Код безопасности
ГК «Информзащита»

Средство криптографической защиты информации

Континент-АП
Версия 3.5

Руководство пользователя
Абонентский пункт

УВАЛ. 00300-99 92



© Компания "Код Безопасности", 2011. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес:	**127018, г. Москва, ул. Сущевский вал, дом 47, стр. 2, помещение №1**
Телефон:	**(495) 980-23-45**
Факс:	**(495) 980-23-45**
e-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Версия: 3.5 Последнее обновление: 31.03.11

Оглавление

Введение **4**

Глава 1. Общие сведения **6**
Что следует знать 6
Что необходимо иметь 6
Что нужно сделать 7
Что важно помнить 7

Глава 2. Установка, переустановка и удаление **8**
Требования к аппаратному и программному обеспечению 8
Установка Абонентского пункта 8
Изменение, исправление и удаление Абонентского пункта 11
Изменение Абонентского пункта 12
Исправление Абонентского пункта 12
Удаление Абонентского пункта 12
Переустановка Абонентского пункта 13
Обновление версии Абонентского пункта 13
Загрузка обновления 13
Установка обновления 14

Глава 3. Настройка параметров **16**
Вызов меню управления Абонентским пунктом 16
Выбор режима запуска Абонентского пункта 17
Запуск Абонентского пункта вручную 17
Выбор режима работы Абонентского пункта 17
Настройка параметров сетевого подключения 18
Настройка аутентификации 21
Вызов диалога свойств протокола проверки подлинности 21
Формирование списков разрешенных сертификатов 21
Настройка запроса на добавление сертификатов в списки разрешенных 21
Отмена сертификата по умолчанию 21
Настройка времени ожидания ответа от сервера доступа 22
Настройка автоматической проверки обновления 23
Выход из программы 23

Глава 4. Управление сертификатами **24**
Общие сведения о сертификатах 24
Получение пользователем сертификатов 24
Создание запроса на получение сертификата пользователя 25
Регистрация сертификатов 28
Регистрация сертификатов при подключении к серверу доступа 30
Просмотр сведений о сертификатах 31
Просмотр сертификата пользователя 31
Просмотр корневого сертификата 31
Резервное копирование сертификатов 32

Глава 5. Соединение с сервером доступа **33**
Об устанавливаемых соединениях 33
Установка соединения с сервером доступа 33
Разрыв соединения с сервером доступа 35

Глава 6. Регистрация событий **36**
Просмотр событий 36

Приложение **37**
Перечень регистрируемых событий 37

Документация **39**

Предметный указатель **40**

Введение

Данное руководство предназначено для пользователей изделия "Средство криптографической защиты информации "Континент-АП" (далее — Комплекс или Абонентский пункт). В нем содержатся сведения, необходимые пользователю для установки, настройки и эксплуатации программного обеспечения Комплекса.

Материал руководства организован следующим образом:

- **Глава 1** содержит общие сведения об организации удаленного доступа к ресурсам корпоративной сети, защищенной средствами АПКШ "Континент". В ней также рассматриваются организационные вопросы, которые должны быть решены до начала работы в защищенной среде.
- В **Главе 2** описаны процедуры установки, переустановки и удаления Абонентского пункта.
- **Глава 3** содержит необходимые сведения о настройке Абонентского пункта.
- В **Главе 4** описывается работа с сертификатами.
- В **Главе 5** рассказано, как установить соединение с сервером доступа.
- **Глава 6** содержит сведения о регистрации происходящих событий.
- **Приложение** содержит перечень регистрируемых событий.

Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие источники информации заключены в квадратные скобки и выглядят так: [**1**].

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.



- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Некоторые примечания могут и не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru и hotline@infosec.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте http://www.itsecurity.ru/. Связаться с представителем учебного центра можно по электронной почте (edu@infosec.ru).

Соглашения о терминах. Смысл основной части терминов объясняется при первом их употреблении в тексте руководства.

Термины, используемые для описания работы с мышью:

Для того чтобы...	Необходимо...
Выбрать с помощью мыши	Совместите указатель мыши с нужным объектом, а затем нажмите и отпустите левую кнопку мыши
Активировать	Выберите на экране объект, сделав его активным
Дважды нажать левую кнопку мыши	Дважды с коротким промежутком нажмите и отпустите левую кнопку мыши
Нажать	Совместите указатель мыши с объектом на экране и нажмите левую кнопку мыши
Перетащить	Совместите указатель мыши с объектом на экране, нажмите левую кнопку и, продолжая удерживать кнопку нажатой, переместите указатель в нужное положение
Вызвать контекстное меню	Подведите к объекту на экране указатель мыши и нажмите кнопку мыши (допускается нажатие как левой, так и правой кнопки)
Активировать команду меню	Вызовите меню, установите указатель мыши на нужную команду меню и нажмите левую кнопку мыши

Термины, используемые при описании элементов интерфейса:

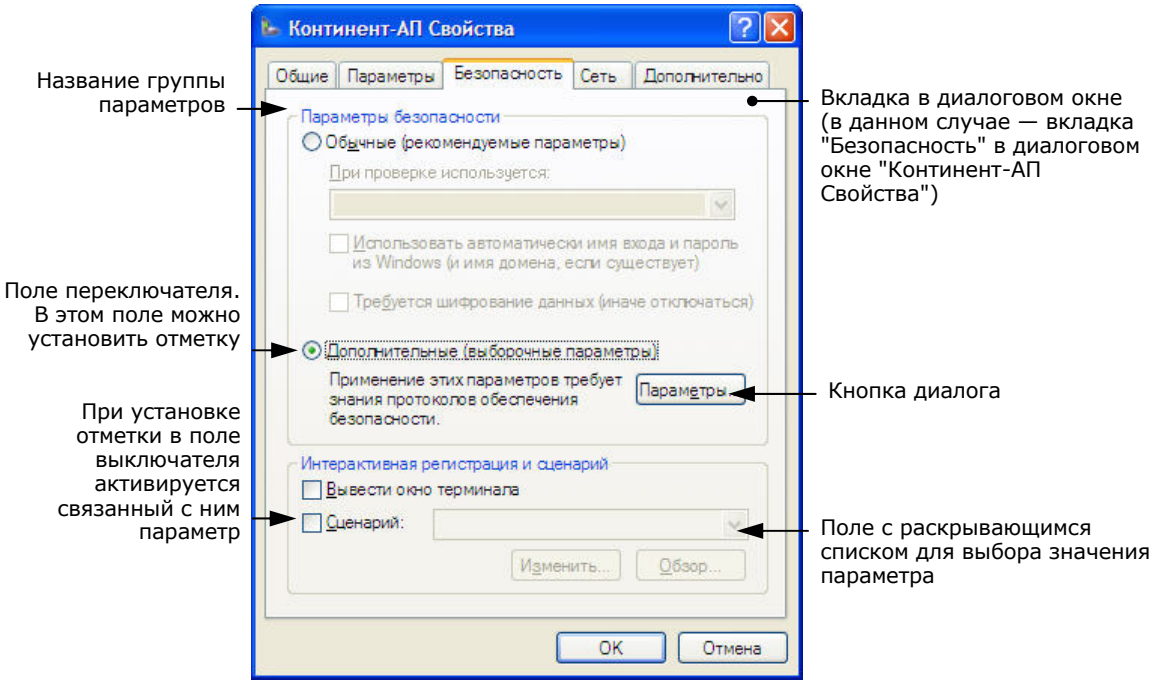


Рис. 1. Пример диалогового окна

При заполнении текстовых полей. Если при вводе имени или пароля была неправильно нажата какая-либо клавиша, удалите ошибочно набранные символы в строке ввода с помощью клавиши <Backspace> или <Delete> и заново повторите ввод символов.

При вводе пароля. Поле для ввода пароля также является текстовым. Однако на экране вместо символа, соответствующего каждой нажатой клавише, появится символ "*" (звездочка). При вводе пароля следует помнить, что строчные и заглавные буквы различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.

Глава 1
Общие сведения

Что следует знать

С внедрением в повседневную работу различных средств обмена информацией в электронном виде актуальной становится проблема обеспечения ее конфиденциальности, целостности и авторства.

Изделие "Аппаратно-программный комплекс шифрования (АПКШ) "Континент" предназначено 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.

АПКШ "Континент" включает в свой состав компоненты, обеспечивающие удаленный доступ пользователей к ресурсам защищенной корпоративной сети с компьютеров, не входящих в защищаемые сегменты сети. На этих компьютерах устанавливается СЗИ "Континент-АП", которое для передачи данных соединяется с компьютером — сервером доступа, проверяющим полномочия на доступ и разрешающим доступ к ресурсам защищенной сети.

Для взаимодействия Абонентского пункта и сервера доступа используются следующие сертификаты:

- 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.



Внимание! С 1 января 2008 года запрещается использовать сертификаты, изданные в соответствии с ГОСТ Р 34.10-94.

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 сертификат пользователя и носитель с закрытым ключом этого сертификата.

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

3 Необходимо иметь установочный комплект программного обеспечения Абонентского пункта.

Что нужно сделать

Для ввода в эксплуатацию Абонентского пункта:

1. Установите и настройте криптопровайдер КриптоПро CSP (в частности, необходимо, чтобы в КриптоПро CSP был настроен датчик случайных чисел). Процедуры установки и настройки подробно рассматриваются в эксплуатационной документации на данный программный продукт.

2. Установите программное обеспечение Абонентского пункта. Процедура установки подробно рассматривается на стр. 8.

3. Получите у администратора безопасности сертификаты, необходимые для работы. Для получения сертификата пользователя, возможно, потребуется создать файл запроса (см. стр. 25) и передать его администратору.

4. Зарегистрируйте полученные сертификаты. Эта процедура подробно рассматривается на стр. 28.

5. Настройте параметры соединения с сервером доступа (см. стр. 18).

6. Установите соединение с сервером доступа (см. стр. 33) 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.

Глава 2
Установка, переустановка и удаление

Программное обеспечение Абонентского пункта поставляется на компакт-дисках. В комплект поставки входит программный продукт компании "КРИПТО-ПРО" КриптоПро CSP.

Перед установкой Абонентского пункта убедитесь, что компьютер удовлетворяет всем требованиям, предъявляемым к аппаратному и программному обеспечению.

Требования к аппаратному и программному обеспечению

Абонентский пункт предназначен для использования на компьютерах, оснащенных процессорами семейства Intel X86 или совместимыми с ними. Требования к конфигурации компьютеров приведены в Табл. 1.

