Код Безопасности

Аппаратно-программный комплекс шифрования

Континент
Версия 3.7

Руководство администратора

Начало работы

RU.88338853.501430.006

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

Оглавление

Список сокращений

VPN	Virtual Private Network
АП	Абонентский пункт
АПКШ	Аппаратно-программный комплекс шифрования
ДА	Детектор (компьютерных) атак
ДСЧ	Датчик случайных чисел
ЕКН	Единый ключевой носитель
КИС	Корпоративная информационная система
КШ	Криптографический шлюз
ЛВС	Локальная вычислительная сеть
МСЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ППЖ	Программа просмотра журналов
ПУ	Программа управления
ПУ СД	Программа управления сервером доступа
ПУ ЦУС	Программа управления ЦУС
СД	Сервер доступа
СКЗИ	Средство криптографической защиты информации
ЦС	Центр сертификации
ЦУС	Центр управления сетью КШ

Введение

Данный документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования «Континент». Версия 3.7" RU.88338853.501430.006 (далее — Комплекс). В нем содержатся сведения, необходимые администраторам для развертывания комплекса в тестовом режиме.

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

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

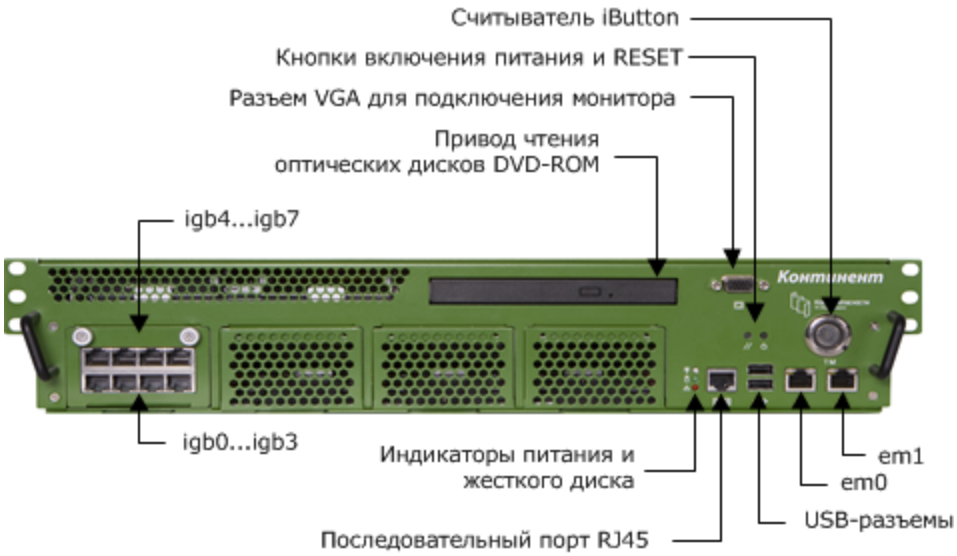
Комплект поставки и внешний вид

Комплект поставки

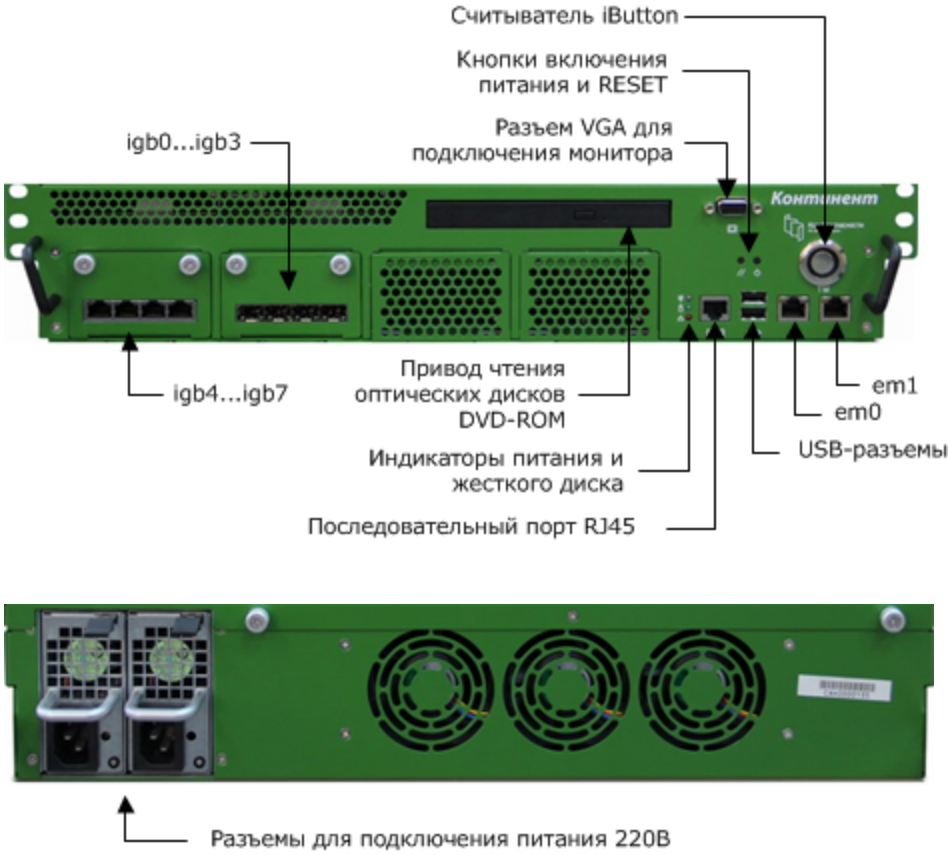
Комплектность комплекса определяется договором о поставке. Комплектность комплекса в зависимости от варианта исполнения представлена в формуляре, входящем в комплект поставки. Комплектность криптографического шлюза — в паспорте на этот криптографический шлюз.

Внешний вид криптографического шлюза

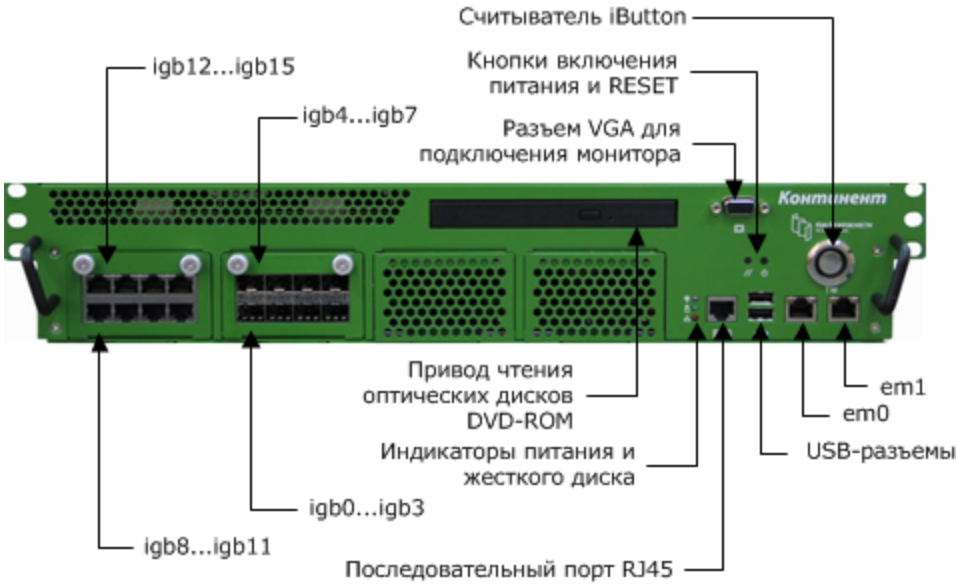
АПКШ "Континент" — платформа IPC-1000 (S021)



