НИП ИНФОРМЗАЩИТА

Программный комплекс

Континент-АП

Руководство пользователя

УВАЛ. 00300-51 91

© НИП “ИНФОРМЗАЩИТА”, 2004. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения НИП “ИНФОРМЗАЩИТА” 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 НИП “ИНФОРМЗАЩИТА”.

Научно-инженерное предприятие
"ИНФОРМЗАЩИТА"

Почтовый адрес:	127018, Москва, а/я 55
Телефон:	(7-095) 937-33-85
Факс:	(7-095) 219-31-88
e-mail:	hotline@infosec.ru
Web:	http: // www.infosec.ru

Версия: 2.00.82.0

Последнее обновление: 07.07.04

Оглавление

Введение ... **5**

Глава 1 Общие сведения ... **9**
- Что следует знать ... 10
- Что необходимо иметь ... 10
- Что нужно сделать ... 11
- Что важно помнить ... 11

Глава 2 Установка, переустановка и удаление абонентского пункта ... **13**
- Требования к аппаратному и программному обеспечению ... 14
- Установка абонентского пункта ... 14
- Переустановка абонентского пункта ... 16
- Удаление абонентского пункта ... 16

Глава 3 Настройка абонентского пункта ... **19**
- Вызов окна настроек ... 20
- Настройка общих параметров абонентского пункта ... 20
- Управление сертификатами ... 22
  - Общие сведения о сертификатах ... 22
  - Регистрация сертификата сервера доступа ... 22
  - Регистрация сертификата пользователя ... 23
  - Регистрация корневого сертификата ... 27
  - Регистрация сертификатов со стандартными именами файлов ... 28
  - Резервное копирование сертификатов ... 29
  - Просмотр сертификата ... 29
  - Удаление информации о регистрации сервера ... 30
  - Удаление сертификата пользователя ... 30

Глава 4 Управление соединением с сервером доступа ... **33**
- Управление программой SAgent ... 34
  - Подключение к защищенной сети ... 34
  - Отключение от защищенной сети ... 35
  - Завершение работы программы SAgent ... 35
- Ошибки подключения и способы их преодоления ... 35
- Особенности работы в различных режимах соединения ... 36
  - Запрет незащищенных соединений ... 36
  - Повтор попыток соединения при неудаче ... 36
  - Автоматическое восстановление соединений ... 36
- Контроль успешности доступа ... 37

Глава 5 Работа с журналом соединений ... **39**
- Включение и отключение журнала соединений ... 40
- Настройка параметров журнала соединений ... 40
  - Определение способа очистки журнала ... 41
  - Выбор файла для хранения журнала ... 41
- Очистка журнала соединений ... 42
- Программа просмотра журнала ... 42
  - Общие сведения о журнале соединений ... 42
  - Интерфейс программы просмотра журнала ... 43
  - Управление окнами просмотра ... 44
- Типовые операции при работе с журналом ... 46
  - Обновление записей журнала ... 46
  - Сортировка записей в окне просмотра ... 46

Изменение состава и порядка отображения полей журнала ... 46
Печать записей журнала ... 47
Очистка журнала ... 49
Поиск нужной записи ... 49

Приложение ... 51
Перечень событий, регистрируемых в журнале соединений ... 52
Управление свойствами сетевого окружения ... 52
Программный модуль SStart ... 54
Общие сведения ... 54
Необходимые условия для работы модуля ... 54
Команды и коды завершения работы ... 54

Предметный указатель ... 56

Введение

Из этого раздела вы узнаете:

- О назначении и структуре Руководства
- Об используемых терминах и текстовых обозначениях

Данное Руководство предназначено для пользователей Программного комплекса "Континент-АП" (далее по тексту — комплекс или абонентский пункт). В нем содержатся сведения, необходимые пользователю для установки, настройки и эксплуатации программного обеспечения комплекса.

Структура руководства

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 все необходимые сведения для подготовки абонентского пункта к работе.
- В **Главе 4** описываются основные приемы работы, обсуждаются причины возможных затруднений и способы их преодоления.
- В **Главе 5** описаны правила работы с журналом регистрации соединений.
- **Приложение** содержит необходимую справочную информацию.

Условные обозначения

В Руководстве используется ряд условных обозначений.

Перекрестные ссылки. В тексте Руководства могут встречаться ссылки на другие части данного Руководства или другие источники информации.

Внутренние ссылки, как правило, содержат указание на номер страницы с нужными сведениями. Например, ссылка на начало данного раздела выглядит так: (см. стр. 5).

См. также:
Так выглядит ссылка на полях.

Ссылки на другие документы или источники информации, как правило, размещаются в тексте примечаний или на полях.

Примечания. Особо 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 или 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

Справочная система

В состав комплекса входит справочная система, содержащая информацию об основных элементах интерфейса. Для вызова справки к отдельным элементам диалогового окна воспользуйтесь одним из следующих способов:

- нажмите с помощью мыши кнопку контекстной справки в строке заголовка диалогового окна, а затем — элемент в диалоговом окне;
- выберите нужный элемент и нажмите <F1>.

Сайт в Интернете

Если у вас есть доступ в Интернет, то вы можете посетить сайт компании НИП "ИНФОРМЗАЩИТА" (http://www.infosec.ru/) или связаться с представителями компании по электронной почте (hotline@infosec.ru).

Соглашения о терминах

Смысл основной части терминов объясняется при первом их употреблении в тексте Руководства.

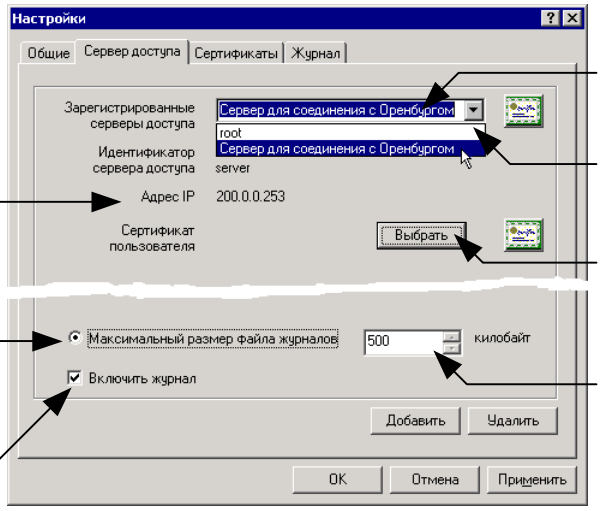
При работе с мышью

Термины, используемые для описания работы с мышью.

Для того чтобы …	Необходимо …
Выбрать с помощью мыши	Совместите указатель (курсор) мыши с нужным объектом, а затем нажмите и отпустите левую кнопку мыши
Дважды нажать левую кнопку мыши	Дважды с коротким промежутком нажмите и отпустите левую кнопку мыши
Нажать	Совместите указатель мыши с объектом, нажмите и удерживайте в нажатом положении левую кнопку мыши
Активизировать	Выберите объект, сделав его активным
Перетащить	Совместите указатель мыши с объектом, нажмите левую кнопку и, продолжая удерживать кнопку нажатой, переместите указатель в нужное положение
Вызвать контекстное меню	Подведите к объекту указатель мыши и нажмите на правую кнопку мыши
Активизировать команду меню	Вызовите меню, установите указатель мыши на нужную команду меню и нажмите левую кнопку мыши

При описании интерфейса

Термины, используемые при описании элементов интерфейса.



Текстовое поле для ввода информации

Поле с открывающимся списком для выбора значения параметра

Кнопка диалога

Это информационное поле. Оно недоступно для редактирования

Поле переключателя. В этом поле можно установить отметку

При установке отметки в поле выключателя, активизируется связанный с ним параметр настройки

В такое поле нужное значение можно ввести с клавиатуры, а можно установить, нажимая с помощью мыши на кнопки-стрелки

При выполнении типовых операций

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 прописные буквы различаются. Допущенные ошибки при вводе исправляются также как и при заполнении текстового поля.



Общие сведения

Из этой главы вы узнаете:

- О базовых понятиях, связанных с работой комплекса
- О подготовительных действиях, предшествующих началу работы
- О важной роли администратора безопасности

Что следует знать

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

О корпоративной сети

Аппаратно-программный комплекс шифрования (АПКШ) "Континент" предназначен для безопасной передачи данных через общедоступные (незащищенные) сети, в частности, для безопасной передачи данных через Интернет. Эта технология называется "виртуальная частная сеть" (VPN). Защита данных обеспечивается криптографическими методами, вследствие чего через общедоступную сеть данные передаются в зашифрованном виде.

Об удаленном доступе

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 программный комплекс "Континент-АП", который для передачи данных соединяется с компьютером — сервером доступа, проверяющим полномочия на доступ и разрешающим доступ к ресурсам защищенной сети.

О сертификатах

Для взаимодействия абонентского пункта и сервера доступа используются следующие сертификаты:

- сертификат сервера доступа — для подтверждения подлинности сервера доступа, взаимодействующего с абонентским пунктом;
- сертификат пользователя — для аутентификации пользователя на сервере доступа;
- сертификат корневого центра сертификации — для подтверждения подлинности сертификата сервера доступа и сертификата пользователя.

Что необходимо иметь

Итак, перед тем как начать работу с ресурсами защищенной корпоративной сети:

1 Необходимо получить у администратора безопасности:

Сертификат пользователя

Сертификат сервера доступа

Корневой сертификат

> **Внимание!** Если при регистрации в системе администратор не потребовал от вас сформировать запрос на получение сертификата пользователя, необходимо получить от администратора кроме сертификата пользователя 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 программные продукты КриптоПро CSP и КриптоПро TLS. Процедуры установки и настройки подробно рассматриваются в эксплуатационной документации на эти программные продукты. См. документ "Установка и регистрация КриптоПро CSP".

2. Установите программное обеспечение абонентского пункта. Процедура установки подробно рассматривается на стр. 14.

3. Получите у администратора безопасности сертификаты, необходимые для работы. Для получения сертификата пользователя, возможно, потребуется создать файл запроса (см. стр. 23) и передать его администратору.

4. Зарегистрируйте полученные сертификаты. Эта процедура подробно рассматривается на стр. 22.

5. Настройте параметры соединения с сервером доступа (см. стр. 20) и параметры хранения журнала регистрации (см. стр. 40).

6. Установите соединение с сервером доступа (см. стр. 34) и попробуйте обменяться информацией с каким-либо из доступных вам абонентов, находящихся в защищенном сегменте корпоративной сети.

   Если пробное соединение с сервером установлено успешно и обмен информацией с абонентами корпоративной сети возможен, значит, все подготовительные действия выполнены правильно. С этого момента абонентский пункт готов к работе.

Что важно помнить

1. Никому не передавайте файлы сертификатов, полученные у администратора, а также ключевые носители, содержащие закрытые ключи.

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.

   Если по каким либо причинам требуется изменить свойства сетевого окружения, необходимо временно отключить защиту сетевых адаптеров, внести необходимые изменения, а затем восстановить защиту. Эта процедура подробно рассматривается в Приложении на стр. 52.

3. Во всех сложных ситуациях, связанных с работой комплекса, которые вы сами не в состоянии разрешить, обращайтесь к администратору. Так, 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 абонентского пункта

Из этой главы вы узнаете:

- Какие требования предъявляются к компьютеру
- Как установить программное обеспечение абонентского пункта
- Как выполнить его переустановку
- Как удалить программное обеспечение абонентского пункта

Программное обеспечение абонентского пункта поставляется на компакт-дисках. В комплект поставки входят программные продукты фирмы "КриптоПро" КриптоПро CSP и КриптоПро TLS.

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, работающих под управлением ОС Windows 98 SE, Windows NT 4.0 (SP6), Windows 2000 (SP4), Windows XP (SP1). Требования к аппаратной конфигурации компьютеров приведены в Табл. 1.

Табл. 1. Требования к конфигурации компьютера

Элемент	Минимально	Рекомендуется
Процессор	Pentium 166 МГц	Pentium III 600 МГц
Оперативная память	64 Мб	128 Мб
Жесткий диск (свободное пространство)	20 Мб + свободное дисковое пространство для хранения журнала	50 Мб + свободное дисковое пространство для хранения журнала

На компьютере должны быть установлены компоненты операционной системы, обеспечивающие работу с сетевыми протоколами TCP/IP. Требуется также наличие MS Internet Explorer версии 5.5 или выше.

Внимание! При использовании абонентского пункта совместно с устройством ЭЗ "Соболь", а также с криптопровайдером КриптоПро CSP и программным обеспечением КриптоПро TLS, необходимо перед установкой абонентского пункта установить эти аппаратные и программные продукты согласно эксплуатационной документации на них.

Установка абонентского пункта

Перед установкой программного обеспечения абонентского пункта необходимо завершить работу ранее открытых приложений.

