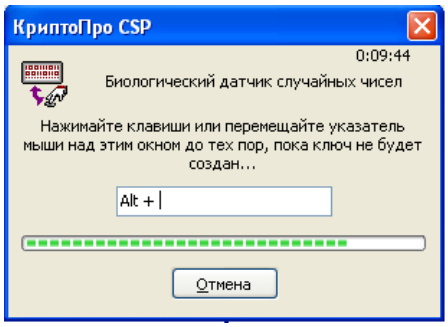
2. Вставьте носитель, нажмите кнопку "Сведения" и укажите устройство.



3. Нажмите кнопку "OK".

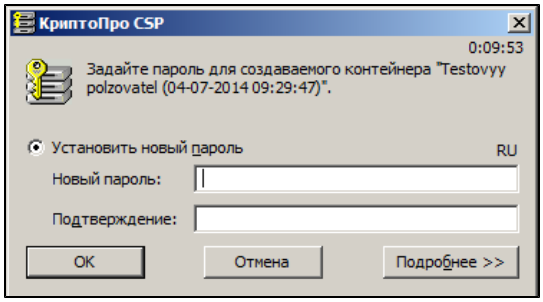
   На экране появится окно "Биологический датчик случайных чисел".

> **Примечание.** Если в КриптоПро CSP настроен датчик случайных чисел ПАК "Соболь", на экране появится окно задания пароля для доступа к содержимому ключевого контейнера (см. **п.4**). Перейдите к выполнению **п.5**.



4. Следуйте отображаемой в окне инструкции и дождитесь завершения создания ключа.

   На экране появится окно задания пароля для доступа к содержимому ключевого контейнера.



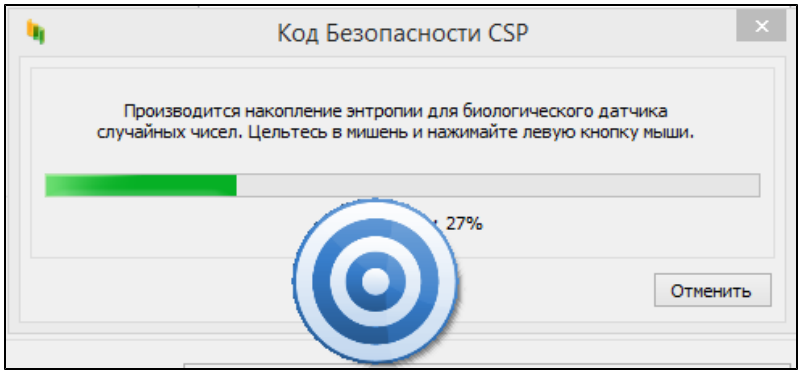
5. Введите и подтвердите пароль на создаваемый ключевой контейнер и нажмите кнопку "OK".

   Начнется запись закрытого ключа пользователя на ключевой носитель, и после ее окончания на экране появится сообщение об успешном завершении создания запроса.

Код Безопасности CSP

Для формирования закрытого ключа:

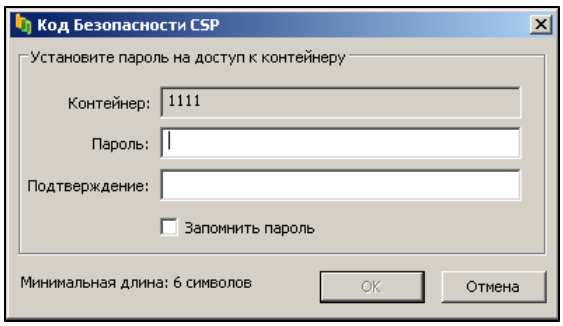
1. После нажатия в окне создания запроса кнопки "OK" на экране появится окно накопления энтропии для биологического датчика случайных чисел.



Примечание. При использовании физического ДСЧ вместо окна накопления энтропии появится окно задания пароля. Перейдите к выполнению **п.3**.

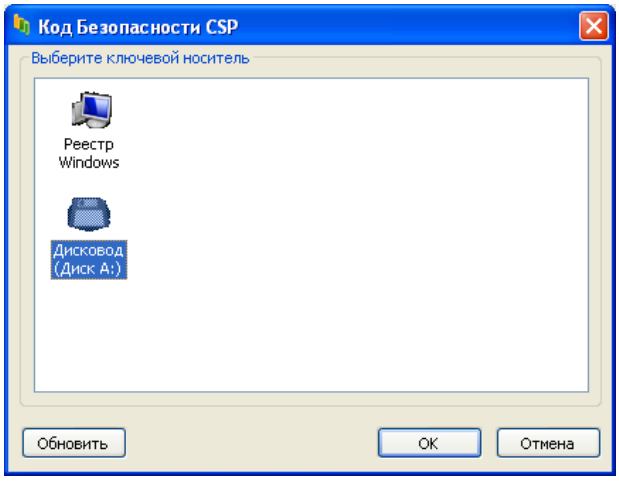
2. Следуйте отображаемой в окне инструкции, стараясь попасть в мишень, и дождитесь завершения операции.