Табл. 1. Требования к конфигурации компьютера

Элемент	Минимально	Рекомендуется
Процессор	Celeron 300 МГц	Pentium IV 1,8 ГГц
Оперативная память	128 Мб	512 Мб
Жесткий диск (свободное пространство)	512 Мб	512 Мб
Операционная система	Windows 2000 Professional 32 bit SP4, Update RollUp 1 for Windows 2000 SP4 (KB891861), MS04-011 (KB835732); или Windows XP 32 bit SP3; или Windows Vista 32 bit SP2	
Установленное ПО	КриптоПро CSP версии 3.0.3293 и выше для Windows 2000 Professional и Windows XP Professional, КриптоПро CSP версии 3.6 для Windows Vista, MS Internet Explorer версии 6.0 или выше	

На компьютере должны быть установлены компоненты операционной системы, обеспечивающие работу с сетевыми протоколами TCP/IP.

Пропускная способность сетевого канала, по которому устанавливается соединение абонентского пункта с сервером доступа, должна быть не менее 9.6 Кбит/с.



Внимание! Компьютер, на который устанавливают Абонентский пункт, должен содержать средства, обеспечивающие контроль целостности программного обеспечения (например, ПАК "Соболь").

При использовании Абонентского пункта совместно с ПАК "Соболь", а также с криптопровайдером КриптоПро CSP необходимо перед установкой Абонентского пункта установить эти аппаратные и программные продукты согласно эксплуатационной документации на них, а также настроить КриптоПро CSP на использование аппаратного датчика случайных чисел ПАК "Соболь". В случае если ПАК "Соболь" не используется, требуется настроить любой другой датчик случайных чисел, например, биологический.

Установка Абонентского пункта

После установки Абонентского пункта все работающие сетевые подключения будут автоматически разорваны.

Для установки Абонентского пункта:

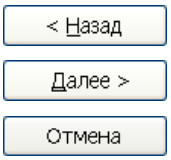
1. Войдите в систему с правами администратора компьютера.

   Примечание. Правами администратора компьютера обладает пользователь, входящий в локальную группу администраторов.

2. Завершите работу всех приложений, выполняющихся на компьютере.
3. Поместите установочный диск в устройство чтения компакт-дисков и запустите на исполнение файл Setup.exe, находящийся в каталоге с дистрибутивом Абонентского пункта, путь к которому указан в документе Release Notes.

Совет. Для установки Абонентского пункта с жесткого диска скопируйте файлы с установочного диска в любой рабочий каталог (локальный или сетевой) и запустите на исполнение файл Setup.exe.

Программа установки начнет выполнение подготовительных действий, и на экране появится сообщение об этом. После завершения подготовительных действий на экран будет выведен стартовый диалог мастера установки.



Совет. Для управления процессом установки используйте кнопки:

- "Назад" — для возврата к предыдущему диалогу;
- "Далее" — для перехода к следующему диалогу;
- "Отмена" — для прекращения процесса установки. После нажатия этой кнопки подтвердите свое решение в появившемся окне запроса.

4. Нажмите кнопку "Далее >" для продолжения установки.

   На экране появится диалог, содержащий лицензионное соглашение на использование программного продукта.

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



Внимание! Если вы не согласны с условиями лицензионного соглашения, поставьте отметку в поле "Я не принимаю условия лицензионного соглашения" и нажмите кнопку "Отмена". Установка Абонентского пункта будет прекращена.

   На экране появится диалог выбора папки для размещения файлов программы.

   По умолчанию программа установки копирует файлы в каталог \ Program Files \ SecurityCode \ ClientContinent. Для установки программы в другую папку нажмите кнопку "Изменить..." и укажите нужную папку в открывшемся диалоге.

6. Нажмите кнопку "Далее >".

   На экране появится диалог для выбора вида установки.

7. Определите вид установки (количество устанавливаемых компонентов):

   - "Полная" — для установки Абонентского пункта и межсетевого экрана (МСЭ);
   - "Выборочная" — для возможности установки Абонентского пункта без МСЭ (см. Рис. 5 на стр. 12).

Примечание. МСЭ — это компонент Абонентского пункта, обеспечивающий фильтрацию IP-пакетов сетевого трафика компьютера, на котором установлен Абонентский пункт. Рекомендуется установка Абонентского пункта с МСЭ. Для отключения установки пакетного фильтра выберите вариант "Выборочная". Подробные сведения о МСЭ содержатся в документе "Средство защиты информации "Континент-АП". Межсетевой экран. Руководство администратора".

8. Нажмите кнопку "Далее >".

   На экране появится диалог для ввода IP-адреса сервера доступа.

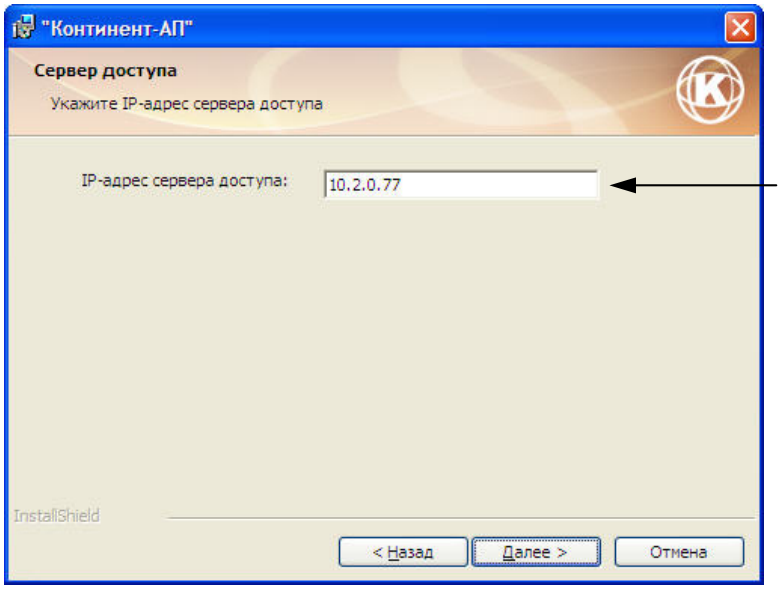


Рис. 2. Диалог ввода IP-адреса сервера доступа

9. Введите IP-адрес сервера доступа и нажмите кнопку "Далее >".

> **Примечание.** IP-адрес сервера доступа можно уточнить у администратора. В дальнейшем IP-адрес может быть изменен. Если вы не знаете, какое значение следует ввести, то продолжите процедуру установки, оставив значение по умолчанию.

На экране появится диалог с информацией о том, что программа установки готова приступить к установке.

10. Проверьте правильность значений, введенных в предыдущих диалогах, и нажмите кнопку "Установить".

Программа установки приступит к копированию файлов.

> В процессе установки на экране будут появляться сообщения о том, что устанавливаемое программное обеспечение не тестировалось на совместимость с операционной системой. В окне таких сообщений следует нажимать кнопку "Все равно продолжить".
>
> В ОС Vista для предотвращения появления таких сообщений установите отметку в поле "Always trust software from "Security Code Ltd".

Сообщения, появляющиеся на экране, отображают этапы процесса установки.

> Если по какой-то причине отсутствует какой-либо из файлов, входящих в комплект поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. В этом случае проверьте компьютер на наличие вирусов и повторите установку. Если в дальнейшем данная ошибка будет повторяться, обратитесь к поставщику Комплекса.

По окончании процесса копирования на экране появится заключительное окно мастера установки.

11. Нажмите кнопку "Готово".

На экране появится запрос на перезагрузку компьютера. Выберите вариант завершения установки:

- для немедленной перезагрузки компьютера и начала работы с Абонентским пунктом нажмите кнопку "Да";
- для продолжения работы без перезагрузки компьютера нажмите кнопку "Нет". В этом случае работа с Абонентским пунктом будет возможна только после окончания сеанса работы и перезагрузки компьютера.

> Если до установки Абонентского пункта были установлены какие-либо сетевые подключения, то они будут разорваны, а на экране появится соответствующее сообщение. Восстановление сетевых подключений будет возможно только после перезагрузки компьютера.

После установки Абонентского пункта и перезагрузки компьютера:

- в элементе управления Windows "Панель управления \ Сетевые подключения" появится новое сетевое подключение "Континент-АП";
- в меню "Все программы" главного меню Windows появится подменю "Код Безопасности \ Абонентский Пункт Континент", которое содержит пункты "Программа управления", "Проверка контрольных сумм";
- на панели задач Windows появится пиктограмма Абонентского пункта.



Пиктограмма Абонентского пункта

Изменение, исправление и удаление Абонентского пункта

Изменение, исправление и удаление Абонентского пункта выполняются из специального диалога обслуживания программы.

Для вызова диалога обслуживания программы:

1. Нажмите кнопку "Пуск" и в главном меню Windows найдите и активируйте команду "Панель управления".
2. В окне "Панель управления" активируйте элемент "Установка и удаление программ".

   На экране появится диалог "Установка и удаление программ".

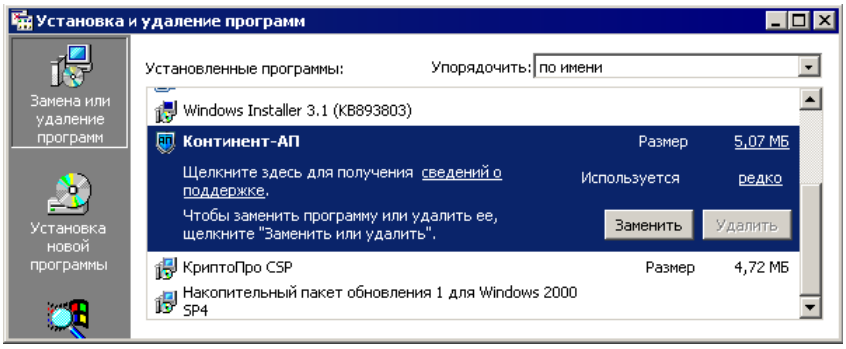


Рис. 3. Диалог "Установка и удаление программ"

3. Выберите в списке установленных программ элемент "Континент-АП" и нажмите кнопку "Изменить".

   После выполнения подготовительных действий на экране появится стартовое окно программы удаления.

4. Нажмите кнопку "Далее >".

   На экране появится диалог обслуживания программы.

