КОД безопасности

Аппаратно-программный комплекс шифрования

Континент
Версия 3.9

Руководство администратора

Сервер доступа

RU.88338853.501430.022 90 7

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

Оглавление

Список сокращений ... **5**

Введение ... **6**

Общие сведения ... **7**

Состав используемого программного обеспечения ... 7

Сервер доступа ... 7

Программа управления сервером доступа ... 8

Абонентский пункт ... 8

Принципы функционирования ... 9

Доступ удаленных пользователей к ресурсам защищенной сети ... 9

Аутентификация удаленного пользователя ... 10

Защита от DoS-атак ... 11

Управление сервером доступа ... 12

Лицензирование ... 12

Ввод сервера доступа в эксплуатацию ... **13**

Общий порядок ввода в эксплуатацию ... 13

Установка и настройка внешнего криптопровайдера ... 13

Программа управления сервером доступа ... **14**

Запуск программы управления сервером доступа ... 14

Интерфейс программы ... 15

Настройка параметров соединения с сервером доступа ... 17

Управление соединением с сервером доступа ... 17

Завершение работы программы ... 18

Управление работой сервера доступа ... **19**

Регистрация лицензий ... 19

Настройка параметров подключения абонентских пунктов ... 20

Блокировка сервера доступа ... 21

Механизм синхронизации СД в кластере КШ ... 21

Резервное копирование базы данных сервера доступа ... 21

Восстановление базы данных из резервной копии ... 22

Управление правилами фильтрации ... **23**

О правилах фильтрации ... 23

Управление списками объектов ... 24

Просмотр списка объектов ... 24

Создание объекта ... 24

Удаление объекта ... 24

Настройка параметров объектов ... 25

Вызов окна для настройки параметров объекта ... 25

Настройка подсети ... 25

Настройка сервисов ... 25

Настройка правил фильтрации ... 26

Настройка групп правил фильтрации ... 27

Управление сертификатами ... **29**

Управление списками сертификатов ... 29

Вызов списков сертификатов ... 29

Вызов списка сертификатов пользователя ... 30

Регистрация сертификатов внешнего центра сертификации ... 31

Регистрация корневого сертификата ... 31

Регистрация сертификата сервера доступа ... 31

Регистрация сертификата пользователя ... 33

Издание сертификатов средствами программы управления ... 33

Издание корневого сертификата ... 33

Издание сертификата сервера доступа ... 35

Издание сертификата пользователя ... 35

Просмотр информации о сертификатах ... 38
Хранение списка отозванных сертификатов ... 39
Удаление недействительных сертификатов ... 39

Управление пользователями ... 40
Доступ к ресурсам защищенной сети ... 40
Управление списком пользователей ... 40
Просмотр списка пользователей ... 40
Регистрация пользователей ... 41
Удаление пользователей ... 45
Управление параметрами работы пользователя ... 45
Вызов окна для настройки свойств пользователя ... 45
Блокировка учетной записи пользователя ... 46
Ограничение времени работы пользователя ... 46
Действия по результатам проверки ПАК "Соболь" ... 47
Разрешение и запрет на подключение по HTTP-туннелю ... 48
Назначение пользователю IP-адреса ... 48
Управление индивидуальным списком правил фильтрации ... 48
Просмотр прав доступа пользователя ... 49
Запрет сторонних соединений ... 49
Предупреждение об окончании срока действия сертификата ... 50

Мониторинг и оперативное управление ... 51
Просмотр информации о состоянии сервера доступа ... 51
Просмотр списка подключенных пользователей ... 51
Список зарегистрированных событий ... 52
Принудительное отключение абонентов ... 52

Приложение ... 53
Рекомендуемый порядок смены сертификатов ... 53
Управление ключами криптопровайдера "Код Безопасности CSP" ... 54
Варианты использования криптопровайдера при формировании закрытого ключа пользователя ... 57
"КриптоПро CSP" ... 57
"Код Безопасности CSP" ... 59
Совместимость для СД ... 60
Порядок установления связи между абонентскими пунктами ... 60
Доступ абонентского пункта в защищенные сети других КШ ... 60
Программные модули, требующие контроля целостности ... 61
Обмен данными по протоколу AH (IP-протокол 51) ... 61

Документация ... 63

Список сокращений

АП	Абонентский пункт
АПКШ	Аппаратно-программный комплекс шифрования
ДСЧ	Датчик случайных чисел
КШ	Криптографический шлюз
МЭ	Межсетевой экран
ООИ	Область отображения информации
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПУ СД	Программа управления сервером доступа
РМ	Рабочее место
СД	Сервер доступа
СКЗИ	Средство криптографической защиты информации
ЦУС	Центр управления сетью КШ
CSP	Cryptography Service Provider
DoS	Denial of Service
FTP	File Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network

Введение

Документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.9" (далее — комплекс, АПКШ "Континент"). Документ содержит сведения, необходимые для управления работой сервера доступа.

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Список учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru. Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Глава 1
Общие сведения

Аппаратно-программный комплекс шифрования "Континент" предназначен для создания виртуальных частных сетей. Технология VPN позволяет объединить локальные вычислительные сети, их сегменты или отдельные компьютеры предприятия в единую защищенную виртуальную сеть на базе общих сетей передачи данных. Основным назначением АПКШ "Континент" является защита информации, передаваемой по общим каналам связи, а также защита сегментов VPN от проникновения извне.

АПКШ "Континент" включает в свой состав средства, позволяющие организовать доступ пользователей удаленных рабочих станций, не входящих в состав защищаемых сегментов сети, к ресурсам VPN. В дальнейшем будем называть таких пользователей удаленными пользователями.

Для организации доступа удаленных пользователей к ресурсам защищаемой сети используется сервер доступа, входящий в состав программного обеспечения криптографического шлюза АПКШ "Континент", а также дополнительное программное обеспечение — средство криптографической защиты информации "Континент-АП" (далее — абонентский пункт).

Состав используемого программного обеспечения

Для организации доступа удаленных пользователей к ресурсам защищаемой сети используется следующее программное обеспечение:

- сервер доступа;
- программа управления сервером доступа;
- абонентский пункт.

Сервер доступа

Сервер доступа представляет собой предварительно устанавливаемое на одном из криптографических шлюзов программное средство, обеспечивающее доступ удаленных пользователей к ресурсам сегментов VPN.

Сервер доступа обеспечивает:

- защищенное соединение между АП и сетью, защищенной КШ;
- формирование симметричного ключа (ГОСТ 28147-89) для аутентификации администратора и запись ключевой информации на ключевой носитель;
- аутентификацию администратора при установлении защищенного соединения с программой управления;
- взаимодействие с программой управления;
- хранение необходимой для работы информации;
- аутентификацию удаленных пользователей посредством технологии сертификатов открытых ключей стандарта x509v3;
- загрузку в фильтр IP-пакетов криптографического шлюза правил фильтрации в соответствии с правами подключившегося пользователя;
- контроль состояния установленных защищенных соединений абонентских пунктов с криптографическим шлюзом и выгрузку сессионной информации при разрыве соединения;
- регистрацию событий, связанных с работой сервера, использованием программы управления и подключением удаленных пользователей.

Внимание! При высокой нагрузке КШ, реализующего функции МЭ и/или VPN, не рекомендуется использовать СД на этом КШ.

Программа управления сервером доступа

Программа управления сервером доступа предназначена для управления объектами базы данных СД и оперативного контроля его состояния. Программа устанавливается на одном или нескольких компьютерах защищаемого сегмента сети — РМ администратора.

В состав программы управления входят криптопровайдер "Код Безопасности CSP" и программа управления сгенерированными им ключами.

Программа управления обеспечивает:

- установление защищенного соединения и обмен данными с сервером доступа;
- мониторинг состояния сервера доступа и оперативное управление сервером;
- получение от сервера доступа и отображение информации о состоянии базы данных сервера;
- добавление, удаление и модификацию объектов базы данных сервера доступа;
- резервное копирование и восстановление базы данных сервера доступа;
- управление сертификатами открытых ключей;
- получение от сервера доступа журнала событий, его отображение и управление записями журнала.

Программа поставляется на оптическом носителе.

Абонентский пункт

Абонентский пункт является специализированным программным обеспечением, которое устанавливается на рабочих местах удаленных пользователей для организации их доступа к ресурсам защищаемой сети.

В состав абонентского пункта входят криптопровайдер "Код Безопасности CSP" и программа управления сгенерированными им ключами, а также программа управления абонентским пунктом и межсетевым экраном.

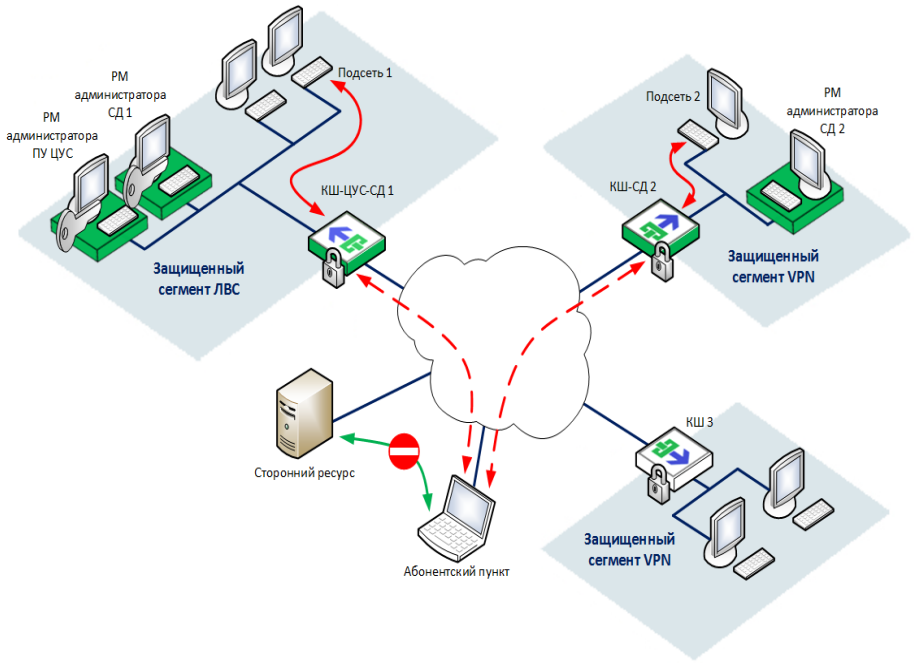
Абонентский пункт обеспечивает:

- установление защищенного соединения и обмен данными с сервером доступа;
- обоюдную аутентификацию с сервером доступа в процессе установления защищенного соединения посредством технологии сертификатов открытых ключей стандарта x509v3;
- защищенное соединение с сервером доступа по протоколу UDP и TCP;
- доступ к ресурсам VPN при установлении соединения с СД;
- необходимый функционал для работы с сертификатами открытых ключей;
- протоколирование подключений к серверу доступа в журнале соединений;
- отображение записей журнала соединений и управление ими;
- фильтрацию всего входящего и исходящего IP-трафика средствами встроенного МЭ.

Абонентский пункт поставляется на оптическом носителе.

Принципы функционирования

Доступ удаленных пользователей к ресурсам защищенной сети



Для организации доступа удаленного пользователя к корпоративным ресурсам криптографический шлюз комплектуется сервером доступа, а на компьютере удаленного пользователя устанавливается абонентский пункт. Один сервер доступа обслуживает защищенные сети только того КШ, на котором он установлен.

Удаленный пользователь, зарегистрированный на нескольких серверах доступа, может подключаться к любому из этих серверов с одного и того же абонентского пункта. Связь удаленного пользователя с внутренними ресурсами защищенной сети осуществляется по каналам связи общих сетей передачи данных. Одновременное подключение с одного абонентского пункта к нескольким серверам доступа невозможно.

Инициатором соединения абонентского пункта с сервером доступа может быть только удаленный пользователь. Разорвать соединение может как пользователь, так и администратор сервера доступа. В некоторых случаях разрыв соединения может автоматически выполняться самим сервером доступа.

Защищенное (с зашифрованным трафиком) соединение между абонентским пунктом и сервером доступа устанавливается только после их успешной взаимной аутентификации, которая осуществляется на основе сертификатов открытых ключей стандарта x509v3.

Для повышения устойчивости к сетевым атакам вида "отказ в обслуживании" (DoS-атакам) администратор имеет возможность вводить ограничения на количество одновременно подключенных к серверу доступа абонентских пунктов, а также на некоторые параметры таких соединений.

После установления соединения сервер доступа осуществляет загрузку правил фильтрации IP-пакетов из индивидуального списка правил данного пользователя в фильтр IP-пакетов криптографического шлюза. Кроме того, список доступных пользователю защищаемых подсетей передается на абонентский пункт. Далее обмен данными между абонентским пунктом и абонентами защищенной сети осуществляется через сервер доступа. При этом весь трафик, передаваемый между абонентским пунктом и защищенной сетью, шифруется с использованием алгоритма ГОСТ 28147–89.

Для упрощения настройки маршрутизации трафика между абонентским пунктом и абонентами защищенной сети абонентскому пункту назначается внутрисетевой IP-адрес. Трафик от абонента защищенной сети поступает на этот внутрисетевой IP-адрес абонентского пункта, а сервер доступа перенаправляет трафик непосредственно на абонентский пункт. При назначении абонентским пунктам внутрисетевых адресов может использоваться как динамическая, так и статическая адресация.

Резервирование IP-адресов из выделенного диапазона X.X.X.1 — X.X.X.N:

- X.X.X.1 — IP-адрес сервера доступа;
- X.X.X.2 — IP-адрес только для статической адресации;
- X.X.X.N — широковещательный IP-адрес (broadcast).

Остальные IP-адреса диапазона используются как для статической, так и динамической адресации.

Назначение абонентскому пункту статического адреса предоставляет возможность устанавливать связь абонентских пунктов между собой. Для установления такой связи необходимо дополнительно составить соответствующие правила фильтрации. Подробнее об установлении связи между абонентскими пунктами см. стр. **60**.

Предусмотрен режим работы абонентского пункта, который запрещает все незащищенные соединения со сторонними абонентами (например, с веб-узлами или FTP-серверами) во время связи с абонентами защищенной сети.

Внимание! Если на пути трафика, передаваемого между абонентским пунктом и сервером доступа или между программой управления и сервером доступа, находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать на этих устройствах правила фильтрации, разрешающие прохождение служебных пакетов комплекса.

Аутентификация удаленного пользователя

Аутентификация удаленного пользователя при установлении соединения между абонентским пунктом и сервером доступа осуществляется на основе сертификатов открытых ключей стандарта X.509v3.

Сертификат содержит имя владельца сертификата и его открытый ключ, а также дополнительную системную информацию. Достоверность этой информации подтверждается подписью доверенного центра сертификации.

Используются следующие сертификаты — корневой сертификат, сертификат сервера доступа и сертификат пользователя.

Возможны два варианта организации работы с сертификатами:

- Доверенным центром является внешний центр сертификации. Центр сертификации предоставляет корневой сертификат, сертификат сервера доступа, а также все сертификаты пользователей. Сертификат сервера доступа издается по запросу, сформированному администратором средствами программы управления. Сертификаты пользователей издаются по запросам, сформированным средствами абонентского пункта. Администратор не имеет доступа к закрытому ключу центра сертификации и закрытым ключам пользователей. Полученные сертификаты регистрируются на сервере доступа и передаются пользователям.
- Доверенным центром сертификации является программа управления сервером доступа. Администратор средствами программы управления и криптопровайдера, совместно с которым работает программа, издает корневой сертификат, сертификат сервера доступа, а также все сертификаты пользователей. Сертификат сервера доступа и сертификаты пользователей подписываются закрытым ключом центра сертификации — программы управления сервером доступа.

  В СД с режимом 3.x имеется возможность издания сертификатов пользователей по запросам, сформированным средствами абонентского пункта. В этом случае администратор не имеет доступа к закрытым ключам

пользователей. При работе с СД с режимом 4.x файл закрытого ключа передается в конфигурации пользователя.

Программа управления сервером доступа и абонентские пункты имеют свой встроенный криптопровайдер, а также поддерживают работу с криптопровайдером "КриптоПро CSP".

При использовании сертификатов внешнего центра сертификации наличие криптопровайдера "КриптоПро CSP" необходимо и на компьютере с программой управления сервером доступа, и на компьютерах с установленным абонентским пунктом.

При использовании корневого сертификата, созданного средствами программы управления сервером доступа с помощью криптопровайдера "КриптоПро CSP", этот криптопровайдер должен быть установлен и на компьютерах с абонентским пунктом.

Предусмотрена возможность одновременного использования в системе нескольких корневых сертификатов и нескольких сертификатов сервера доступа. Каждому пользователю также может быть выдано несколько сертификатов. При этом разные сертификаты пользователя могут быть заверены закрытыми ключами разных удостоверяющих центров, а могут — закрытым ключом одного и того же удостоверяющего центра. При плановой смене сертификатов такая возможность позволяет зарегистрировать новые сертификаты до истечения сроков действия заменяемых. Рекомендуется также регистрировать в системе резервные сертификаты на случай внеплановой смены действующих сертификатов, например, при компрометации закрытого ключа удостоверяющего центра.