   На экране появится окно задания пароля для доступа к содержимому ключевого контейнера.



3. Введите и подтвердите пароль на создаваемый ключевой контейнер и нажмите кнопку "OK". Длина пароля должна быть не менее 6 символов.

   На экране появится окно выбора ключевого носителя.



4. Выберите ключевой носитель и нажмите кнопку "OK".

   Примечание. Если используется съемный носитель, он должен быть предварительно вставлен в устройство.

   Начнется запись закрытого ключа пользователя на ключевой носитель, и после ее окончания на экране появится сообщение об успешном завершении создания запроса.

Регистрация сертификатов

Пользователь абонентского пункта получает от администратора безопасности сертификат пользователя и сертификат корневого центра сертификации. Эти сертификаты необходимо зарегистрировать в хранилище сертификатов на компьютере, на котором установлен абонентский пункт.

Регистрация сертификатов производится в следующем порядке. Средствами абонентского пункта выполняется регистрация сертификата пользователя. Затем в хранилище сертификатов автоматически производится поиск корневого сертификата для только что зарегистрированного сертификата пользователя. Если корневой сертификат уже был зарегистрирован и действителен, то процедура прекращается. Если корневой сертификат не найден (не был зарегистрирован или попал в список отозванных сертификатов), то на экран выведется предложение выполнить его регистрацию. Таким образом, регистрация корневого сертификата осуществляется совместно с регистрацией сертификата пользователя. Отдельная регистрация корневого сертификата средствами абонентского пункта не производится.

Внимание! Перед тем как приступить к регистрации сертификатов, предъявите ключевой носитель с закрытым ключом пользователя.

Совет. Если необходимо зарегистрировать корневой сертификат одновременно с сертификатом пользователя, то рекомендуется хранить корневой сертификат в той же папке, что и сертификат пользователя.

Для регистрации сертификатов:

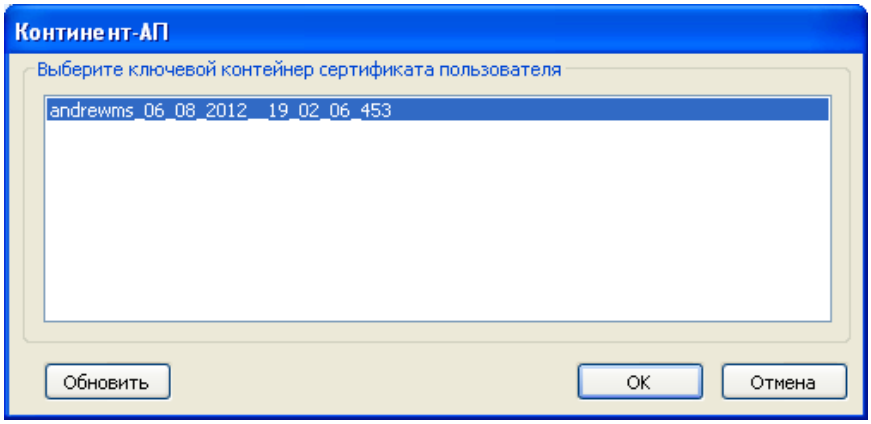
1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. В меню "Сертификаты" активируйте команду "Установить сертификат пользователя".

   На экране появится стандартное диалоговое окно Windows для работы с файлами.
3. Выберите файл сертификата user.cer и нажмите кнопку "Открыть".

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

4. Вставьте в устройство ключевой носитель и нажмите кнопку "Обновить".

   В диалоге появится список ключевых контейнеров.



Примечание. Если ключевым носителем является eToken, а в качестве криптопровайдера используется "Код Безопасности CSP", ключевой контейнер может не появиться в списке. Необходимо ввести PIN-код с помощью программы Код Безопасности CSP (см. [1]).