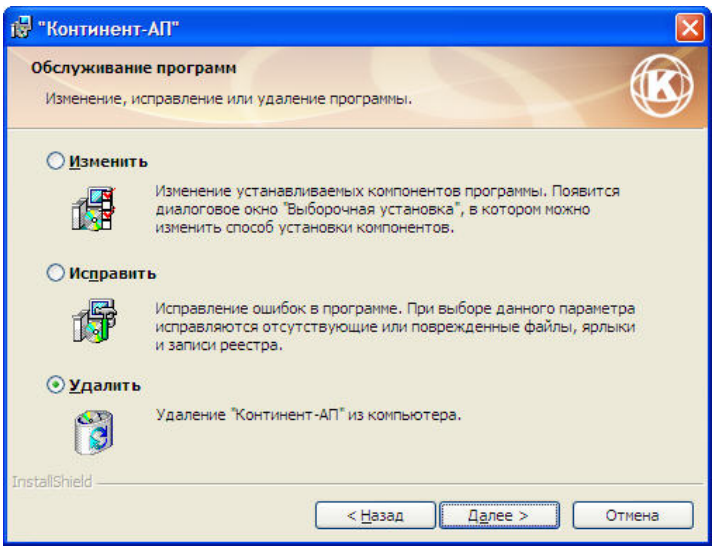


Рис. 4. Диалог обслуживания программы

Изменение Абонентского пункта

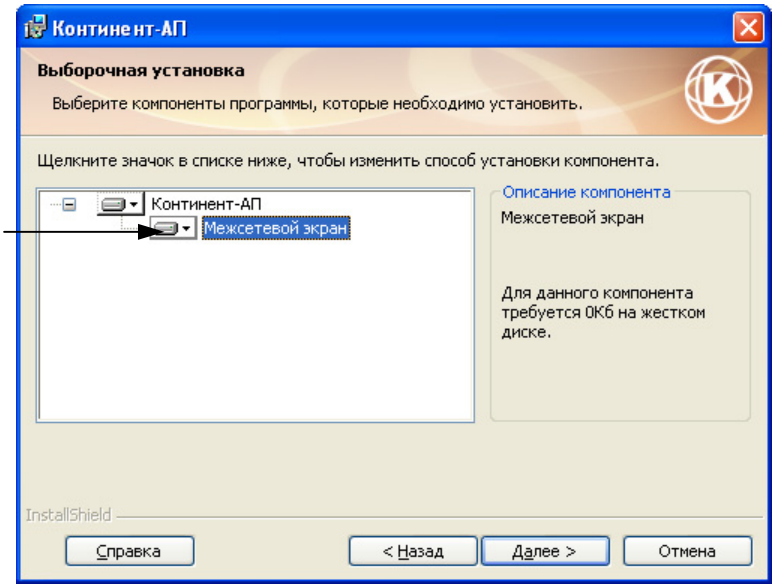
Изменение Абонентского пункта выполняется, если необходимо изменить набор устанавливаемых компонентов программы. Например, если при первоначальной установке не был установлен МСЭ, то для его установки выполните изменение Абонентского пункта.

Внимание! Перед тем как приступить к изменению Абонентского пункта, вставьте установочный диск в устройство чтения компакт-дисков.

Для изменения Абонентского пункта:

1. Вызовите на экран диалог обслуживания программы (см. выше).
2. Выберите действие "Изменить" и нажмите кнопку "Далее >".

   На экране появится диалог выборочной установки,



Нажмите для вызова раскрывающегося списка с

Рис. 5. Диалог выборочной установки

   По умолчанию МСЭ устанавливается в ту же папку, что и Абонентский пункт.

3. Перейдите к выполнению п. **8** процедуры установки Абонентского пункта (см. стр. 9).

Исправление Абонентского пункта

Исправление программы выявляет и исправляет поврежденные файлы, ошибки в реестре и т. д.

Для исправления Абонентского пункта:

1. Вызовите на экран диалог обслуживания программы (см. стр. 11).
2. Выберите действие "Исправить" и нажмите кнопку "Далее >".
3. Перейдите к выполнению п. **8** процедуры установки Абонентского пункта (см. стр. 9).

Удаление Абонентского пункта

Для удаления Абонентского пункта:

1. Вызовите на экран диалог обслуживания программы (см. стр. 11).
2. Выберите действие "Удалить" и нажмите кнопку "Далее >".

   На экране появится диалог для подтверждения удаления. По умолчанию в поле "Удалить также все соединения, использующие виртуальный адаптер Континент" установлена отметка. Это означает, что одновременно с удалением программы будут удалены все соединения, использующие виртуаль-

ный адаптер Continent 3 PPP Adapter. Для того чтобы после удаления Абонентского пункта такие соединения сохранились, удалите отметку в этом поле.

3. Нажмите кнопку "Удалить".

   Программа удаления приступит к удалению файлов. По завершении процесса удаления на экране появится сообщение о необходимости перезагрузки компьютера.

4. Выберите вариант завершения удаления:
   - отметьте поле "Да, перезагрузить компьютер сейчас" для немедленной перезагрузки компьютера;
   - отметьте поле "Нет, перезагрузить компьютер позже", чтобы продолжить работу без перезагрузки компьютера.

Переустановка Абонентского пункта

Переустановка Абонентского пункта обычно выполняется в следующих случаях:

- после неудачного завершения установки;
- при нарушении работоспособности программного обеспечения;
- при обновлении программного обеспечения версии ниже 3.2.

Для переустановки Абонентского пункта:

1. Удалите Абонентский пункт с компьютера (см. стр. 12).
2. Установите Абонентский пункт на компьютер (см. стр. 8).

Обновление версии Абонентского пункта

Сведения, представленные в данном разделе, предназначены для обновления программного обеспечения абонентских пунктов версии 3.2 и выше. Для обновления абонентских пунктов версии ниже 3.2 требуется полная переустановка программного обеспечения (см. предыдущий раздел).

- Пользователь, выполняющий обновление, должен входить в локальную группу администраторов компьютера.
- В процессе обновления Абонентского пункта МСЭ не устанавливается.
- После обновления Абонентского пункта все работающие сетевые подключения будут автоматически разорваны.

Файлы обновления поставляются запакованными в самораспаковывающийся архивный файл SetupAP.exe. Обновление версии Абонентского пункта выполняют в следующем порядке:

1. Загрузка файлов обновления на компьютер.
2. Извлечение файлов обновления из архива.
3. Установка обновления на компьютер.

Загрузка обновления

Архивный файл с обновлением можно получить у администратора комплекса или загрузить самостоятельно.

Для автоматической проверки наличия обновлений нужно включить и настроить одноименный режим (см. стр. 23). В этом случае при каждом запуске Абонентского пункта происходит обращение к адресу, указанному в настройках программы. Если по указанному адресу обнаруживаются файлы дистрибутива новой версии Абонентского пункта, на экран выводится окно с уведомлением.

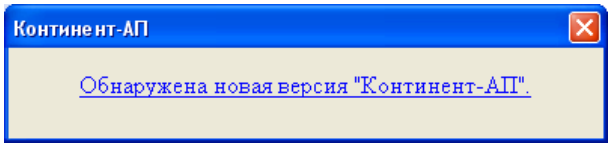


Рис. 6. Уведомление о наличии обновления

Для загрузки обновления на компьютер:

1. Активируйте ссылку в появившемся окне уведомления.

   На экране появится диалог самораспаковывающегося архива.

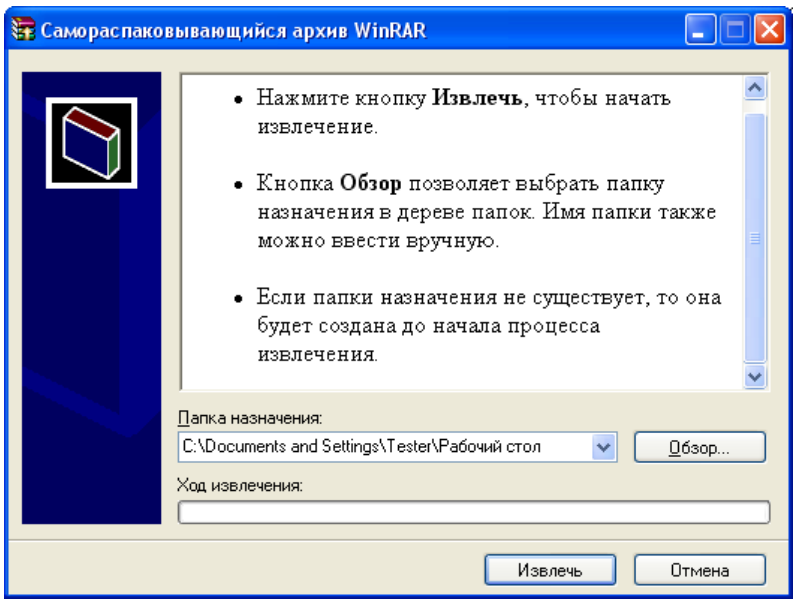


Рис. 7. Диалог самораспаковывающегося архива

2. Укажите папку назначения и нажмите кнопку "Извлечь".

   Файлы обновления будут извлечены из архива и сохранены в указанной папке.

Установка обновления

Для установки обновления на компьютер:

1. Войдите в систему с правами администратора компьютера.

   Примечание. Правами администратора компьютера обладает пользователь, входящий в локальную группу администраторов.

2. Завершите работу всех приложений, выполняющихся на компьютере.
3. Запустите на исполнение файл Setup.exe, извлеченный из архивного файла с обновлением (см. предыдущий подраздел).

   На экране появится диалог для подтверждения обновления.

4. Нажмите кнопку "Да".

   Программа начнет выполнение подготовительных действий, и на экране появится сообщение об этом. После завершения подготовительных действий на экран будет выведен стартовый диалог мастера обновления.

5. Нажмите кнопку "Далее >" для подтверждения обновления.

   Программа приступит к обновлению версии продукта.

   В процессе обновления на экране будут появляться сообщения о том, что устанавливаемое программное обеспечение не тестировалось на совместимость с операционной системой. В окне таких сообщений следует нажимать кнопку "Все равно продолжить".

   Сообщения, появляющиеся на экране, отображают этапы процесса установки.

   Если по какой-то причине отсутствует какой-либо из файлов, входящих в комплект поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. В этом случае проверьте компьютер на наличие вирусов и повторите установку. Если в дальнейшем данная ошибка будет повторяться, обратитесь к поставщику Комплекса.

   По окончании процесса копирования на экране появится заключительный диалог мастера установки.

6. Нажмите кнопку "Готово".

На экране появится запрос на перезагрузку компьютера.

7. Выберите вариант завершения обновления:

- нажмите кнопку "Да" для немедленной перезагрузки компьютера и начала работы с Абонентским пунктом;
- нажмите кнопку "Нет", чтобы продолжить работу без перезагрузки компьютера. В этом случае работа с Абонентским пунктом будет возможна только после окончания сеанса работы и перезагрузки компьютера.

Если до обновления версии Абонентского пункта были установлены какие-либо сетевые подключения, то они будут разорваны, а на экране появится соответствующее сообщение. Восстановление сетевых подключений будет возможно только после перезагрузки компьютера.

Глава 3
Настройка параметров

Вызов меню управления Абонентским пунктом

Управление Абонентским пунктом выполняется с помощью специального меню.

Для вызова меню управления Абонентским пунктом:



Пиктограмма Абонентского пункта

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

  На экране появится меню управления Абонентским пунктом.