Если в текущем сеансе работы вносились какие-либо изменения в свойства сетевого окружения, перед выполнением установки необходимо обязательно перезагрузить компьютер, чтобы изменения вступили в силу.

< Назад

Далее >

Отмена

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 на эту кнопку подтвердите свое решение в появившемся на экране окне запроса.

▶ Для установки абонентского пункта:

Запуск программы установки

1. Поместите установочный компакт-диск в привод CD-ROM и запустите на исполнение файл \ Cont_Client \ Setup\ SETUP.EXE, находящийся на этом диске.

   Совет. Для установки системы защиты 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 дейст-

вий на экран будет выведен стартовый диалог программы установки, предлагающий завершить работу с другими приложениями.

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

   На экране появится диалог, содержащий лицензионное соглашение на использование программного продукта. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца.

Принятие лицензионного соглашения

3. Нажмите кнопку "Да" для подтверждения своего согласия с условиями лицензионного соглашения и продолжения установки.

   Если лицензионное соглашение вами не принимается, нажмите кнопку "Нет" и откажитесь от продолжения установки.

Копирование файлов

Далее программа установки создает каталог \ Program Files \ Infosec \ ContinentClient на жестком диске компьютера и копирует файлы в созданный каталог. Кроме того, некоторые файлы копируются в системные каталоги Windows.

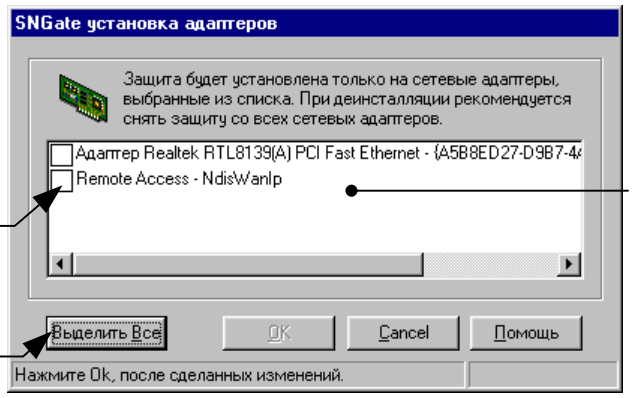
Если по какой-то причине отсутствует какой-либо из файлов, входящих в комплект поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. В этом случае проверьте компьютер на наличие вирусов и повторите установку. Если в дальнейшем данная ошибка будет повторяться,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

При успешном завершении копирования файлов осуществляется регистрация программных компонент абонентского пункта.

Защита устройств доступа к сети

Затем выполняются действия, необходимые для защиты устройств доступа к сети.

- Если установка осуществляется в среде ОС Windows 98 SE или Windows NT 4.0 на экране появится следующий диалог:



Установите с помощью мыши отметки слева от названий защищаемых устройств

Нажмите на эту кнопку, чтобы выбрать все устройства

Список имеющихся на компьютере устройств доступа к сети (сетевых адаптеров, устройства "Удаленный доступ к сети")

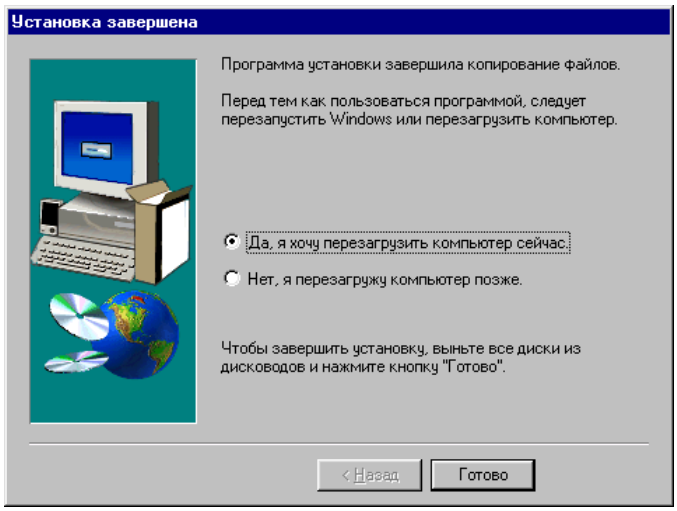
Выберите в списке те устройства, посредством которых будет выполняться доступ к защищенной корпоративной сети, установив отметки (●) слева от названий защищаемых устройств. Нажмите кнопку "OK".

- Если установка осуществляется в среде ОС Windows 2000 или Windows XP, указанный диалог на экране не появляется. В этом случае защита включается автоматически для всех устройств доступа к сети, имеющихся на компьютере.



Внимание! После включения защиты устройств доступа к сети запрещается вносить любые изменения в свойства сетевого окружения компьютера. Порядок изменения свойств сетевого окружения и перечня защищенных устройств доступа к сети приводится на стр. 52.

Процедуру установки завершает следующий диалог:



4. Выберите вариант завершения установки и нажмите кнопку "Готово":
   - отметьте поле "Да, я хочу перезагрузить компьютер сейчас" для немедленной перезагрузки компьютера и начала работы с абонентским пунктом;
   - отметьте поле "Нет, я перезагружу компьютер позже", чтобы продолжить работу без перезагрузки компьютера. В этом случае работа с абонентским пунктом будет возможна только после окончания сеанса работы и перезагрузки компьютера.

В результате установки в состав меню "Программы" главного меню Windows будет добавлено подменю "Continent", содержащее команды "Клиент Континента" и "Удаление Клиента Континента".

Переустановка абонентского пункта

Переустановка абонентского пункта обычно выполняется в следующих случаях:

- после неудачного завершения установки;
- при нарушении работоспособности программного обеспечения;
- для обновления версии абонентского пункта.

Внимание! Перед выполнением переустановки обязательно завершите работу программы SAgent (см. стр. 35), иначе переустановка завершится с ошибкой.

Порядок переустановки полностью соответствует процедуре установки программного обеспечения абонентского пункта на компьютер (см. стр. 14).

Текущие настройки абонентского пункта, в том числе зарегистрированные сертификаты, при переустановке не изменяются. Поэтому если абонентский пункт был корректно настроен до выполнения переустановки, после ее завершения дополнительные действия по настройке абонентского пункта не требуются.

Удаление абонентского пункта

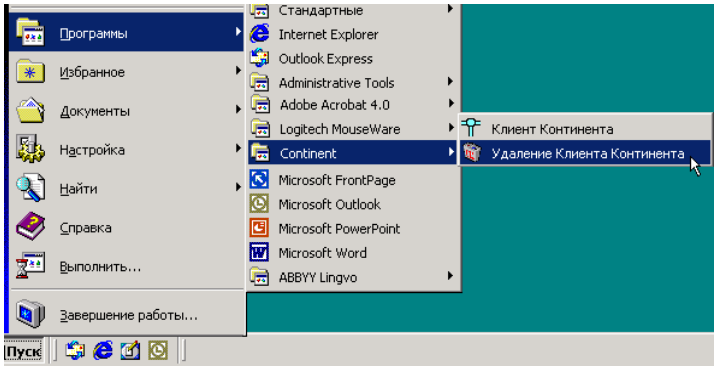
Удаление абонентского пункта обычно выполняется в следующих случаях:

- при переходе на другой компьютер;
- при замене на компьютере сетевого адаптера (см. также стр. 52).

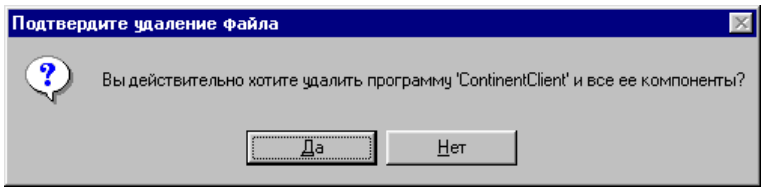
Внимание! Перед запуском процедуры удаления необходимо завершить работу программы SAgent (см. стр. 35).

Для удаления абонентского пункта:

1. Нажмите кнопку "Пуск" ("Start") и активизируйте в главном меню Windows команду "Программы \ Continent \ Удаление Клиента Континента".



На экране появится окно запроса:



2. Нажмите кнопку "Да" для подтверждения удаления.

В том случае, если работа программы SAgent не была завершена до запуска процедуры удаления, на экране появится сообщение о необходимости завершить работу этой программы. Для продолжения процедуры удаления выполните следующие действия:

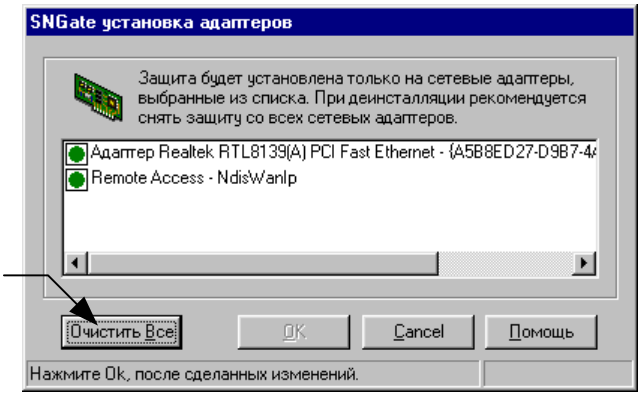
- завершите работу программы SAgent так, как это описано на стр. 35;
- нажмите кнопку "OK" в окне сообщения.

Далее выполняются действия, необходимые для отключения защиты устройств доступа к сети.

Внимание! Для нормальной работы устройств доступа к сети после удаления абонентского пункта необходимо отключить защиту всех этих устройств.

- Если удаление осуществляется в среде ОС Windows 98 SE или Windows NT 4.0 на экране появится диалог, содержащий список имеющихся на компьютере устройств доступа к сети. Те устройства, которые были защищены при установке абонентского пункта, отмечены символом ●.

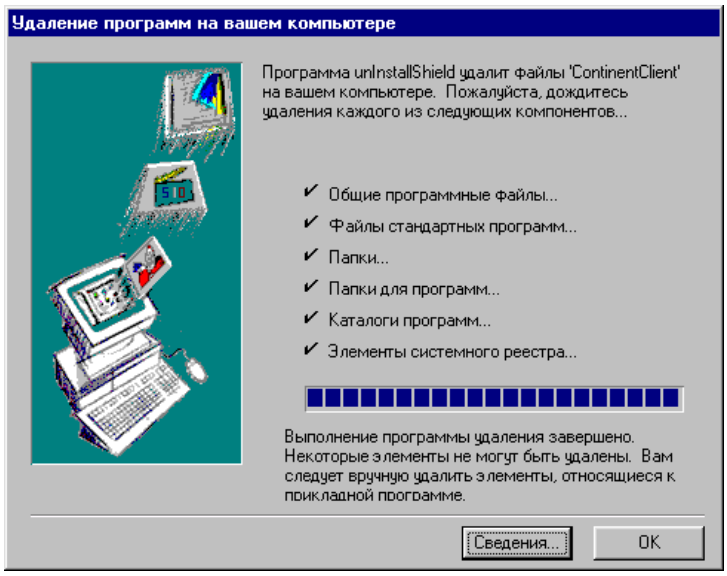
Нажмите эту кнопку, чтобы отключить защиту всех устройств доступа к сети



Для отключения защиты удалите отметки (●) слева от названий всех показанных в списке устройств. Для продолжения удаления нажмите кнопку "OK".

- Если удаление осуществляется в среде ОС Windows 2000 или Windows XP, указанный диалог на экране не появляется. В этом случае отключение защиты устройств доступа к сети выполняется автоматически.

Процесс удаления отображается на экране в следующем окне:



3. По завершении процесса удаления нажмите кнопку "OK".

Пояснение. Некоторые компоненты программы, список которых можно посмотреть, нажав кнопку "Сведения", не могут быть удалены немедленно. Эти компоненты будут удалены при перезагрузке компьютера.

На экране появится сообщение о необходимости перезагрузки компьютера для завершения удаления программных компонент.

4. Нажмите кнопку "Да" для немедленной перезагрузки компьютера.

глава 3

Настройка абонентского пункта

Из этой главы вы узнаете:

- О настройке параметров абонентского пункта
- О форматах используемых сертификатов
- О порядке регистрации сертификатов
- О резервном копировании сертификатов
- О том, как посмотреть информацию о сертификате
- О том, как удалить сертификаты

Настройка абонентского пункта выполняется в следующем порядке:

- настройка общих параметров абонентского пункта (см. ниже);
- регистрация сертификата сервера доступа (см. стр. 22);
- регистрация сертификата пользователя (см. стр. 23);
- регистрация сертификата корневого центра сертификации (см. стр. 27);
- настройка параметров журнала соединений (см. стр. 40).