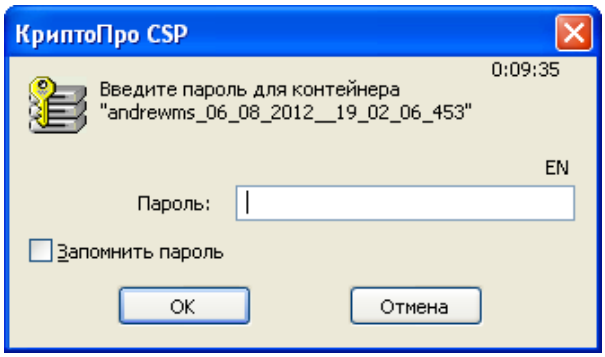
5. Выберите нужный ключевой контейнер и нажмите кнопку "OK".

   Если ключевой носитель защищен PIN-кодом, появится запрос на его ввод. Введите PIN-код.

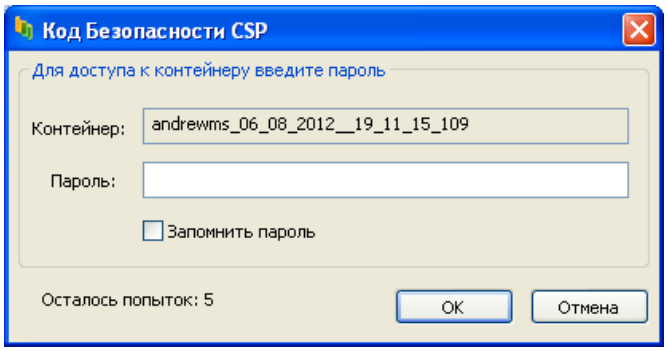
   Внимание! Если сертификат должен использоваться как сертификат компьютера, установите отметку в поле "Запомнить PIN".

   На экране появится запрос пароля доступа к выбранному ключевому контейнеру. Внешний вид окна запроса зависит от используемого криптопровайдера.

   Ниже на рисунке приведено окно запроса для "КриптоПро CSP".



   На следующем рисунке приведено окно запроса для "Код Безопасности CSP".

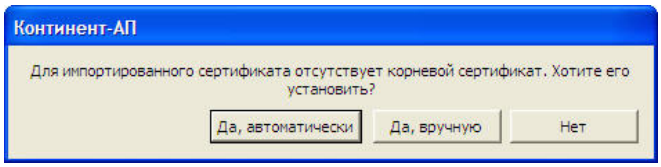


Примечание. При использовании криптопровайдера "Код Безопасности CSP" предусмотрено 5 попыток ввода пароля. После 5-й неудачной попытки ввода пароля необходимо заново начать процедуру регистрации.

6. Заполните поля диалога и нажмите кнопку "OK".

Пароль	Пароль доступа к ключевому контейнеру, полученный у администратора
Запомнить пароль	Установите отметку, если требуется, чтобы введенный пароль был сохранен в реестре компьютера. В дальнейшем при обращении к этому ключевому контейнеру запрос на ввод пароля выводиться не будет. **Внимание!** Если сертификат должен использоваться как сертификат компьютера, установка отметки обязательна

На экране появится запрос на установку корневого сертификата.



7. Для регистрации корневого сертификата нажмите кнопку:

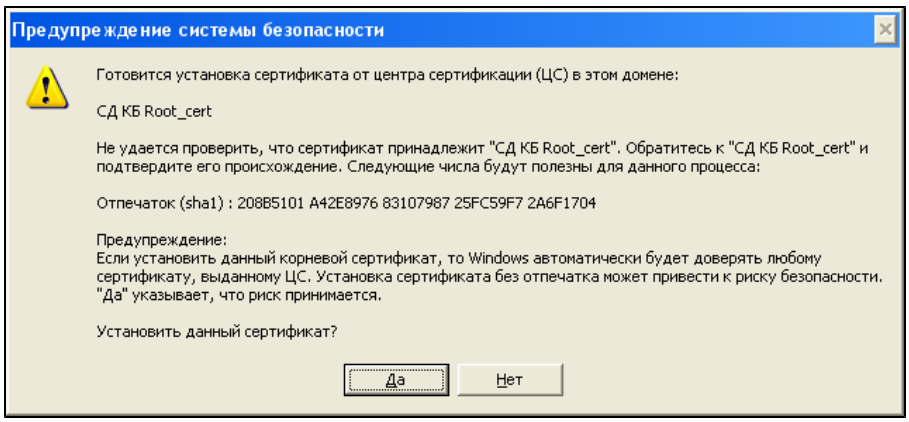
- "Да, автоматически" — в случае если корневой сертификат хранится в одной папке с сертификатом пользователя. Будет выполнен автоматический поиск сертификата;

  Примечание. Если корневой сертификат не будет найден, пользователю будет предложено самостоятельно указать расположение корневого сертификата.