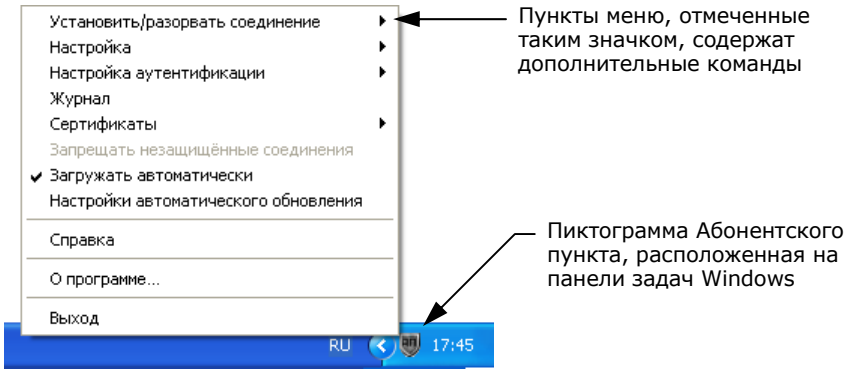


Рис. 8. Меню управления Абонентским пунктом

Пояснение. Цвет пиктограммы Абонентского пункта указывает на наличие или отсутствие соединения с сервером доступа:

- серый — соединение не установлено;
- синий — соединение установлено.

Табл. 2. Команды меню управления Абонентским пунктом

Команда	Описание
Установить/разорвать соединение	Запускает процедуру установки или разрыва выбранного в подменю подключения
Настройка	Вызывает на экран диалог настройки для выбранного в подменю подключения. **Внимание!** Изменение настроек соединения, выполненное с помощью этой команды, приведет к изменению настроек аутентификации всех пользователей Абонентского пункта. В ОС Windows Vista эта команда доступна только пользователю, обладающему правами локального администратора. Остальным пользователям для выполнения команды необходимо ввести пароль администратора.
Настройка аутентификации	Вызывает на экран диалог свойств протокола проверки подлинности для выбранного в подменю подключения
Журнал	Вызывает на экран окно просмотра событий
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
Запрещать незащищенные соединения	Включает/выключает режим запрета незащищенных соединений
Загружать автоматически	Включает/выключает режим автоматического запуска Абонентского пункта при запуске Windows

Команда	Описание
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

Выбор режима запуска Абонентского пункта

После установки Абонентского пункта и перезагрузки компьютера на панели задач Windows появится пиктограмма Абонентского пункта. Пользователь может выбрать дальнейший режим запуска Абонентского пункта:

- автоматический режим — Абонентский пункт будет запускаться одновременно с запуском Windows (установлен по умолчанию);
- ручной режим — Абонентский пункт запускается пользователем вручную.

Для выбора режима запуска:

1. Вызовите контекстное меню пиктограммы Абонентского пункта, расположенной на панели задач Windows.
2. Выберите режим запуска Абонентского пункта:
   - для включения автоматического режима установите отметку слева от параметра "Загружать автоматически";
   - для включения ручного режима удалите отметку слева от параметра "Загружать автоматически".

   Выбранный режим вступит в действие при следующем запуске программы.

Запуск Абонентского пункта вручную

Для запуска Абонентского пункта вручную:

- В главном меню Windows активируйте команду "Все Программы \ Код Безопасности \ Абонентский Пункт Континент \ Программа управления".

  Абонентский пункт будет запущен. На панели задач Windows появится пиктограмма Абонентского пункта.

Выбор режима работы Абонентского пункта

Режим работы Абонентского пункта определяется на сервере доступа. Администратор сервера доступа может разрешить или запретить пользователю во время работы Абонентского пункта незащищенные (без шифрования трафика) соединения с абонентами, не входящими в защищенную сеть. Администратор может также оставить выбор этого режима на усмотрение пользователя Абонентского пункта.

Если администратор сервера доступа оставил выбор режима работы на усмотрение пользователя, то можно выбрать один из двух режимов работы Абонентского пункта:

- режим запрета незащищенных соединений — в этом режиме на время сеанса связи Абонентского пункта и сервера доступа будут запрещены любые соединения, кроме соединений через данный сервер;



Внимание! Рекомендуется запрещать незащищенные соединения.

- режим разрешения незащищенных соединений — в этом режиме во время сеанса связи Абонентского пункта и сервера доступа любые другие соединения разрешены.

Выбор режима работы Абонентского пункта можно осуществить только при установленном соединении с сервером доступа.

Для выбора режима работы Абонентского пункта:

1. Установите соединение Абонентского пункта с сервером доступа (см. стр. 33).
2. Вызовите контекстное меню пиктограммы Абонентского пункта, расположенной на панели задач Windows.



Пиктограмма Абонентского пункта

3. Выберите режим работы Абонентского пункта:
   - для включения режима запрета незащищенных соединений установите отметку слева от параметра "Запрещать незащищенные соединения" (см. Рис. 8 на стр. 10);
   - для включения режима разрешения незащищенных соединений удалите отметку слева от параметра "Запрещать незащищенные соединения".

Пояснение. Если соединение с сервером доступа не установлено, данный параметр будет недоступен для изменений.

Выбранный режим вступит в действие немедленно.

Настройка параметров сетевого подключения

Перед тем как устанавливать соединение с сервером доступа, необходимо выполнить настройку параметров сетевого подключения, посредством которого устанавливается соединение. Невыполнение рекомендуемых действий может повлечь за собой некорректную работу Абонентского пункта.

Для настройки сетевого подключения:

1. Вызовите контекстное меню пиктограммы Абонентского пункта, расположенной на панели задач Windows.
2. В меню "Настройка" активируйте команду с названием нужного подключения (по умолчанию "Континент-АП").

   На экране появится диалог для настройки выбранного сетевого подключения.

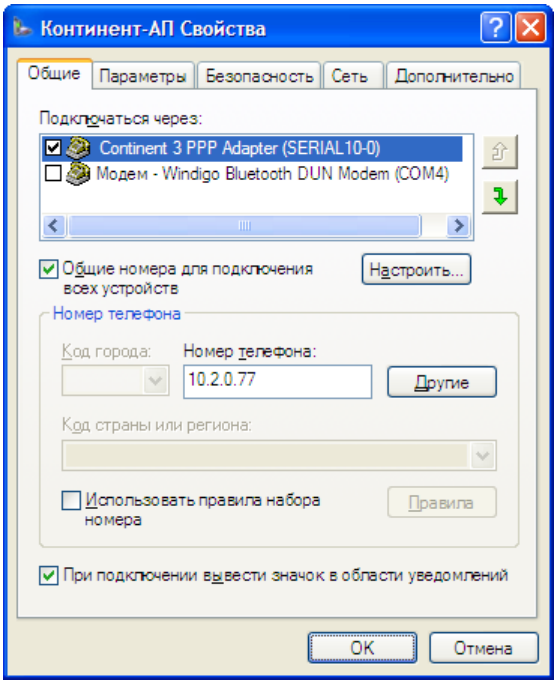


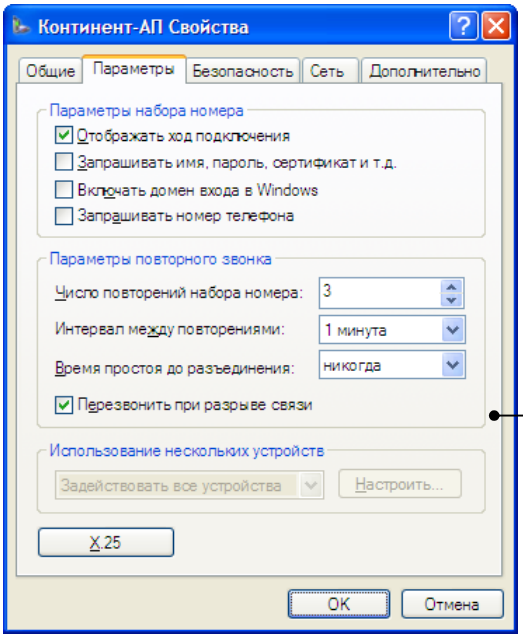
Рис. 9. Настройка общих параметров сетевого подключения

3. На вкладке "Общие" выполните настройку следующих параметров:
   - убедитесь, что в поле "Номер телефона" указан IP-адрес сервера доступа;

     Примечания:

     - По умолчанию в поле "Номер телефона" указан IP-адрес, который был задан при установке Абонентского пункта (см. Рис. 2 на стр. 10). В случае необходимости введите IP-адрес или измените его. IP-адрес сервера доступа можно уточнить у администратора.
     - По умолчанию номер порта сервера доступа, на котором ожидается соединение от Абонентского пункта, имеет значение 4433. Если в программе управления сервера доступа задан другой номер порта, то заданный номер необходимо указать через двоеточие после значения IP-адреса. Например, 10.2.0.77:4434.

   - установите отметку в поле "При подключении вывести значок в области уведомлений" для того, чтобы во время соединения с сервером доступа на панели задач Windows отображалась пиктограмма сетевого подключения.
4. Перейдите к вкладке "Параметры".



На рисунке указаны значения параметров повторного звонка по умолчанию

Рис. 10. Настройка параметров сетевого подключения

5. Установите отметку в поле "Отображать ход подключения", чтобы процесс соединения с сервером доступа отображался на экране.
6. В группе "Параметры повторного звонка" оставьте значения по умолчанию или укажите нужные значения параметров:

Параметр	Описание
Число повторений набора номера	Количество попыток подключения к серверу доступа. Если за указанное число попыток соединение не будет установлено, то на экране появится сообщение об ошибке
Интервал между повторениями	Интервал времени, по прошествии которого необходимо повторить попытку соединения
Время простоя до разъединения	Интервал времени, по прошествии которого следует разорвать соединение с сервером доступа в случае, если установленное соединение не используется для передачи информации. Значение по умолчанию "никогда" означает, что соединение не будет разорвано из-за отсутствия передаваемой информации
Перезвонить при разрыве связи	Если отметка установлена (по умолчанию), то соединение с сервером доступа в случае разрыва связи будет устанавливаться автоматически. Количество попыток соединений в случае разрыва связи указано в поле "Число повторений набора номера"

7. Перейдите к вкладке "Безопасность", установите отметку в поле "Дополнительные" и нажмите кнопку "Параметры".

На экране появится диалог "Дополнительные параметры безопасности".