Вызов окна настроек

Для вызова окна настроек:



Пиктограмма SAgent

1. Вызовите контекстное меню пиктограммы SAgent, размещающейся на панели задач Windows.
2. Активизируйте команду "Настройки".

Совет. При отсутствии на панели задач Windows пиктограммы SAgent, активизируйте в главном меню Windows команду "Программы \ Continent \ Клиент Континент".

При работе с окном настроек используйте кнопки:

- "OK" — чтобы сохранить изменения и закрыть окно;
- "Применить" — для сохранения изменений без закрытия окна;
- "Отмена" — чтобы закрыть окно без сохранения изменений.

Настройка общих параметров абонентского пункта

Для настройки параметров:

1. Вызовите на экран окно управления настройками абонентского пункта (см. выше).
2. Активизируйте закладку "Общие":

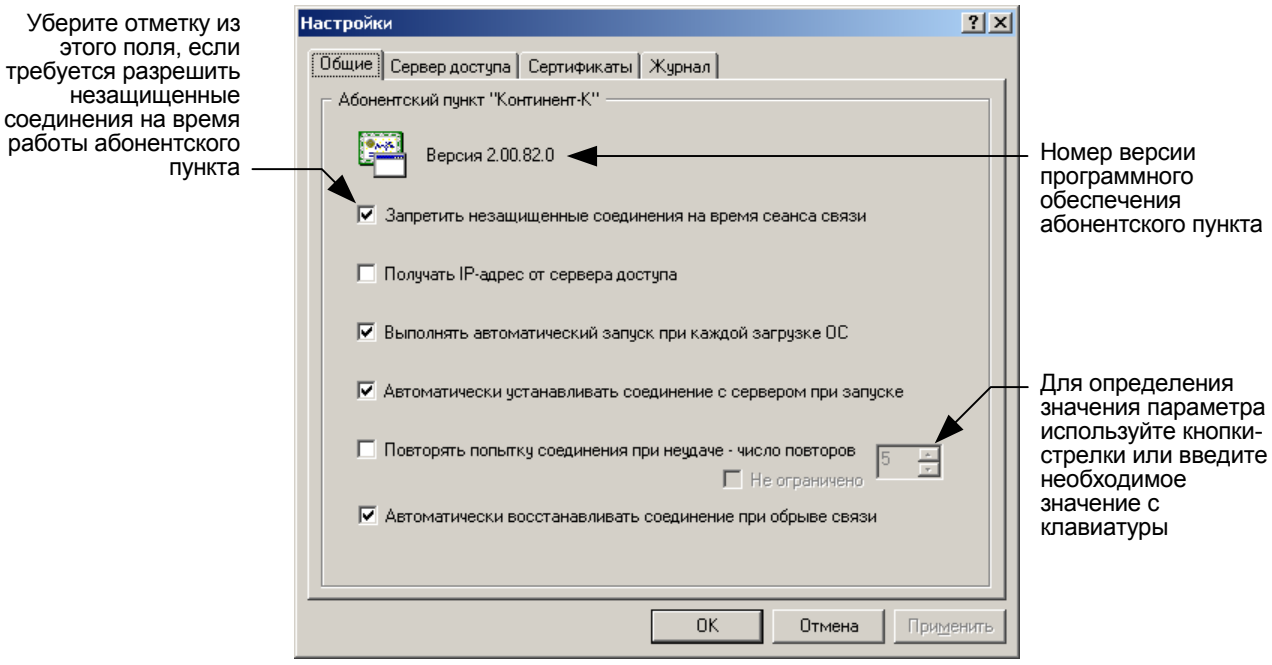


Рис. 1. Диалог "Общие"

3. Отметьте поле "Запретить незащищенные соединения на время сеанса связи", чтобы запретить на все время сеанса связи абонентского пункта и сервера доступа любые другие соединения, кроме соединений через данный сервер.

   В этом случае абонентским пунктом будут передаваться в сеть только те IP-пакеты, которые удовлетворяют правилам фильтрации, установленным на сервере доступа для текущего пользователя.



Внимание! Рекомендуется запрещать незащищенные соединения.

4. Для получения внутрисетевого IP-адреса от сервера доступа при установке соединения с ним отметьте поле "Получать IP-адрес от сервера доступа".

Пояснение. Для использования этого режима необходимо также включить его и на сервере доступа. См. документ "Аппаратно-программный комплекс Континент. Сервер доступа. Руководство по администрированию".

5. Отметьте поле "Выполнять автоматический запуск при каждой загрузке ОС", чтобы включить режим автоматического запуска программы SAgent при каждой загрузке операционной системы. В этом случае пиктограмма SAgent всегда будет присутствовать на панели задач Windows.

6. Для автоматической установки соединения с сервером доступа после запуска программы SAgent отметьте поле "Автоматически устанавливать соединение с сервером при запуске".

Пояснение. Сервер доступа, с которым будет устанавливаться автоматическое соединение, определяется наличием отметки в поле "По умолчанию" диалога "Сервер доступа" (см. Рис. 2 на стр. 22).

7. Если требуется автоматически повторять заданное число раз попытки подключения к серверу доступа в случае неудачи, выполните следующие действия:

   - отметьте поле "Повторять попытку соединения при неудаче";
   - определите число повторов в одноименном поле. Этот параметр может принимать значения от 5 до 255 попыток. Если за указанное число попыток соединение с сервером не будет установлено, на экране появится сообщение об ошибке;
   - при необходимости установите отметку в поле "Не ограничено". В этом случае попытки будут повторяться до установки соединения.

Совет. Рекомендуется использовать этот режим в тех случаях, когда абонентский пункт работает автоматически без постоянного контроля со стороны оператора.

8. Для автоматического восстановления соединения с сервером доступа при обрыве связи после того, как подключение к серверу успешно выполнено, отметьте поле "Автоматически восстанавливать соединение при обрыве связи". Попытки автоматического восстановления соединения повторяются неограниченное число раз до восстановления соединения с сервером доступа.

Совет. Рекомендуется использовать этот режим в тех случаях, когда абонентский пункт работает автоматически без постоянного контроля со стороны оператора.

9. Нажмите кнопку "OK".

Управление сертификатами

Общие сведения о сертификатах

Сертификат — это цифровой документ, содержащий определенную, цифровым образом подписанную информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название доверенного центра сертификации и т.д. В зависимости от используемого стандарта и хранимого содержимого, существуют различные форматы сертификатов.

Сертификаты в файлах формата *.cer

Сертификаты в файлах с расширением *.cer соответствуют стандарту X.509v3 Международного телекоммуникационного союза (ITU-T). Для удобства изложения мы будем называть их "сертификаты в формате .cer". Этот формат применяется для хранения сертификатов сервера доступа и сертификатов пользователя.

Сертификаты в файлах формата *.p7b

Файлы с расширением *.p7b содержат данные в формате PKCS#7. Этот формат позволяет упаковывать несколько сертификатов в единый массив. В нашем случае в нем содержится цепочка подтверждающих друг друга сертификатов. Этот формат применяется для хранения сертификатов корневого центра сертификации.

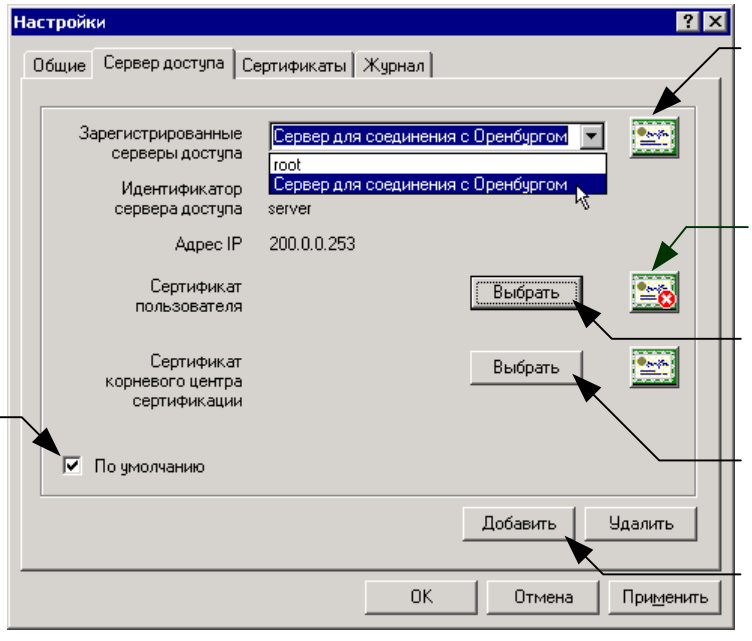
Регистрация сертификата сервера доступа

Первоначально ни один сервер доступа на абонентском пункте не зарегистрирован. Регистрация сертификата сервера доступа необходима как для соединения с сервером, так и для регистрации сертификата пользователя и корневого сертификата.

Внимание! Существует быстрый способ регистрации сертификатов. Этот способ применим только при соблюдении ряда требований. Подробные сведения об использовании этой возможности содержатся на стр. 28.

Для регистрации сертификата сервера:

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Сервер доступа".



Используйте такие кнопки для просмотра информации о сертификатах. Пиктограммы отображают статус сертификатов:
- действителен;
- истек срок действия сертификата

Нажмите эту кнопку для регистрации сертификата пользователя

Нажмите эту кнопку для регистрации сертификат корневого центра сертификации

Нажмите эту кнопку для регистрации нового сервера доступа

Установите отметку, если необходимо, чтобы после запуска программы SAgent автоматическое соединение устанавливалось с данным сервером доступа

Рис. 2. Диалог "Сервер доступа"

3. Нажмите кнопку "Добавить".
   На экране появится стандартный диалог Windows для работы с файлами.

4. Укажите диск (каталог), содержащий файлы сертификатов, и выберите файл сертификата сервера доступа (имя файла по умолчанию — srvNN.cer, где NN — порядковый номер сертификата). Затем нажмите кнопку "Открыть".

   Если выбранный вами файл имеет правильный формат, то в поле "Зарегистрированные серверы доступа" и в поле "Идентификатор сервера доступа" появится название сервера, содержащееся в сертификате. Ниже в поле "Адрес IP" появится IP-адрес добавленного сервера доступа.

   Совет. Для изменения названия сервера доступа, отображаемого в меню программы SAgent, а также в списке зарегистрированных серверов, активизируйте поле "Зарегистрированные серверы доступа" и введите с клавиатуры нужное название. Название сервера, прочитанное из сертификата, будет отображаться в неизменном виде в поле "Идентификатор сервера доступа".

5. Нажмите кнопку "OK".

Регистрация сертификата пользователя

Для того чтобы осуществлять доступ к ресурсам защищенной сети, необходимо зарегистрировать сертификат пользователя.

При успешной регистрации сертификата пользователя сертификат будет помещен в хранилище сертификатов и установлен как применяемый при соединении с указанным сервером доступа. В поле "Сертификат пользователя" (см. Рис. 2 на стр. 22) отобразится имя пользователя, содержащееся в сертификате.

Создание запроса на получение сертификата

Если требуется, чтобы сертификат пользователя создавался администратором с помощью специального файла запроса, необходимо создать этот файл и передать его администратору.

Создание запроса на получение сертификата

► **Для создания запроса:**

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Сертификаты":

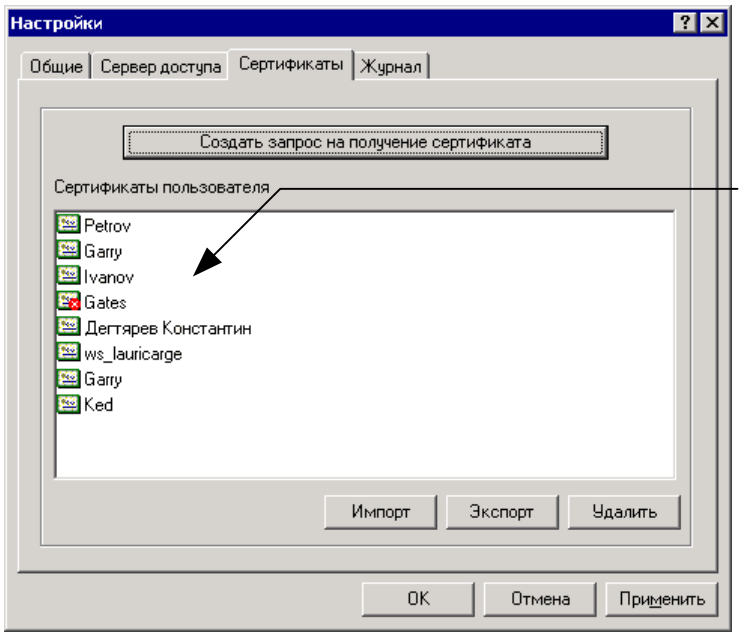
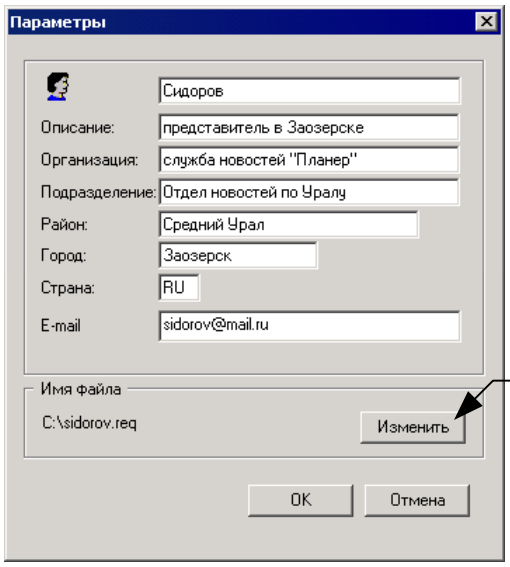


Рис. 3. Диалог "Сертификаты"

3. Нажмите кнопку "Создать запрос на получение сертификата".