При смене сертификатов работа пользователей, уже подключенных к серверу доступа, продолжается вплоть до завершения текущего сеанса работы. Если обновление сертификатов вызвано потерей доверия к существующим сертификатам, необходимо выполнить процедуру обновления и принудительно отключить всех пользователей от сервера доступа.

Защита от DoS-атак

Для повышения устойчивости сервера доступа к сетевым атакам вида "отказ в обслуживании" (DoS- атакам) администратор может вводить ограничения на следующие параметры:

- количество абонентских пунктов в очереди на подключение;
- число одновременно подключенных к СД абонентских пунктов;
- длина цепочки связанных сертификатов в сертификате пользователя;
- время, по истечении которого следует разорвать связь сервера доступа с неактивным абонентским пунктом.

Управление сервером доступа

Администратор управляет сервером доступа с помощью программы управления, которая устанавливается на одном или нескольких компьютерах защищенного сегмента сети — РМ администратора.

Примечание. При одновременном управлении СД с нескольких РМ возможны сбои в работе программы управления, поэтому рекомендуется их поочередное использование.

Соединение программы управления с сервером доступа устанавливается только после предъявления администратором персонального идентификатора. Этот идентификатор создается средствами локального управления сервером доступа и содержит уникальную ключевую информацию. Соединение программы управления с сервером доступа осуществляется по защищенному каналу.

Администратор осуществляет оперативный контроль состояния сервера доступа и управляет базой данных сервера.

Лицензирование

Лицензия на использование сервера доступа определяет максимальное количество пользователей, которые могут быть подключены к нему одновременно.

Лицензии являются накопительными. Общее количество разрешенных к использованию объектов равно сумме объектов, указанных в каждой лицензии.

При отсутствии зарегистрированных в базе данных лицензий подключение пользователей к серверу доступа становится невозможным. Пользователь также не сможет подключиться к серверу доступа, если количество подключенных в данный момент пользователей достигло максимального количества, указанного в лицензии. В этом случае на экране отобразится соответствующее сообщение.

Количество вакантных подключений проверяется при очередном подключении пользователя к серверу доступа.

Глава 2
Ввод сервера доступа в эксплуатацию

Общий порядок ввода в эксплуатацию

Внимание! При работе ПО СД на криптографических шлюзах, объединенных в кластер, необходимо использовать только один интерфейс резервирования (см. [**2**]).

Ввод сервера доступа в эксплуатацию осуществляется в следующем порядке:

1. Установка внешних компонентов криптопровайдера на РМ администратора (при необходимости):
   - При использовании внешнего криптопровайдера — установка и настройка внешнего криптопровайдера (см. стр. **13**).
   - При использовании собственным криптопровайдером физического ДСЧ— установка платы и ПО ПАК "Соболь" (см. документацию ПАК "Соболь").
2. Установка ПО СД на КШ.
3. Инициализация сервера доступа (см. [**1**]).
4. Установка программы управления на РМ администратора (см. [**1**]).
5. Запуск и настройка программы управления (см. стр. **14** и стр. **17**).
6. Регистрация лицензий (см. стр. **19**).
7. Издание и регистрация корневого сертификата и сертификата сервера доступа (см. стр. **29**).
8. Регистрация пользователей (см.стр. **41**) и предоставление им прав доступа (см. стр. **48**).

Примечание. При работе ПО СД на криптографических шлюзах, объединенных в кластер, при переинициализации основного КШ на резервном необходима переустановка ПО СД.

Установка и настройка абонентских пунктов описана в документации СКЗИ "Континент-АП".

Установка и настройка внешнего криптопровайдера

Наличие криптопровайдера необходимо для работы следующих программ комплекса:

- программа управления сервером доступа;
- абонентский пункт.

Эти программы имеют свой встроенный криптопровайдер, а также поддерживают работу с криптопровайдером "КриптоПро CSP".

При необходимости использования внешнего криптопровайдера установите его на том же компьютере, что и перечисленные программы, и выполните его настройку. В ходе настройки необходимо:

- зарегистрировать лицензию на использование "КриптоПро CSP";
- настроить считыватели ключевой информации;
- настроить параметры датчика случайных чисел.

Подробная информация об установке, настройке и порядке использования "КриптоПро CSP" содержится в эксплуатационной документации на этот программный продукт.

Внимание! Для корректной работы комплекса криптопровайдер, используемый в программе управления сервером доступа и в абонентских пунктах, должен быть одного и того же типа (встроенный или внешний).

Глава 3
Программа управления сервером доступа

Управление сервером доступа осуществляется с помощью специальной программы, устанавливаемой на одном или нескольких компьютерах, находящихся в защищаемом сегменте сети — РМ администратора сервера доступа. Программа управления устанавливает защищенное соединение с криптографическим шлюзом, на котором размещается сервер доступа, и позволяет в диалоговом режиме управлять работой сервера и редактировать данные, содержащиеся в его базе данных.

Внимание! Запуск программы управления возможен только при предъявлении идентификатора администратора, создаваемого при инициализации сервера доступа. При первом запуске программы на экране появится сообщение о том, что не задан IP-адрес сервера доступа. Для успешного подключения необходимо настроить параметры соединения с сервером доступа.

Далее в этом разделе рассматриваются общие вопросы использования программы управления. Порядок управления объектами и правила работы с журналом регистрации событий рассматриваются в следующих главах документа. Описание установки, исправления и удаления системы управления АПКШ "Континент" см. [**1**].

Запуск программы управления сервером доступа

Программа управления в процессе загрузки автоматически устанавливает соединение с сервером доступа.

Внимание! Для соединения программы управления с сервером доступа необходимо предъявить идентификатор администратора, который создается при инициализации сервера доступа (см. [**1**]). Кроме того, необходимо правильно настроить параметры соединения программы с сервером доступа (см. стр. 17).

Для запуска программы управления:

1. Предъявите идентификатор администратора.
2. Нажмите кнопку "Пуск" ("Start") и в меню "Программы" выберите "Код Безопасности | Континент 3.9 | Программа управления СД (ПУ СД)".

   На экране появится основное окно программы и окно ввода пароля для расшифровки ключей администратора.

   Примечание. Если идентификатор администратора не предъявлен, на экране появится соответствующий запрос. Предъявите идентификатор администратора.
3. Введите пароль и нажмите кнопку "ОК".

   При успешном чтении служебной информации из идентификатора программа управления выполнит попытку установить соединение с сервером доступа.

   Примечание. Возможен вариант использования восстановленной конфигурации СД более ранней версии, в которой ключи администратора не шифровались. В этом случае используется пустой пароль.

После установления защищенного соединения с сервером доступа программа управления загрузит необходимые данные и отобразит в основном окне структуру объектов управления (см. стр. **15**).

Совет. Если при установлении соединения произошел сбой и на экран выведено сообщение о невозможности соединения с сервером доступа:

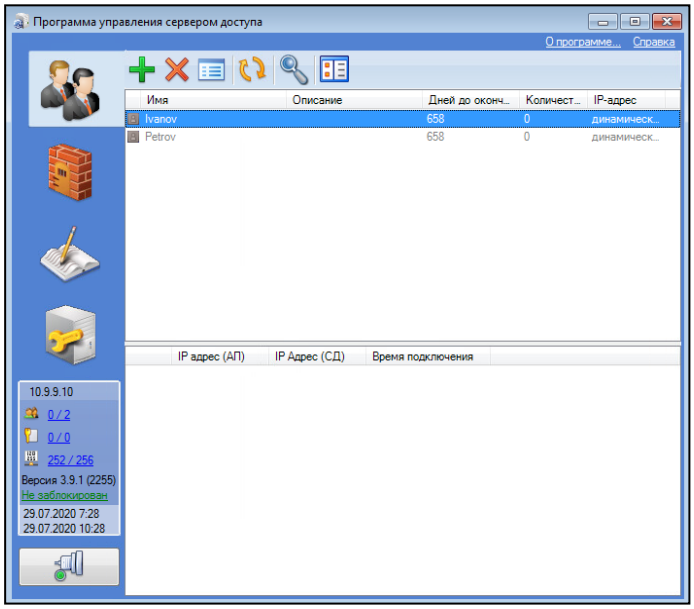
- проверьте правильность настройки параметров соединения;
- проверьте состояние идентификатора администратора и наличие на нем нужной ключевой информации;
- проверьте наличие доступа к серверу по сети и его работоспособность.

Устраните выявленные нарушения и повторите попытку соединения еще раз (см. стр. **17**).

Внимание! Для корректной работы с ключевыми носителями eToken и Рутокен в настройках Windows необходимо запустить системную службу "Смарт-карты", предварительно установив тип запуска – "Авто".

Интерфейс программы

При успешном соединении программы управления с сервером доступа в основном окне программы отобразится список учетных записей.



Элементы управления основного окна представлены в таблице ниже.

Табл.1 Элементы управления основного окна

Элемент	Описание
Панель переходов	Содержит вкладки для доступа к объектам управления (см. Табл.2)
Область отображения информации	Отображает выбранные на панели переходов объекты управления
Панель инструментов	Содержит кнопки для управления записями в информационном окне

Элемент	Описание
Панель состояния (под панелью переходов)	Содержит следующую информацию (для просмотра подробной информации активируйте соответствующую ссылку): • подключенные учетные записи/активные подключения; • общее количество лицензий/количество свободных лицензий; • состояние сервера доступа (для изменения состояния активируйте ссылку); • свободно IP-адресов/всего IP-адресов в пуле; • текущие дата и время на сервере доступа (сверху) и на локальном компьютере (снизу). Информация отображается верно, если соединение с сервером доступа установлено
Кнопка соединения с сервером	Предназначена для установления или разрыва связи с сервером доступа

На панели переходов расположены вкладки для доступа к объектам управления. Ниже в таблице приведено описание информации, доступ к которой предоставляют вкладки.

Табл.2 Объекты управления

Вкладка	Объект	Содержимое информационного окна
	Учетные записи	Список пользователей, зарегистрированных в базе данных сервера доступа (см. стр. **40**)
	Правила фильтрации	Переход к настройкам групп правил фильтрации IP-пакетов (см. стр. **27**). Настройка защищенных подсетей (см. стр. **25**) и сервисов (см. стр. **25**), необходимых для формирования правил фильтрации
	Журналы	Регистрационные журналы сервера доступа
	Настройки сервера	Параметры соединения с сервером доступа, список сертификатов и лицензий

Настройка параметров соединения с сервером доступа

Для настройки параметров соединения:

1. Выберите вкладку "Настройки сервера".
2. Настройте параметры соединения с сервером доступа:

Адрес сервера	IP-адрес внутреннего интерфейса криптографического шлюза, через который осуществляется обмен данными с сервером доступа
Режим входа	Ключевой носитель, на котором содержится ключевая информация для входа в систему. Выберите нужное значение из списка
Максимальное время ожидания...	Время, по истечении которого будет разорвано соединение между программой управления и сервером доступа в том случае, если сервер неактивен. Значение по умолчанию — 60 секунд. Для изменения введите новое значение вручную (от 30 до 600 секунд)

3. Нажмите кнопку "Сохранить настройки".

   Применение новых настроек осуществится при последующем подключении к серверу доступа.
4. Установите соединение программы управления с сервером доступа.

Управление соединением с сервером доступа

Для подключения к серверу:

1. Предъявите идентификатор администратора.
2. Нажмите в левой нижней части окна кнопку "Установка/разрыв связи с сервером".

   На экране появится окно ввода пароля для расшифровки ключей администратора.
3. Введите пароль и нажмите кнопку "ОК".

   При успешном чтении служебной информации из идентификатора программа управления выполнит попытку установить соединение с сервером.

   Совет. Если при установлении соединения произошел сбой и на экран выведено сообщение о невозможности соединения с сервером доступа:
   - проверьте правильность настройки параметров соединения;
   - проверьте состояние идентификатора администратора и наличие на нем нужной ключевой информации;
   - проверьте наличие доступа к серверу по сети и его работоспособность.

   Устраните выявленные нарушения и повторите попытку соединения еще раз.

   При успешном соединении программы с сервером доступа в основном окне программы отобразится список учетных записей.

Для разрыва соединения с сервером:

- Нажмите в левой нижней части окна кнопку "Установка/разрыв связи с сервером".

  Защищенное соединение программы управления с сервером доступа будет немедленно разорвано.

Завершение работы программы

Для завершения работы с программой управления нажмите кнопку "Закрыть" в правом верхнем углу основного окна программы. При этом защищенное управляющее соединение программы с сервером доступа будет разорвано, а основное окно программы исчезнет с экрана.

Глава 4
Управление работой сервера доступа

Управление сервером доступа может осуществляться как средствами программы управления, так и локально, на криптографическом шлюзе, на котором функционирует сервер.

Этот раздел содержит сведения о том, как управлять работой сервера доступа средствами программы управления. Локальное управление описано в [**2**].

Перед тем как приступить к управлению сервером, выполните запуск программы управления и убедитесь, что соединение с сервером доступа установлено (см. стр. **14**).

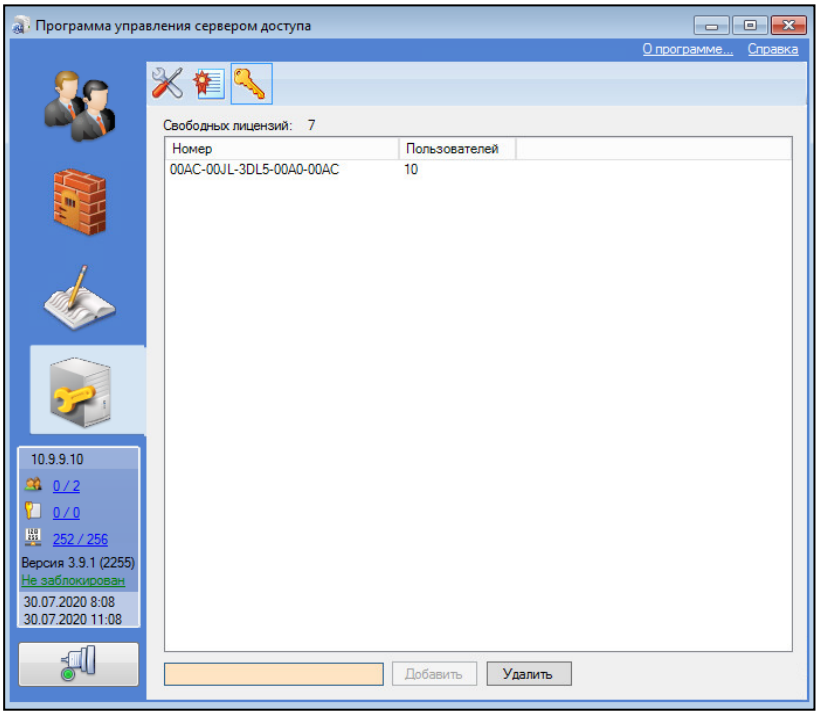
Регистрация лицензий

Лицензии определяют максимальное количество активных (не заблокированных администратором) учетных записей пользователей.

Для регистрации лицензий:

1. Выберите вкладку "Настройки сервера | Лицензии".

   В информационном окне отобразится список зарегистрированных лицензий.



   Для каждой лицензии указано количество активных учетных записей пользователей, которое данная лицензия разрешает хранить в базе данных сервера доступа. Под активными учетными записями в данном случае понимаются учетные записи пользователей, у которых отсутствует признак их блокировки администратором (см. стр. **46**).

   В поле "Свободных лицензий:" отображается общее количество вакансий для регистрации новых пользователей.

2. В поле в нижней части окна введите серийный номер лицензии и нажмите кнопку "Добавить".

Совет. Для удаления выбранной в списке лицензии нажмите кнопку "Удалить".

Настройка параметров подключения абонентских пунктов

Для настройки параметров подключения:

1. Выберите вкладку "Настройки сервера | Настройка сервера".

   В информационном окне отобразится список параметров работы сервера.

2. В группе полей "Параметры работы с АП" введите с клавиатуры нужные значения параметров:

Максимальное количество запросов на подключение от АП	Максимальное количество абонентских пунктов, стоящих в очереди на подключение к серверу доступа
Максимальное количество подключенных АП	Максимальное количество одновременно подключенных к серверу доступа абонентских пунктов
Максимальное количество сертификатов в цепочке	Максимальная длина цепочки связанных сертификатов в сертификате пользователя абонентского пункта
Разрывать связь с неактивным АП через, сек.	Время, по истечении которого следует разорвать связь сервера доступа с неактивным абонентским пунктом
Порт соединения с АП	Номер порта сервера доступа, на котором ожидается соединение с абонентским пунктом. По умолчанию устанавливается значение 4433. Если значение изменено, то этот же номер необходимо указать при настройке общих параметров сетевого подключения абонентского пункта — через двоеточие после значения IP-адреса сервера доступа
Активные на СД каналы связи	Одно из двух возможных значений: "стандартный VPN-канал" или "стандартный VPN-канал и HTTP-туннель". По умолчанию установлено значение "стандартный VPN-канал". В этом случае используются только UDP-подключения к СД, о чем рекомендуется оповестить пользователей АП. Если установлено значение "стандартный VPN-канал и HTTP-туннель", подключение к СД осуществляется по каналу, указанному в настройках АП: • без использования прокси (стандартное подключение); • подключение через прокси (HTTP-туннель); • потоковое подключение (TCP) (подключение к СД по защищенному TCP-каналу без использования прокси). При этом HTTP-туннель разрешен только в том случае, если его использование разрешено для пользователя
DNS-серверы	IP-адреса DNS-серверов в защищенной сети
Пул адресов	IP-адрес и маска, задающие диапазон внутрисетевых адресов для назначения абонентским пунктам. **Примечание.** Пул адресов КШ с СД не должен пересекаться с его защищенными подсетями и адресами его внешнего интерфейса

Совет. При помещении курсора мыши в поле появляется всплывающая подсказка с указанием граничных значений параметра.