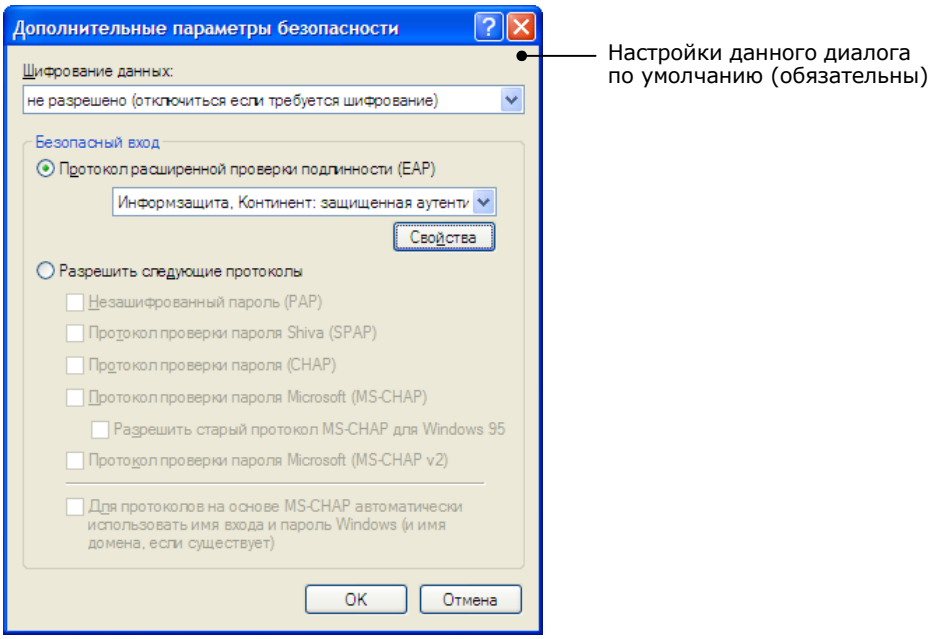


Рис. 11. Дополнительные параметры безопасности

8. В поле "Протокол расширенной проверки подлинности" выберите "Код Безопасности. Континент: защищенная аутентификация" и нажмите кнопку "Свойства".

На экране появится диалог свойств протокола проверки подлинности.

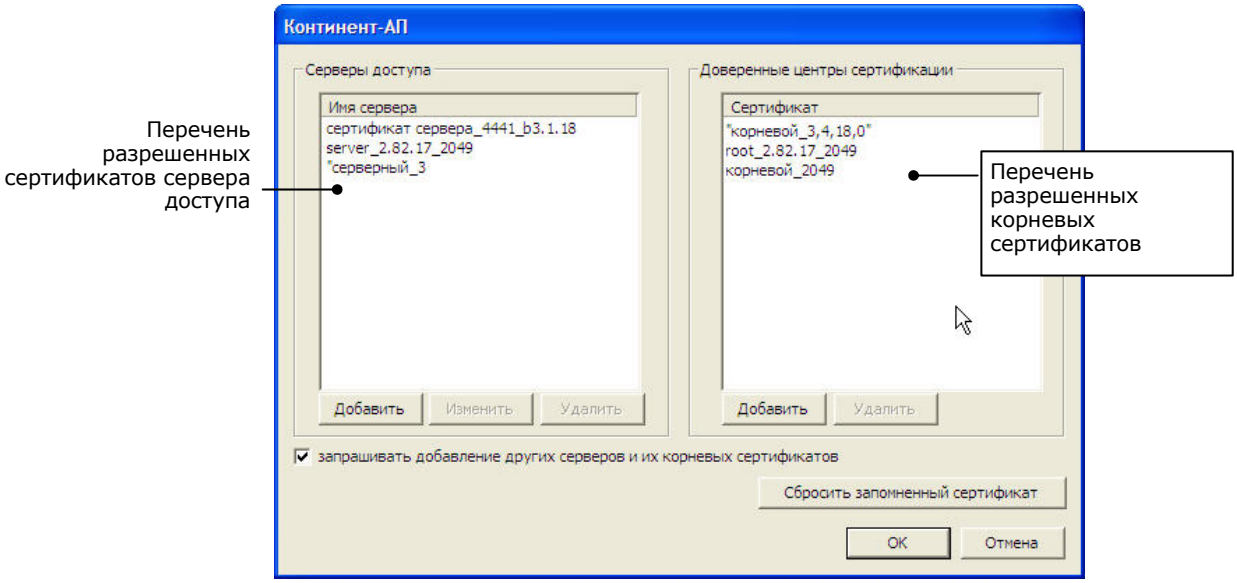


Рис. 12. Свойства протокола проверки подлинности

Примечание. Этот диалог можно также вызвать командой "Настройка аутентификации" контекстного меню пиктограммы Абонентского пункта.

Убедитесь, что в поле "Запрашивать добавление других серверов и их корневых сертификатов" установлена отметка.

Примечание. Если отметка не установлена, то соединение с сервером доступа будет установлено только в том случае, если в списке "Серверы доступа" содержится имя сертификата сервера доступа, а в списке "Доверенные центры сертификации" содержится корневой сертификат, подтверждающий сертификат сервера доступа.

9. Закройте все открытые диалоги. Для подтверждения настроек используйте кнопку "ОК".

Настройка аутентификации

Настройку аутентификации выполняют в диалоге свойств протокола проверки подлинности (см. Рис. 12 на стр. 20). Имеется возможность выполнения следующих настроек:

- просмотр и формирование списка разрешенных сертификатов сервера доступа;
- просмотр и формирование списка сертификатов доверенных центров сертификации;
- отображение/скрытие запроса на добавление сертификата сервера и корневого сертификата в списки разрешенных;
- отмена сертификата по умолчанию.

Вызов диалога свойств протокола проверки подлинности

Для вызова диалога:

- Выберите команду "Настройка аутентификации" контекстного меню пиктограммы Абонентского пункта и в ней активируйте сетевое подключение.

  Появится диалог свойств протокола проверки подлинности (см. Рис. 12 на стр. 20).

Формирование списков разрешенных сертификатов

Добавление имен сертификатов в списки осуществляется автоматически при наличии отметки в поле "Запрашивать добавление других серверов и их корневых сертификатов".

Для ручного формирования списка:

- Используйте кнопки, расположенные под списком. Имя сертификата сервера вводят или корректируют с клавиатуры в текстовом поле. Корневой сертификат выбирают в стандартном диалоге Windows.

Настройка запроса на добавление сертификатов в списки разрешенных

С помощью этой настройки устанавливают порядок первого подключения к серверу доступа: с запросом на добавление сертификатов в списки разрешенных или без запроса.

Данный запрос (см. Рис. 25 на стр. 34) содержит имена сертификата сервера доступа и корневого сертификата. Необходимо убедиться в верности этих имен перед занесением их в списки разрешенных. Если отображение запроса отключено, то при отсутствии сертификатов в списке разрешенных соединение не устанавливается.

Для отображения/скрытия запроса:

- Установите/удалите отметку в поле "Запрашивать добавление других серверов и их корневых сертификатов".

Отмена сертификата по умолчанию

При подключении к серверу доступа можно использовать один из сертификатов пользователя по умолчанию. Сертификат по умолчанию назначается в диалоге выбора сертификата (см. Рис. 23 на стр. 33). После назначения сертификата по умолчанию данный диалог при подключении к серверу доступа не отображается.

Для отмены сертификата по умолчанию:

- В диалоге свойств протокола проверки подлинности нажмите кнопку "Сбросить запомненный сертификат".

При очередном подключении АП к СД диалог выбора сертификата появится на экране.

Настройка времени ожидания ответа от сервера доступа

Пользователь может указать время, по истечении которого будет разорвано соединение Абонентского пункта с сервером доступа в том случае, если сервер неактивен.

Примечание. Данная функция настраивается для эмулятора модема Continent 3 PPP Adapter, посредством которого устанавливается соединение с сервером доступа. По умолчанию это время составляет 1 минуту.

Этот параметр будет действовать для всех соединений, которые можно устанавливать из меню управления Абонентским пунктом, т. е. соединений, указанных в пункте "Установить/разорвать соединение" в контекстном меню пиктограммы Абонентского пункта.

Для изменения времени ожидания ответа от сервера доступа:

1. Вызовите на экран стандартное окно Windows "Диспетчер устройств".

Совет. Для этого нажмите кнопку "Пуск" и в главном меню Windows найдите и активируйте команду "Панель управления". В окне "Панель управления" активируйте элемент "Система". В появившемся диалоге перейдите к вкладке "Оборудование" и нажмите кнопку "Диспетчер устройств".

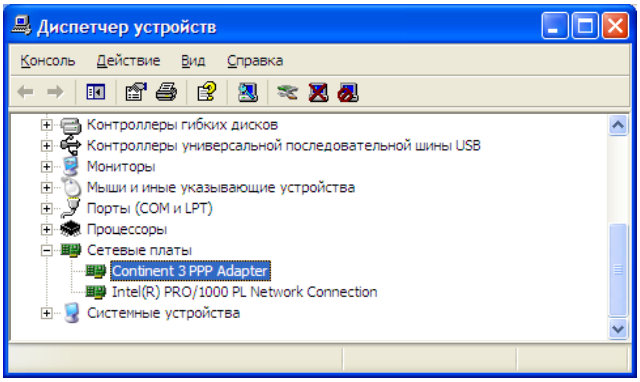


Рис. 13. Окно Windows "Диспетчер устройств"

2. Перейдите к группе устройств "Сетевые платы" и активируйте команду "Свойства" в контекстном меню эмулятора модема Continent 3 PPP Adapter.
3. В появившемся диалоге "Свойства: Continent 3 PPP Adapter" перейдите к вкладке "Дополнительно":

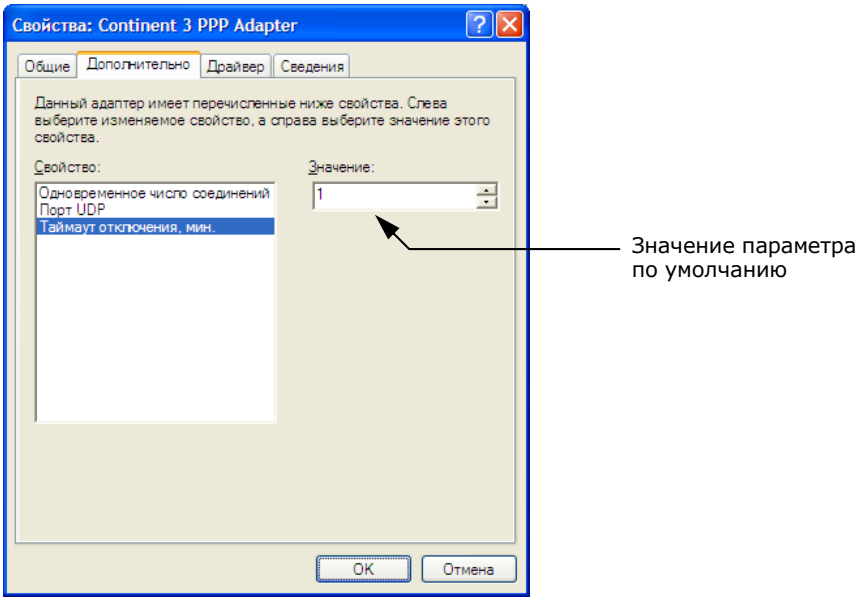


Рис. 14. Дополнительные свойства эмулятора модема

4. В списке "Свойство" выберите значение "Тайм-аут отключения, мин." и в поле "Значение" укажите время ожидания ответа от сервера доступа в минутах.
5. Нажмите кнопку "ОК" для подтверждения изменений.