На экране появится диалог формирования параметров запроса:



Нажмите эту кнопку, если требуется изменить расположение или название файла запроса

4. Укажите необходимые сведения в текстовых полях диалога.

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

По умолчанию файл запроса создается в корневом каталоге диска "C" с расширением *.req под именем, содержащим имя текущего пользователя Windows, а также информацию о текущей дате и текущем времени.

5. Нажмите кнопку "Изменить", если требуется изменить расположение или имя файла запроса. В стандартном окне Windows, появившемся на экране, укажите:
   - диск (каталог) для создания файла;
   - имя файла запроса;
   - нажмите кнопку "Открыть" (или "Сохранить").

Совет. Если компьютер работает под управлением ОС Windows 2000, на экране появится запрос о создании файла. Нажмите кнопку "Да".

На экране появится запрос ключевого носителя для записи закрытого ключа сертификата пользователя:

Выберите в поле с открывающимся списком ключевой носитель, на который будет записан секретный ключ пользователя

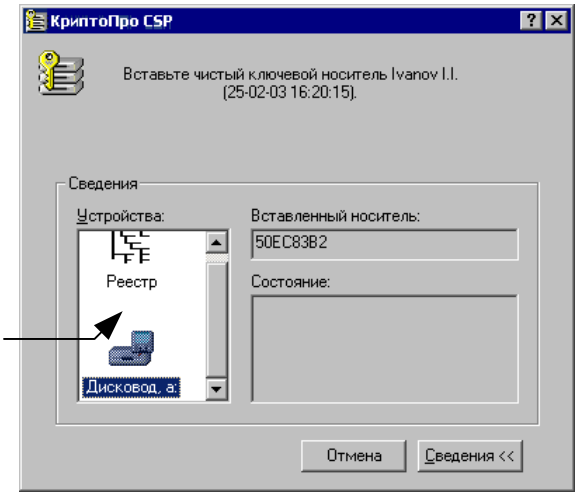


Рис. 4. Запрос ключевого носителя

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

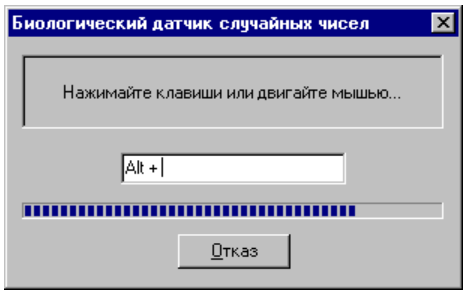
Совет. Если выбрано значение "Дисковод", вставьте чистую отформатированную дискету в выбранный дисковод.

Система 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.

Например, при использовании биологического датчика случайных чисел на экране появится следующий диалог:



Для запуска и продолжения процесса генерации ключа нажимайте любые клавиши на клавиатуре или перемещайте мышь.

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

Пояснение. С помощью этого пароля ограничивается доступ к ключевой информации. Запомните введенный пароль. Этот пароль запрашивается каждый раз при чтении информации с данного ключевого носителя.

7. Заполните поля диалога:

- введите пароль в поле "Пароль";
- введите тот же пароль в поле "Подтверждение";
- отметьте поле "Всегда использовать значения по умолчанию" для чтения информации с данного ключевого носителя на данном компьютере без запроса пароля.

8. Предъявите ключевой носитель и нажмите кнопку "OK".

9. После того как выполнены все действия, необходимые для создания ключевой информации, закройте окно управления настройками абонентского пункта с сохранением изменений.

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

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

Регистрация сертификата

Для регистрации сертификата пользователя:

Регистрация сертификата пользователя

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Сервер доступа" (см. Рис. 2 на стр. 22).
3. Выберите в списке "Зарегистрированные серверы доступа" сервер доступа, для которого регистрируется сертификат пользователя.
4. Нажмите кнопку "Выбрать", расположенную справа от поля "Сертификат пользователя".

   На экране появится диалог:

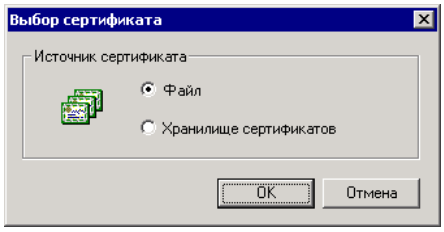


Рис. 5. Диалог "Выбор сертификата"

Совет. Если нужный сертификат пользователя регистрировался ранее и содержится в хранилище сертификатов, отметьте поле "Хранилище сертификатов". После нажатия кнопки "OK" на экране появится список сертификатов пользователя, имеющихся в хранилище. Выберите нужный сертификат и нажмите кнопку "OK". Перейдите к шагу **8**.

5. Отметьте поле "Файл" и нажмите кнопку "OK".

   На экране появится стандартный диалог Windows для работы с файлами.

6. Укажите диск (каталог), содержащий файлы сертификатов, и выберите файл сертификата пользователя (имя файла по умолчанию — user.cer). Затем нажмите кнопку "Открыть".

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

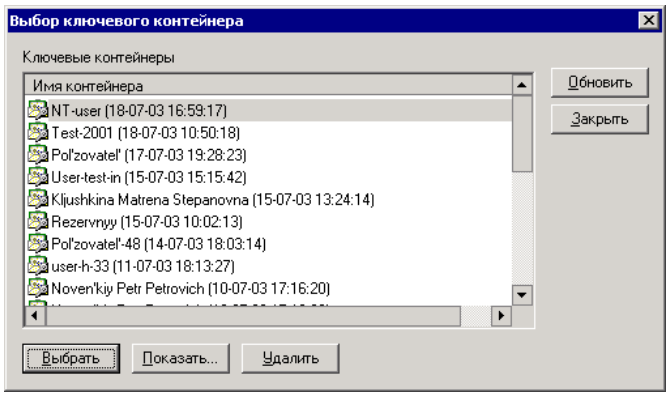


Рис. 6. Диалог выбора ключевого контейнера

Пояснения:

- Если закрытый ключ сертификата пользователя хранится в системном реестре, диалог выбора ключевого контейнера на экран не выводится. Перейдите к выполнению п. **9**.
- Если в данном сеансе работы с абонентским пунктом запрос ключа сертификата пользователя уже выполнялся, вместо диалога выбора ключевого контейнера на экран выводится запрос ключевого носителя (см. Рис. 4 на стр. 24). Предъявите носитель, содержащий закрытый ключ сертификата пользователя, и перейдите к выполнению п. **9**.

7. Предъявите ключевой носитель, содержащий закрытый ключ сертификата пользователя и нажмите кнопку "Обновить".

   На экране появится список ключевых контейнеров, находящихся на предъявленном ключевом носителе.

   Примечание. Название контейнера включает в себя имя пользователя, указанное при создании запроса, а также дату и время создания запроса.

8. Выберите в этом списке нужный ключевой контейнер, предъявите ключевой носитель и нажмите кнопку "Выбрать".

   На экране появится запрос пароля.

9. Введите пароль, которым был ограничен доступ к личной ключевой информации. Предъявите ключевой носитель и нажмите кнопку "OK".

   Пояснение. Если регистрируется сертификат, созданный по запросу, укажите пароль, который был задан вами при создании файла запроса (см. п. **7** на стр. 25). Во всех остальных случаях пароль вам должен сообщить администратор при передаче соответствующего ключевого носителя.

10. После того как выполнены все действия, необходимые для регистрации сертификата, закройте окно управления настройками абонентского пункта с сохранением изменений.

Регистрация корневого сертификата

Для того чтобы использование сертификатов сервера доступа и пользователя стало возможным, необходимо получить и зарегистрировать заверяющий их сертификат корневого центра сертификации.

▶ Для регистрации корневого сертификата:

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Сервер доступа" (см. Рис. 2 на стр. 22).
3. Выберите в списке "Зарегистрированные серверы доступа" сервер доступа, для которого регистрируется сертификат корневого центра сертификации.
4. Нажмите кнопку "Выбрать", расположенную справа от поля "Сертификат корневого центра сертификации".
5. В диалоге, появившемся на экране (см. Рис. 5 на стр. 26), отметьте поле:
   - "Файл" — если производится первичная регистрация сертификата;
   - "Хранилище сертификатов" — если сертификат уже зарегистрирован на данном компьютере.

   Нажмите кнопку "OK". На экране появится стандартное окно для доступа к файлам, либо окно с содержимым хранилища корневых сертификатов.
6. Выберите нужный сертификат и нажмите кнопку "OK".

   При первоначальной установке корневого сертификата на компьютер операционная система попросит вас подтвердить свое согласие на добавление этого сертификата в хранилище корневых сертификатов компьютера.

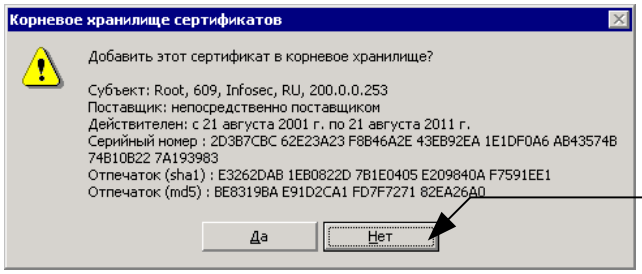


Рис. 7. Запрос на добавление сертификата в корневое хранилище

7. Проверьте данные в окне запроса и нажмите кнопку "Да".
8. Закройте окно управления настройками абонентского пункта с сохранением изменений.

При успешной первичной регистрации сертификата корневого центра сертификации, сертификат будет помещен в хранилище сертификатов. Зарегистрированный сертификат будет установлен как применяемый при соединении с указанным сервером доступа. В поле "Сертификат корневого центра сертификации" (см. Рис. 2 на стр. 22) отобразится название сертификата.

Регистрация сертификатов со стандартными именами файлов

Регистрация сертификатов данным способом позволяет автоматически зарегистрировать сертификаты пользователя и корневого центра сертификации при регистрации сертификата сервера доступа. Этот способ применим только при соблюдении следующих условий:

- файлы сертификатов размещаются в одном каталоге;
- файлы сертификатов имеют стандартные имена:

  srvNN.cer — сертификат сервера доступа (NN — порядковый номер сертификата сервера);

  user.cer — сертификат пользователя;

  root.p7b (root.cer) — сертификат корневого центра сертификации.

Для регистрации сертификатов:

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Сервер доступа" (см. Рис. 2 на стр. 22).
3. Нажмите кнопку "Добавить".

   На экране появится стандартный диалог Windows для работы с файлами.
4. Укажите диск (каталог), содержащий файлы сертификатов, и выберите файл сертификата сервера доступа. Затем нажмите кнопку "Открыть".

   На экране появится окно запроса, в котором операционная система попросит вас подтвердить свое согласие на добавление корневого сертификата в хранилище корневых сертификатов компьютера (см. Рис. 7 на стр. 27).
5. Проверьте данные в окне запроса и нажмите кнопку "Да".

   На экране появится диалог выбора ключевого контейнера для чтения закрытого ключа сертификата пользователя (см. Рис. 6 на стр. 26).

   Пояснения:
   - Если закрытый ключ сертификата пользователя хранится в реестре, диалог выбора ключевого контейнера на экран не выводится. Перейдите к выполнению п. **8**.
   - Если в данном сеансе работы с абонентским пунктом запрос ключа сертификата пользователя уже выполнялся, вместо диалога выбора ключевого контейнера на экран выводится запрос ключевого носителя (см. Рис. 4 на стр. 24). Предъявите носитель, содержащий закрытый ключ сертификата пользователя, и перейдите к выполнению п. **8**.
6. Предъявите ключевой носитель, содержащий закрытый ключ сертификата пользователя, и нажмите кнопку "Обновить".

   На экране появится список ключевых контейнеров, находящихся на предъявленном ключевом носителе.