3. В раскрывающемся списке "Режим СД" выберите режим сервера для соединения с АП.

Примечание. Убедитесь, что выбранный режим СД совместим с версией АП (см. стр. 60).

4. Нажмите кнопку "Сохранить настройки".

Блокировка сервера доступа

В тех случаях, когда существует угроза нарушения работоспособности сервера или несанкционированного доступа к конфигурационной информации, хранящейся на сервере, или же угроза несанкционированного доступа к ресурсам защищаемой сети, работа сервера доступа может быть заблокирована.

Внимание! После блокировки сервера доступа подключение к нему новых пользователей невозможно. Все пользователи, подключенные к серверу ранее, продолжают работать в обычном режиме и не теряют доступ к ресурсам защищенной сети до завершения сеанса работы (отключения от сервера).

Для блокировки сервера:

1. Выберите вкладку "Настройки сервера | Настройка сервера".

   В информационном окне отобразится список параметров работы сервера.

2. В группе параметров "Параметры соединения" нажмите кнопку "Заблокировать сервер".

   Сервер доступа будет немедленно заблокирован. В окне состояния отобразится значение "Заблокирован", а название кнопки изменится на "Разблокировать сервер".

   Примечание. Для блокировки доступа подключенных пользователей к ресурсам защищаемой сети принудительно отключите их от сервера (см. стр. 52).

Для разблокировки сервера:

1. Выберите вкладку "Настройки сервера | Настройка сервера".

   В информационном окне отобразится список параметров работы сервера.

2. В группе параметров "Параметры соединения" нажмите кнопку "Разблокировать сервер".

   Возможность подключения пользователей к серверу доступа будет немедленно восстановлена. В окне состояния отобразится значение "Не заблокирован", а название кнопки изменится на "Заблокировать сервер".

Механизм синхронизации СД в кластере КШ

При работе СД в кластере КШ не требуется специальных настроек СД.

Синхронизация между СД на основном и резервном КШ кластера происходит при изменении базы данных/конфигурации СД, подключении или отключении абонентов.

В случае смены активного узла в кластере абонентским пунктам необходимо переподключение.

Резервное копирование базы данных сервера доступа

Резервное копирование базы данных сервера доступа предназначено для быстрого восстановления работы сервера в случае нарушения его работоспособности или выхода из строя криптографического шлюза АПКШ "Континент", на котором функционирует сервер доступа.

В резервной копии базы данных сохраняется вся информация о текущей конфигурации сервера доступа, включая информацию об имеющихся сертификатах. Исключение составляет содержимое журнала регистрации сервера доступа.

Также необходимо сохранить ключевую информацию (ключ администратора сервера доступа) и создать ее резервную копию, так как после восстановления сохраненной конфигурации будут действительны ключи, относящиеся к этой конфигурации. А в случае утери ключей придется создавать нового администратора сервера доступа.

Внимание! Сохраняйте резервную копию базы данных сервера доступа каждый раз после внесения очередного изменения в параметры объектов управления.

Для создания резервной копии:

1. В основном окне выберите вкладку "Настройки сервера | Настройка сервера".

   В информационном окне отобразится список параметров работы сервера.

2. Активируйте ссылку "Архивировать" в нижней части окна.

   На экране появится окно сохранения файла.

3. Выберите папку, укажите имя файла для создания резервной копии и нажмите кнопку "Сохранить".

   При успешном завершении операции на экране появится соответствующее сообщение. В указанной папке будет создан файл резервной копии базы данных сервера доступа. Файлы этого типа имеют стандартное расширение *.asb.

Восстановление базы данных из резервной копии

Перед восстановлением базы данных из резервной копии выполните все необходимые действия для восстановления ПО сервера доступа и криптографического шлюза, на котором он функционирует. Кроме того, учитывайте, что восстановление базы данных на работоспособном сервере доступа приводит к полной замене имеющегося содержимого базы данных, которое будет утеряно. При этом если информация о сертификате сервера и корневом сертификате, хранящаяся в резервной копии, не соответствует текущим сертификатам, все пользователи потеряют право доступа к ресурсам защищенной сети. Для восстановления утраченных прав потребуется обновить сертификаты всех зарегистрированных пользователей.

Для восстановления базы данных:

1. Выберите вкладку "Настройки сервера | Настройка сервера".

   В ООИ отобразится список параметров работы сервера.

2. Активируйте ссылку "Восстановить" в нижней части окна.

   На экране появится окно открытия файла.

3. Выберите папку, укажите файл резервной копии и нажмите кнопку "Открыть".

   Конфигурационная информация будет прочитана из файла резервной копии и загружена в базу данных сервера доступа. При успешном завершении операции на экране появится соответствующее сообщение. Если же структура файла резервной копии нарушена, на экране появится сообщение об ошибке.

Внимание! При переносе БД СД на СД, управляемый другим ЦУС, необходимо, чтобы оба ЦУС были инициализированы одинаково – с применением либо встроенного ДСЧ ПАК "Соболь", либо идентичного ключевого блокнота РДП-006.

Глава 5
Управление правилами фильтрации

О правилах фильтрации

Права доступа удаленных пользователей к ресурсам сети, защищаемой средствами АПКШ "Континент", определяются правилами фильтрации IP-пакетов. Для каждого пользователя создают индивидуальные списки правил.

Правило фильтрации представляет собой сложный составной объект, параметры которого устанавливают порядок действий над IP-пакетами с заданными характеристиками при их обработке фильтром IP-пакетов криптографического шлюза.

Параметры правила, использующиеся при проверке соответствия IP-пакета правилу, определяются параметрами объектов более низкого уровня — элементами правил. К элементам правил фильтрации относятся следующие объекты:

- "Подсеть" — этот элемент используется в правиле фильтрации для определения отправителя или получателя IP-пакетов. Содержит описание части сегмента защищаемой сети — IP-адрес и маску подсети;
- "Сервис" — этот элемент используется в правиле фильтрации для определения характеристик IP-пакетов, к которым следует применять правило. К этим характеристикам относятся протокол (TCP, UDP, ICMP или номер протокола), в случае TCP и UDP — диапазоны портов отправителя и получателя, в случае ICMP — тип и код ICMP-сообщения.

Для каждого пользователя создается индивидуальный список правил фильтрации, содержащий отдельные правила и группы правил.

Для удобства составления индивидуального списка используется механизм группирования правил. Этот механизм позволяет создать набор стандартных групп и в дальнейшем формировать индивидуальные списки правил не из отдельных правил, а из поименованных групп правил.

Группа правил фильтрации есть объект, содержащий упорядоченный набор правил фильтрации, как активных, так и временно отключенных.

Итак, прежде чем приступить к составлению индивидуальных списков правил фильтрации, выполните предварительную настройку:

- создайте все необходимые элементы правил фильтрации;
- на основе имеющихся элементов создайте нужные правила фильтрации;
- сформируйте из имеющихся правил группы правил фильтрации.

Завершив предварительную настройку, перейдите к составлению для каждого пользователя индивидуальных списков правил фильтрации (см. стр. **48**).

Примечание. Изменения в правилах фильтрации вступают в силу только в следующем сеансе пользователя. При необходимости отключите пользователя от сервера доступа принудительно (см. стр. **52**).

Управление списками объектов

Просмотр списка объектов

Для просмотра списка объектов:

1. Выберите вкладку "Правила фильтрации" —  .

   В ООИ появится содержимое вкладки "Правила" — список всех правил фильтрации.
2. Для перехода к другим объектам воспользуйтесь вкладками:

Правила	Список всех правил фильтрации
Группы правил	Список папок, содержащих набор правил фильтрации
Защищенные подсети	Список защищенных подсетей и подсетей, которые можно использовать для настройки незащищенных соединений
Сервисы	Список сервисов

Создание объекта

Для создания объекта:

1. Перейдите к списку объектов и на панели инструментов нажмите кнопку "Добавить" —  .

   На экране появится окно настройки параметров объекта.
2. Задайте параметры создаваемого объекта:
   - "Защищенная подсеть" (см. стр. **25**);
   - "Сервис" (см. стр. **25**);
   - "Правило фильтрации" (см. стр. **26**);
   - "Группа правил фильтрации" (см. стр. **27**).
3. Нажмите кнопку "OK".

   В выбранной вкладке добавится новый объект. Сведения об этом объекте будут сохранены в базе данных сервера доступа.

Удаление объекта

Примечание. Запрещено удаление объекта, входящего в состав других объектов. Например, запрещено удаление правила, входящего в группу правил, или элемента правила, использующегося в одном или нескольких правилах фильтрации.

Для удаления объекта:

1. Выберите в списке удаляемый объект и на панели инструментов нажмите кнопку "Удалить"  или клавишу <Delete>.

   На экране появится окно запроса.
2. Нажмите кнопку "Да", чтобы подтвердить удаление объекта.

   Ярлык объекта будет немедленно исключен из списка. Сведения об этом объекте будут удалены из базы данных сервера доступа без возможности восстановления.

Настройка параметров объектов

Вызов окна для настройки параметров объекта

Для вызова окна настройки:

- Выберите объект и нажмите на панели инструментов кнопку "Свойства"  .

  На экране появится окно настройки параметров объекта.

Примечание. Для вызова окна настройки можно также использовать контекстное меню выбранного объекта и двойное нажатие левой кнопки мыши.

Настройка подсети

Эти объекты размещаются во вкладке "Защищенные подсети". Параметры подсети определяют диапазон IP-адресов абонентов-отправителей или абонентов-получателей, для которых будет действовать правило фильтрации.

Для настройки параметров подсети:

1. Выберите вкладку "Правила фильтрации | Защищенные подсети".
2. Укажите параметры подсети и нажмите кнопку "ОК".

Имя	Введите название подсети
Описание	Введите дополнительную информацию о подсети
IP-адрес	Введите IP-адрес сегмента подсети или отдельного компьютера. Если это поле содержит значение "0.0.0.0", тогда подсеть будет определена в диапазоне всех известных IP-адресов, т. е. не будет устанавливать ограничений на IP-адреса отправителей или получателей. В этом случае значение поля "Маска" не учитывается
Маска	Введите маску для подсети
Защищенная подсеть	Установите отметку, если соединение абонентских пунктов с данной подсетью должно быть защищенным (с зашифрованным трафиком). При отсутствии отметки соединение с данной подсетью осуществляется без шифрования трафика

Настройка сервисов

Эти объекты размещаются в одноименной вкладке. Параметры сервиса определяют характеристики IP-пакетов, к которым применяется правило.

При инициализации СД автоматически создается набор наиболее часто используемых сервисов (pop-3, smtp, imap4, http, FTP, FTP-data и пр.).

Для настройки параметров сервиса:

1. Выберите вкладку "Правила фильтрации | Сервисы".
2. Укажите параметры сервиса.

Имя	Введите название сервиса. По возможности давайте сервисам осмысленные названия, так как при настройке параметров правил фильтрации выбор этого элемента правила осуществляется только по его названию
Описание	Введите дополнительную информацию о сервисе
Протокол	Выберите из раскрывающегося списка название нужного протокола. Если требуется указать номер протокола, введите его в это поле с клавиатуры

Порты отправителя Порты получателя	Настройте параметры, специфичные для выбранного протокола: • если выбран протокол TCP или UDP, укажите порты отправителя и получателя IP-пакетов в одноименных полях. Эти поля позволяют задать либо номер одного из портов, либо диапазон портов, например — "20–150". Значение "0" соответствует диапазону всех имеющихся портов; • если выбран протокол ICMP, укажите тип ICMP-сообщения в одноименном поле, выбрав его название из раскрывающегося списка. Кроме этого, для ICMP-сообщений Destination Unreachable, Redirect и Time Exceeded укажите код ICMP-сообщения, выбрав его название из раскрывающегося списка

3. Нажмите кнопку "OK".

Настройка правил фильтрации

Эти объекты размещаются во вкладке "Правила фильтрации | Правила". Пиктограмма возле объекта свидетельствует о его свойствах:

	Отправителем IP-пакета является клиент Континента (абонентский пункт). Правило фильтрации разрешает прохождение трафика
	Отправителем IP-пакета является клиент Континента. Правило фильтрации запрещает прохождение трафика
	Получателем IP-пакета является клиент Континента (абонентский пункт). Правило фильтрации разрешает прохождение трафика
	Получателем IP-пакета является клиент Континента. Правило фильтрации запрещает прохождение трафика
	При обработке IP-пакета использование данного правила является приоритетным по сравнению с остальными

Для настройки параметров правила фильтрации:

1. В контекстном меню правила выберите пункт "Свойства" (см. стр. **25**).
2. Отредактируйте параметры правила фильтрации.

Имя	Введите название правила фильтрации
Описание	Введите дополнительную информацию о правиле фильтрации
Отправитель Получатель	Выберите из раскрывающегося списка имя нужного объекта "Подсеть". Правило фильтрации применяется к IP-пакетам, отправляемым из этой подсети или в эту подсеть. Если требуется указать IP-адрес компьютера, на котором находится абонентский пункт, выберите в списке значение "Клиент Континента". В этом случае для каждого удаленного пользователя вместо этого значения указывается IP-адрес компьютера, с которого он подключился к серверу доступа. Одно из этих двух полей обязательно должно содержать значение "Клиент Континента"
Сервисы	Сформируйте список сервисов, используемых в правиле фильтрации. Для формирования списка используйте кнопки "Добавить" и "Удалить". Правило фильтрации применяется к IP-пакетам с указанными параметрами
Действие	Выберите из раскрывающегося списка действия, которые необходимо выполнить с IP-пакетом, если он соответствует заданным характеристикам: • "Пропустить пакет" — разрешить прохождение пакета; • "Отбросить пакет" — запретить прохождение пакета

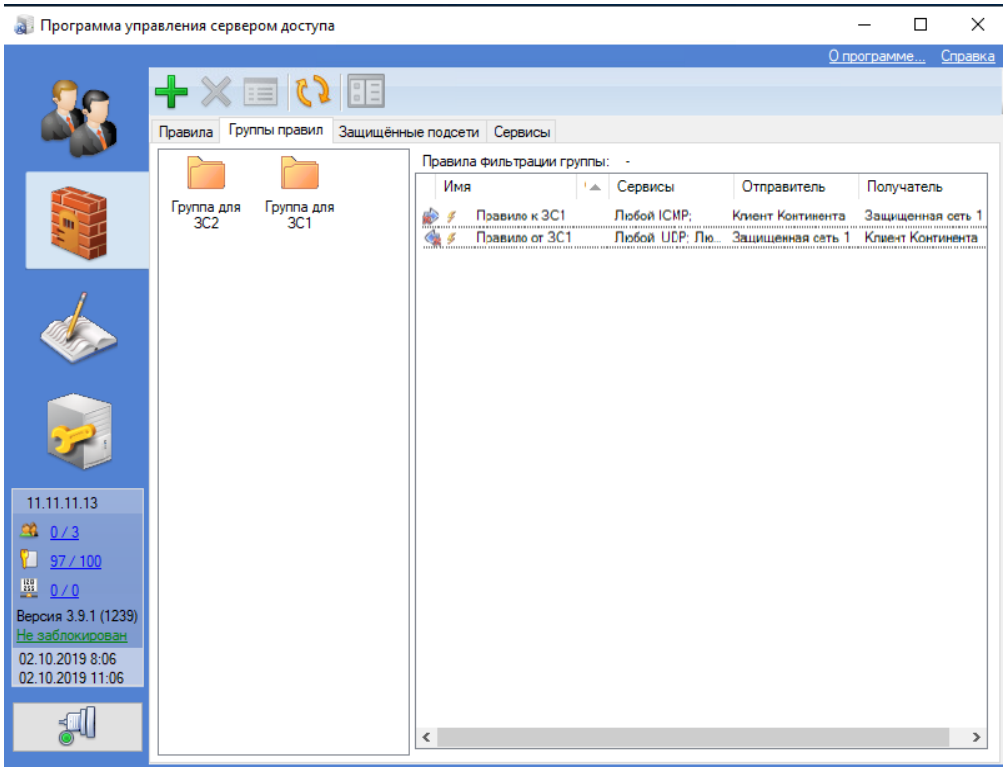
Протоколирование	Выберите из раскрывающегося списка режим регистрации IP-пакета. Учитывайте, что объем информации, помещаемой в журнал сетевого трафика, может оказаться большим, что может затруднить обработку этой информации. Поэтому не рекомендуется протоколировать применение разрешающих правил — содержащих в поле "Действие" значение "Пропустить пакет". Кроме этого, рекомендуется помещать в журнал сетевого трафика только заголовки IP-пакетов. • "Не записывать в журнал" — не регистрировать IP-пакет; • "Запись в журнал заголовка" — регистрировать в журнале сетевого трафика заголовок пакета; • "Запись в журнал тела пакета" — регистрировать заголовок и первые 128 байт содержания пакета после заголовка. Просмотр зарегистрированных пакетов осуществляется средствами программы просмотра журналов
Контроль состояния соединения	Установите отметку для пакетов, открывающих соединение. В этом случае автоматически создаются правила фильтрации, которые разрешают прохождение всех пакетов, относящихся к этому соединению. Автоматически созданные правила на экране не отображаются
Применить и завершить обработку	Установите отметку, чтобы данное правило являлось приоритетным при обработке IP-пакета

3. Нажмите кнопку "ОК".