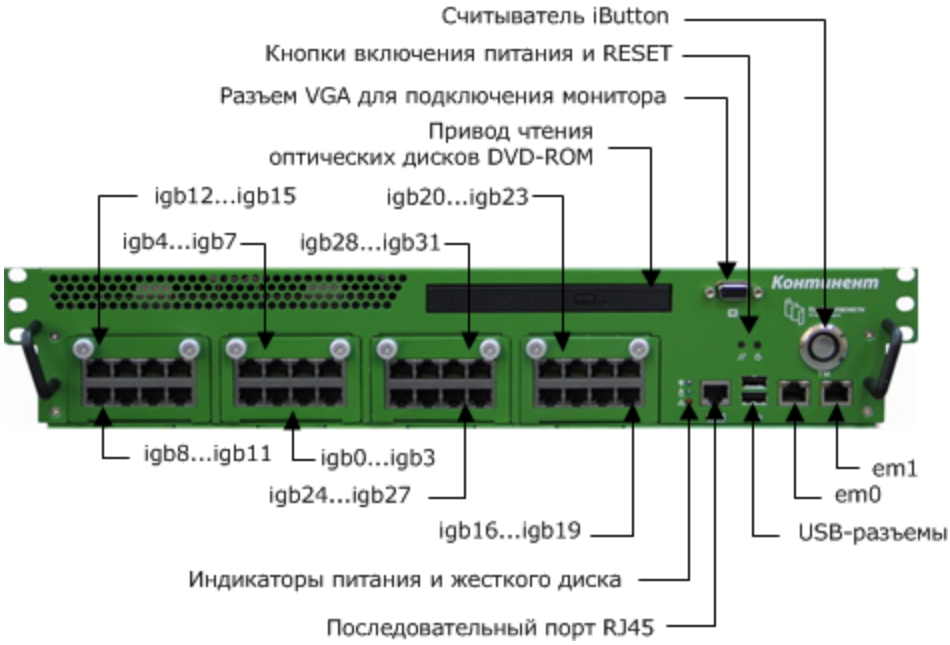
АПКШ "Континент" — платформа IPC-1000F (S021)



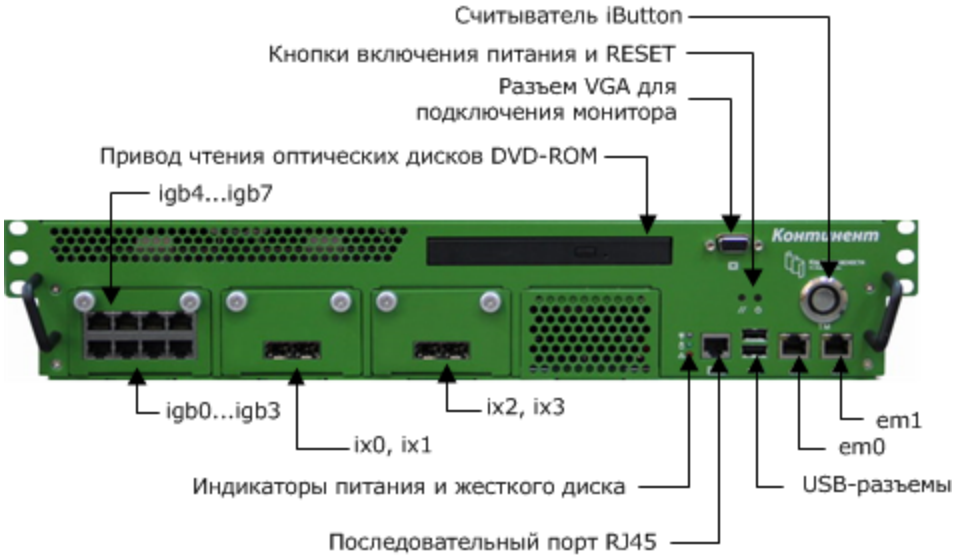
АПКШ "Континент" — платформа IPC-1000F2 (S021)