- "Да, вручную" — в случае если корневой сертификат и сертификат пользователя хранятся в разных папках. Пользователю будет предложено самостоятельно указать расположение корневого сертификата.

  Пояснение. На экране появится стандартное диалоговое окно Windows для работы с файлами. Выберите файл с корневым сертификатом и нажмите кнопку "Открыть".

На экране появится сообщение системы безопасности Windows о том, что сейчас будет выполнена регистрация корневого сертификата.



8. Нажмите кнопку "Да".

На экране появится сообщение об успешном завершении импорта пользовательского сертификата.

9. Нажмите кнопку "ОК".

Внимание! Пользователь АП, установленного в соответствии с требованиями высокого уровня безопасности, после регистрации сертификата должен обратиться к администратору для выполнения настройки аутентификации. Без настройки аутентификации пользователь не сможет подключиться к СД.

Просмотр сведений о сертификатах

В зависимости от установленного уровня безопасности комплекса абонентский пункт предоставляет возможность просмотра сведений о сертификате пользователя и корневом сертификате, которым подписан сертификат сервера доступа.

Примечание. Данный корневой сертификат необязательно совпадает с корневым сертификатом, которым подписан сертификат пользователя.

Просмотр сертификата пользователя

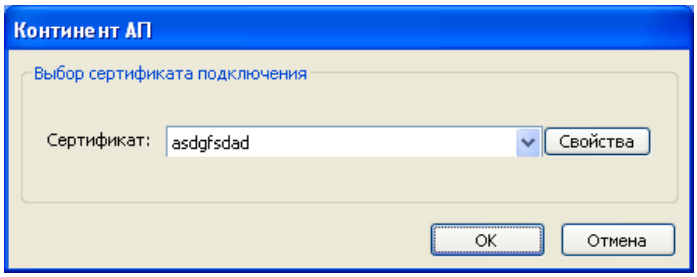
Сертификат пользователя хранится в хранилище сертификатов текущего пользователя на компьютере, где установлен абонентский пункт. Имеется возможность просмотреть сертификат как стандартными средствами Windows, так и средствами абонентского пункта (см. ниже).

Примечание. Если сертификат пользователя и сертификат сервера доступа заверены разными корневыми сертификатами, то просмотреть корневой сертификат, которым заверен сертификат пользователя, возможно только стандартными средствами Windows.

Для просмотра сертификата пользователя:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. В меню "Установить/разорвать соединение" активируйте команду "Установить соединение Континент-АП".

   На экране появится диалог выбора сертификата.



3. В поле "Сертификат пользователя" из раскрывающегося списка выберите нужный сертификат и нажмите кнопку "Свойства".

   На экране появится диалоговое окно с информацией о выбранном сертификате.

Просмотр корневого сертификата

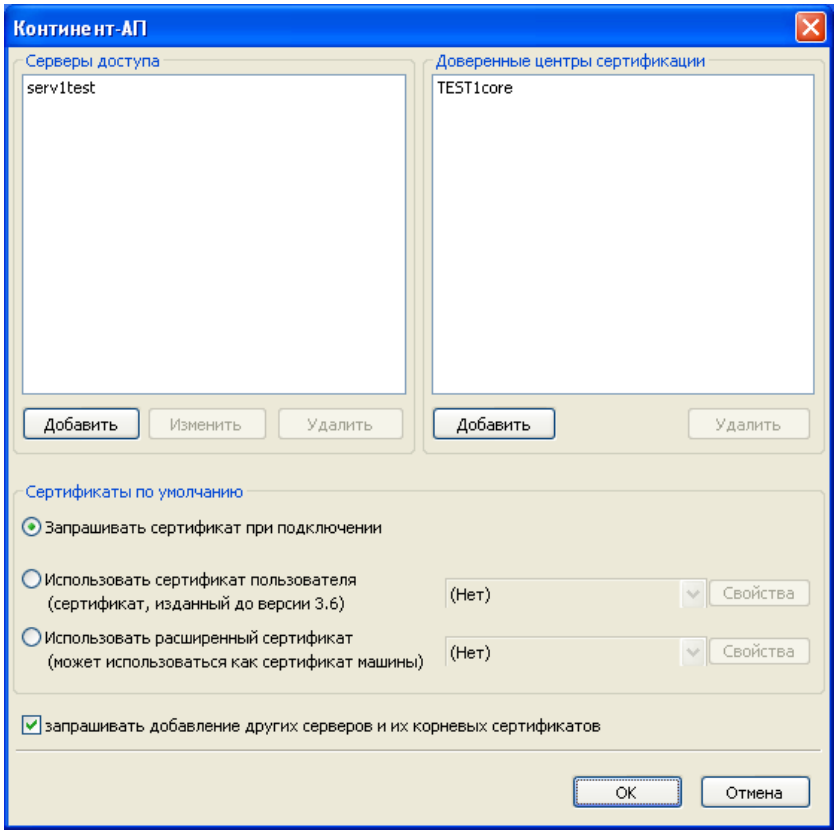
Корневой сертификат, которым подписан сертификат сервера доступа, не заносится в хранилище сертификатов на компьютере, на котором установлен абонентский пункт. Сведения о корневом сертификате, а также об имени сервера доступа передаются на компьютер, на котором установлен абонентский пункт, при установлении первого соединения между абонентским пунктом и сервером доступа.