Настройка групп правил фильтрации

Эти объекты размещаются на вкладке "Правила фильтрации | Группы правил".

Примечание. Редактирование свойств правил внутри группы невозможно.



Для настройки параметров группы правил:

1. В контекстном меню группы правил выберите пункт "Свойства" (см. стр. **25**).
   Откроется окно "Свойства группы правил фильтрации".
2. Укажите параметры группы правил фильтрации.

Имя	Введите название группы правила фильтрации. По возможности давайте группам правил короткие осмысленные названия, так как при формировании индивидуальных списков правил для пользователей выбор группы правил осуществляется из контекстного меню, содержащего только названия
Описание	Введите дополнительную информацию

   Для редактирования параметров используйте следующие кнопки:

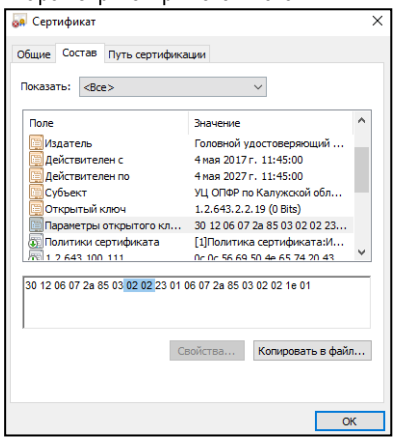
Добавить	Нажмите для добавления правила фильтрации в данную группу. В появившемся окне выберите нужное правило и нажмите кнопку "ОК". Учитывайте, что: одно и то же правило может входить в состав нескольких групп, но не может быть дважды добавлено в состав одной и той же группы; при добавлении правила в группу оно всегда добавляется в конец списка. Для изменения его положения в списке используйте кнопки "Вверх" и "Вниз"
Удалить	Нажмите для удаления выбранного правила из группы

3. Нажмите кнопку "ОК".

Глава 6
Управление сертификатами

Для функционирования СД необходимо выполнить регистрацию корневого сертификата и сертификата сервера доступа при первом запуске программы управления. Без корневого сертификата невозможна регистрация пользователей, без сертификата сервера доступа невозможно соединение пользователей с сервером.

Внимание! При работе со сторонними провайдерами сервер доступа поддерживает работу только с ключами, созданными с использованием параметров 1.2.643.2.2.35.1, 1.2.643.2.2.35.2, 1.2.643.2.2.35.3, 1.2.643.2.2.36.0, 1.2.643.2.2.36.1. Для проверки валидности сертификата откройте окно просмотра свойства сертификата. Выберите вкладку "Состав" и выберите поле "Параметры открытого ключа".



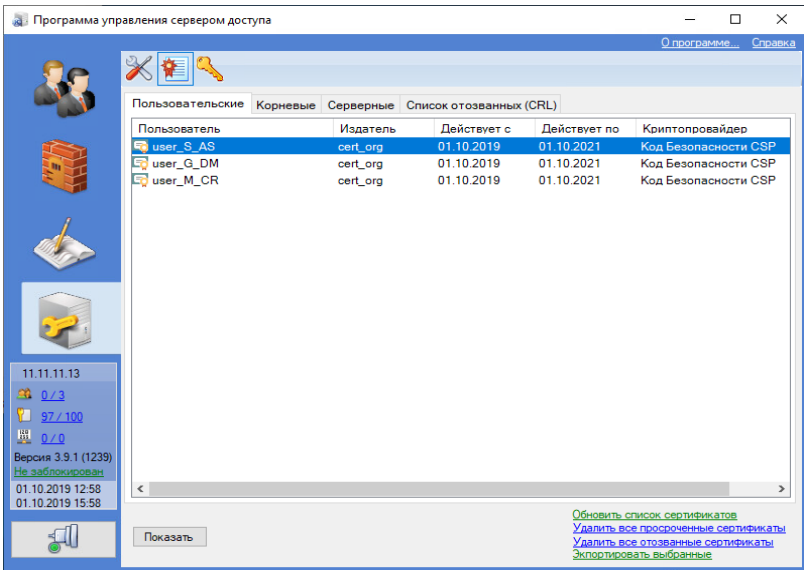
Убедитесь, что восьмой и девятый байты слева имеют значение "02". Если значение не совпадает, создайте запрос на другой сертификат или получите новый сертификат из внешних источников.

Управление списками сертификатов

Вызов списков сертификатов

Для вызова списка сертификатов:

- Выберите вкладку "Настройки сервера | Сертификаты".



В окне отобразятся списки сертификатов, зарегистрированных в системе.

Каждая вкладка содержит табличное представление списка сертификатов, зарегистрированных в системе, и их характеристики. Описание полей и управляющих элементов списка сертификатов представлено в таблицах ниже.

Примечание. На вкладке "Пользовательские" добавить новый сертификат или удалить действующий невозможно. Данные действия выполняют в окне настройки свойств пользователя (см. стр. 30).

Табл.3 Поля списка сертификатов

Поле	Описание
Состояние сертификата	Пиктограмма, отображающая состояние сертификата: — сертификат действителен, пригоден для использования; — сертификат отозван; — сертификат недействителен (не наступил или истек срок действия)
Издатель	Имя издателя сертификата
Срок действия	Дата начала и окончания срока действия сертификата
Криптопровайдер	Имя поставщика услуг криптографии

Табл.4 Управляющие элементы списка сертификатов

Управляющий элемент	Описание
Добавить	Выводит на экран стартовое окно мастера сертификатов
Удалить	Удаляет из списка выбранный сертификат
Показать	Открывает окно с параметрами выбранного сертификата
Удалить все просроченные	Удаляет из списка все просроченные сертификаты
Удалить все отозванные	Удаляет из списка все отозванные сертификаты
Обновить список сертификатов	Обновляет отображаемый список

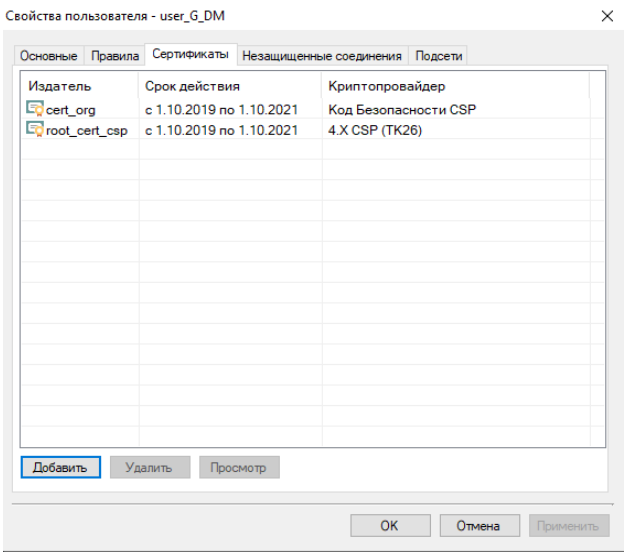
Вызов списка сертификатов пользователя

Для вызова списка сертификатов пользователя:

1. В основном окне выберите вкладку "Пользователи".

   В окне отобразится список пользователей.

2. В контекстном меню окна выберите пункт "Свойства" (см. стр. 45) и выберите вкладку "Сертификаты".



Вкладка "Сертификаты" содержит табличное представление списка зарегистрированных в системе сертификатов данного пользователя и их характеристики. Описание полей списка сертификатов представлено в Табл.3, управляющих элементов — в Табл.4.

Регистрация сертификатов внешнего центра сертификации

При использовании сертификатов внешнего центра сертификации наличие криптопровайдера "КриптоПро CSP" необходимо и на компьютере с программой управления сервером доступа, и на компьютерах с установленным абонентским пунктом.

Регистрация корневого сертификата

Для регистрации в системе корневого сертификата внешнего центра сертификации необходимо заранее получить из центра сертификации файл, содержащий сертификат этого центра или цепочку доверенных сертификатов, и сохранить этот файл на диске. Файл должен содержать сертификат в DER-кодировке. Для получения сертификата воспользуйтесь веб-страницей центра сертификации или запросите сертификат у администратора центра по электронной почте.

Для регистрации корневого сертификата:

1. Выберите вкладку "Настройки сервера | Сертификаты | Корневые" (см. стр. **29**) и нажмите кнопку "Добавить".

   На экране появится окно "Добавление корневого сертификата".

2. В окне "Добавление корневого сертификата" выполните следующие действия:

   - Установите отметку в поле "Загрузить из файла".

     Откроется окно добавления файла.

   - Нажмите кнопку "..." и выберите файл в окне выбора файла.
   - Нажмите кнопку "Создать сертификат".

   Если формат выбранного файла сертификата не соответствует установленным требованиям, на экране появится сообщение об ошибке. Повторите процедуру выбора файла.

   При успешном чтении информации из файла сертификата сведения о сертификате будут добавлены в базу данных сервера доступа.

Регистрация сертификата сервера доступа

Регистрация сертификата сервера доступа состоит из следующих этапов:

- формирование запроса на создание сертификата;
- издание сертификата центром сертификации;
- регистрация сертификата в системе.

Для формирования запроса:

1. Выберите вкладку "Настройки сервера | Сертификаты | Серверные" (см. стр. **29**) и нажмите кнопку "Добавить".

   На экране появится окно "Добавление сертификата сервера".

2. В окне "Добавление сертификата сервера" выполните следующие действия:

   - Установите отметку в поле "Создать запрос".
   - В раскрывающемся списке "Поставщик услуг криптографии" выберите "КриптоПро".
   - В поле "Имя файла" укажите имя файла (включая путь к нему), в котором будет сохранен запрос на издание сертификата. Для этого нажмите кнопку "...", выберите нужный диск (каталог) и укажите имя файла в окне сохранения файла.

- Укажите сведения, необходимые для формирования запроса на издание сертификата сервера:
  - Имя сервера;

  Примечание. Имя сервера может состоять из латинских букв нижнего регистра, цифр и символов "-" и ".". Например, example.domain.ru или 1.1.1.1.

  - Организация;
  - Подразделение.

  Примечание. Введите имя сервера доступа и укажите название организации и подразделения, отвечающего за эксплуатацию сервера. Для продолжения процедуры необходимо заполнить все поля этого окна.

- Установите отметки у нужных значений поля в разделе "Назначение ключа".

  Примечание. Значение "Согласование ключей" включается в сертификат по умолчанию.

- Нажмите кнопку "Создать запрос".

На экране появится сообщение об успешном создании запроса.

3. Нажмите кнопку "ОК" для закрытия окна сообщения.

Для издания сертификата внешним центром сертификации:

1. Передайте созданный файл запроса администратору внешнего центра сертификации для издания сертификата сервера.
2. Получите от администратора внешнего центра сертификации файл с изданным сертификатом сервера.

Для регистрации сертификата сервера:

Перед началом процедуры в системе должен быть зарегистрирован корневой сертификат внешнего центра сертификации, которым подписан сертификат сервера доступа.

1. Выберите вкладку "Настройки сервера | Сертификаты | Серверные" (см. стр. **29**) .
2. Нажмите кнопку "Добавить".

   На экране отобразится окно "Создание сертификата сервера".
3. Выполните следующие действия:
   - Установите отметку в поле "Загрузить из файла".
   - Укажите файл сертификата сервера доступа, полученный от администратора центра сертификации.
   - Нажмите кнопку "Создать сертификат".

   Если формат выбранного файла сертификата не соответствует установленным требованиям, на экране появится сообщение об ошибке. Повторите процедуру выбора файла.

   При успешном чтении информации из файла сертификата сведения о сертификате будут добавлены в базу данных сервера доступа.

Регистрация сертификата пользователя

Внимание! Перед началом описанной ниже процедуры в системе должен быть зарегистрирован корневой сертификат внешнего центра сертификации, которым подписан сертификат пользователя. При создании сертификата внешним центром сертификации в его форме обязательно должны быть заполнены следующие поля: "Имя", "Организация", "Подразделение".

Для регистрации сертификата пользователя:

1. Выберите вкладку "Учетные записи".
2. В контекстном меню учетной записи пользователя выберите пункт "Свойства".

   Примечание. Если планируется создание нового пользователя, нажмите кнопку "Добавить" на панели управления или в контекстном меню вкладки "Учетные записи".

   Откроется окно свойств пользователя.
3. В окне свойств пользователя выберите вкладку "Сертификаты" и нажмите кнопку "Добавить".

   Откроется окно "Добавление сертификата пользователя".
4. Выполните следующие действия:
   - Перейдите по ссылке "Импортируйте сертификат из файла" и в появившемся окне Windows укажите файл сертификата.

     Если формат выбранного файла сертификата не соответствует требованиям, на экране появится сообщение об ошибке.
   - Укажите диск (папку), в которую будут сохранены файлы сертификатов. Для этого нажмите кнопку "Обзор" и выберите папку в окне выбора каталогов.
   - Нажмите кнопку "Готово".

   При успешном импорте сертификата пользователя и регистрации этого сертификата в базе данных сервера доступа в каталоге (на диске), указанном ранее, будет записан файл корневого сертификата root.p7b.

   В противном случае на экране появится сообщение об ошибке. Выясните причину возникновения ошибки, устраните ее и повторите процедуру регистрации сертификата еще раз.

   Примечание. Если файл сертификата записывается на дискету, на экране появится сообщение, предлагающее вставить в дисковод дискету, предназначенную для экспорта сертификатов. В том случае, если указанный диск (папка) содержит одноименные файлы, новые файлы сертификатов будут записаны поверх существующих с предварительным запросом на перезапись.
5. Нажмите кнопку "ОК" в окне настройки свойств пользователя.
6. Передайте файлы сертификатов пользователю, без этих атрибутов невозможно обновление сертификатов на рабочем месте пользователя.

Издание сертификатов средствами программы управления

При издании сертификатов средствами программы управления их регистрация в системе осуществляется автоматически.

Выбор криптопровайдера, используемого для издания корневого сертификата, зависит от криптопровайдера, установленного на компьютере с абонентским пунктом, а также версии абонентского пункта.

Издание корневого сертификата

Для издания корневого сертификата:

1. Выберите вкладку "Настройки сервера | Сертификаты | Корневые" (см. стр. 29) и нажмите кнопку "Добавить".

   Откроется окно "Добавление корневого сертификата".

2. Выполните следующие действия:
   - Установите отметку в поле "Создать по имеющимся сведениям".
   - В раскрывающемся списке "Поставщик услуг криптографии" выберите криптопровайдер (см. Табл.3 на стр.**30**).
   - Укажите сведения, необходимые для издания корневого сертификата.

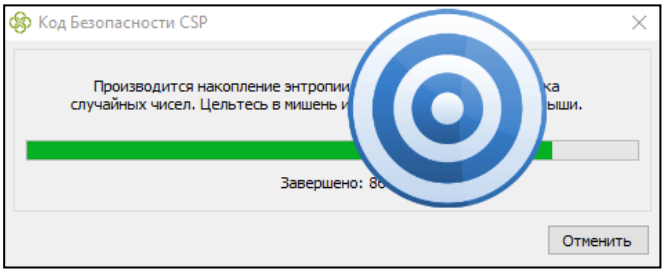
     Введите в соответствующих полях:
     - название сертификата;
     - название организации, выдающей сертификат;
     - название подразделения, выдающего сертификат.

     Примечание. Эти поля обязательны для заполнения.

     В полях "Срок действия" укажите даты начала и окончания срока действия сертификата. Для выбора даты в календаре нажмите кнопку в правой части поля. По умолчанию срок действия сертификата — два года, начиная с текущей даты.
   - Нажмите кнопку "Создать сертификат".

   На экране появится сообщение о создании ключевого контейнера, записи в него закрытого ключа центра сертификации и необходимости использовать для этого отчуждаемый носитель.
3. Нажмите кнопку "ОК".

   На экране появится окно криптопровайдера.