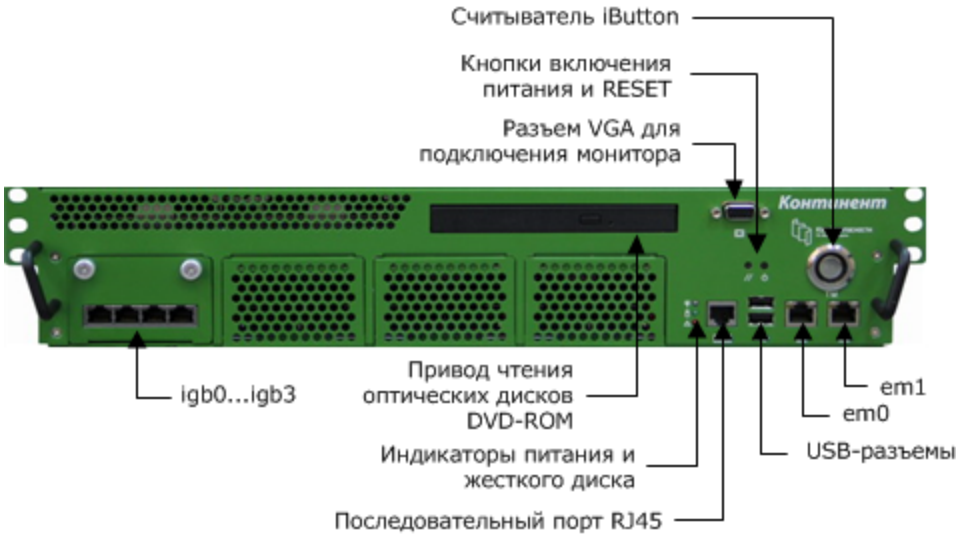
АПКШ "Континент" — платформа IPC-3034 (S021)



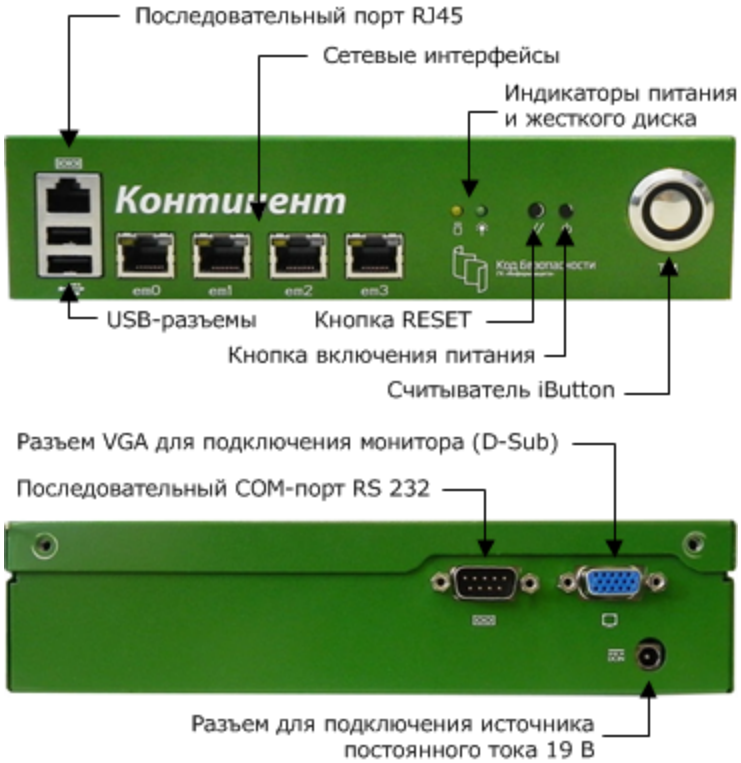
АПКШ "Континент" — платформа IPC-3000F (S021)