Внимание! Просмотр корневого сертификата на абонентском пункте, работающем в режиме высокого уровня безопасности, недоступен.

Для просмотра корневого сертификата:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. В меню "Настройка аутентификации" активируйте команду с названием любого подключения.

   На экране появится диалог свойств протокола проверки подлинности.



В диалоге отображаются два списка: "Серверы доступа" и "Доверенные центры сертификации".

В списке "Серверы доступа" приводится перечень разрешенных серверов доступа.

В списке "Доверенные центры сертификации" перечислены корневые сертификаты, которыми подписаны сертификаты серверов доступа.

Примечание. Если список пуст — значит, соединение между абонентским пунктом и сервером доступа еще ни разу не было установлено. Установите соединение и вновь вызовите данный диалог. Данные в поля "Серверы доступа" и "Доверенные центры сертификации" могут быть добавлены пользователем самостоятельно (только для АП, работающего в режиме низкого или среднего уровня безопасности), без установки связи с сервером доступа. Для этого в поле "Серверы доступа" нажмите кнопку "Добавить", введите имя сертификата сервера и нажмите клавишу "Enter". В поле "Доверенные центры сертификации" нажмите кнопку "Добавить", в появившемся списке выберите корневой сертификат, которым заверен сертификат указанного сервера доступа, и нажмите кнопку "ОК". Выбранный сертификат будет добавлен в поле "Доверенные центры сертификации".

3. Выберите нужный корневой сертификат и дважды щелкните по нему мышью.

   На экране появится диалоговое окно с информацией о сертификате.

Использование сертификата пользователя в качестве сертификата компьютера

Этот режим предоставляет возможность применения доменных политик к компьютеру, на котором установлен комплекс, до входа пользователя в систему (при условии вхождения компьютера в домен).

Режим доступен только в режиме высокого уровня безопасности и только для сертификатов пользователя, изданных средствами программы управления сервером доступа версии 3.6 и выше.

Внимание! Подключение абонентского пункта к серверу доступа возможно только с предъявлением ключевого контейнера с закрытым ключом пользователя при сохраненном пароле доступа к ключевому контейнеру и сохраненном PIN-коде (для ключевых носителей, защищенных PIN-кодом).

Для настройки режима:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. В меню "Настройка аутентификации" активируйте команду с названием любого подключения.

   На экране появится диалог свойств протокола проверки подлинности.
3. Выберите значение "Использовать расширенный сертификат" и укажите нужный сертификат.

   Внимание! Должно выполняться следующее условие: указанный сертификат должен был быть зарегистрирован тем же пользователем, от имени которого осуществляется переключение в режим использования расширенного сертификата. В противном случае после выполнения данной процедуры подключение к серверу доступа станет невозможным и будет сопровождаться ошибкой подписи ключа. Для исправления некорректного переключения в режим использования расширенного сертификата обратитесь к администратору абонентского пункта.

   Примечание. Если в списке отсутствует необходимый сертификат, зарегистрируйте его с сохранением пароля доступа к ключевому контейнеру и PIN-кода (если используется).
4. Выполните контрольное подключение к серверу доступа (см. стр. **25**). В запросах на ввод защитного PIN-кода и пароля доступа к ключевому контейнеру сохраните PIN-код и пароль.
5. Отключите абонентский пункт от сервера доступа и перезагрузите компьютер.

   Компьютер готов к работе в режиме использования сертификата пользователя в качестве сертификата компьютера.

Процедура подключения к серверу доступа зависит от ОС, установленной на компьютере.