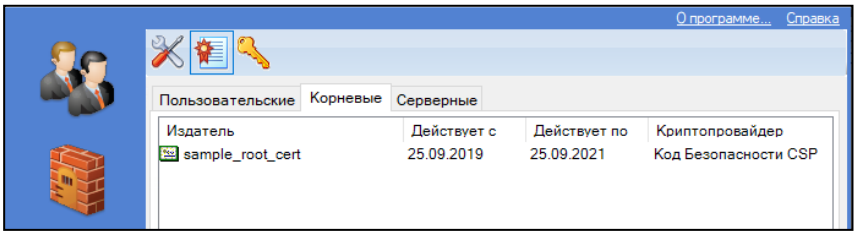
4. Сформируйте закрытый ключ с помощью датчика случайных чисел — нажимайте левой кнопкой мыши на мишень, перемещающуюся по экрану, до завершения процесса накопления энтропии.
5. Выполните следующие операции:
   - выберите тип ключевого носителя для записи закрытого ключа;
   - введите пароль для ограничения доступа к ключевому контейнеру.

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

   Порядок действий зависит от используемого криптопровайдера, датчика случайных чисел и ключевого носителя, выбранного для хранения ключевой информации (см. стр. **57**).
6. Следуйте указаниям, появляющимся на экране.

   После завершения процедуры на экране появится сообщение о завершении создания запроса на сертификат.

   При успешном завершении процедуры в списке корневых сертификатов появится новая запись.



Издание сертификата сервера доступа

При издании сертификата сервера доступа поля "Использование ключа" и "Улучшенный ключ" имеют значения "Согласование ключей" и "Проверка подлинности сервера" соответственно. Эти значения устанавливаются автоматически и изменению не подлежат.

Для издания сертификата сервера:

1. Выберите вкладку "Настройки сервера | Настройка сервера | Серверные" (см. стр. **29**) .
2. Нажмите кнопку "Добавить".

   Откроется окно "Добавление сертификата сервера".
3. Выполните следующие действия:
   - Установите отметку в поле "По имеющимся сведениям".
   - Укажите сведения, необходимые для издания сертификата сервера:
     - Имя сервера;

     Примечание. Имя сервера может состоять из латинских букв нижнего регистра, цифр и символов "-" и ".". Например, example.domain.ru или 1.1.1.1.

     - Название организации;
     - Подразделение.
   - При необходимости укажите назначение ключей.

     Примечание. Значение "Согласование ключей" выбрано по умолчанию. При использовании абонентских пунктов предыдущих версий требуется дополнительно указать следующие значения:
     - Электронная подпись;
     - Неотрекаемость;
     - Зашифрование ключей.
   - Укажите даты начала и окончания срока действия сертификата. Для выбора даты в календаре нажмите кнопку в правой части поля. Значения по умолчанию устанавливают срок действия сертификата в течение двух лет, начиная с текущей даты.
   - Выберите в представленном списке нужный корневой сертификат, закрытым ключом которого будет заверен издаваемый сертификат сервера доступа. Для просмотра подробной информации о выбранном сертификате нажмите кнопку "Просмотр".
   - Нажмите кнопку "Создать сертификат".

   На экране появится предупреждение о том, что будет выполнено чтение закрытого ключа.
4. Нажмите кнопку "ОК".

   На экране появится запрос на ввод пароля.

   Примечание. Данное окно не появится, если при издании корневого сертификата была установлена отметка в поле "Запомнить пароль".
5. Введите пароль, которым был ограничен доступ к ключевой информации при издании корневого сертификата (см. стр. **33**), и нажмите кнопку "ОК".

   При успешном чтении закрытого ключа корневого сертификата сертификат сервера доступа заверяется этим ключом и сохраняется в базе данных сервера.

Издание сертификата пользователя

Издание сертификата пользователя средствами программы управления возможно двумя способами:

- по информации о пользователе, введенной администратором;

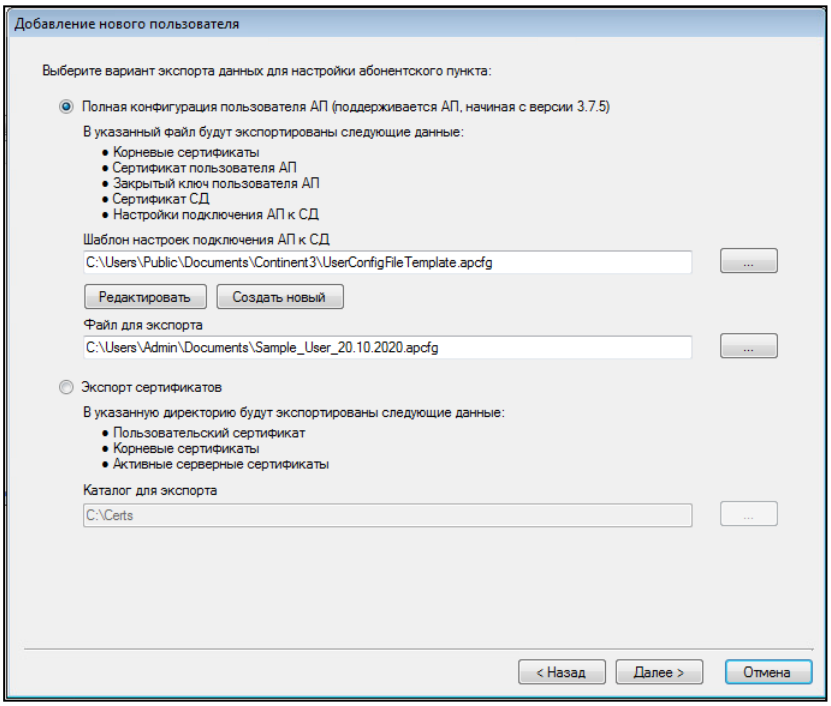
- по запросу, сформированному пользователем в абонентском пункте.

Для издания сертификата по информации, введенной администратором:

1. Выберите вкладку "Настройки сервера | Сертификаты | Пользовательские" (см. стр. **30**) и нажмите кнопку "Добавить".
2. В стартовом окне мастера укажите сведения, необходимые для издания сертификата пользователя, и нажмите кнопку "Далее >".
3. В окне мастера выполните следующие действия:
   - Выберите в представленном списке корневой сертификат, закрытым ключом которого будет заверен издаваемый сертификат пользователя (см. Табл.3 на стр.**30**), и нажмите кнопку "Далее >".

     Примечание. Для просмотра информации о выбранном сертификате нажмите кнопку "Просмотр".
   - Укажите даты начала и окончания срока действия сертификата.

     Для выбора даты в календаре нажмите кнопку в правой части поля.
   - Нажмите кнопку "Далее >".
4. В следующем окне мастера выполните следующие действия:
   - Выберите вариант экспорта данных для настройки абонентского пункта:



   - Нажмите кнопку "Далее >".

     На экране появится сообщение о записи закрытого ключа пользователя.
5. Нажмите кнопку "ОК".

   На экране появится окно криптопровайдера. Необходимо выполнить следующие операции:
   - сформировать закрытый ключ с помощью датчика случайных чисел;
   - ввести пароль для ограничения доступа к ключевому контейнеру;
   - выбрать тип ключевого носителя для записи закрытого ключа.

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

Порядок действий зависит от используемого криптопровайдера, датчика случайных чисел и ключевого носителя, выбранного для хранения ключевой информации (см. стр. **57**). Следуйте указаниям, появляющимся на экране.

Дождитесь появления сообщения о чтении закрытого ключа центра сертификации и нажмите кнопку "OK".

На экране появится запрос пароля.

Примечание. Данное окно не появится, если при издании корневого сертификата была установлена отметка в поле "Запомнить пароль".

6. Введите пароль, которым был ограничен доступ к ключевой информации при издании корневого сертификата (см. стр. **33**), и нажмите кнопку "OK".

   После того как выполнены все действия, необходимые для создания ключевой информации, в указанном ранее каталоге (на диске) будут размещены следующие файлы:

   - root.p7b — файл корневого сертификата;
   - user.cer — файл сертификата пользователя.

   Примечание. Если указанный диск (каталог) содержит одноименные файлы, новые файлы сертификатов будут записаны поверх существующих с предварительным запросом на перезапись.

7. В появившемся заключительном окне мастера нажмите кнопку "Готово".
8. Передайте файлы сертификатов и носитель с закрытой ключевой информацией данному пользователю для регистрации на абонентском пункте.

Для издания сертификата по информации из файла запроса:

1. В контекстном меню учетной записи выберите вкладку "Сертификаты" (см. стр. **30**).
2. Нажмите кнопку "Добавить".

   Откроется окно мастера добавления сертификата пользователя.
3. В стартовом окне мастера выполните следующие действия:
   - Активируйте ссылку "загрузите их из файла запроса" и укажите файл запроса в появившемся окне Windows.

     Поля стартового окна мастера сертификатов будут заполнены сведениями о данном пользователе. При необходимости внесите нужные изменения.

     Примечание. Если формат выбранного файла и информация, содержащаяся в нем, не соответствуют требованиям, предъявляемым к файлам запросов, на экране появится сообщение об ошибке. Повторите процедуру выбора файла.
   - Нажмите кнопку "Далее >".

   Откроется следующее окно мастера.
4. В окне мастера выполните действия:
   - Выберите в списке корневой сертификат, закрытым ключом которого будет заверен издаваемый сертификат пользователя (см. Табл.3 на стр.**30**), и нажмите кнопку "Далее >".
   - Укажите даты начала и окончания срока действия сертификата. Для выбора даты в календаре нажмите кнопку в правой части поля.

     Примечание. В верхней части окна указаны сведения о пользователе, содержащиеся в файле запроса. Эта информация будет добавлена в создаваемый сертификат.
   - Нажмите кнопку "Далее >".

   Откроется следующее окно мастера.
5. В очередном окне мастера выполните следующие действия:
   - Укажите диск (каталог), на (в) котором будут сохранены файлы сертификатов. Для этого нажмите кнопку "..." и выберите нужный диск и каталог в стандартном окне выбора каталогов.
   - Нажмите кнопку "Далее >".

На экране появится сообщение о чтении закрытого ключа центра сертификации.

6. Нажмите кнопку "OK".

   На экране появится запрос пароля.

   Примечание. Данное окно не появится, если при издании корневого сертификата была установлена отметка в поле "Запомнить пароль".

7. Введите пароль, которым был ограничен доступ к ключевой информации при издании корневого сертификата (см. стр. **33**), и нажмите кнопку "OK".

   После успешного чтения закрытого ключа корневого сертификата в указанном ранее каталоге (на диске) будут размещены следующие файлы:

   - root.p7b — файл корневого сертификата;
   - user.cer — файл сертификата пользователя.

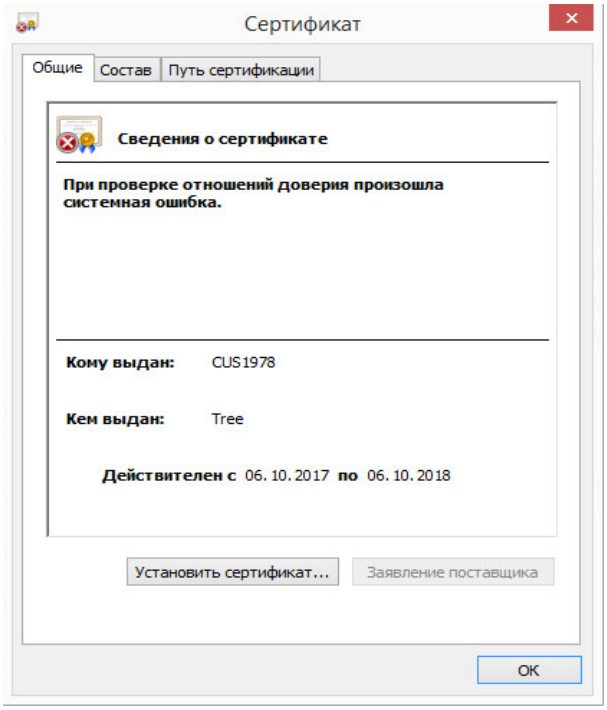
   Внимание! Если файлы сертификатов записываются на дискету, на экране появится сообщение, предлагающее вставить в дисковод дискету, предназначенную для экспорта сертификатов. Если закрытый ключ корневого сертификата хранится на дискете, то, прежде чем продолжить процедуру, обязательно извлеките эту дискету из дисковода.

   Примечание. В том случае, если указанный диск (каталог) содержит одноименные файлы, новые файлы сертификатов будут записаны поверх существующих с предварительным запросом на перезапись.

8. В заключительном окне мастера нажмите кнопку "Готово".
9. Передайте созданные файлы сертификатов данному пользователю для регистрации на абонентском пункте.

Просмотр информации о сертификатах

Информация о сертификатах отображается в стандартном диалоговом окне.



Показанное на рисунке диалоговое окно содержит информацию о сертификате сервера доступа. Сообщения о недостатке информации или об отсутствии доверия появляются при отсутствии корневого сертификата в хранилище доверенных сертификатов данного компьютера.

Примечание. Для нормальной работы программы управления добавление корневого сертификата в хранилище доверенных сертификатов компьютера не требуется.

Для просмотра информации о сертификате:

1. Вызовите на экран список сертификатов (см. стр. **29**).
2. Выберите в списке сертификат и нажмите кнопку "Показать...".

   На экране появится окно с информацией о выбранном сертификате.
3. Для возврата к списку сертификатов нажмите кнопку "ОК".

Хранение списка отозванных сертификатов

При установлении соединения с абонентским пунктом сервер доступа проверяет списки отозванных сертификатов, пути к которым указаны в сертификатах. Для сокращения времени установления соединения предусмотрен режим работы, при котором копии списков отозванных сертификатов хранятся на сервере доступа.

Для настройки режима хранения:

1. Выберите вкладку "Настройки сервера | Настройка сервера".

   В информационном окне отобразится список параметров работы сервера.
2. Установите отметку в поле "Использовать кэш-списки отозванных сертификатов" для хранения копии списка отозванных сертификатов на сервере доступа. Если отметка не установлена, копии списка отозванных сертификатов на сервере доступа не хранятся.
3. Укажите период обновления копии списка.
4. Нажмите кнопку "Сохранить настройки".

Удаление недействительных сертификатов

Предусмотрена возможность единовременного удаления из базы данных сервера доступа всех недействительных сертификатов:

- сертификатов с истекшим сроком действия;
- отозванных сертификатов.

Для удаления недействительных сертификатов:

1. Выберите вкладку "Настройки сервера | Сертификаты".

   В информационном окне отобразятся списки сертификатов.
2. Активируйте одну из ссылок в правой нижней части окна и подтвердите свое решение в окне запроса:
   - "Удалить все просроченные сертификаты" — для удаления всех сертификатов с истекшим сроком действия.
   - "Удалить все отозванные сертификаты" — для удаления всех отозванных сертификатов.

Глава 7
Управление пользователями

Доступ к ресурсам защищенной сети

Для предоставления удаленному пользователю прав доступа к ресурсам защищенной сети необходимо выполнить следующие действия:

1. Создать в базе данных сервера доступа учетную запись пользователя, а также сертификат этого пользователя (см. стр. **41**).
2. Составить для пользователя индивидуальный список правил фильтрации (см. стр. **48**).
3. Передать пользователю файлы сертификатов, созданные при его регистрации в базе данных сервера доступа, а также при необходимости закрытый ключ пользователя.

   Кроме файлов сертификатов и ключа пользователю может быть передан файл с настройками абонентского пункта (конфигурационный файл).

Управление списком пользователей

Все действия, связанные с управлением пользователями, выполняются в основном окне программы управления. Здесь вы можете получить информацию о пользователях, зарегистрированных на сервере доступа, добавить или удалить учетную запись пользователя, управлять свойствами и сертификатами пользователей.

Каждому пользователю в программе управления соответствует учетная запись.

Просмотр списка пользователей

Для просмотра списка пользователей:

- Выберите вкладку "Учетные записи".

  В правой части главного окна появится список учетных записей пользователей.

Информация о пользователях представлена в табличной форме и включает в себя следующие сведения:

- имя пользователя;
- дополнительная информация о пользователе (описание);
- количество дней до окончания действия сертификата;
- количество подключений под данной учетной записью;
- разрешенный канал связи с СД — стандартный VPN-канал или VPN-канал и HTTP-туннель;
- IP-адрес — динамический или статический.

Отключенная учетная запись пользователя сопровождается пиктограммой в виде замка и выделяется синим цветом.

Регистрация пользователей

Порядок регистрации пользователя определяется способом издания сертификата пользователя:

- сертификат издается внешним центром сертификации. Информация о пользователе импортируется из файла сертификата пользователя;
- сертификат издается средствами программы управления. Информация о пользователе вводится администратором вручную или импортируется из файла запроса, сформированного пользователем средствами абонентского пункта.

Подробнее об использовании сертификатов см. стр. **10**.

При регистрации пользователя можно сформировать конфигурационный файл, содержащий все необходимые сведения для настройки подключения пользователя абонентского пункта к серверу доступа. Администратор сервера доступа передает файл пользователю, который использует его при создании нового подключения.

Регистрация пользователя с сертификатом внешнего центра

Для регистрации пользователя:

1. Нажмите на панели инструментов кнопку "Добавить"  .

   Совет. Используйте также команду "Добавить" контекстного меню.