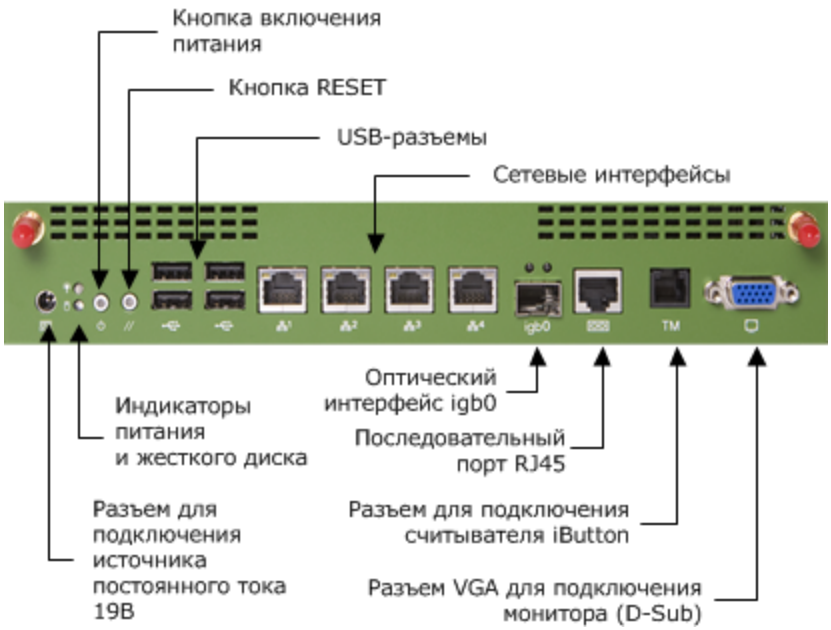
АПКШ "Континент" — платформа IPC-400 (S021)



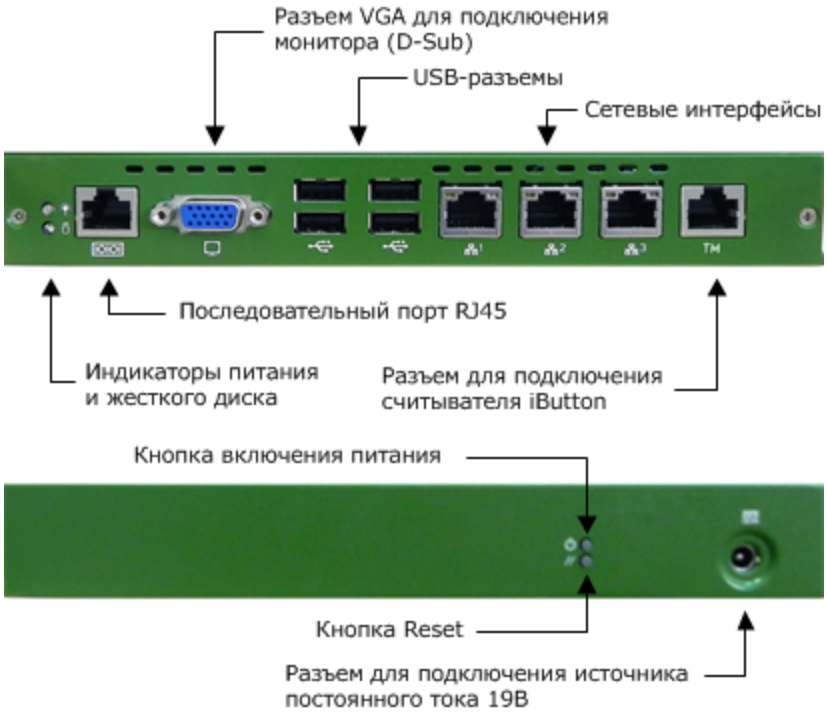
АПКШ "Континент" — платформа IPC-25 (92D9)



АПКШ "Континент" — платформа IPC-25 (S115)



АПКШ "Континент" — платформа IPC-10 (S088)



Подготовка к установке комплекса

Общий порядок подготовки к установке комплекса

Шаг 1. Проверка комплектации

1. Проверьте соответствие комплекта указанному в паспорте.
2. Проверьте внешний вид комплектующих на отсутствие повреждений.

Шаг 2. Подготовка необходимого оборудования

1. Обеспечьте наличие необходимого оборудования в соответствии с приведенными ниже требованиями.
2. Проверьте работоспособность оборудования.
3. Установите необходимое ПО и проверьте его работоспособность.

Шаг 3. Сбор необходимых сведений

- Получите необходимые сведения у провайдера или подготовьте данные самостоятельно на основе топологии КИС и корпоративной политики информационной безопасности. Необходимые исходные данные представлены для каждого сценария ввода комплекса в эксплуатацию.