Соединение с сервером доступа

Об устанавливаемых соединениях

Абонентский пункт позволяет устанавливать удаленные защищенные соединения посредством эмулятора модема Continent 3 PPP Device.

Примечание. Эмулятор модема Continent 3 PPP Device устанавливается на компьютер при установке абонентского пункта.

При установке абонентского пункта на компьютере автоматически создается сетевое подключение, использующее для установления соединения Continent 3 PPP Device. По умолчанию оно называется "Континент-АП".

Пользователь компьютера с административными правами может создавать свои сетевые подключения, использующие Continent 3 PPP Device, и устанавливать через них соединения с сервером доступа. При необходимости созданные соединения могут быть удалены.

Для создания/удаления сетевого подключения используются команды меню управления абонентским пунктом. Доступность команд по созданию/удалению сетевых подключений зависит от уровня безопасности комплекса и административных прав пользователя.

Примечание. Это означает, что в пункте контекстного меню пиктограммы абонентского пункта "Установить/разорвать соединение" будут отображены названия всех сетевых подключений, которые используют для установления соединения Continent 3 PPP Device.

Создание нового соединения с использованием конфигурационного файла

Если администратор сервера доступа создал нового пользователя абонентского пункта и при этом сформировал конфигурационный файл, пользователь может самостоятельно создать новое соединение на основе настроек, содержащихся в конфигурационном файле.

Внимание! Если абонентский пункт работает в режиме высокого уровня безопасности, приведенная ниже процедура создания нового соединения пользователю недоступна.

Для создания нового соединения:

1. Получите у администратора сервера доступа конфигурационный файл пользователя, включающий в себя настройки подключения и файлы сертификатов с ключевым контейнером, а также пароль доступа к файлу конфигурации.
2. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите пункт "Создать соединение | Применение настроек из файла конфигурации".

   Появится диалог выбора файла конфигурации.
3. Укажите файл, введите пароль доступа к файлу и нажмите кнопку "Далее".

   На экране появится диалог настройки соединения.
4. При необходимости измените имя соединения и удалите отметку в поле "Установить как соединение по умолчанию".

   Если соединение с таким именем уже существует, на экране появится соответствующее сообщение. Для продолжения измените имя соединения.
5. Если подключение к серверу доступа осуществляется через прокси-сервер, укажите имя пользователя и пароль.
6. Нажмите кнопку "Далее".

На экране появится запрос на ввод пароля доступа к ключевому контейнеру пользователя.

7. Введите пароль и при необходимости установите отметку в поле "Запомнить пароль".

   Нажмите кнопку "ОК".

   На экране появится диалог смены пароля на доступ к ключевому контейнеру пользователя.

8. Введите и подтвердите новый пароль и нажмите кнопку "ОК".

   На экране появится окно выбора ключевого носителя.

9. Выберите ключевой носитель, на который будет помещен закрытый ключ пользовательского сертификата, и нажмите кнопку "ОК".

   - Если корневой сертификат на компьютер не устанавливался, на экране появится запрос на его установку.

     Нажмите кнопку "Да".

   На экране появится завершающее окно мастера создания нового соединения. В окне приводятся подробные сведения о настройках соединения, выполненных на основе конфигурационного файла.

10. Для завершения процедуры создания соединения нажмите кнопку "Готово".

Установление соединения с сервером доступа

Перед подключением к серверу доступа пользователь абонентского пункта должен выполнить настройку абонентского пункта, а также зарегистрировать на своем компьютере сертификат пользователя и сертификат корневого центра сертификации. Одновременно абонентским пунктом может быть установлено только одно подключение.

Для ОС Windows 7 и выше. Если используется криптопровайдер "КриптоПро CSP", перед подключением к серверу доступа рекомендуется в настройках ПО криптопровайдера установить значение параметра "Интервал времени ожидания ввода" равным 30 секундам.

Перед подключением к серверу доступа подсоедините к считывателю ключевой носитель с закрытым ключом пользователя.

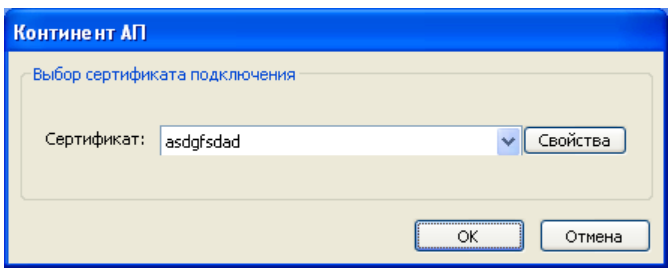
Для установления соединения с сервером доступа:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.