   На экране появится окно "Добавление нового пользователя".
2. Активируйте ссылку "импортируйте сертификат из файла".

   На экране появится окно Windows для выбора файлов.

   Примечание. При импорте сертификата "КриптоПро CSP"в каталог копируются все серверные сертификаты, созданные на криптопровайдере, и их корневые сертификаты.
3. Выберите файл сертификата и нажмите кнопку "Открыть".

   Примечание. Если указанный сертификат уже зарегистрирован в БД СД, на экране появится сообщение о необходимости выбрать другой сертификат. Нажмите кнопку "ОК" в окне сообщения и начните процедуру с п. **2**.

   В полях окна "Добавление нового пользователя" отобразится регистрационная информация о пользователе, содержащаяся в сертификате.

   При необходимости уточните информацию: внесите изменения в поле "Имя учетной записи" и заполните поле "Описание".

   Совет. Для удаления импортированных данных используйте кнопку "Очистить".

   Если в базе данных СД уже зарегистрирован пользователь с таким именем, на экране появится соответствующее сообщение и предложение создать нового пользователя или добавить уже имеющемуся пользователю новый сертификат.
4. При необходимости установите ограничения учетной записи пользователя:

Ограничение по времени работы	Установите отметку, затем нажмите ссылку "Настройка" и в появившемся окне установите расписание работы пользователя (см. стр. **46**)
Разрешить множественные подключения	Установите отметку для подключения под данной учетной записью одновременно с нескольких компьютеров
Отключена	Установите отметку для блокировки учетной записи (см. стр. **46**)
Действия по результату проверки наличия ПАК "Соболь"	Укажите действия по результату проверки наличия ПАК "Соболь" на компьютере пользователя (см. стр. **47**)

Разрешенный канал связи с СД	Выберите одно из двух значений – "стандартный VPN-канал" или "стандартный VPN-канал и HTTP-туннель". Если установлено "стандартный VPN-канал", пользователю будут доступны только UDP-подключения к СД. Если установлено "стандартный VPN-канал и HTTP-туннель", подключение осуществляется по каналу, указанному в настройках АП: без использования прокси (стандартный VPN-канал), через прокси (HTTP-туннель) или потоковое подключение (по защищенному TCP-каналу без использования прокси)

5. Нажмите кнопку "Далее >".

   На экране появится окно добавления пользователю правил фильтрации.

6. Нажмите кнопку "Добавить".

   На экране появится список групп и правил фильтрации.

7. Выберите из списка назначаемые пользователю группы или правила.

   Выбранные правила отобразятся в окне добавления правил пользователя.

8. При необходимости откорректируйте список правил пользователя, используя кнопки "Удалить" и "Добавить".

9. Нажмите кнопку "Далее >".

   На экране появится окно выбора варианта продолжения процедуры:

   - сформировать конфигурационный файл, содержащий все необходимые сведения для подключения пользователя к серверу доступа;
   - экспортировать только корневой сертификат и сертификат пользователя.

10. Если необходимо сформировать конфигурационный файл, выберите вариант "Полная конфигурация пользователя АП" и перейдите к п. **11**.

    Если необходимо экспортировать только файлы сертификатов, выберите вариант "Экспорт сертификатов" и перейдите к п. **13**.

11. В конфигурационный файл включается шаблон настроек подключения абонентского пункта к серверу доступа с параметрами, установленными по умолчанию.

    При необходимости отредактируйте шаблон настроек или создайте новый. При редактировании шаблона можно указать новое место его хранения. При создании нового шаблона он сохраняется в папке по умолчанию.

12. Нажмите кнопку "Далее >".

    Если выполняется экспорт сертификатов, на экране появится окно "Добавление нового пользователя". В окне отображаются введенные данные о пользователе и результаты выполненных операций по экспортированию сертификатов. Перейдите к п. **19**.

    Если формируется конфигурационный файл, появится окно задания пароля для доступа к файлу конфигурации пользователя.

13. Введите пароль и нажмите кнопку "ОК".

    На экране появится окно "Добавление нового пользователя". В окне приводятся введенные данные о пользователе и результаты выполненных операций по регистрации пользователя.

14. Нажмите кнопку "Готово".

    Процедура регистрации пользователя завершена.

После того как сертификат пользователя успешно зарегистрирован, в списке учетных записей появится новый объект либо уже имеющемуся пользователю будет добавлен новый сертификат.

Передайте администратору абонентского пункта файл конфигурации (если он был сформирован) с паролем или файлы сертификатов.

Регистрация пользователя с изданием сертификата

Для регистрации пользователя:

1. Нажмите на панели инструментов кнопку "Добавить"  .

   Совет. Используйте также команду "Добавить" контекстного меню.

   На экране появится окно "Добавление нового пользователя".

2. Введите регистрационную информацию о пользователе.

   Предусмотрено два способа ввода: заполнение соответствующих полей вручную и автоматическое заполнение загрузкой из файла запроса (если такой запрос имеется).

   Если выполняется ручной ввод, заполните требуемые поля в окне и перейдите к п. **4**.

   Если выполняется автоматическое заполнение загрузкой из файла запроса, активируйте ссылку "загрузите их из файла запроса".

   На экране появится стандартное окно выбора файла.

3. Выберите файл запроса.

   Поля в окне "Добавление нового пользователя" будут заполнены автоматически. При необходимости внесите нужные изменения.

4. При необходимости установите ограничения учетной записи пользователя:

Ограничение по времени работы	Установите отметку, затем нажмите ссылку "Настройка" и в появившемся окне установите расписание работы пользователя (см. стр. **46**)
Разрешить множественные подключения	Установите отметку для подключения под данной учетной записью одновременно с нескольких компьютеров
Отключена	Установите отметку для блокировки учетной записи (см. стр. **46**)
Действия по результату проверки наличия ПАК "Соболь"	Укажите действия по результату проверки наличия ПАК "Соболь" на компьютере пользователя (см. стр. **47**)
Разрешенный канал связи с СД	Выберите одно из двух значений – "стандартный VPN-канал" или "стандартный VPN-канал и HTTP-туннель". Если установлено "стандартный VPN-канал", пользователю будут доступны только UDP-подключения к СД. Если установлено "стандартный VPN-канал и HTTP-туннель", подключение осуществляется по каналу, указанному в настройках АП: без использования прокси (стандартный VPN-канал), через прокси (HTTP-туннель) или потоковое подключение (по защищенному TCP-каналу без использования прокси)

5. Нажмите кнопку "Далее >".

   Если в базе данных СД уже зарегистрирован пользователь с таким именем, на экране появится соответствующее сообщение и предложение создать нового пользователя или добавить уже имеющемуся пользователю новый сертификат.

6. Нажмите кнопку в окне сообщения:

Да	Будет создан новый пользователь
Нет	Пользователю будет добавлен новый сертификат

   Окно сообщения закроется.

7. Нажмите кнопку "Далее >".

В окне "Добавление нового пользователя" появится список корневых сертификатов. Выберите сертификат, который будет использоваться для подписи создаваемого сертификата пользователя.

Примечание. Для выбранного сертификата при необходимости можно выполнить следующие действия:

- посмотреть информацию о корневом сертификате. Для этого нажмите кнопку "Просмотр";
- изменить срок действия создаваемого сертификата пользователя, указанный по умолчанию, в полях "Срок действия сертификата".

8. Нажмите кнопку "Далее >".

На экране появится окно добавления пользователю правил фильтрации.

9. Нажмите кнопку "Добавить".

На экране появится список групп и правил фильтрации.

10. Выберите из списка назначаемые пользователю группы или правила.

Выбранные правила отобразятся в окне добавления правил пользователя.

11. При необходимости откорректируйте список правил пользователя, используя кнопки "Удалить" и "Добавить".

12. Нажмите кнопку "Далее >".

На экране появится окно выбора варианта продолжения процедуры:

- сформировать конфигурационный файл, содержащий все необходимые сведения для подключения пользователя к серверу доступа;
- экспортировать только корневой сертификат и сертификат пользователя.

13. Если необходимо сформировать конфигурационный файл, выберите вариант "Полная конфигурация пользователя АП" и перейдите к п. **14**.

Если необходимо экспортировать только файлы сертификатов, выберите вариант "Экспорт сертификатов" и перейдите к п. **16**.

14. В конфигурационный файл включается шаблон настроек подключения абонентского пункта к серверу доступа с параметрами, установленными по умолчанию.

При необходимости отредактируйте шаблон настроек или создайте новый. При редактировании шаблона можно указать новое место его хранения. При создании нового шаблона он сохраняется в папке по умолчанию.

15. Нажмите кнопку "Далее >".

На экране появится предупреждение о создании ключевого контейнера с секретным ключом пользователя.

Перейдите к п. **17**.

16. Укажите папку, в которую будут экспортированы файлы сертификатов, и нажмите кнопку "Далее >".

Если пользователь создается по имеющимся данным, на экране появится предупреждение о создании ключевого контейнера с секретным ключом пользователя.

17. Вставьте ключевой носитель и нажмите кнопку "ОК" в окне предупреждения.

На экране появится сообщение с инструкцией по накоплению энтропии для биологического датчика случайных чисел.

18. Следуя инструкции, нажимайте левой кнопкой мыши на мишень, перемещающуюся по экрану, до завершения процесса накопления энтропии.

После завершения операции накопления энтропии на экране появится окно установки пароля на доступ к ключевому контейнеру.

19. Введите и подтвердите пароль.

При необходимости установите отметку в поле "Запомнить пароль" и нажмите кнопку "ОК".

На экране появится предупреждение о чтении секретного ключа центра сертификации.

20. Нажмите кнопку "ОК" в окне предупреждения.

На экране появится запрос на ввод пароля доступа к контейнеру, созданному при формировании корневого сертификата.

21. Введите пароль и нажмите кнопку "ОК".

Если выполняется экспорт сертификатов, на экране появится окно "Добавление нового пользователя". В окне приводятся введенные данные о пользователе и результаты выполненных операций по экспортированию сертификатов. Перейдите к п. **22**.

Если формируется конфигурационный файл, появится окно задания пароля для доступа к файлу конфигурации пользователя.

22. Введите пароль и нажмите кнопку "ОК".

На экране появится окно "Добавление нового пользователя". В окне приводятся введенные данные о пользователе и результаты выполненных операций по регистрации пользователя.

23. Нажмите кнопку "Готово".

Процедура регистрации пользователя завершена.

В случае успешного издания сертификата пользователя в списке пользователей появится новый объект.

Передайте администратору абонентского пункта файл конфигурации (если он был создан) или файлы сертификатов и ключевого контейнера (если были сгенерированы ключи).

Удаление пользователей

Внимание! При удалении пользователя все сведения о нем, в том числе информация о сертификате, немедленно удаляются из базы данных сервера доступа. После этого установить соединение с сервером под именем этого пользователя невозможно.

Для удаления пользователя (пользователей):

1. Выберите вкладку "Учетные записи".
2. Выберите в списке ярлык с именем удаляемого пользователя и нажмите на панели инструментов кнопку "Удалить"  или клавишу <Delete>.

Совет. Используйте также команду "Удалить" контекстного меню.

Для удаления одновременно нескольких пользователей выделите их в списке, используя клавишу <Ctrl>. Для удобства группового выделения используйте упорядочение списка по столбцам.

На экране появится окно запроса.

3. Нажмите кнопку "Да", чтобы подтвердить удаление выбранного пользователя.

Ярлык пользователя (пользователей) будет исключен из списка пользователей. Сведения об этом пользователе (пользователях) будут удалены из базы данных сервера доступа без возможности восстановления.

Управление параметрами работы пользователя

Вызов окна для настройки свойств пользователя

Для вызова окна настройки:

- Подведите указатель к строке с именем пользователя и дважды нажмите левую кнопку мыши или выберите эту строку и нажмите на панели инструментов кнопку "Свойства"  .

Совет. Используйте также команду "Свойства" контекстного меню.

Блокировка учетной записи пользователя

Для блокировки учетной записи:

1. В контекстном меню учетной записи пользователя выберите пункт "Свойства" (см. стр. **45**).

   Откроется окно свойств учетной записи.
2. Во вкладке "Основные" установите отметку в поле "Отключена".
3. Нажмите кнопку "ОК".

   Учетная запись пользователя будет немедленно заблокирована и пользователь не сможет установить соединение с сервером доступа. Слева от имени пользователя появится пиктограмма  .

   Примечание. Если пользователь в данный момент подключен к серверу доступа, соединение будет разорвано.

Для разблокирования учетной записи:

1. В контекстном меню учетной записи пользователя выберите пункт "Свойства" (см. стр. **45**).

   Совет. Пользователей с заблокированной учетной записью можно отличить по пиктограмме  .
2. Во вкладке "Основные" удалите отметку из поля "Отключена".
3. Нажмите кнопку "ОК".

   Блокировка учетной записи пользователя будет немедленно снята.

Ограничение времени работы пользователя

Примечание. Время работы пользователя определяется по часам сервера доступа, а не абонентского пункта.

Для настройки расписания работы пользователя:

1. В контекстном меню учетной записи выберите пункт "Свойства" (см. стр. **45**).

   Откроется окно свойств учетной записи.
2. Во вкладке "Основные" установите отметку в поле "Ограничение по времени работы" и нажмите ссылку "Настройка".

   Пояснение. Если для пользователя уже установлен некоторый график работы, поле "Ограничение по времени работы" будет содержать отметку.

   На экране появится окно "Режим работы".
3. Определите еженедельное расписание работы пользователя. Для этого:
   - В группе полей "Дни недели" установите отметки ниже названий тех дней недели, которые являются для пользователя рабочими.
   - В поле "Временной период" укажите время работы пользователя в течение суток по рабочим дням. Для этого укажите один или несколько интервалов времени, разделяя интервалы символом ";" (точка с запятой).

     Пример. Если в течение дня пользователю следует предоставить подключение с девяти часов утра до часа дня, затем с двух часов дня до шести часов вечера, то следует ввести: "9-00–13-00; 14-00–18-00".
   - Нажмите кнопку "ОК".

   Будет выполнен возврат на вкладку "Свойства пользователя | Основные".
4. Нажмите кнопку "ОК".

   Измененные параметры, ограничивающие время работы пользователя, вступают в силу при подключении пользователя к серверу доступа.

   Примечание. Если во время изменения параметров пользователь был подключен к серверу доступа, новые параметры вступят в силу только при следующем подключении.

По истечении разрешенного времени работы соединение пользователя с сервером доступа разрывается.

Действия по результатам проверки ПАК "Соболь"

Данный параметр определяет возможность подключения абонентского пункта к серверу доступа в зависимости от того, установлен ли на компьютере ПАК "Соболь" или нет.

Для настройки параметра:

1. В контекстном меню учетной записи выберите пункт "Свойства" (см. стр. **45**).

   Откроется окно свойств учетной записи.

2. Во вкладке "Основные" в раскрывающемся списке "Действие по результату проверки наличия ПАК Соболь" выберите одно из значений:

Игнорировать результат	Проверка на наличие ПАК "Соболь" не выполняется. Сразу производится подключение к серверу доступа
Предупреждать	Перед подключением к серверу доступа выполняется проверка на наличие ПАК "Соболь". При его отсутствии выдается предупреждение, процедура подключения продолжается
Запрещать работу	Перед подключением к серверу доступа выполняется проверка на наличие ПАК "Соболь". При его отсутствии выдается предупреждение, а подключение прерывается

Разрешение и запрет на подключение по HTTP-туннелю

Если на СД разрешено подключение пользователей по HTTP-туннелю (см. стр. **20**), каждому пользователю можно индивидуально установить запрет или разрешение на подключение через прокси.

Для установки запрета/разрешения:

1. В контекстном меню учетной записи выберите пункт "Свойства" (см. стр. **45**).
   Откроется окно свойств учетной записи.
2. Во вкладке "Основные" в поле "Разрешенный канал связи с СД" выберите одно из значений:

Стандартный VPN-канал	Подключение по HTTP-туннелю запрещено (значение по умолчанию)
Стандартный VPN-канал и HTTP-туннель	Если в настройках пользователя установлено значение "Стандартный VPN-канал и HTTP-туннель", подключение по HTTP-туннелю разрешено. Если в настройках пользователя установлено значение "Стандартный VPN-канал", подключение будет осуществляться по стандартному VPN-каналу

3. Нажмите кнопку "OK", чтобы сохранить изменения.

Назначение пользователю IP-адреса

IP-адрес назначается пользователю из пула адресов, определенного на вкладке "Настройка сервера" (см. стр. **20**). Имеются следующие способы назначения IP-адреса:

- динамический;
- статический.

При выборе статического адреса автоматически указывается первый свободный адрес из пула адресов. Этот адрес можно вручную изменить. При этом необходимо учитывать автоматическое резервирование адресов используемого пула: первый адрес резервируется для адреса СД, второй — для статической адресации, третий и последующие — для статической и динамической, последний — broadcast.

Внимание! После выбора или смены статического IP-адреса, а также после изменения пула адресов необходимо перезагрузить СД.

При назначении пользователю статического IP-адреса становится недоступным поле "Разрешить множественные подключения".