Настройка автоматической проверки обновления

Автоматическая проверка обновления программного обеспечения Абонентского пункта предусматривает:

- поиск файлов обновления по адресу, заданному пользователем;
- оповещение пользователя о найденных файлах.

Проверка наличия новой версии программного обеспечения производится при каждом запуске Абонентского пункта. По умолчанию режим автоматической проверки выключен.

Для настройки автоматической проверки обновления:

1. Вызовите контекстное меню пиктограммы Абонентского пункта, расположенной на панели задач Windows.
2. Активируйте команду "Настройки автоматического обновления".

   На экране появится диалог настройки автоматической проверки обновления.

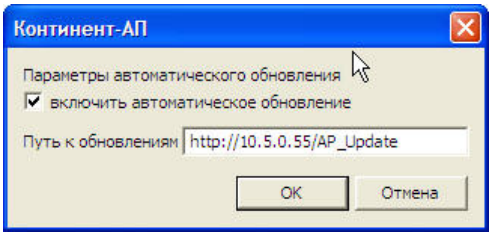


Рис. 15. Настройка автоматической проверки обновления

3. Заполните поля диалога:
   - установите отметку в поле "Включить автоматическое обновление";
   - в поле "Путь к обновлениям" введите путь к папке с обновлениями, расположенной на удаленном сервере (путь можно указывать как для протоколов http, так и для ftp).
4. Нажмите кнопку "ОК".

   Если при очередном запуске Абонентского пункта по указанному адресу будет найдено обновление, то на экране появится сообщение об этом.

Выход из программы

При завершении работы программы управления Абонентским пунктом автоматически разрывается связь между Абонентским пунктом и сервером доступа.

Для выхода из программы:



Пиктограмма Абонентского пункта

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.

Глава 4
Управление сертификатами

Общие сведения о сертификатах

Внимание! С 1 января 2008 года запрещается использовать сертификаты, изданные в соответствии с ГОСТ Р 34.10-94.

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 КриптоПро CSP, установленного на том же компьютере, что и Абонентский пункт. Рекомендуется использовать отчуждаемый ключевой носитель (например, USB Flesh-накопитель).

В зависимости от указаний администратора безопасности пользователь Абонентского пункта может получить сертификаты двумя способами:

- администратор безопасности передает пользователю Абонентского пункта сертификат 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 любым удобным способом.

  От пользователя в этом случае не требуется никаких предварительных действий;

- 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 пользователя и передает его пользователю вместе с сертификатом корневого центра сертификации.

  Примечание. Передача запроса на получение сертификата от пользователя к администратору, а затем сертификатов от администратора к пользователю осуществляется любым удобным способом (например, вложением электронной почты).

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.

Создание запроса на получение сертификата пользователя

Запрос на получение сертификата создается пользователем средствами Абонентского пункта по требованию администратора безопасности. 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 одном из ключевых носителей, указанных в настройках КриптоПро CSP.



Для создания запроса необходимо, чтобы в настройках КриптоПро CSP был настроен датчик случайных чисел.

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

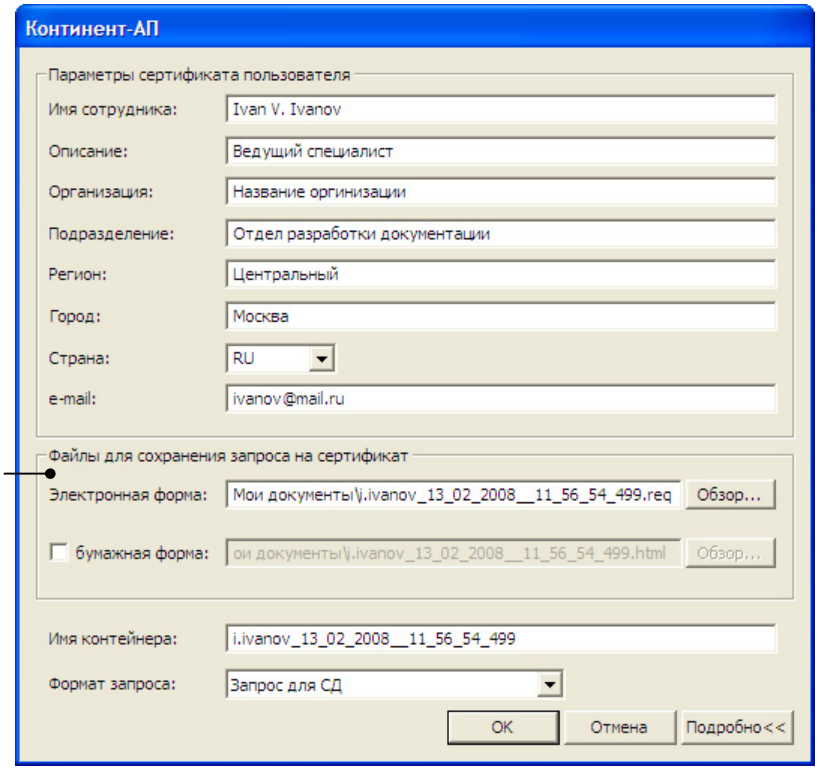
Для создания запроса на получение сертификата:



Пиктограмма Абонентского пункта

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.



Значения группы параметров по умолчанию

Рис. 16. Диалог 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 "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 СА" — формат запроса для создания сертификата внешним центром сертификации.

6. 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)

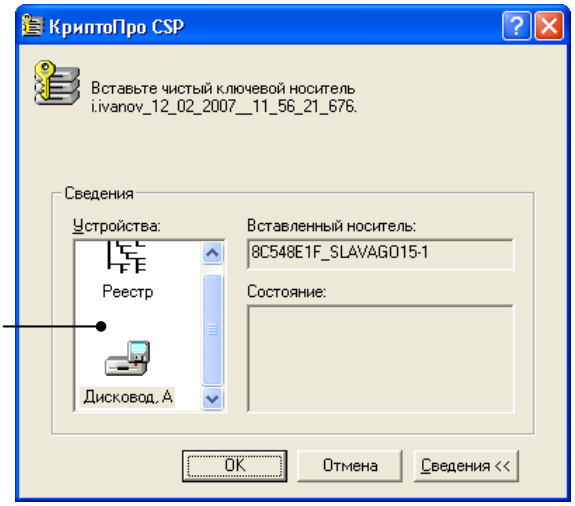


Рис. 17. Запрос ключевого носителя

Примечание. В случае конфигурации КриптоПро CSP с одним видом ключевого носителя данное окно не отображается.

7. В списке "Устройства" выберите устройство для записи ключевой информации и предъявите ключевой носитель.

Если выбрано значение "Дисковод", вставьте в дисковод чистую отформатированную дискету.

8. Нажмите кнопку "OK".

КриптоПро CSP приступит к созданию закрытого ключа сертификата пользователя.

Дальнейший порядок действий зависит от используемого криптопровайдером КриптоПро CSP датчика случайных чисел и ключевого носителя, выбранного для хранения ключевой информации. Следуйте инструкциям, появляющимся на экране.

Подробная информация о настройке и порядке использования КриптоПро CSP содержится в эксплуатационной документации на этот программный продукт.

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

По умолчанию поле не содержит отметку

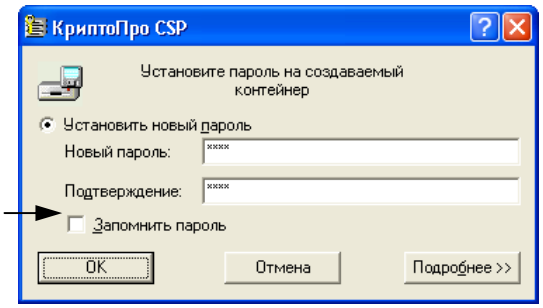


Рис. 18. Диалог КриптоПро CSP для назначения пароля

Пояснение. С помощью этого пароля ограничивается доступ к ключевой информации. Запомните введенный пароль и никому его не сообщайте.

9. Заполните поля диалога:

- в поле "Новый пароль" введите пароль доступа к ключевому контейнеру;

- в поле "Подтверждение" введите тот же пароль;
- 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.

10. Нажмите кнопку "ОК".

На экране появится сообщение о завершении 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.

11. Нажмите кнопку "ОК" в окне сообщения.

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

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 регистрируемого сертификата 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:



Пиктограмма Абонентского пункта

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 пользователя и нажмите кнопку "Открыть".

Примечание. Сертификат, изданный средствами сервера доступа, хранится в файле user.cer.

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

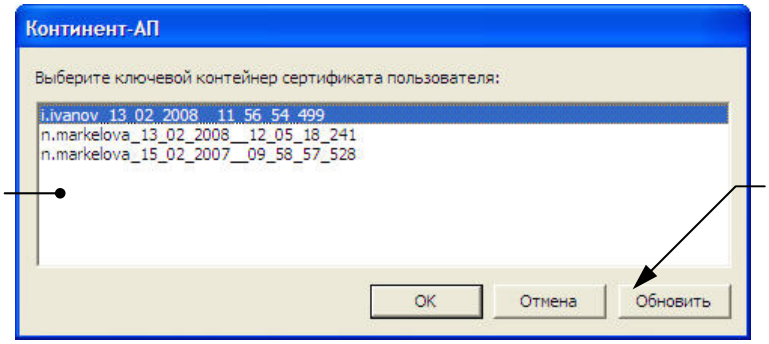


Рис. 19. Диалог выбора ключевого контейнера

4. Выберите нужный ключевой контейнер и нажмите кнопку "ОК".

Пояснение. При нажатии кнопки "Отмена" процедура регистрации сертификатов будет продолжена (сертификаты будут установлены в хранилище сертификатов), но сертификат пользователя не будет связан с закрытым ключом. В дальнейшем подключение к серверу доступа с использованием такого сертификата будет невозможно.

На экране появится запрос пароля доступа к выбранному ключевому контейнеру.

Пояснение. Если регистрируется сертификат, созданный по запросу на получение сертификата средствами Абонентского пункта, и при установке пароля доступа к ключевому контейнеру было отмечено поле "Запомнить пароль" (см. Рис. 18 на стр. 27), то запрос пароля не появится.