   Пояснение. Название контейнера включает в себя имя пользователя, указанное при создании запроса, а также дату и время создания запроса.

7. Выберите в этом списке нужный ключевой контейнер, предъявите ключевой носитель и нажмите кнопку "Выбрать".

   На экране появится запрос пароля.

8. Введите пароль, которым был ограничен доступ к личной ключевой информации. Предъявите ключевой носитель и нажмите кнопку "ОК".

   Пояснение. Если регистрируется сертификат, созданный по запросу, укажите пароль, который был задан вами при создании файла запроса (см. п. **7** на стр. 25). Во всех остальных случаях пароль вам должен сообщить администратор при передаче соответствующего ключевого носителя.

   В результате выполненных действий (см. Рис. 2 на стр. 22):

   - в поле "Зарегистрированные серверы доступа" и в поле "Идентификатор сервера доступа" появится название сервера, содержащееся в зарегистрированном сертификате сервера доступа. Ниже, в поле "Адрес IP", появится IP-адрес добавленного сервера доступа;
   - в поле "Сертификат пользователя" появится имя пользователя, содержащееся в сертификате пользователя;
   - сертификат корневого центра сертификации будет помещен в хранилище сертификатов. Зарегистрированный сертификат будет установлен как применяемый при соединении с указанным сервером доступа. В поле "Сертификат корневого центра сертификации" отобразится название сертификата.

9. Закройте окно управления настройками абонентского пункта с сохранением изменений.

Резервное копирование сертификатов

Резервное копирование сертификатов сервера доступа, корневого центра сертификации и сертификатов пользователя выполняется обычными средствами копирования файлов. При необходимости вы сможете использовать копии файлов сертификата сервера и 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.

Просмотр сертификата

Для получения информации о сертификате:



1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Сервер доступа" (см. Рис. 2 на стр. 22).
3. Нажмите кнопку , расположенную справа от поля:
   - "Зарегистрированные серверы доступа" — чтобы посмотреть информацию о сертификате сервера доступа;
   - "Сертификат пользователя" — чтобы посмотреть сведения о сертификате пользователя;
   - "Сертификат корневого центра сертификации" — чтобы посмотреть сведения о корневом сертификате.

На экране появится стандартное диалоговое окно операционной системы, содержащее информацию о выбранном сертификате. Описание диалогового окна содержится в документации к операционной системе.

4. Изучив информацию о сертификате, закройте окно, нажав кнопку "ОК".

Удаление информации о регистрации сервера

Для удаления регистрационной информации:

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Сервер доступа" (см. Рис. 2 на стр. 22).
3. Выберите в списке "Зарегистрированные серверы доступа" сервер доступа, информацию о регистрации которого требуется удалить.
4. Нажмите кнопку "Удалить".
5. Закройте окно управления настройками абонентского пункта с сохранением изменений.

В результате выполненных действий будет удалена информация о регистрации выбранного сервера доступа, включая сведения о сертификатах пользователя и корневого центра сертификации, используемых для соединения с этим сервером.

При удалении информации о регистрации сертификатов, информация о них не будет удалена из хранилища сертификатов.

Удаление сертификата пользователя

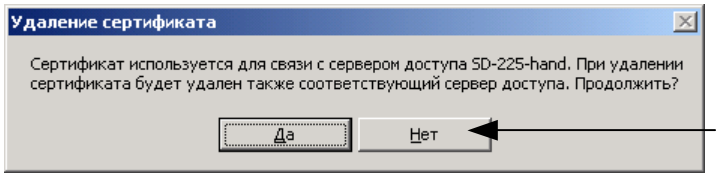
Для удаления сертификата:

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Сертификаты" (см. Рис. 3 на стр. 23).
3. Выберите удаляемый сертификат в списке "Сертификаты пользователя".

Совет. Для просмотра информации о сертификате совместите указатель с элементом списка, затем дважды нажмите левую кнопку мыши. На экране появится стандартное окно для просмотра сведений о сертификате.

4. Нажмите кнопку "Удалить".
5. Подтвердите удаление сертификата в окне запроса.

Если удаляется сертификат, используемый для аутентификации пользователя на одном из зарегистрированных серверов доступа, на экране появится окно запроса:



6. Нажмите кнопку "Да".

На экране появится диалог выбора ключевого носителя для чтения личной ключевой информации пользователя (см. Рис. 4 на стр.24).

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

Окно запроса ключевого носителя закроется и появится запрос пароля.

8. Введите пароль, которым был ограничен доступ к личной ключевой информации. Предъявите ключевой носитель и нажмите кнопку "ОК".

Пояснение. Если удаляется сертификат, созданный по запросу, укажите пароль, который был задан вами при создании файла запроса (см. п. **7** на стр. 25). Во всех остальных случаях пароль вам должен сообщить администратор при передаче соответствующего ключевого носителя.

Дальнейший порядок действий зависит от типа выбранного ключевого носителя. Следуйте инструкциям, появляющимся на экране.



Внимание! При использовании криптопровайдера КриптоПро CSP во время удаления сертификата предлагается очистить ключевой носитель, содержащий закрытый ключ сертификата. Помните, что при очистке ключевого носителя удаляется вся информация, которую он содержал, в том числе информация, записанная на носитель другими программами. Если в качестве ключевого носителя используется дискета, удалена будет только служебная информация КриптоПро CSP.

9. Закройте окно управления настройками абонентского пункта с сохранением изменений.

В результате выполненных действий сертификат пользователя будет удален из локального хранилища сертификатов. Удаление сертификата из хранилища не уничтожает файл, в котором хранится сертификат.

глава 4

Управление соединением с сервером доступа

Из этой главы вы узнаете:

- Как подключиться к защищенной сети
- Как отключиться от защищенной сети
- Как действовать при наличии ошибок соединения

Управление программой SAgent

Управление программой SAgent осуществляется с помощью контекстного меню пиктограммы SAgent, размещающейся на панели задач Windows:

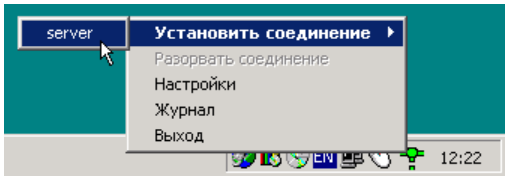


Рис. 8. Контекстное меню пиктограммы SAgent

Кроме того, эта пиктограмма отображает состояние соединения абонентского пункта и сервера доступа:

- (красная) — режим "offline", ожидание команды пользователя;
- (желтая) — режим "handshake", инициализация соединения с сервером доступа;
- (зеленая) — режим "online", соединение с сервером доступа установлено.

Совет. При отсутствии на панели задач Windows пиктограммы SAgent, активизируйте в главном меню Windows команду "Программы \ Continent \ Клиент Континент".

Подключение к защищенной сети

Для подключения к сети:



Пиктограмма SAgent

1. Вызовите контекстное меню пиктограммы SAgent.
2. Выберите команду "Установить соединение".

   Пояснение. Если не зарегистрирован ни один сервер доступа, команда "Установить соединение" будет недоступна.

   На экране появится подменю, содержащее перечень зарегистрированных серверов доступа.
3. Активизируйте команду с названием нужного сервера доступа.

   На экране появится диалог выбора ключевого носителя для чтения личной ключевой информации пользователя (см. Рис. 4 на стр.24).

   Пояснение. Диалог появится на экране только при установке первого соединения в текущем сеансе работы с программой SAgent. В остальных случаях попытка соединения с сервером осуществляется немедленно.
4. В списке "Устройства" выберите устройство для чтения ключевой информации и предъявите ключевой носитель.

   Окно запроса ключевого носителя закроется и появится запрос пароля.
5. Введите пароль, которым был ограничен доступ к личной ключевой информации. Предъявите ключевой носитель и нажмите кнопку "OK".

   Пояснение. Если регистрируется сертификат, созданный по запросу, укажите пароль, который был задан вами при создании файла запроса (см. п. **7** на стр. 25). Во всех остальных случаях пароль вам должен сообщить администратор при передаче соответствующего ключевого носителя.

   Дальнейший порядок действий зависит от типа выбранного ключевого носителя. Следуйте инструкциям, появляющимся на экране.



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

После того как выполнены все необходимые действия, происходит установка управляющего соединения с выбранным сервером доступа и обмен аутентификационной информацией. После успешной аутентификации устанавливается соединение с защищенной сетью.

Отключение от защищенной сети

Отключение пользователя от защищенной сети может осуществляться как по инициативе пользователя (см. ниже), так и принудительно администратором сервера доступа. В случае принудительного отключения на экране монитора появляется сообщение об этом.

Для отключения от сети:



Пиктограмма SAgent

1. Вызовите контекстное меню пиктограммы SAgent.
2. Активизируйте команду "Разорвать соединение".

   В результате выполненных действий защищенное соединение будет разорвано, а ключевая информации сессии — удалена.

Завершение работы программы SAgent

Для завершения работы программы SAgent:



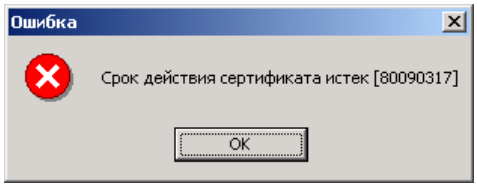
Пиктограмма SAgent

1. Вызовите контекстное меню пиктограммы SAgent.
2. Активизируйте команду "Выход".

Ошибки подключения и способы их преодоления

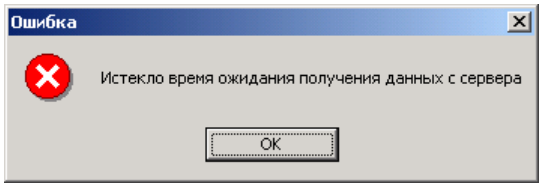
В процессе работы возможны ситуации, когда в силу тех или иных причин установка защищенного соединения невозможна. В этом случае на экране появляется сообщение об ошибке.

Совет. Ошибки установки соединений регистрируются в журнале соединений, записи которого могут оказаться полезными для диагностики причин ошибок. Работа с журналом соединений рассматривается в Главе 5 (см. стр. 39).



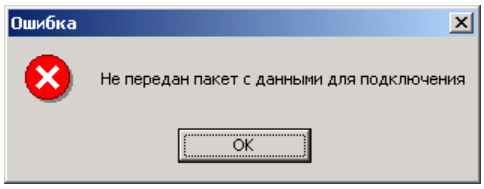
Причина Истек срок действия зарегистрированных сертификатов.

Действия Нажмите кнопку "OK". Свяжитесь с администратором безопасности для получения новых сертификатов и зарегистрируйте их. Предварительно, если это необходимо, создайте файл запроса и передайте его администратору.



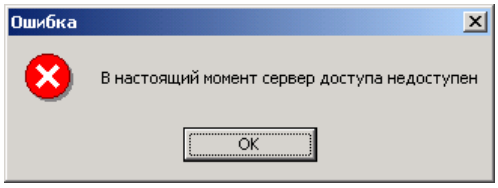
Причина Сервер доступа заблокирован.

Действия Нажмите кнопку "OK". Свяжитесь с администратором безопасности для выяснения причин блокировки сервера.



Причина Заблокирована учетная запись пользователя на сервере доступа.

Действия Нажмите кнопку "OK". Свяжитесь с администратором безопасности для выяснения причин блокировки вашей учетной записи.



Причина В связи с ограничениями по времени работы, установленными для вас администратором, в данный момент времени вам запрещено подключение к серверу доступа.

Действия Нажмите кнопку "OK". Обратитесь к администратору безопасности для уточнения вашего расписания работы с ресурсами защищаемой сети.

Особенности работы в различных режимах соединения

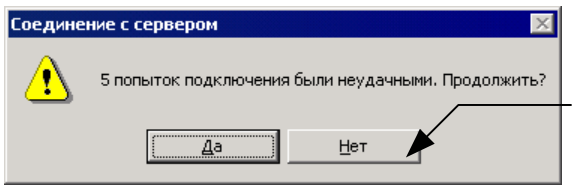
Запрет незащищенных соединений

При включении этого режима во время установленного защищенного соединения запрещается доступ к любым сетевым ресурсам, кроме ресурсов защищенной сети.

Повтор попыток соединения при неудаче

При использовании этого режима после неудачной попытки подключиться к серверу доступа попытки соединения с ним повторяются автоматически.

Если число попыток не ограничено, то они будут повторяться до установки соединения. Если число попыток задано, и все они окажутся безуспешными, то появится следующее сообщение:



Если требуется повторить попытки подключения к серверу доступа, нажмите кнопку "Да".

Автоматическое восстановление соединений

При работе в этом режиме в случае разрыва соединения абонентский пункт пытается автоматически восстановить соединение с сервером доступа. Попытки автоматического восстановления соединения повторяются неограниченное число раз до восстановления соединения с сервером доступа.