2. В меню "Установить/разорвать соединение" активируйте команду с названием нужного подключения (по умолчанию "Континент-АП").

   На экране появится диалог выбора сертификата.

   Внимание! Данный диалог появляется только в том случае, если при выборе режима аутентификации указано значение "Запрашивать сертификат при подключении" (см. [**1**]).



3. В поле "Сертификат пользователя" в раскрывающемся списке выберите сертификат, соответствующий предъявленному закрытому ключу.

Пояснение. В данном списке указаны действительные сертификаты пользователя, для которых зарегистрирован корневой сертификат. Для просмотра сведений о сертификате нажмите кнопку "Свойства".

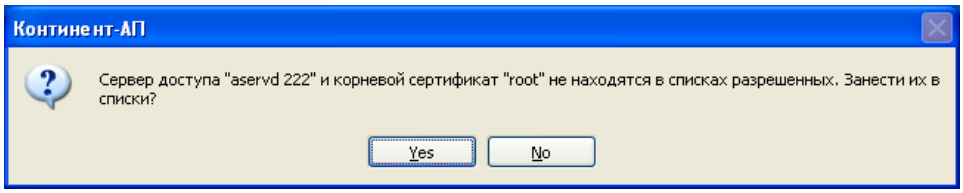
Нажмите кнопку "OK".

На экране будут появляться системные сообщения, оповещающие о ходе подключения.

Примечание. Появление системных сообщений зависит от настроек абонентского пункта.

Если подключение к данному серверу доступа выполняется впервые, на экране появится запрос на добавление сервера доступа в списки разрешенных. Запрос появляется в случае, если в диалоге для настройки свойств протокола проверки подлинности установлена отметка в поле "Запрашивать добавление других серверов и их сертификатов" (см. [**1**]) (запрос не появится, если выбрано подключение, созданное с помощью конфигурационного файла).

Примечание. Если подключение к данному серверу доступа выполняется не впервые и пароль доступа к ключевому контейнеру не был сохранен, на экране появится диалог для ввода пароля. Перейдите к выполнению п. 5 данной процедуры.



Если абонентский пункт работает в режиме высокого уровня безопасности и настройка аутентификации не выполнялась (пустые списки в диалоге свойств протокола проверки подлинности), на экране появится окно предупреждения о необходимости внести сертификат сервера доступа и корневой сертификат в списки разрешенных.

- Запишите названия сертификатов и обратитесь к администратору для настройки аутентификации.

4. Убедитесь в верности имен сервера доступа и его корневого сертификата, отображенных в запросе, и нажмите кнопку "Yes".

   Внимание! При нажатии кнопки "No" подключение к серверу доступа выполнено не будет.

   Имена сервера доступа и корневого сертификата центра сертификации будут включены в списки разрешенных.

   Совет. Для просмотра списков вызовите на экран диалог свойств протокола проверки подлинности (см. [**1**]).

   На экране появится диалог для ввода пароля доступа к ключевому контейнеру.

   Примечание. Если ранее при вводе пароля доступа к данному ключевому контейнеру было отмечено поле "Запомнить пароль" (см. стр.**18**), то этот диалог на экране не появится. Начнется подключение к серверу доступа.
   Срок действия пароля криптопровайдера "Код Безопасности CSP" 180 дней. Если этот срок истек, то на экране появится сообщение с предложением сменить пароль, в противном случае соединение с сервером доступа установлено не будет. Для смены пароля выполняйте указания, появляющиеся на экране.

5. Заполните поля диалога:
   - в поле "Пароль" введите пароль доступа к ключевому контейнеру;
   - в поле "Запомнить пароль":
     - установите отметку, если требуется, чтобы введенный пароль был сохранен в реестре компьютера. В дальнейшем при обращении к этому ключевому контейнеру запрос на ввод пароля выводиться не будет;

- не устанавливайте отметку, если требуется, чтобы запрос на ввод пароля выводился всякий раз при обращении к этому ключевому контейнеру.

6. Нажмите кнопку "ОК".

   В случае успешного подключения цвет пиктограммы абонентского пункта изменится с серого на зеленый.

   Если по истечении 30 секунд пароль не был введен, сервер доступа прерывает установление соединения и выдает сообщение об ошибке аутентификации абонентского пункта. При этом на экране остается диалог для ввода пароля к ключевому контейнеру. Диалог следует закрыть принудительно. В ОС Windows Vista и выше, если установлено значение параметра "Интервал времени ожидания ввода" 30 секунд, диалог закроется автоматически.