Требования к оборудованию и программному обеспечению

Перечень необходимого оборудования

Табл.1 Перечень необходимого оборудования

Устройство	Назначение	Примечание
Сетевое устройство с установленным ПО	Подключение ЦУС	Из комплекта поставки
	Подключение сетевого устройства	Из комплекта поставки
Клавиатура и монитор	Выполнение процедуры инициализации ЦУС	
	Выполнение процедуры инициализации сетевого устройства	
АРМ администратора	Управление сетью КШ	АРМ администратора и сервер БД рекомендуется развертывать на разных компьютерах. Требования к оборудованию и программному обеспечению см. стр.**15**
	Управление сервером доступа	
Сервер БД	Хранение регистрационных журналов	
Удаленная рабочая станция	Установка абонентского пункта	Требования к оборудованию и программному обеспечению см. стр.**18**

Устройство	Назначение	Примечание
Чистый и отформатированный USB-флеш-накопитель	Создание идентификатора администратора комплекса при инициализации ЦУС	Если роли администраторов комплекса и сервера доступа выполняет один сотрудник, можно использовать один и тот же носитель. Одновременно можно хранить только один ключ ЦУС и один ключ сервера доступа
	Создание идентификатора администратора сервера доступа при инициализации сервера доступа	
	Создание единого ключевого носителя для агента ЦУС и СД	
	Запись конфигурации сетевого устройства	
	Запись закрытого ключа ЦС при издании корневого сертификата	Можно использовать носитель — идентификатор администратора сервера доступа
	Запись ключей пользователя и сертификата ЦС при регистрации удаленного пользователя	

Состав и варианты размещения подсистемы управления

В подсистему управления комплексом входят следующие компоненты:

- программа управления ЦУС;
- агент ЦУС и СД;
- программа создания ключевого носителя для агента ЦУС и СД;
- программа управления СД (при наличии в комплекте поставки);
- конфигуратор БД журналов ЦУС и СД;
- программа просмотра журналов ЦУС и СД;
- программа просмотра отчетов ЦУС;
- агент обновлений базы решающих правил СОВ;
- агент Роскомнадзора;
- программа копирования ключей.

Регистрационные журналы комплекса хранятся в базе данных на сервере СУБД. Перечень СУБД, с которыми поддерживается работа, представлен в Табл.2 и в Табл.3.

Примечание. При использовании MS SQL Express все его базы данных не могут занимать более 4 Гбайт дискового пространства (ограничение производителя).

Возможны следующие варианты размещения подсистемы управления:

- размещение программ управления и сервера баз данных на одном компьютере (АРМ администратора);
- размещение программ управления и сервера баз данных на разных компьютерах (АРМ администратора и сервер БД).

Подсистема управления комплексом

На компьютерах должны быть установлены компоненты ОС, обеспечивающие работу с протоколами TCP/IP.

Компьютер, на который устанавливают программу управления, должен входить в сеть, защищаемую ЦУС.

В качестве идентификатора администратора комплекса могут использоваться устройства следующих типов:

- дискета 3,5";
- USB-флеш-накопитель;
- USB-ключи eToken (PRO 32k, PRO 64k, JAVA 72k);
- Smart Card Pro (Java), USB-считыватель Athena ASEDrive IIIe USB V2;
- ruToken (v.1, v.2 (S, RF S));
- iKey 2032;
- ПАК "Соболь" с iButton 1995, 1996;
- Secret Net Card/Secret Net Touch Memory Card с iButton 1995, 1996.

При использовании перечисленных устройств необходимо до установки подсистемы управления установить соответствующее программное обеспечение, считывающее устройство или устройство аппаратной поддержки.

Составной частью программы управления сервером доступа является криптопровайдер "Код Безопасности". При необходимости использования этим криптопровайдером физического ДСЧ на компьютере должны быть установлены плата и ПО ПАК "Соболь".

Внимание! Компьютер, на который устанавливают программу управления, должен содержать средства, обеспечивающие контроль целостности программного обеспечения (например ПАК "Соболь"). Перечень программных модулей и ключей реестра Windows, требующих контроля целостности, см. стр.**136**.