Контроль успешности доступа

Абонентский пункт не выдает экранных сообщений и не помещает в журнал регистрации записей, свидетельствующих о наличии запретов на прохождение тех или иных IP-пакетов. Для контроля успешности доступа следует ориентироваться на сообщения прикладных программ, с которыми вы работаете, например, **Internet Explorer**, **Outlook** и т.д.

В тех случаях, когда:

- прикладная программа сообщает о невозможности выполнения какой-либо операции, например, о невозможности соединения с Web-сервером или открытия нужной Internet-страницы;
- при этом вы правильно выполняете все необходимые действия;
- и прикладная программа настроена правильно.

  Следует предположить, что ошибка в работе прикладной программы связана с ограничениями доступа, установленными средствами абонентского пункта.

Подробные сведения о том, как контролировать успешность доступа к ресурсам защищенной сети и на какие сообщения об ошибках прикладных программ нужно обратить внимание, должны предоставляться администратором безопасности.



Работа с журналом соединений

Из этой главы вы узнаете:

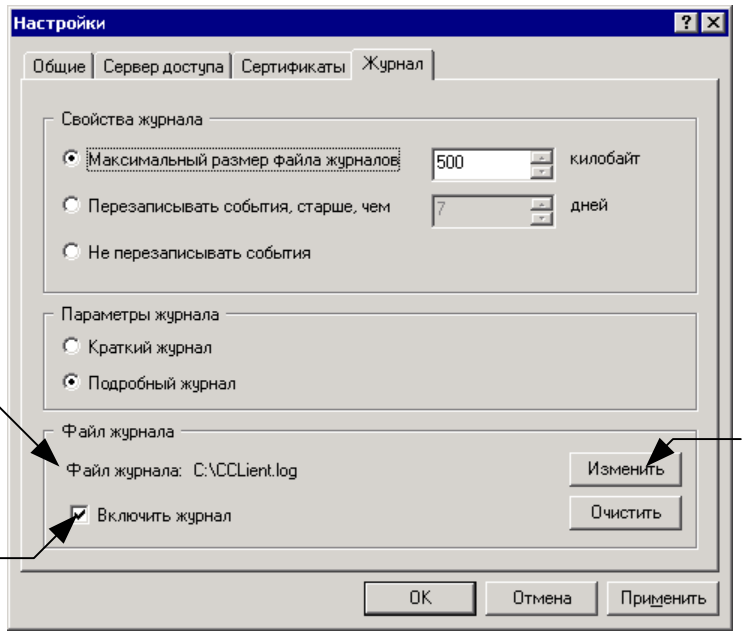
- Как настроить параметры журнала соединений
- Как пользоваться программой для просмотра журнала
- Как очистить журнал соединений

Журнал соединений предназначен для регистрации событий, относящихся к соединениям абонентского пункта с сервером доступа. Необходимость ведения журнала соединений определяется пользователем.

Включение и отключение журнала соединений

Для управления журналом:

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Журнал":



Название и расположение файла журнала соединений

Отметьте это поле, чтобы включить режим регистрации событий в журнале соединений

Используйте эту кнопку для выбора файла журнала

Рис. 9. Диалог "Журнал"

3. Определите необходимость ведения журнала соединений:
   - поставьте отметку в поле "Включить журнал" — для включения режима регистрации событий в журнале соединений;
   - уберите отметку из поля "Включить журнал" — чтобы отключить режим регистрации событий в журнале.

Внимание! Отключение режима регистрации событий в журнале соединений не очищает файл журнала, а приостанавливает его заполнение. Включение режима регистрации событий возобновляет регистрацию событий в том же самом файле журнала.

4. Нажмите кнопку "OK".

Настройка параметров журнала соединений

Для настройки параметров:

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Журнал" (см. Рис. 9).
3. Определите способ очистки журнала (описание процедуры см. ниже).
4. Для выбора формата ведения журнала отметьте одно из полей:
   - "Краткий журнал" — регистрация событий подключения абонентского пункта к серверу доступа будет производиться без детализации по фазам соединения;

- "Подробный журнал" — подробная регистрация событий.

  Совет. Этот режим рекомендуется для диагностики ошибок соединения с сервером доступа.

5. Выберите файл для хранения журнала соединений (см. стр. 41).
6. Нажмите кнопку "OK".

Определение способа очистки журнала

Для настройки параметров:

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Журнал" (см. Рис. 9 на стр. 40).
3. Для автоматической очистки журнала соединений при достижении заданного размера файла журнала:
   - отметьте поле "Максимальный размер файла журналов";
   - укажите в числовом поле справа размер файла журнала (в килобайтах), при превышении которого будет осуществляться автоматическая очистка журнала.

   Для перезаписи событий старше заданного количества дней:
   - отметьте поле "Перезаписывать события, старше, чем";
   - укажите в числовом поле справа срок хранения записей журнала (в днях).

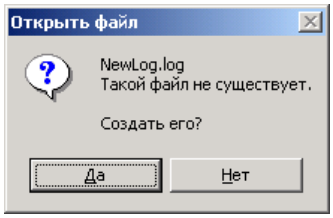
   Чтобы отказаться от автоматической очистки журнала:
   - отметьте поле "Не перезаписывать события".
4. Нажмите кнопку "OK".

Выбор файла для хранения журнала

Для смены файла журнала:

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Журнал" (см. Рис. 9 на стр. 40).
3. Нажмите кнопку "Изменить".
4. В стандартном окне Windows, появившемся на экране, укажите:
   - диск (каталог) для создания файла;
   - имя файла журнала;
   - нажмите кнопку "Открыть" (или "Сохранить").

   При создании нового файла на экране появится запрос:



5. Нажмите кнопку "Да".

   Заданное имя файла отобразится в текстовом поле "Файл журнала".
6. Нажмите кнопку "OK".

Очистка журнала соединений

Для очистки журнала:

1. Вызовите на экран окно управления настройками абонентского пункта.
2. Активизируйте закладку "Журнал" (см. Рис. 9 на стр. 40).
3. Нажмите кнопку "Очистить".
4. В появившемся на экране диалоге нажмите кнопку:
   - "Да" — чтобы удалить все записи журнала;
   - "Нет" — чтобы отменить удаление.
5. Нажмите кнопку "OK".

Программа просмотра журнала

Для просмотра журнала соединений используется программа SView.exe.

Для запуска программы:

1. Вызовите контекстное меню пиктограммы SAgent (см. Рис. 8 на стр. 34).
2. Активизируйте команду "Журнал".

Для завершения работы программы:

Выполните одно из следующих действий:

- выберите команду "Выход" в меню "Файл";
- нажмите комбинацию клавиш <Alt>+<F4>.

Общие сведения о журнале соединений

Перечень событий, регистрируемых в журнале, дан в Приложении на стр. 52.

Каждая запись журнала состоит из нескольких полей, перечисленных в Табл. 2.

Табл. 2. Список полей журнала соединений

Поле	Содержимое
Тип	Тип события. Обозначается пиктограммой, которая соответствует типу события: сообщение, предупреждение, ошибка. Название поля в заголовке таблицы не отображается
Дата и время	Дата и время регистрации события
Модуль	Программный компонент, действия которого привели к появлению события
Событие	Название события
Параметр	Дополнительная информация, характеризующая событие. Обычно это — IP-адрес сервера доступа или название операции, при выполнении которой произошла ошибка

Интерфейс программы просмотра журнала

Окно программы просмотра имеет вид:

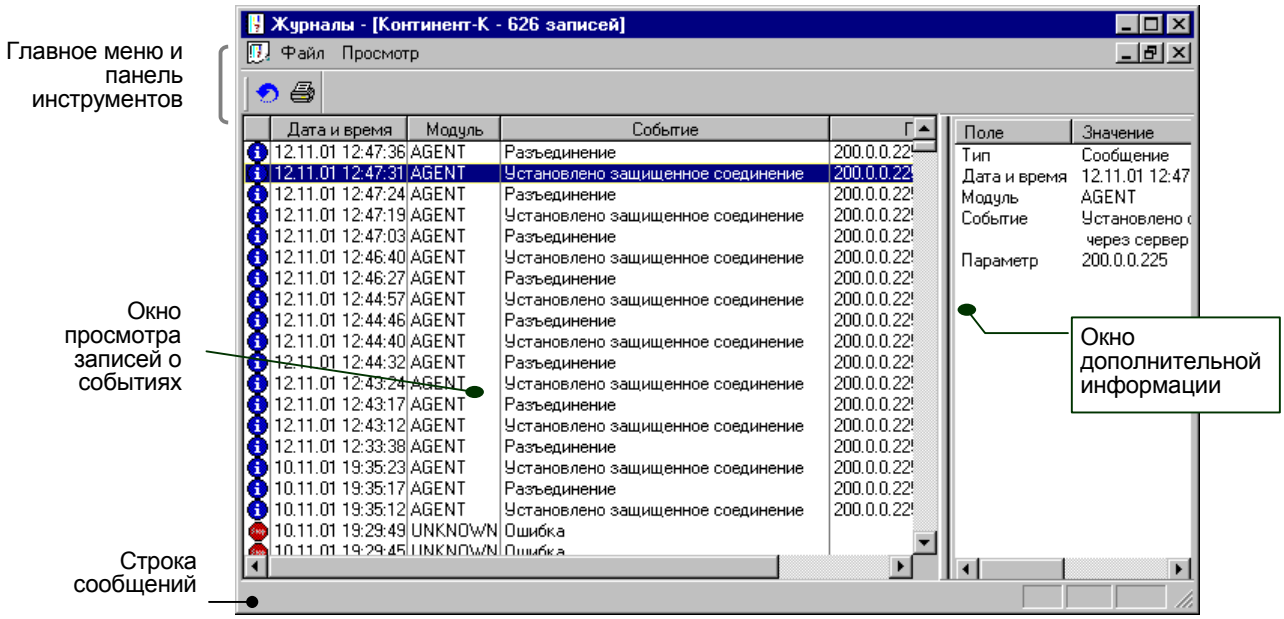


Рис. 10. Окно программы просмотра журнала

Основное окно программы состоит из следующих частей:

- **окно просмотра записей** (левая часть) — окно, в котором отображаются записи журнала, представленные в виде таблицы. Каждая строка этой таблицы представляет собой запись об отдельном событии, а столбцы соответствуют полям, перечисленным в Табл. 2. Записи приводятся в порядке регистрации соответствующих событий (при условии, что вы сами не изменили порядок сортировки отображения записей журнала);
- **окно дополнительной информации** (правая часть) — отображает подробную информацию о выбранной записи. Информация представлена в виде таблицы. В столбце "Поле" отображаются названия полей записи. В столбце "Значение" отображается содержимое каждого поля текущей записи. Если ни одна запись не выбрана, окно дополнительной информации будет пустым.

Отдельными элементами интерфейса являются всплывающие окна. Они появляются при совмещении указателя мыши с определенной областью основного окна (например, с кнопкой панели инструментов, ячейкой таблицы записей). Всплывающие окна могут содержать справочную информацию или подробные сведения, относящиеся к текущему элементу основного окна.

Управление программой просмотра журнала осуществляется с помощью команд основного меню, панели инструментов и контекстного меню. Некоторые команды можно выполнить и с помощью "горячих клавиш". В Табл. 3 приведен перечень "горячих клавиш" и соответствующих им кнопок панели инструментов.

Табл. 3. Кнопки панели инструментов программы SView

"Горячие клавиши"	Кнопка	Назначение
F5		Обновить журнал событий
Ctrl+P		Печать журнала (целиком или выделенных записей)
Alt+Enter		Открыть/закрыть окно просмотра дополнительной информации
Alt+F4		Завершить работу программы просмотра журнала

Краткую информацию об элементах основного меню и кнопках панели инструментов можно получить из подсказки в строке сообщений. Сообщение появляется в строке при выборе пункта меню или кнопки панели инструментов.

Всплывающие информационные окна

Чтобы увидеть всю запись, которая не помещается в поле целиком, наведите на нее курсор мыши. Через 1-2 секунды значение записи будет выведено полностью во всплывающем окне светло-желтого цвета. Это позволяет экономить место на экране и получать всю необходимую информацию, не изменяя размера окон и столбцов таблицы.

Управление окнами просмотра

При необходимости положение и размер окон программы SView можно изменить. Для управления окнами используйте следующие операции:

- включение/отключение отображения окна дополнительной информации;
- перемещение окон;
- изменение размеров окон.

► Для отображения окна дополнительной информации:

Выполните одно из следующих действий:

- нажмите комбинацию клавиш <Alt>+<Enter>;
- в меню "Просмотр" активизируйте команду "Дополнительная информация".

Примечание. Для отключения отображения окна дополнительной информации повторите те же действия еще раз.