Для назначения IP-адреса:

1. В контекстном меню учетной записи выберите пункт "Свойства" (см. стр. **45**).
   Откроется окно свойств учетной записи.
2. Во вкладке "Основные" установите отметку в нужное поле:

Получить IP-адрес динамически	Автоматически назначает динамический адрес из указанного диапазона
Статический IP-адрес	Назначает пользователю постоянный IP-адрес

3. Нажмите кнопку "OK".
   - Если выбран статический IP-адрес, перезагрузите СД.

Управление индивидуальным списком правил фильтрации

Индивидуальный список правил фильтрации определяет права пользователя на доступ к ресурсам защищаемой сети. Индивидуальный список составляется из

отдельных правил и групп правил. Первоначально список правил фильтрации пуст.

Проверка соответствия IP-пакетов правилам и группам правил индивидуального списка выполняется последовательно в порядке расположения правил в списке сверху вниз. Определяются те правила фильтрации, которые соответствуют параметрам данного IP-пакета. Если таких правил несколько, над IP-пакетом выполняются действия, заданные последним из найденных правил.

Если IP-пакет не удовлетворяет параметрам ни одного из правил, заданных индивидуальным списком, он отбрасывается без уведомления об этом абонента-отправителя.

Примечание. Изменения в правилах фильтрации вступают в силу только в следующем сеансе пользователя. При необходимости отключите пользователя от сервера доступа принудительно (см. стр. 52).

Для составления индивидуального списка правил:

1. В контекстном меню учетной записи выберите пункт "Свойства" (см. стр. 45).

   Откроется окно свойств учетной записи.
2. Выберите вкладку "Правила фильтрации".
3. Составьте индивидуальный список правил фильтрации и определите последовательность их применения. Для этого используйте кнопки:

Добавить	Добавляет правило или группу правил. В появившемся списке выберите название отдельного правила (верхняя часть списка) или группы правил (нижняя часть списка)
Удалить	Удаляет выбранное правило или группу правил
Вверх	Поднимает выбранный элемент списка на одну позицию вверх
Вниз	Опускает выбранный элемент списка на одну позицию вниз

При составлении списка учитывайте следующие особенности:
- один и тот же объект (отдельное правило или группу правил) нельзя дважды добавить в список, но одно и то же правило может несколько раз входить в список в составе разных групп правил;
- при включении в список нового объекта он всегда добавляется в конец списка.

4. Нажмите кнопку "ОК".

Просмотр прав доступа пользователя

При составлении индивидуального списка правил фильтрации администратор может оценить результат своих действий в специальном окне, отображающем список доступных пользователю подсетей и правил фильтрации, определяющих права доступа пользователя к этим подсетям.

Для просмотра прав доступа пользователя:

1. В контекстном меню учетной записи выберите пункт "Свойства" (см. стр. 45).

   Откроется окно свойств учетной записи.
2. Выберите вкладку "Подсети".

   Окно содержит иерархический список объектов. Объекты верхнего уровня списка соответствуют подсетям, права на доступ к которым заданы для пользователя индивидуальным списком правил фильтрации. Для просмотра списка групп правил и отдельных правил откройте ветвь списка, относящуюся к нужной подсети.
3. Нажмите кнопку "ОК".

Запрет сторонних соединений

В соответствии с принятой политикой безопасности администратор может разрешить или запретить пользователю во время работы абонентского пункта

незащищенные (без шифрования трафика) соединения со сторонними абонентами.

Внимание! Чтобы в режиме запрета сторонних соединений абонентский пункт мог обращаться к серверам DHCP и DNS, необходимо внести их в список подсетей, разрешенных для незащищенных соединений. Без формирования такого списка функционирование абонентского пункта невозможно.

Для запрета сторонних соединений:

1. Вызовите окно настройки свойств пользователя (см. стр. **45**).

   Откроется окно свойств учетной записи.
2. Выберите вкладку "Незащищенные соединения".
3. Укажите режим работы абонентского пункта:

Разрешено	Разрешить сторонние соединения
Запрещено	Запретить сторонние соединения

4. При выборе режима "Запрещено" сформируйте список незащищенных подсетей, соединение с которыми в режиме запрета незащищенных соединений разрешено:
   - чтобы добавить новую подсеть, нажмите кнопку "Добавить" и выберите нужное название в появившемся списке. В этом списке отображаются только те подсети, в свойствах которых отсутствует отметка в поле "Защищенная подсеть".

     Для выбора будут доступны сети, созданные в разделе "Правила фильтрации | Защищенные подсети";
   - для удаления выбранной подсети из списка нажмите кнопку "Удалить".

   Примечание. При выборе режима "Разрешено" формировать список не требуется, а содержание имеющегося списка системой не учитывается.
5. Нажмите кнопку "ОК".

Предупреждение об окончании срока действия сертификата

Предусмотрена возможность предупреждения администратора об окончании срока действия сертификатов. В этом режиме сертификаты пользователей, срок действия которых подходит к концу, отмечаются в списке специальным значком  .

Для настройки режима:

1. Выберите вкладку "Настройки сервера | Настройка сервера".

   В информационном окне отобразится список параметров работы сервера.
2. Установите отметку в поле "Предупреждение об окончании срока действия сертификата пользователя" и укажите срок оповещения (от 1 до 365 дней).
3. Нажмите кнопку "Сохранить настройки".

Глава 8
Мониторинг и оперативное управление

Контроль состояния сервера доступа, осуществляемый в рамках аудита, описан в [**3**].

Просмотр информации о состоянии сервера доступа

Информация о состоянии сервера доступа содержится в основном окне программы управления в окне состояния (см. стр. **15**).

Актуальная информация отображается при наличии соединения с сервером доступа.

Просмотр списка подключенных пользователей

Для просмотра подключенных пользователей:

- В главном окне программы выберите вкладку "Учетные записи".

В правой части окна отобразится список всех зарегистрированных учетных записей пользователей (см. стр. **15**). Информация отображается в табличном виде. Описание полей приведено в таблице ниже.

Табл.5 Поля таблицы "Учетные записи"

Поле	Описание
Состояние	Пиктограмма, указывающая на текущее состояние пользователя:  — пользователь не подключен к серверу доступа;  — пользователь подключен к серверу доступа;  — учетная запись пользователя заблокирована, он не может устанавливать соединение с сервером доступа
Имя	Имя, под которым пользователь зарегистрирован на сервере доступа
Описание	Дополнительные сведения о пользователе
Количество подключений	Количество подключений, установленных под данной учетной записью. Если пользователь не подключен к серверу доступа, то количество подключений всегда равно 0
Дней до окончания срока действия сертификата	Количество дней до окончания срока действия сертификата. Если кроме числа поле содержит пиктограмму  , значит, сертификат пользователя в настоящий момент недействителен. Пиктограмма появляется также в том случае, если задан срок оповещения об окончании действия сертификата (см. стр. **50**)
IP-адрес	Динамический или статический
Разрешенный канал связи с СД	Стандартный VPN-канал или VPN-канал и HTTP-туннель. По умолчанию поле в таблице не отображается. Для добавления поля в таблицу используйте кнопку "Выбор отображаемых полей", расположенную в панели инструментов

Информация о подключенных пользователях обновляется автоматически каждые 30 секунд.

При выборе учетной записи в списке в нижней части окна появится информация об абонентах, подключенных к серверу доступа под данной учетной записью. Описание параметров подключения представлено в таблице ниже.

Табл.6 Параметры подключения пользователя

Поле	Описание
Количество подключений	Количество абонентов, одновременно подключившихся под данной учетной записью
IP-адрес (АП)	IP-адрес компьютера, с которого абонент выполнил подключение к серверу доступа
IP-адрес (СД)	Выделенный сервером динамический адрес
Время подключения	Дата и время момента подключения абонента к серверу доступа

Список зарегистрированных событий

События, зарегистрированные сервером доступа (в том числе операции локального управления), временно хранятся в его буфере. Срок хранения событий определяется расписанием автоматической передачи журналов в базу данных. Расписание настраивается в свойствах агента (см. [**3**]). С момента регистрации до передачи журналов в базу данных события доступны для просмотра в программе управления сервером доступа.

Для просмотра событий:

1. Выберите вкладку "Журналы".

   В информационном окне появится список хранящихся в буфере событий.
2. Выберите событие в списке "Источник:".

   В нижней части информационного окна появится описание события.

Примечание. Для работы с журналами используется "Программа просмотра журналов ЦУС и СД". Описание программы и порядок работы с ней приведены в [**3**].

Принудительное отключение абонентов

В программе управления сервером доступа предусмотрена возможность отключения одного или нескольких абонентов, подключенных под одной учетной записью пользователя.

Для отключения абонента:

1. Выберите учетную запись.

   В нижней части основного окна отобразится список абонентов, подключенных под выбранной учетной записью.
2. В контекстном меню абонента выберите пункт "Отключить абонента(ов)".

   Совет. Для отключения нескольких или всех пользователей в списке подключенных выделите их, используя клавишу <Shift>, и затем активируйте команду "Отключить абонента(ов)".

   На экране появится окно подтверждения отключения абонента.
3. Нажмите кнопку "Да".

   Выбранные абоненты будут немедленно отключены от сервера доступа.

   Совет. При принудительном отключении пользователя его учетная запись не блокируется, и пользователь сможет самостоятельно восстановить соединение с сервером доступа. Если требуется запретить пользователю доступ к ресурсам защищенной сети, вначале заблокируйте его учетную запись (см. стр. 46), затем, если он в данный момент подключен к серверу, отключите его.

Приложение

Рекомендуемый порядок смены сертификатов

После смены корневого сертификата находящиеся в эксплуатации сертификат сервера доступа и сертификаты пользователей становятся недействительными, а пользователи абонентских пунктов теряют доступ к ресурсам защищенной корпоративной сети. Поэтому рекомендуется выполнять плановую смену сертификатов до истечения их срока действия.

Для смены сертификатов внешнего центра сертификации:

1. Запросите и получите от всех зарегистрированных пользователей файлы запросов на издание сертификатов.

   Пояснение. Запрос на издание сертификата создается пользователем средствами абонентского пункта.

2. Создайте запрос на издание сертификата сервера доступа (см. стр. **31**).
3. Передайте все файлы запросов администратору центра сертификации для издания сертификата сервера и сертификатов пользователей.
4. Получите от администратора центра сертификации файлы сертификатов.
5. Зарегистрируйте полученные корневой сертификат и сертификат сервера доступа (см. стр. **31**), а также полученные сертификаты пользователей.
6. Разошлите всем удаленным пользователям персональный комплект сертификатов для их регистрации на абонентских пунктах и получите от каждого пользователя уведомление о регистрации сертификатов.

   Пояснение. В сопроводительной записке к комплекту сертификатов нужно указать, что после регистрации сертификатов пользователи должны устанавливать соединение только с закрытым ключом, соответствующим новому сертификату (записанным на ключевой носитель при создании запроса на этот сертификат).

7. Удалите из списков зарегистрированных сертификатов старые сертификаты: корневой сертификат, сертификат сервера и сертификаты пользователей (удаление действительных сертификатов см. стр. **29** , удаление недействительных сертификатов см. стр. **39**).

   При попытке удаленного пользователя установить соединение с использованием старого закрытого ключа на экран будет выводиться сообщение об ошибке.

Для смены сертификатов средствами программы управления:

1. Запросите и получите от всех зарегистрированных пользователей файлы запросов на издание сертификатов.

   Пояснение. Запрос на издание сертификата создается пользователем средствами абонентского пункта.

2. Издайте средствами программы управления корневой сертификат и сертификат сервера доступа (см. стр. **33**), а также сертификаты всех зарегистрированных пользователей (см. стр. **35**).
3. Разошлите всем удаленным пользователям персональный комплект сертификатов с закрытыми ключами (если для новых сертификатов ключи были сгенерированы) для их регистрации на абонентских пунктах и получите от каждого пользователя уведомление о регистрации сертификатов.

   Пояснение. В сопроводительной записке к комплекту сертификатов нужно указать, что после регистрации сертификатов пользователи должны устанавливать соединение только с закрытым ключом, соответствующим новому сертификату.

4. Удалите из списков зарегистрированных сертификатов старые сертификаты: корневой сертификат, сертификат сервера и сертификаты пользователей

(удаление действительных сертификатов см. стр. **29** , удаление недействительных сертификатов см. стр. **39**).

При попытке удаленного пользователя установить соединение с использованием старого закрытого ключа на экране отобразится сообщение об ошибке.

Управление ключами криптопровайдера "Код Безопасности CSP"

Управление ключами, сгенерированными криптопровайдером "Код Безопасности CSP", осуществляют с помощью одноименной программы. Данная программа предназначена для решения следующих задач:

- Выбор датчика случайных чисел, используемого криптопровайдером для генерации ключей.
- Удаление сохраненных на компьютере паролей для ключевых контейнеров, созданных криптопровайдером.
- Управление ключевыми контейнерами, созданными криптопровайдером:
  - определение наличия ключей на ключевых носителях;
  - просмотр информации о ключевых контейнерах;
  - копирование ключевых контейнеров на другой носитель;
  - перемещение ключевого контейнера с одного носителя на другой;
  - изменение пароля на доступ к ключевому контейнеру;
  - ввод защитного PIN-кода ключевого носителя;
  - удаление ключевых контейнеров с носителя.

Запуск программы

Для запуска программы:

- Нажмите кнопку "Пуск" и в меню "Программы" выберите пункт " Код Безопасности CSP".

Выбор датчика случайных чисел

Внимание! Данный функционал доступен только для пользователей, наделенных правами администратора данного компьютера.

Криптопровайдер "Код Безопасности CSP" для генерации ключей может использовать следующие устройства:

- встроенный биологический датчик случайных чисел;
- физический датчик случайных чисел ПАК "Соболь".

Для выбора датчика случайных чисел:

1. Выберите вкладку "Общие" и нажмите кнопку "Сменить тип ДСЧ".

   Примечание. Кнопка "Сменить тип ДСЧ" доступна только при запуске криптопровайдера с правами администратора.

   - Чтобы перезапустить криптопровайдер, выберите ссылку "Запустить с правами администратора".

   На экране появится окно выбора датчика случайных чисел.

   Внимание! По умолчанию для низкого уровня безопасности (КС1) выбран биологический датчик случайных чисел, для среднего (КС2) — физический датчик случайных чисел ПАК "Соболь" (требуется наличие платы). Смена датчика нарушает требования использования комплекса по соответствию уровню безопасности.

2. Укажите устройство и нажмите кнопку "ОК".

   Появится сообщение о необходимости перезагрузки компьютера.

3. Для перезагрузки нажмите кнопку "Да" в окне сообщения.

Если необходимо отказаться от выбранного в п. **2** датчика, нажмите в окне сообщения кнопку "Нет".

Окно сообщения закроется, и на вкладке "Общие" появится требование перезагрузки компьютера.

Перезагрузите компьютер.

Удаление сохраненных паролей

Внимание! Данный функционал доступен только для пользователей, наделенных правами администратора данного компьютера.

Для удаления сохраненных паролей:

- Выберите "Общие" и нажмите кнопку "Удалить сохраненные пароли".

Просмотр списка ключевых контейнеров

Программа отображает в иерархическом виде список подключенных носителей и хранящихся на них ключевых контейнеров.

Внимание! При подключении защищенного носителя требуется ввод его PIN-кода.

Для просмотра списка:

- Выберите вкладку "Ключевые контейнеры". Для управления списком используйте следующие кнопки:

Обновить	Обновляет отображаемый список носителей и ключевых контейнеров
PIN-код	Вызывает на экран окно для ввода PIN-кода выбранного в списке носителя eToken
Информация	Вызывает на экран окно с информацией о выбранном ключевом контейнере
Копировать...	Запускает процедуру копирования выбранного ключевого контейнера
Переместить...	Запускает процедуру перемещения ключевого контейнера с одного носителя на другой
Изменить пароль...	Вызывает на экран окно для смены пароля выбранного ключевого контейнера
Удалить	Удаляет выбранный контейнер с носителя

Примечание. В списке отображаются только контейнеры, созданные средствами криптопровайдера "Код Безопасности CSP". Если контейнер носителя eToken не отображается, необходимо ввести PIN-код (см. ниже). Кроме того, процедура ввода PIN-кода выполняется для носителей eToken перед началом установки пользовательского сертификата криптопровайдера "Код Безопасности CSP".

Для ввода PIN-кода:

1. Выберите в списке носитель eToken и нажмите кнопку "PIN-код".

   На экране появится окно для ввода PIN-кода.

2. Введите PIN-код.

   Совет. Если необходимо отменить запрос PIN-кода при последующих обращениях к ключевому контейнеру, установите отметку в поле "Запомнить PIN".

3. Нажмите кнопку "OK".

   Окно ввода PIN-кода закроется.

4. Нажмите кнопку "Обновить".

   В списке появится контейнер с указанием его имени.

Копирование ключевого контейнера

Для копирования контейнера:

1. Выберите в списке нужный ключевой контейнер и нажмите кнопку "Копировать".

   На экране появится запрос пароля на доступ к ключевому контейнеру.
2. Введите пароль и нажмите кнопку "ОК".