Размещение ПУ и сервера баз данных на одном компьютере

Требования к конфигурации АРМ администратора представлены в Табл.2.

Табл.2 Требования к конфигурации АРМ администратора

Элемент	Минимально	Рекомендуется
Процессор	Pentium IV 2,6 ГГц	Core 2 Duo 3 ГГц
Оперативная память	2 ГБ	4 ГБ
Жесткий диск (свободное пространство)	Не менее 20 ГБ. Только NTFS, установка на FAT не поддерживается	
Устройство ввода ключевой информации	USB-порт для USB-флеш-накопителя	
Порты (свободные)	1 x USB 2.0 — при использовании USB-флеш-накопителя; 1 x слот PCI-E — для установки платы ПАК "Соболь 3.0"	
Сетевой адаптер	Ethernet	
Операционная система	• Windows 7 SP1 x86/x64 (кроме всех Starter и Home Edition); • Windows 8.1 x86/x64; • Windows Server 2012 Server R2 x64; • Windows 10	
Установленное ПО	ПАК "Соболь" 3.0 (при необходимости). Версии СУБД для хранения журналов: • MS SQL 2015 Express x32/x64; • MS SQL 2012 Express x32/x64; • MS SQL 2012 x32/x64. MS Internet Explorer 6.0 и выше	

Операционная система компьютера, на который устанавливают агент или программу управления с агентом, должна поддерживать русский язык. В

региональных настройках этого компьютера должны быть указаны язык и региональные настройки России.

Примечание. При использовании Oracle Server на компьютере должна быть установлена операционная система с поддержкой русского языка. В мастере установки Oracle рекомендуется выбрать для выполнения установки и дальнейшей работы русский язык. Это необходимо для корректного отображения сообщений сервера Oracle в программе просмотра журналов.

Размещение ПУ и сервера баз данных на разных компьютерах

Требования к конфигурации сервера БД и АРМ администратора представлены в Табл.3 и Табл.4 соответственно.

Табл.3 Требования к конфигурации сервера БД

Элемент	Минимально	Рекомендуется
Процессор	Pentium IV 2,6 ГГц	Core 2 Duo 3 ГГц
Оперативная память	2 ГБ	4 ГБ
Жесткий диск (свободное пространство)	Не менее 20 ГБ. Только NTFS, установка на FAT не поддерживается	
Устройство ввода ключевой информации	USB-порт для USB-флеш-накопителя	
Порты (свободные)	1 x USB 2.0 — при использовании USB-флеш-накопителя	
Сетевой адаптер	Ethernet	
Операционная система	• Windows 7 SP1 x86/x64 (кроме всех Starter и Home Edition); • Windows 2008 Server R2 SP1 x64; • Windows 2008 Server SP2 x86/x64; • Windows Vista SP2 x86/x64 (кроме всех выпусков Starter иHome Edition)	
Установленное ПО	Версии СУБД для хранения журналов: • MS SQL 2015 Express x32/x64; • MS SQL 2012 Express x32/x64; • MS SQL 2012 x32/x64. MS Internet Explorer 6.0 и выше	

Примечание. При использовании Oracle Server на компьютере должна быть установлена операционная система с поддержкой русского языка. В мастере установки Oracle рекомендуется выбрать для выполнения установки и дальнейшей работы русский язык. Это необходимо для корректного отображения сообщений сервера Oracle в программе просмотра журналов.

Табл.4 Требования к конфигурации АРМ администратора

Элемент	Минимально	Рекомендуется
Процессор	Pentium IV 1,8 ГГц	Core 2 Duo 2,6 ГГц
Оперативная память	512 МБ	2 ГБ
Жесткий диск (свободное пространство)	Не менее 2 ГБ. Только NTFS, установка на FAT не поддерживается	
Устройство ввода ключевой информации	USB-порт для USB-флеш-накопителя	
Порты (свободные)	1 x USB 2.0 — при использовании USB-флеш-накопителя; 1 x PCI-слот — для установки платы ПАК "Соболь 3.0"; 1 x слот PCI- E — для установки платы ПАК "Соболь 3.0"	
Сетевой адаптер	Ethernet	

Элемент	Минимально	Рекомендуется
Операционная система	• Windows 2012 Server R2 x64; • Windows 10; • Windows 8.1 x86/x64; • Windows 7 SP1 x86/x64 (кроме всех выпусков Starter и Home Edition)	
Установленное ПО	MS Internet Explorer 6.0 и выше	

Операционная система компьютера, на котором установлена ПУ ЦУС или агент с программой управления, должна поддерживать русский язык. В региональных настройках этого компьютера должны быть указаны язык и региональные настройки для России.