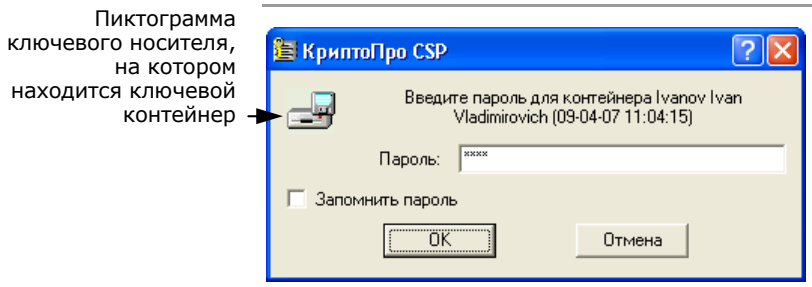


Рис. 20. Диалог ввода пароля

5. Заполните поля диалога:
   - в поле "Пароль" введите пароль доступа к ключевому контейнеру;

     Пояснение. Если регистрируется сертификат, созданный по запросу пользователя на получение сертификата средствами Абонентского пункта, укажите назначенный вами пароль (см. Рис. 18 на стр. 27). Во всех остальных случаях укажите пароль, который сообщил вам администратор при передаче соответствующего ключевого носителя.

   - 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 том случае, если в хранилище сертификатов на компьютере отсутствует корневой сертификат, подтверждающий зарегистрированный сертификат пользователя, на экране появится запрос на его установку.

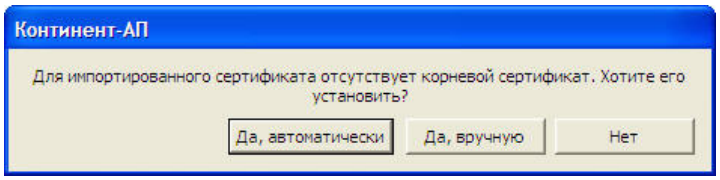


Рис. 21. Запрос на установку корневого сертификата

Пояснение. В том случае, если для зарегистрированного сертификата пользователя уже имеется корневой сертификат, процедура будет завершена и на экране появится сообщение о завершении импорта сертификата пользователя.

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.

Имя корневого сертификата

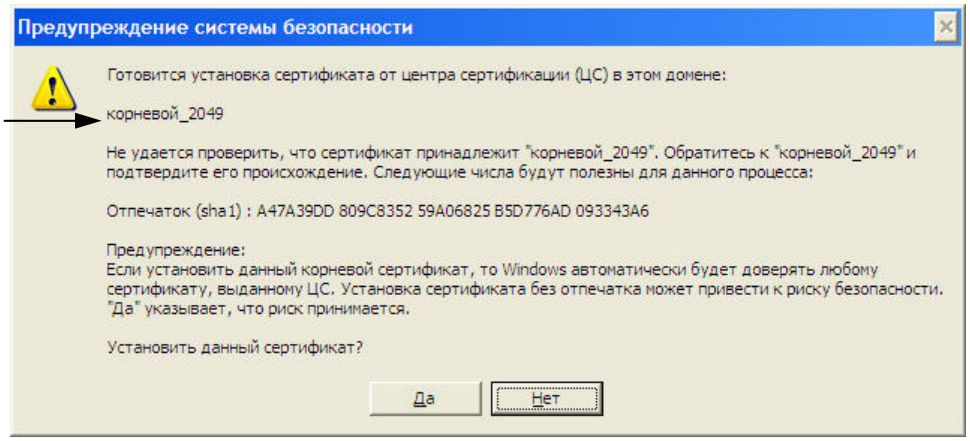


Рис. 22. Предупреждение системы безопасности Windows

8. Нажмите кнопку "Да", если вы согласны зарегистрировать данный сертификат.

   Корневой сертификат будет зарегистрирован. На экране появится сообщение о завершении регистрации сертификата пользователя.

9. Нажмите кнопку "ОК".

Регистрация сертификатов при подключении к серверу доступа

Абонентский пункт предоставляет дополнительную возможность для регистрации сертификатов — сертификаты можно зарегистрировать при установке соединения с сервером доступа.

Для регистрации сертификатов при установке соединения:



Пиктограмма Абонентского пункта

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 (см. Рис. 23 на стр. 33).
3. В поле "Сертификат пользователя" из раскрывающегося списка выберите команду "<Импорт…>.

   На экране появится стандартное диалоговое окно Windows для работы с файлами.
4. Выполните пп. **3**–**9** процедуры регистрации сертификатов (см. выше).

Просмотр сведений о сертификатах

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 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 (см. Рис. 23 на стр. 33).
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 установке первого соединения между Абонентским пунктом и сервером доступа.

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 (см. Рис. 12 на стр. 20).

   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 "Имя сервера" и "Сертификат" могут быть добавлены пользователем самостоятельно, без установки связи с сервером доступа. Для этого в поле "Имя сервера" нажмите кнопку "Добавить", введите имя сертификата сервера и нажмите клавишу "Enter". В поле "Сертификат" 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 "Сертификат".
3. Выберите нужный корневой сертификат и дважды щелкните по нему мышью.

   На экране появится диалоговое окно с информацией о сертификате.

Резервное копирование сертификатов

Резервное копирование сертификата пользователя и сертификата корневого центра сертификации выполняется обычными средствами копирования файлов. При необходимости вы сможете использовать копию корневого сертификата на другом компьютере или на том же компьютере после переустановки операционной системы и программного обеспечения. Для того чтобы использовать подобным образом копию сертификата пользователя, необходимо иметь в наличии ключевой носитель, содержащий ключевую информацию, соответствующую данному сертификату.



Внимание! Физический носитель информации, на котором будут храниться резервные копии файлов сертификатов, должен отличаться от физического носителя, на котором находятся рабочие экземпляры файлов. Иначе при отказе этого носителя будут потеряны и рабочие файлы, и их резервные копии.

Глава 5
Соединение с сервером доступа

Об устанавливаемых соединениях

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

Примечание. Эмулятор модема Continent 3 PPP Adapter устанавливается на компьютер при установке Абонентского пункта.

При установке Абонентского пункта на компьютер автоматически создается сетевое подключение, использующее для установки соединения Continent 3 PPP Adapter. По умолчанию оно называется "Континент-АП".

Пользователь компьютера может создавать свои сетевые подключения, использующие Continent 3 PPP Adapter, и устанавливать через них соединения с сервером доступа, используя как интерфейс Абонентского пункта, так и стандартный интерфейс Windows.

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

Управление сетевыми подключениями на компьютере можно осуществлять из стандартного окна Windows "Сетевые подключения".

Установка соединения с сервером доступа

Внимание! 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 Vista. Перед подключением к серверу доступа рекомендуется в настройках ПО КриптоПро CSP установить значение параметра "Интервал времени ожидания ввода" равным 30 секундам.

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

Процесс установки соединения зависит от настройки данного сетевого подключения (см. стр. 18).

Для установки соединения с сервером доступа:



Пиктограмма Абонентского пункта

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.

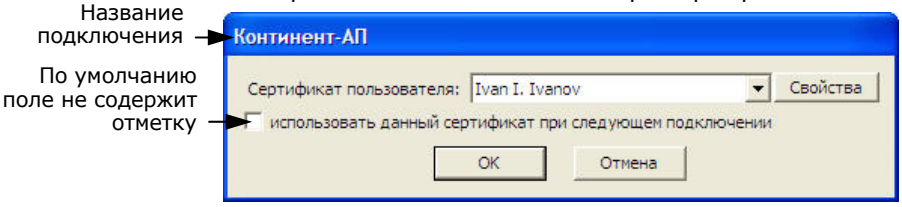


Рис. 23. Диалог выбора сертификата

3. Заполните поля диалога:
   - в поле "Сертификат пользователя" в раскрывающемся списке выберите ваш сертификат;

     Пояснение. В данном списке указаны действительные сертификаты пользователя, для которых зарегистрирован корневой сертификат.

- при необходимости использовать выбранный сертификат по умолчанию установите отметку в поле "Всегда использовать данный сертификат при подключении". В этом случае при последующих подключениях к серверу доступа диалог выбора сертификата выводиться на экран не будет.

> **Совет.** Для отмены сертификата по умолчанию см. стр. 21. При очередном подключении АП к СД диалог выбора сертификата появится на экране.

4. Нажмите кнопку "ОК".

В случае если срок действия выбранного сертификата истекает в течение 30 дней (или меньше), на экране появится сообщение, оповещающее об окончании срока действия выбранного сертификата.

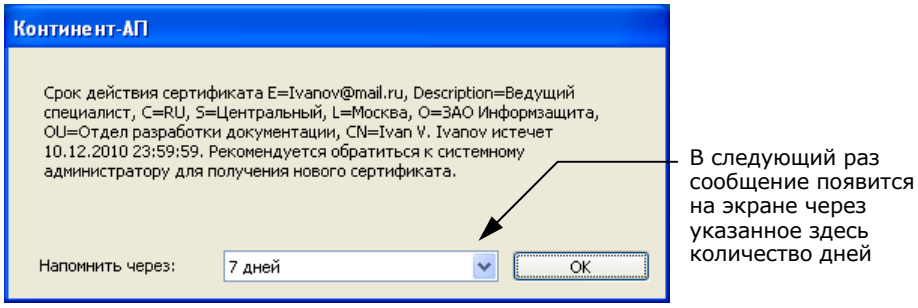


Рис. 24. Сообщение о сроке действия сертификата

5. В раскрывающемся списке выберите промежуток времени (от 1 до 14 дней), по истечении которого следует еще раз напомнить о сроке действия сертификата. Значение "не напоминать" откладывает оповещение до последних суток срока действия сертификата. Нажмите кнопку "ОК".

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 сертификатов 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. стр. 21).

> **Примечание.** Если подключение к данному серверу доступа выполняется не впервые, то на экране появится диалог для ввода пароля доступа к ключевому контейнеру (см. стр. 29). Перейдите к выполнению п. **7** данной процедуры.

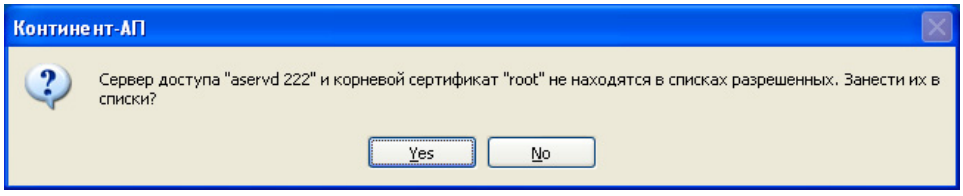


Рис. 25. Запрос на добавление сертификатов в списки разрешенных

6. Убедитесь в верности имен сертификатов, отображенных в запросе, и нажмите кнопку "Yes".

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

Имена сертификатов сервера доступа и корневого сертификата центра сертификации появятся в списках разрешенных.

> **Совет.** Для просмотра списков вызовите на экран диалог свойств протокола проверки подлинности (см. стр. 21).

На экране появится диалог для ввода пароля доступа к ключевому контейнеру (см. Рис. 20 на стр. 29).