Управление окном просмотра записей

Управление положением и размером окна осуществляется стандартными способами, используемыми в Windows для работы с окнами.

Управление окном дополнительной информации

Окно дополнительной информации программы SView может отображать информацию в следующих режимах:

- режим области просмотра — информация представлена в области просмотра внутри основного окна программы. По умолчанию окно дополнительной информации отображается в этом режиме (см. Рис. 10 на стр. 43);
- оконный режим — информация представлена в отдельном окне.

В режиме области просмотра окно дополнительной информации "причалено" к внутренней границе основного окна программы (см. Рис. 10). При этом размер области просмотра записей уменьшен за счет занимаемой области для отображения окна дополнительной информации.

В оконном режиме дополнительная информация отображается в отдельном окне, не зависящем от положения и размера основного окна программы. В этом режиме окно дополнительной информации можно разместить в любом месте экрана.

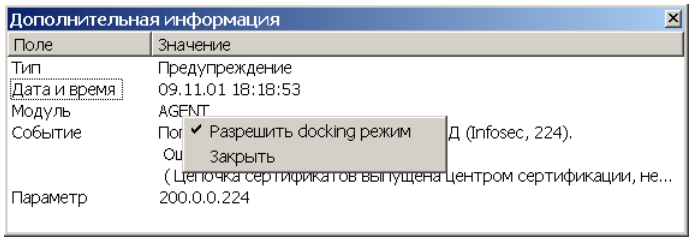


Рис. 11. Окно дополнительной информации (оконный режим)

Для управления окном используйте команды контекстного меню, которое вызывается в области отображения информации этого окна. Кроме того, можно использовать стандартные средства управления окнами.

Для перевода окна дополнительной информации в оконный режим:

- С отключением режима "причаливания":
  1. Вызовите контекстное меню внутри окна дополнительной информации.
  2. Активизируйте команду "Разрешить docking режим".
- Без отключения режима "причаливания":



  1. Установите указатель мыши на границу окна дополнительной информации. Курсор изменит вид, отображая состояние готовности к перемещению окна.
  2. Дважды нажмите левую кнопку мыши.

Для перевода окна дополнительной информации в режим области просмотра:

1. Вызовите контекстное меню внутри окна дополнительной информации.
2. Если слева от команды "Разрешить docking режим" установлена отметка, перейдите к шагу **3**. Иначе, для включения режима "причаливания", активизируйте эту команду.
3. Установите указатель мыши на заголовок окна.
4. Дважды нажмите левую кнопку мыши.

Совет. Если для окна дополнительной информации включен режим "причаливания" (отмечена команда "Разрешить docking режим"), перевод из одного режима в другой может осуществляться перемещением рамки окна в нужную область экрана. Действия по перемещению окна описаны ниже.

Для перемещения в оконном режиме:

Используйте стандартные способы перемещения.

Для перемещения в режиме области просмотра:



1. Установите указатель мыши на границу окна дополнительной информации. Курсор изменит вид, отображая состояние готовности к перемещению окна.
2. Нажмите левую кнопку мыши, и, удерживая кнопку нажатой, перемещайте рамку окна в нужную область экрана.
3. Завершив перемещение, отпустите кнопку мыши.



Внимание! Если включен режим "причаливания" (отмечена команда "Разрешить docking режим"), во время перемещения рамка окна автоматически подстраивается под ту или иную границу основного окна программы. Чтобы зафиксировать окно дополнительной информации в таком положении (т. е. включить режим области просмотра), прекратите перемещение.

Изменение размеров окна дополнительной информации осуществляется стандартными способами, если окно находится в оконном режиме отображения. Для этого используйте границы окна или команду "Размер" в меню заголовка окна.

Размер окна, отображаемого в режиме области просмотра, изменяется перемещением границы, которая разделяет окно дополнительной информации и область просмотра записей. Операция по перемещению разделяющей границы является стандартной.

Типовые операции при работе с журналом

Обновление записей журнала

Для обновления записей:

Выполните одно из следующих действий:

- Нажмите на клавишу <F5>.
- Нажмите кнопку  на панели инструментов.
- Активизируйте команду "Повторить выборку данных" в меню "Просмотр".

Сортировка записей в окне просмотра

Записи в окне просмотра можно сортировать в соответствии со значениями в каком-либо столбце. Направление сортировки может быть:

- **прямым** — в порядке возрастания значений столбца от первой записи к последней;
- **обратным** — в порядке убывания значений столбца от первой записи к последней.

Первой считается самая верхняя запись в таблице выборки.

Прямая сортировка по датам распределяет записи в соответствии со временем их регистрации, начиная с тех, которые добавлены в журнал последними. Сортировка текстовых значений в прямом порядке выполняется в соответствии с русским или английским алфавитом.

Для сортировки записей по значениям в столбце:

Нажмите на заголовок столбца, по значениям которого будет выполняться сортировка. Записи будут отсортированы в прямом порядке. При повторном нажатии на заголовок, записи будут отсортированы в обратном порядке.

Изменение состава и порядка отображения полей журнала

В окне просмотра записей (см. Рис. 10 на стр. 43) можно изменить состав и порядок отображения полей журнала. Сделать это можно одним из следующих способов:

- непосредственно в окне просмотра событий;
- с помощью диалога "Отображаемые поля".

Для управления отображением полей в окне просмотра:

1. Совместите указатель мыши с заголовком настраиваемого столбца и нажмите правую кнопку мыши. Откроется контекстное меню:

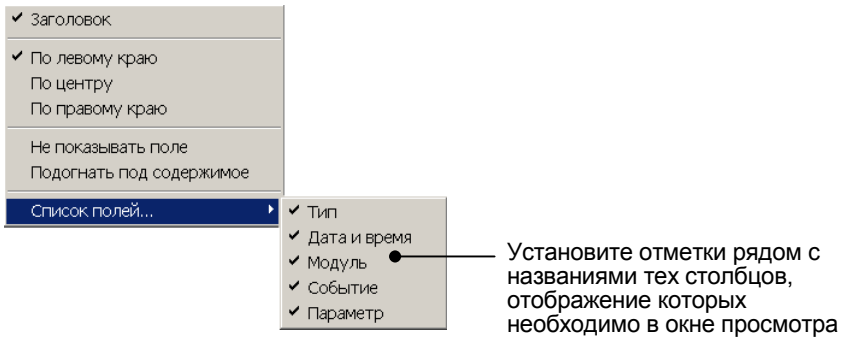


Рис. 12. Контекстное меню для управления отображением полей

2. Активизируйте команду:
   - "Заголовок" — чтобы включить/выключить отображение названия поля в заголовке столбца;
   - "По левому краю", "По центру" или "По правому краю" — чтобы соответствующим образом выровнять содержимое столбца;
   - "Не показывать поле" — чтобы запретить отображение поля в окне просмотра;
   - "Подогнать под содержимое" — чтобы ширина столбца стала равной максимальной длине помещенного в нем текста.
2. Определите перечень отображаемых столбцов с помощью подменю команды "Список полей".
3. Определите порядок следования столбцов в журнале. Для этого нажмите на кнопку-заголовок столбца и, удерживая левую кнопку мыши в нажатом положении, переместите заголовок столбца в нужное место.

Для управления отображением полей из специального диалога:

1. Вызовите на экран диалог "Отображаемые поля" одним из следующих способов:
   - активизируйте команду "Параметры просмотра" в меню "Просмотр";
   - нажмите комбинацию клавиш <Ctrl>+<F>.

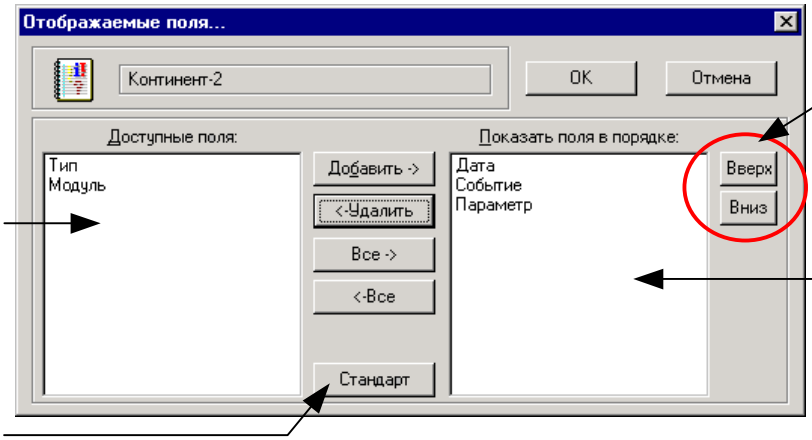


Рис. 13. Диалоговое окно "Отображаемые поля"

2. Определите список полей, отображаемых в журнале.

   Совет. Для использования стандартного набора полей, предлагаемого программой просмотра по умолчанию, нажмите кнопку "Стандарт". Чтобы выбрать все поля используйте кнопку "Все->" или "<-Все".

3. Укажите порядок отображения полей журнала:
   - выберите название поля в списке "Показать поля в порядке";
   - установите необходимое положение поля с помощью кнопок "Вверх" или "Вниз", учитывая, что верхнему полю списка соответствует левый столбец в журнале.
4. Нажмите кнопку "OK".

Печать записей журнала

Программа SView позволяет распечатать записи выборки, причем на печать выводятся только столбцы, отображаемые в таблице записей. Поэтому перед печатью может возникнуть необходимость изменить порядок и состав столбцов таблицы (см. стр. 46).

Для печати всех записей выборки:

1. Выполните одно из следующих действий:



   - нажмите кнопку "Печать";

- нажмите комбинацию клавиш <Ctrl>+<P>;
- в меню "Файл" активизируйте команду "Печать…".

На экране появится следующий диалог.

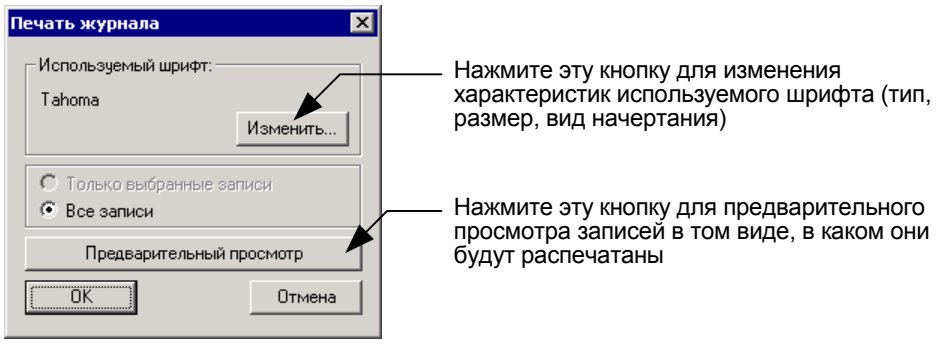


Рис. 14. Диалог "Печать журнала"

2. Установите отметку в поле "Все записи".
3. Если необходимо изменить характеристики шрифта для печати, нажмите кнопку "Изменить…". На экране появится стандартный диалог выбора шрифтов. Выполните настройку необходимых параметров и закройте диалог.
4. Нажмите кнопку "Предварительный просмотр". На экране появится стандартное окно предварительного просмотра.

   Если в ячейках таблицы не умещается нужная информация, закройте окно — процедура отправки на печать прекратится. Увеличить ширину столбцов таблицы можно следующими способами:

   - удалив из таблицы столбцы, содержащие несущественную информацию;
   - расширив область печати документа. Для этого в меню "Файл" активизируйте команду "Параметры страницы". На экране появится стандартный диалог настройки свойств принтера. В диалоге выберите больший размер бумаги (если это возможно) или выберите ориентацию бумаги "Альбомная".

   После этого повторно выполните шаги **1**–**4**.
5. В окне предварительного просмотра нажмите кнопку "Печать…". На экране появится стандартный диалог настройки свойств принтера и параметров печати.
6. Установите необходимые параметры и нажмите кнопку "OK".

▶ Для печати отдельных записей журнала:

1. Выберите записи, которые необходимо распечатать.

   Совет. Для выбора нескольких записей используйте клавиши <Ctrl> или <Shift>.
2. Выполните одно из следующих действий:

   - вызовите контекстное меню одной из выбранных записей и активизируйте команду "Печать…";
   - нажмите кнопку "Печать";
   - нажмите комбинацию клавиш <Ctrl>+<P>;
   - в меню "Файл" активизируйте команду "Печать…".

   На экране появится диалог настройки параметров печати (см. Рис. 14).
3. Оставьте отмеченным поле переключателя "Только выбранные записи" и выполните шаги **3**–**6** процедуры отправки на печать всех записей выборки (см. Выше).