   На экране появится окно ввода имени ключевого контейнера.
3. Введите имя копии ключевого контейнера и нажмите кнопку "ОК".

   На экране появится окно ввода пароля на доступ к ключевому контейнеру.
4. Заполните в окне назначения пароля следующие поля:

Новый пароль	Пароль на доступ к копии ключевого контейнера
Подтверждение	
Запомнить пароль	При наличии отметки пароль сохраняется в специальном хранилище на компьютере и запрос пароля при обращении к данному ключевому контейнеру на экран не выводится

5. Нажмите кнопку "ОК".

   На экране появится окно выбора ключевого носителя.
6. Укажите носитель, на который должен быть скопирован ключевой контейнер, и нажмите кнопку "ОК".

   На экране появится уведомление о завершении процедуры.
7. Нажмите кнопку "ОК".

Внимание! Для подключения абонентского пункта к СД с использованием копии ключевого контейнера необходимо повторно установить сертификат пользователя и связать его с новым ключевым контейнером. Для продолжения работы с исходными ключами необходимо также переустановить сертификат пользователя и связать его с исходным ключевым контейнером.

Перемещение ключевого контейнера

Для перемещения контейнера:

1. Выберите в списке ключевой контейнер и нажмите кнопку "Переместить".

   Если ранее пароль на доступ к данному ключевому контейнеру не сохранялся, на экране появится запрос пароля на доступ к ключевому контейнеру. Введите пароль и нажмите кнопку "ОК".

   На экране появится окно назначения нового пароля на доступ к ключевому контейнеру.
2. Введите и подтвердите новый пароль.

   При необходимости установите отметку в поле "Запомнить пароль".

   Нажмите кнопку "ОК".

   На экране появится окно выбора ключевого носителя.
3. Укажите ключевой носитель, на который должен быть перемещен выбранный ключевой контейнер, и нажмите кнопку "ОК".

   На экране появится уведомление о завершении процедуры.
4. Нажмите кнопку "ОК".

   В списке ключевых контейнеров выбранный контейнер будет перемещен на указанный носитель.

Изменение пароля на доступ к ключевому контейнеру

Для изменения пароля:

1. Выберите в списке нужный ключевой контейнер и нажмите кнопку "Изменить пароль".

На экране появится окно ввода пароля на доступ к ключевому контейнеру.

2. Заполните в окне следующие поля:

Новый пароль	Пароль на доступ к копии ключевого контейнера
Подтверждение	
Запомнить пароль	При наличии отметки пароль сохраняется в специальном хранилище на компьютере и запрос пароля при обращении к данному ключевому контейнеру на экран не выводится

3. Нажмите кнопку "ОК".

   На экране появится уведомление о смене пароля.

4. Нажмите кнопку "ОК".

Примечание. При выполнении каких-либо действий с ключевым контейнером, пароль доступа к которому устаревает, автоматически выводится запрос на смену пароля.

Удаление ключевого контейнера с носителя

Для удаления контейнера:

1. Выберите в списке ключевой контейнер и нажмите кнопку "Удалить".

   На экране появится запрос для подтверждения удаления.

2. Нажмите кнопку "Да".

Примечание. Пользователю, не наделенному правами администратора компьютера, необходимо дополнительно ввести пароль на доступ к ключевому контейнеру.

Варианты использования криптопровайдера при формировании закрытого ключа пользователя

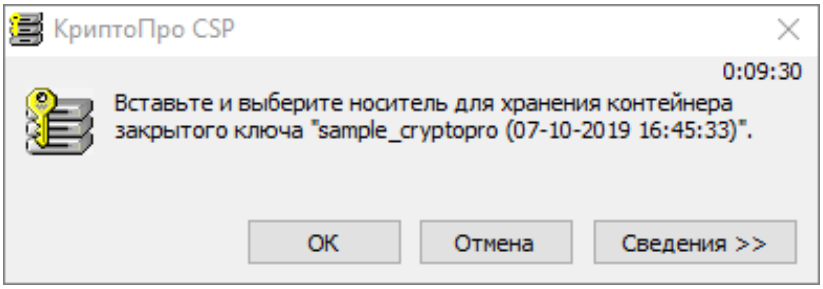
Ниже приведены процедуры формирования закрытого ключа пользователя при его регистрации (см. стр. 41). Представлены варианты использования криптопровайдеров "КриптоПро CSP"и "Код Безопасности CSP".

"КриптоПро CSP"

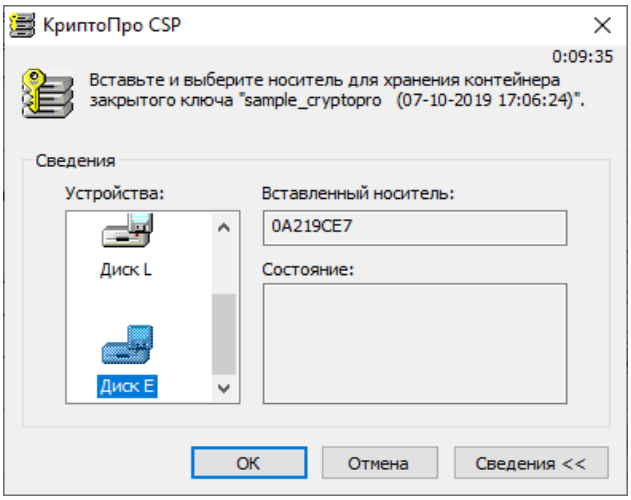
Для формирования закрытого ключа:

1. В окне создания запроса нажмите кнопку "ОК".

   На экране появится окно с требованием вставить чистый ключевой носитель.



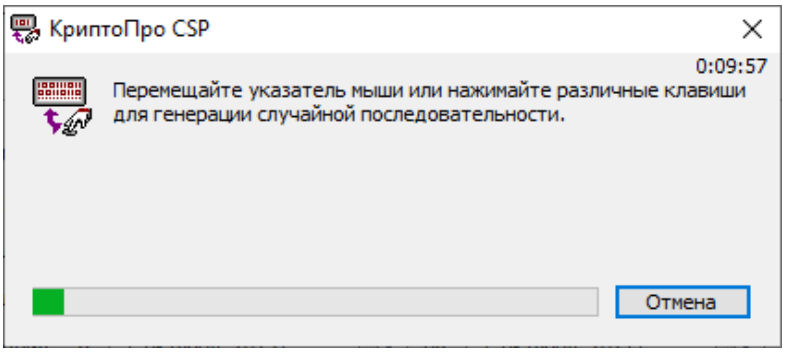
2. Вставьте носитель в считывающее устройство.
3. Нажмите кнопку "Сведения" и в списке "Устройства" выберите считывающее устройство.



4. Нажмите кнопку "OK".

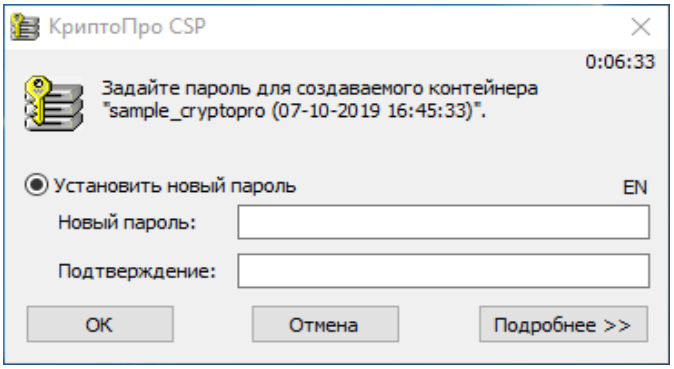
   На экране появится окно генерации случайной последовательности.

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



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

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



6. Введите и подтвердите пароль для создаваемого ключевого контейнера и нажмите кнопку "OK".

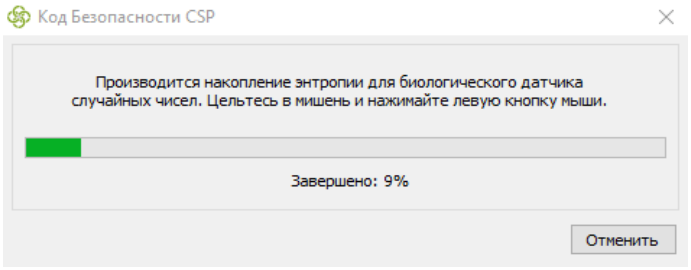
   Начнется запись закрытого ключа пользователя на ключевой носитель, и после ее окончания на экране появится сообщение об успешном завершении создания запроса.

"Код Безопасности CSP"

Для формирования закрытого ключа:

1. В окне создания запроса нажмите кнопку "ОК".

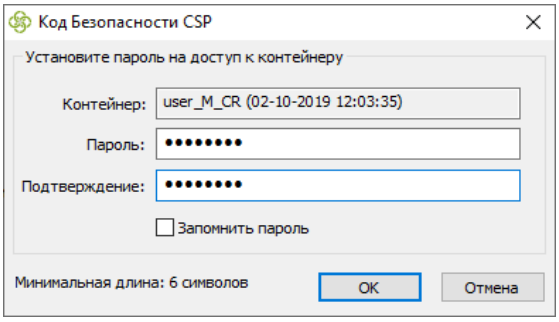
   На экране появится окно накопления энтропии для биологического датчика случайных чисел.



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

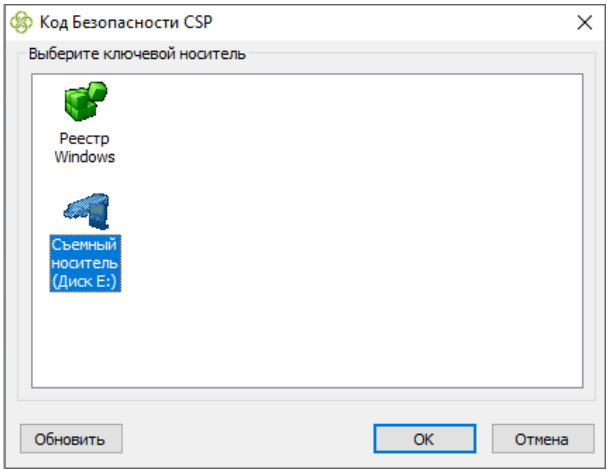
2. Следуйте отображаемой в окне инструкции и дождитесь завершения операции.

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



3. Введите и подтвердите пароль для создаваемого ключевого контейнера и нажмите кнопку "ОК". Длина пароля должна быть не менее 6 символов.

   На экране появится окно выбора ключевого носителя.



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

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

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

Совместимость для СД

В таблицах ниже представлены режимы СД и АП, поддерживающие работу с сертификатами, сформированными в соответствии с ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 и требованиями ТК 26 к OID криптографических алгоритмов.

Табл.7 Совместимость СД в режиме 3.x с АП

	Сертификаты (ГОСТ Р 34.10-2001)	
	КриптоПро CSP	**Код Безопасности CSP**
АП 4.0, АП 3.7.7	Совместимы до 2020 года	Совместимы до 2020 года
АП 4.1 для версии СД 3.x	Совместимы до 2020 года	Совместимы до 2020 года

Табл.8 Совместимость СД в режиме 4.x с АП

	Сертификаты (ГОСТ Р 34.10-2012)		
	Код Безопасности 4.x CSP	**КриптоПро CSP**	**Код Безопасности CSP**
АП 4.1 для версии СД 4.x	Совместимы	Совместимы	Совместимы до 2020 года

Для корректного перехода в режим СД 4 корневой, серверный и пользовательские сертификаты должны быть перевыпущены с соблюдением следующих условий:

- имя сервера в сертификатах соответствует нормальному виду FQDN (например, domain.example.ru или 1.1.1.1);
- для параметра "Поставщик услуг криптографии" установлено значение "4.X CSP (TK26)".

Порядок установления связи между абонентскими пунктами

Для установления связи между абонентскими пунктами АП1 и АП2 (АП1 является инициатором соединения) необходимо выполнение следующих условий:

- учетной записи пользователя АП2 присвоен статический IP-адрес;
- для пользователя АП1 составлены правила фильтрации, разрешающие прохождение трафика от АП1 к АП2.

Для настройки связи между абонентскими пунктами:

1. Назначьте пользователю АП2 статический адрес (см. стр. **48**).
2. Создайте объект "Защищенная подсеть" (см. стр. **24**) и в параметрах его настройки в качестве IP- адреса укажите статический адрес, назначенный пользователю АП2 (см. стр. **25**).
3. Для пользователя АП1 составьте индивидуальный список правил фильтрации (см. стр. **48**), разрешающий прохождение трафика между АП1 и АП2.

Доступ абонентского пункта в защищенные сети других КШ

Ниже приведен порядок организации обмена данными абонентского пункта с сегментами, расположенными в сетях, защищаемых другими КШ.

1. Установите парные связи между КШ с СД и всеми КШ, в защищаемые сети которых необходимо предоставить доступ абонентского пункта.
2. Парные связи задаются в списке связанных КШ в ПУ ЦУС (см. [**1**]). Зарегистрируйте сети, защищаемые другими КШ, как сетевые объекты.

   Создание и настройка сетевых объектов выполняются в ПУ ЦУС (см. [**1**]).
3. В ПУ ЦУС создайте сетевой объект, IP-адрес и маска которого соответствуют пулу адресов сервера доступа, задающему диапазон внутрисетевых адресов, назначаемых абонентскому пункту.
4. В ПУ ЦУС составьте правила фильтрации, обеспечивающие прохождение трафика от сетевого объекта, созданного в п. **3**, к сегментам защищенной сети каждого КШ (см. [**1**]). При составлении правил фильтрации укажите следующие значения:

Поле	Значение
Отправитель	Название сетевого объекта, созданного в п. **3**
Получатель	Название сетевого объекта, созданного в п. **2**

5. В ПУ СД зарегистрируйте сети, защищаемые другими КШ, как сетевые объекты с признаком "защищенная подсеть".

   О создании сетевых объектов в ПУ СД см. стр. **24**.
6. В ПУ СД создайте правила фильтрации, обеспечивающие прохождение трафика от клиента Континента (абонентского пункта) к сегментам защищенной сети каждого КШ.

   В правилах фильтрации установите признак "Контроль состояния соединения" и укажите следующие значения:

Поле	Значение
Отправитель	Клиент Континента
Получатель	Название сетевого объекта, созданного в п. **5**

Программные модули, требующие контроля целостности

Компьютер, на который устанавливается программа управления, должен содержать средства, обеспечивающие контроль целостности программного обеспечения (например ПАК "Соболь"). Контролю целостности подлежат все программные модули, находящиеся в папке RCAS. Расположение папки RCAS указывается при установке программы управления. По умолчанию путь к папке: C:\Program Files\Код Безопасности\Континент\RCAS.

Обмен данными по протоколу AH (IP-протокол 51)

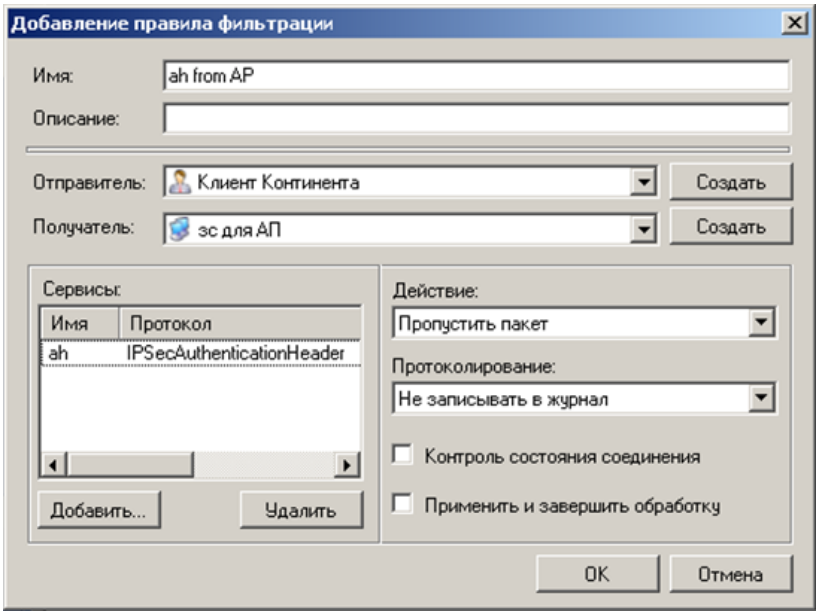
Ниже приведен порядок организации обмена данными абонентского пункта с сегментами сети по протоколу AH (IP-протокол 51).

1. В ПУ СД создайте правило фильтрации, обеспечивающие прохождение пакетов протокола AH от клиента Континента (абонентского пункта) к сегментам сети.

   В правилах фильтрации укажите следующие значения:

Поле	Значение
Отправитель	Клиент Континента
Получатель	Название сетевого объекта
Сервисы	Протокол AH (IP-протокол 51)
Действие	Пропустить пакет

Пример настроек правила фильтрации:



2. В ПУ СД отредактируйте учетную запись, добавив созданное правило фильтрации (см. стр. **48**).

Документация

1. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Ввод в эксплуатацию.
2. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Управление комплексом.
3. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Аудит.
4. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Настройки и использование SNMP.