Примечание. Если ранее при вводе пароля доступа к данному ключевому контейнеру было отмечено поле "Запомнить пароль" (см. Рис. 18 на стр. 27), то этот диалог на экране не появится.

7. 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.
8. Нажмите кнопку "ОК".



Пиктограмма сетевого подключения

В случае успешного подключения к серверу доступа на панели задач Windows появится пиктограмма нового сетевого подключения. Во всплывающем информационном окне отобразятся сведения о подключении.

Примечание. Отображение пиктограммы зависит от настройки параметров данного соединения.

Если по истечении 30 секунд пароль не был введен, сервер доступа прерывает установку 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 Vista, если установлено значение параметра "Интервал времени ожидания ввода" 30 секунд, диалог закроется автоматически.

После установки соединения с сервером доступа Абонентский пункт будет работать в выбранном режиме (см. стр. 17).

Разрыв соединения с сервером доступа

Для разрыва соединения с сервером доступа:



Пиктограмма Абонентского пункта

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.

Глава 6
Регистрация событий

Просмотр событий

События, относящиеся к соединениям Абонентского пункта с сервером доступа, сохраняются в стандартном журнале событий Windows и доступны для просмотра в Windows-приложении "Просмотр событий". Журнал событий заполняется автоматически.

Совет. Об управлении журналом событий смотрите соответствующий раздел документации для используемой операционной системы.

Перечень регистрируемых событий, относящихся к соединениям Абонентского пункта, приведен в Приложении на стр. 37.

Для просмотра информации о событии:



Пиктограмма Абонентского пункта

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

   На экране появится приложение Windows "Просмотр событий".

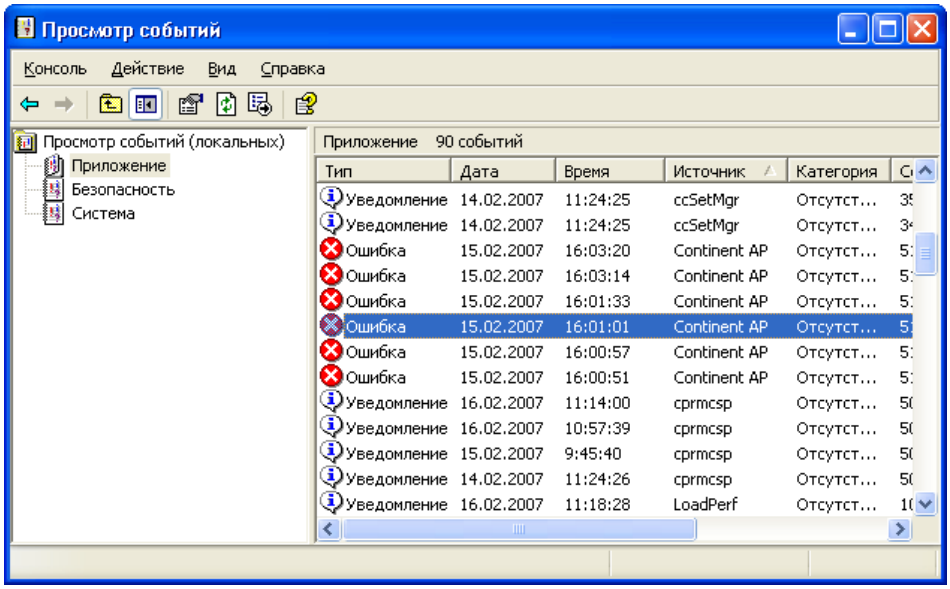


Рис. 26. Окно Windows "Просмотр событий"

3. Перейдите к папке "Приложение".

   Примечание. События, относящиеся к соединениям Абонентского пункта, фиксируются только в этом журнале — журнале приложений.

   Справа отобразится содержимое выбранной папки.
4. Выберите запись, которая в столбце "Источник" содержит "Continent AP".

   Примечание. Все события, относящиеся к соединениям Абонентского пункта, в столбце "Источник" имеют запись "Continent AP".
5. В контекстном меню выбранной записи активируйте команду "Свойства".

   На экране появится диалог просмотра события.
6. Изучив информацию о событии, нажмите кнопку "ОК" для закрытия диалога.

Приложение

Перечень регистрируемых событий

Название зарегистрированного события	Описание произошедшего события/ причина	Действия пользователя
В системе установлен Secret Net	Информационное сообщение. Результат проверки наличия СЗИ «Secret Net» положительный	—
Вход пользователя в неразрешенное время	Отказ сервера. Попытка подключиться к серверу в запрещенное время	• Повторить попытку подключения в разрешенный период времени. • Обратиться к администратору сервера доступа для изменения расписания работы
Вход пользователя заблокирован	Отказ сервера. Учетная запись пользователя заблокирована	Обратиться к администратору сервера доступа
Длина пакета меньше, чем длина служебной информации	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Дуплицированный сертификат сервера	Нарушена целостность пакетов. Возможно наличие в сети злоумышленника	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Завершилось время работы АП	Разрыв подключения по расписанию (закончился период времени, в течение которого абоненту разрешено работать с СД)	• Повторить попытку подключения в разрешенный период времени. • Обратиться к администратору сервера доступа для изменения расписания работы
Нарушена целостность файлов Абонентского Пункта. Обратитесь к системному администратору	Проверка целостности файлов абонентского пункта завершилась неудачей	Запустить инсталлятор АП в режиме «Восстановить»
Не обнаружен Secret Net	Информационное сообщение. Результат проверки наличия СЗИ «Secret Net» отрицательный	—
Неверное значение поля "extended key usage" у сертификата сервера	Проверка значения "extended key usage" у сертификата сервера	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Неверное значение поля "intended key usage" у сертификата сервера.	Проверка значения " intended key usage " у сертификата сервера	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Недостаточная длина буфера	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Некорректный сертификат сервера	При получении цепочки сертификатов было выявлено, что сертификат СД не корректен	Обратиться к администратору сервера доступа
Неправильная длина ключа	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Неправильное или дуплицированное проверочное значение сервера	Нарушена целостность пакетов. Возможно наличие в сети злоумышленника	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Неправильное или дуплицированное случайное число сервера	Нарушена целостность пакетов. Возможно наличие в сети злоумышленника	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Неправильное проверочное значение	Нарушена целостность пакетов. Возможно наличие в сети злоумышленника	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Неправильные данные из сети	Нарушена целостность пакетов. Возможно наличие в сети злоумышленника	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Неправильные данные пользователя	Нарушена целостность пакетов. Возможно наличие в сети злоумышленника	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа

Название зарегистрированного события	Описание произошедшего события/ причина	Действия пользователя
Неправильные данные соединения	Нарушена целостность пакетов. Возможно наличие в сети злоумышленника	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Неправильный или дуплицированный идентификатор сессии	Нарушена целостность пакетов. Возможно наличие в сети злоумышленника	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Нет свободных IP адресов	Отказ сервера. Исчерпан лимит выданных IP адресов их пула адресов	Повторить попытку подключения через некоторое время. В случае неудачи обратиться к администратору сервера доступа
Ошибка генерации ключа	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Ошибка импорта ключа Диффи-Хеллмана	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Ошибка импорта сессионного ключа	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Ошибка подписи ключа	Нарушена целостность пакетов. Возможно наличие в сети злоумышленника	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Ошибка получения криптографического контекста	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Ошибка получения номера телефона из свойств соединения	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Ошибка получения серверного сертификата из бинарных данных	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Ошибка построения цепочки сертификатов сервера. Возможно, один из сертификатов цепочки был отозван	Ошибка построения цепочки сертификатов. Один из сертификатов цепочки отозван.	Обратиться к администратору сервера доступа
Ошибка расшифровки ключа	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Ошибка установки параметра ключа	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Ошибка экспорта ключа	Системная ошибка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Проверка сертификата сервера доступа: не удалось построить цепочку сертификата сервера	Проверка сертификата сервера, ошибка построения цепочки	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Проверка сертификата сервера доступа: один из сертификатов цепочки сертификатов сервера отозван	Проверка сертификата сервера, ошибка цифровой подписи	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Проверка сертификата сервера доступа: присланные сервером данные имеют формат, отличный от PKCS7	Неверный формат сертификата	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Проверка сертификата сервера доступа: срок действия одного из сертификатов цепочки сервера доступа истек или не наступил	Проверка сертификата сервера, ошибка срока действия	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа
Проверка сертификата сервера доступа: цепочка сертификата сервера не полна	Проверка сертификата сервера, неполная цепочка	Повторить попытку подключения. В случае неудачи обратиться к администратору сервера доступа

Документация

1	Аппаратно-программный комплекс шифрования "Континент". Централизованное управление комплексом. Руководство администратора
2	Аппаратно-программный комплекс шифрования "Континент". Локальное управление криптографическим шлюзом. Руководство администратора
3	Аппаратно-программный комплекс шифрования "Континент". Аудит. Руководство администратора
4	Аппаратно-программный комплекс шифрования "Континент". Сервер доступа. Руководство администратора
5	Аппаратно-программный комплекс шифрования "Континент". Программа мониторинга КШ. Руководство пользователя
6	Аппаратно-программный комплекс шифрования "Континент". Тестирование каналов связи. Руководство администратора
7	Аппаратно-программный комплекс шифрования "Континент". Обновление программного обеспечения. Руководство администратора
8	Средство криптографической защиты информации "Континент-АП". Межсетевой экран. Руководство администратора
9	Средство криптографической защиты информации "Континент-АП". Абонентский пункт. Руководство пользователя
10	Аппаратно-программный комплекс шифрования "Континент". Аутентификация хоста. Руководство администратора

Примечание. Набор документов, входящих в комплект поставки, может отличаться от указанного списка.

Предметный указатель

А

Абонентский пункт
- изменение ... 12
- исправление ... 12
- настройка параметров соединения . 18
- обновление ... 13
- переустановка ... 13
- требования к аппаратному и программному обеспечению ... 8
- удаление ... 12
- установка ... 8

К

Как…?
- автоматически запускать Абонентский пункт ... 17
- вызвать меню управления Абонентским пунктом ... 16
- завершить работу программы ... 23
- запретить работу незащищенного соединения на время работы Абонентского пункта ... 17
- запускать Абонентский пункт вручную ... 17
- настроить параметры сетевого подключения ... 18
- разорвать соединение с сервером доступа ... 35
- установить соединение с сервером доступа ... 33

О

Обновление ПО
- загрузка ... 13
- установка ... 14

С

Сертификаты
- в файлах формата *.cer ... 24
- в файлах формата *.p7b ... 24
- общие сведения ... 24
- получение ... 24
- просмотр ... 31
- регистрация сертификатов ... 28
- резервное копирование ... 32
- создание запроса на получение сертификата пользователя ... 25

События
- просмотр событий ... 36