Очистка журнала

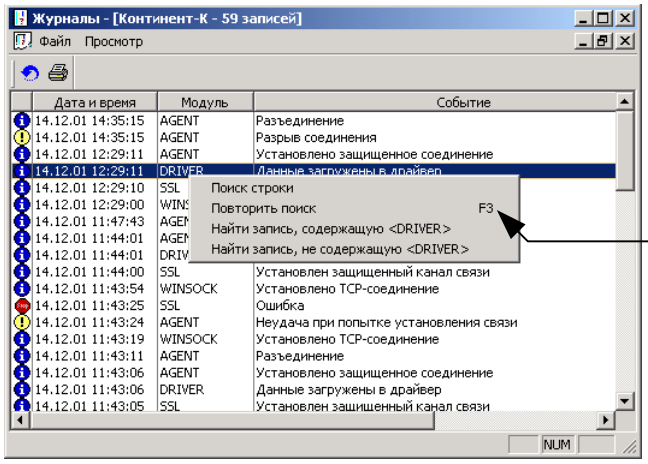
Подробное описание процедуры очистки журнала читайте на стр. 41. и стр. 42.

Поиск нужной записи

Поиск нужной записи осуществляется по значениям, содержащимся в определенном столбце таблицы. Поиск всегда ведется в направлении к последней записи таблицы. Если найдена ячейка столбца, удовлетворяющая заданным условиям, программа выделит запись и прекратит процедуру поиска. Иначе на экране появится диалог, предлагающий повторить поиск с первой записи выборки или отменить процедуру.

▸ Для вызова меню поиска:

Установите указатель мыши на нужный столбец и вызовите контекстное меню:



Эта команда появится в меню **только** после выполнения процедуры поиска

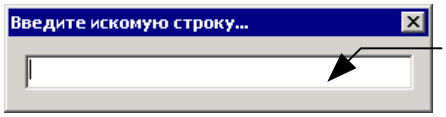
Рис. 15. Меню поиска по содержимому столбца

Поиск произвольной строки символов

Этот способ позволяет найти запись, которая содержит в соответствующем столбце определенную строку символов. Строка может быть частью содержимого столбца. Регистр введенных символов не учитывается.

▸ Для поиска записи:

1. Вызовите меню поиска (см. Выше).
2. Активизируйте команду "Поиск строки". На экране появится диалог ввода строки:



Если в данной выборке записей поиск уже осуществлялся, поле ввода строки символов содержит предыдущее значение поиска. Иначе это поле будет пустым

3. Если поле ввода уже содержит необходимое значение (по которому осуществлялся предыдущий поиск), перейдите к шагу **4**. Иначе выполните одно из следующих действий:
   - введите с клавиатуры строку поиска;
   - вставьте содержимое буфера обмена, используя стандартные способы (например, активизировав команду "Вставить" в контекстном меню поля).

   Совет. В буфер обмена можно поместить содержимое любой ячейки таблицы записей. Для этого перед процедурой поиска вызовите контекстное меню записи в соответствующем столбце и активизируйте команду "Копировать".
4. Нажмите клавишу <Enter>.

Поиск следующей записи, содержащей/не содержащей выбранное значение

Этот способ позволяет найти следующую запись, которая содержит то же (или, напротив, не содержит его) значение столбца текущей записи.

Для поиска записи:

1. Вызовите меню поиска (см. Выше).
2. Активизируйте одну из команд:
   - "Найти запись, содержащую <…>" (где <…> — значение столбца текущей записи) — для поиска следующей записи с таким же значением столбца;
   - "Найти запись, не содержащую <…>" (где <…> — значение столбца текущей записи) — для поиска следующей записи с другим значением столбца.

Повтор поиска

Повтор поиска — это продолжение процедуры поиска среди значений определенного столбца, начиная с текущей записи. Если поиск нужной записи не производился, повтор поиска невозможен.

Для повтора поиска:

1. Выделите запись, начиная с которой необходимо повторить процедуру поиска.
2. Выполните одно из следующих действий:
   - вызовите контекстное меню записи в любом столбце и активизируйте команду "Повторить поиск";
   - нажмите клавишу <F3>;
   - в меню "Просмотр" активизируйте команду "Повторить поиск".

   Программа выполнит поиск следующей записи в соответствии с параметрами предыдущего поиска.

Приложение

В Приложении содержится следующая информация:

- Перечень событий, регистрируемых в журнале соединений
- Порядок настройки свойств сетевого окружения компьютера
- Описание программного модуля SStart

Перечень событий, регистрируемых в журнале соединений

Название события	Комментарий
Создан файл журнала	Первая запись, вносимая в журнал при его создании. В качестве значения поля "Модуль" задано UNKNOWN
Разрыв соединения	Прекращение соединения вопреки желанию пользователя, например, из-за помех в линии связи
Разъединение	Прекращение соединения по инициативе пользователя
Авторизация	Проверка полномочий пользователя на доступ к ресурсам защищенной сети
Неудача при попытке установления связи	Обобщающее сообщение, характеризующее неудачную попытку установки связи
Установлен защищенный канал связи	Аутентификация по протоколу SSL успешно завершена
Установлено TCP-соединение	Установлено соединение с сервером доступа по протоколу TCP/IP
Ошибка	Произошла ошибка
Попытка восстановления соединения	Попытка установления соединения была неудачной, произведена новая попытка установки соединения согласно настройкам программы
Данные загружены в драйвер	Необходимые криптографические данные успешно загружены в драйвер
Установлено защищенное соединение	Обобщающее сообщение, включающее в себя успешное завершение этапов TCP/IP соединения, SSL- соединения и загрузки данных в драйвер

Управление свойствами сетевого окружения

После установки защиты сетевых адаптеров запрещается вносить какие-либо изменения в свойства сетевого окружения. В тех случаях, когда необходимо изменить свойства сетевого окружения, например, осуществить замену сетевого адаптера, добавить сетевой протокол и т.д., следует предварительно временно отключить защиту сетевых адаптеров. Установка ЭЗ "Соболь" также требует временного отключения защиты. Выполняйте процедуру изменения свойств сетевого окружения в следующем порядке:

- отключите защиту сетевых адаптеров;
- выполните настройку свойств сетевого окружения и перезагрузите компьютер;

  Например, при смене сетевого адаптера:
  - установите плату нового адаптера в компьютер;
  - выполните установку и настройку драйвера сетевого адаптера;
  - перезагрузите компьютер и убедитесь, что новый адаптер работает корректно.

- восстановите защиту сетевых адаптеров.

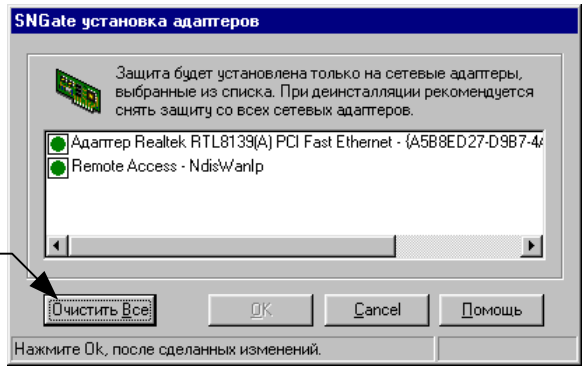
▶ Для временного отключения защиты:

1. Запустите на исполнение файл SetAdapter.exe, находящийся в каталоге \ Program Files \ Infosec \ ContinentClient на системном диске (на том, на котором установлена операционная система).

   Совет. Для поиска и запуска этого файла используйте программу Проводник или команду "Выполнить" из меню "Пуск" ("Start") Windows.

На экране появится диалог, содержащий список имеющихся на компьютере устройств доступа к сети. Те устройства, которые были защищены при установке абонентского пункта, отмечены символом .

Нажмите эту кнопку, чтобы отключить защиту всех устройств доступа к сети



2. Для отключения защиты нажмите кнопку "Очистить Все" или удалите с помощью мыши отметки ( ) слева от названий всех устройств. Затем нажмите кнопку "OK".

   На экране появится сообщение о необходимости перезагрузки компьютера. Для отключения защиты компьютер необходимо перезагрузить.

3. Нажмите кнопку "OK".

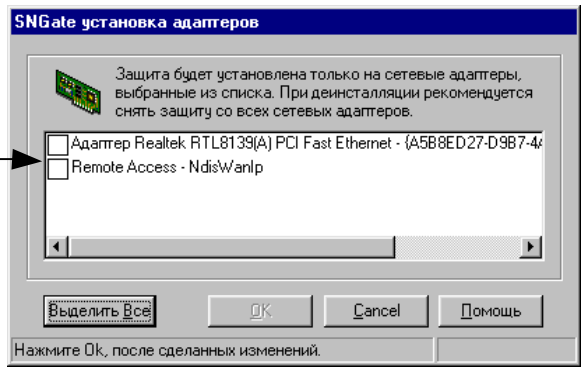
   Осуществится немедленная перезагрузка компьютера.

► Для восстановления защиты:

1. Запустите на исполнение файл SetAdapter.exe.

   На экране появится диалог:

Установите с помощью мыши отметки слева от названий защищаемых устройств



2. Для восстановления защиты установите с помощью мыши отметки ( ) слева от названий защищаемых устройств. Чтобы выбрать все устройства, нажмите кнопку "Выделить Всё". Затем нажмите кнопку "OK".

   На экране появится сообщение о необходимости перезагрузки компьютера. Для восстановления защиты компьютер необходимо перезагрузить.

3. Нажмите кнопку "OK".

   Осуществится немедленная перезагрузка компьютера.

Программный модуль SStart

В данном разделе содержатся сведения, необходимые для разработки программных средств, предназначенных для автоматического управления Абонентским пунктом.

Общие сведения

Программный модуль SStart предназначен для обращения внешнего приложения к Абонентскому пункту. Он позволяет внешнему приложению осуществлять инициализацию пользователя Абонентского пункта, установку и разрыв защищенного соединения Абонентского пункта с сервером доступа АПКШ "Континент" без участия оператора.

При установке ПО на компьютер файл SStart.exe автоматически помещается в папку \ Program Files \ Infosec \ ContinentClient.

Необходимые условия для работы модуля

Запуск модуля SStart осуществляется только после выполнения следующих условий:

- запущено ПО Абонентского пункта (программа SAgent);
- зарегистрирован корневой сертификат, сертификат сервера доступа и сертификат пользователя;
- в настройках Абонентского пункта определен сервер доступа по умолчанию.

Команды и коды завершения работы

Для запуска модуля SStart используйте строку следующего формата:

[диск:][путь]SStart[.exe] <команда>

Модуль SStart обеспечивает выполнение следующих команд:

- **Init** — инициализация пользователя Абонентского пункта, запрос и сохранение ключей шифрования;
- **Connect** — установка защищенного соединения Абонентского пункта с сервером доступа;
- **Break** — разрыв защищенного соединения Абонентского пункта с сервером доступа.

После выполнения команды модуль SStart возвращает код завершения работы. Описание значений кодов представлено ниже.

Табл. 4. Коды завершения работы модуля SStart. Общие

Значение	Описание
0	корректное завершение
1	командная строка не содержит исполняемых команд
2	командная строка содержит исполняемую команду, но программа SAgent не запущена
3	исполнение команды произошло с ошибкой, не поддающейся детализации
100	таймаут (10 минут)

Табл. 5. Коды завершения работы модуля SStart. Команда Init

Значение	Описание
6	не установлен сервер по умолчанию

Табл. 6. Коды завершения работы модуля SStart. Команда Connect

Значение	Описание
4	не удалось установить соединение
5	не выполнена команда Init

Табл. 7. Коды завершения работы модуля SStart. Команда Break

Значение	Описание
5	не выполнена команда Init

Предметный указатель

Абонентский пункт
настройка параметров соединения 20
переустановка 16
требования к аппаратному и программному обеспечению 14
удаление 16
установка 14

Журнал соединений
включение 40
выбор файла для хранения журнала 41
выполнение типовых операций 46
интерфейс программы просмотра 43
настройка параметров 40
общие сведения 42
определение способа очистки 41
отключение 40
очистка журнала пользователем 42
печать записей 47
поиск записей 49
программа просмотра 42
управление окнами просмотра 44
формат ведения 40

Как...?
автоматически запускать программу SAgent после перезагрузки компьютера 20
завершить работу программы SAgent 35
запретить работу незащищенного соединения на время работы абонентского пункта 20
изменить свойства сетевого окружения компьютера 52
подключиться к защищенной сети 34
разорвать защищенное соединение 35

Регистрация сертификатов
корневого центра сертификации 27
пользователя 26
сервера доступа 22
со стандартными именами файлов 28
создание запроса на получение сертификата пользователя 23

Сертификаты
в файлах формата *.cer 22
в файлах формата *.p7b 22
общие сведения 22
просмотр 29

Управление сертификатами
резервное копирование 29
удаление 30