Внимание! Если на сервере доступа в настройке "Активные на СД каналы связи" установлено значение "стандартный VPN-канал", при попытке подключения через прокси или по протоколу TCP соединение установлено не будет, и на экране появится стандартное сообщение об ошибке. Проверить настройки на сервере доступа можно с помощью программы управления СД в настройках параметров подключения абонентских пунктов и в настройках свойств пользователя (параметр "Разрешенный канал связи с СД").

Разрыв соединения с сервером доступа

Для разрыва соединения с сервером доступа:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. В меню "Установить/разорвать соединение" активируйте команду "Разорвать соединение Континент-АП".

   Соединение с сервером доступа будет разорвано. На панели Windows исчезнет пиктограмма сетевого подключения.

Удаление соединения

Удаление соединения осуществляется средствами программы управления абонентским пунктом. Пользователям АП, работающего в режиме высокого уровня безопасности, удаление соединения недоступно.

Не рекомендуется удалять средствами ОС Windows соединения, созданные в программе управления абонентским пунктом.

Для удаления соединения:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. Выберите пункт "Удалить соединение".

   Появится список соединений.
3. Выберите удаляемое соединение.

   На экране появится запрос на подтверждение удаления.
4. Нажмите кнопку "Да".

   Соединение будет удалено.

Внимание! Если соединение по каким-либо причинам было удалено средствами ОС Windows, оно по-прежнему будет отображаться в меню программы управления абонентским пунктом и будет доступно только для просмотра настроек. При этом подключение к серверу доступа для данного соединения будет невозможно. Для удаления соединения из меню программы управления необходимо выполнить процедуру, описанную выше. Перед началом процедуры можно просмотреть настройку соединения и настройку аутентификации. Просмотр настройки аутентификации доступен пользователям абонентского пункта, работающего в режиме только низкого или среднего уровня безопасности.

Приложение

Разделение прав пользователей и администраторов АП

Ниже приведены функции и пункты меню управления АП, доступные пользователям в зависимости от их роли в комплексе, соответствующем высокому уровню безопасности.

Функция АП	Пользователь	Администратор
Создание, удаление, изменение соединения с СД	Нет	Да
Создание личного запроса на сертификат и ключевого контейнера	Да	Да
Установка личного пользовательского сертификата в локальное хранилище и связывание с ключевым контейнером	Да	Да
Установка корневого сертификата (цепочки корневых сертификатов) в локальное хранилище доверенных сертификатов	Да	Да
Выбор личного сертификата пользователя для установления соединения с СД	Да	Да
Выбор расширенного сертификата для установления соединения с СД	Нет	Да
Установление соединения АП с СД с личным сертифи-катом или расширенным сертификатом, используемым как сертификат локального компьютера (последнее настраивается администратором)	Да	Да
Регистрация сертификата СД и его корневого в локальной системе (диалог "Настройка аутентификации")	Нет	Да
Установка зависимостей подключений	Нет	Да
Закрытие приложения	Да	Да
Установка, удаление, изменение приложения	Нет	Да
Обновление приложения	Нет	Да
Просмотр журналов	Нет	Да
Архивирование журналов (выполняется средствами Secret Net)	Нет	Да
Восстановление модифицированных ресурсов по эталонам (выполняется средствами Secret Net)	Нет	Да
Проведение и просмотр отчета КЦ	Нет	Да
Настройка работы АП	Нет	Да

Пункт меню АП	Пользователь	Администратор
Подключить <Название соединения>	Да	Да
Выбор соединения по умолчанию	Да	Да
Выбор криптопровайдера по умолчанию	Да	Да
Установить/Разорвать соединение	Да	Да
Создать новое соединение	Нет	Да
Удалить соединение	Нет	Да
Настройка соединения	Нет	Да

Пункт меню АП	Пользователь	Администратор
Настройка аутентификации	Нет	Да
Настройка зависимости между соединениями	Нет	Да
Журнал	Нет	Да
Сертификаты/Создать запрос на пользовательский сертификат	Да	Да
Сертификаты/Установить сертификат пользователя	Да	Да
Загружать автоматически	Нет	Да
Поддержка модемного соединения	Да	Да
Настройка автоматического обновления	Нет	Да
Справка	Да	Да
О программе	Да	Да
Выход	Да	Да

Документация

1.	Средство криптографической защиты информации "Континент-АП". Руководство администратора. Windows
2.	Средство криптографической защиты информации "Континент-АП". Руководство пользователя. Windows