Примечание. В мастере установки клиента Oracle рекомендуется выбрать для выполнения установки и дальнейшей работы английский язык. Это необходимо для корректного отображения сообщений сервера Oracle в программе просмотра журналов.

Абонентский пункт

Комплекс предназначен для использования на компьютерах, оснащенных процессорами семейства Intel X86 или совместимыми с ними. Требования к конфигурации компьютеров приведены в таблице ниже.

Элемент	Минимально	Рекомендуется
Процессор	Celeron 300 МГц	Pentium IV 1,8 ГГц
Оперативная память	128 МБ	512 МБ
Жесткий диск (свободное пространство)	512 МБ	512 МБ
Операционная система	Windows XP Professional SP3 x86; Windows 2003 Server SP2 x86/x64; Windows 2003 Server R2 SP2 x64/x32; Windows Vista SP2 x86/x64 (кроме всех выпусков Starter и Home Edition); Windows 2008 Server SP2 x86/x64; Windows 2008 Server R2 SP1 x64; Windows 7 SP1 x86/x64 (кроме всех выпусков Starter и Home Edition); Windows 8 x86/x64; Windows 8.1 x86/x64; Windows 10	
Установленное ПО	**Низкий уровень безопасности** MS Internet Explorer версии 6.0 и выше	
	Средний уровень безопасности ПАК "Соболь" 3.0; MS Internet Explorer версии 6.0 и выше	
	Высокий уровень безопасности ПАК "Соболь" 3.0; "КриптоПро CSP" версии 3.6.1; Secret Net версии, соответствующей установленной ОС; поставляется в составе дистрибутива ПО абонентского пункта; MS Internet Explorer версии 6.0 и выше	
Ключевое устройство	Дискета 3,5"; USB-флеш-накопитель; USB-ключ eToken PRO (Java); Смарт-карта eToken Pro (Java) с USB-считывателем Athena ASEDrive IIIe USB V2; RuToken S/ ЭЦП; iButton DS1994/ DS1995/ DS1996; Secret Net Card/ Secret Net Touch Memory Card	

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

Внимание!

- Все службы, реализующие штатные механизмы удаленного управления операционной системой, должны быть отключены.
- Пропускная способность сетевого канала, по которому устанавливается соединение абонентского пункта с сервером доступа, должна быть не менее 9.6 Кбит/с.
- Компьютер, на который устанавливают абонентский пункт, при необходимости соответствия определенному уровню безопасности должен содержать средства, обеспечивающие контроль целостности программного обеспечения (например, ПАК "Соболь").
- При использовании абонентского пункта совместно с ПАК "Соболь", а также с криптопровайдером "КриптоПро CSP" необходимо перед установкой абонентского пункта установить эти аппаратные и программные продукты согласно эксплуатационной документации на них, а также, в зависимости от требований устанвливаемого уровня безопасности, настроить "КриптоПро CSP" на использование аппаратного датчика случайных чисел ПАК "Соболь". В случае если ПАК "Соболь" не используется, требуется настроить любой другой датчик случайных чисел, например биологический.

Установка 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 (ДСЧ).

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).

Требования к сетевым коммуникациям

Если на пути зашифрованного трафика находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать для них правила, разрешающие прохождение служебных пакетов комплекса. Перечень протоколов и портов, по которым осуществляется обмен служебными пакетами между компонентами комплекса, см. стр.**131**.

Требования к квалификации персонала

Сотрудники, выполняющие развертывание комплекса, должны быть квалифицированными специалистами по обслуживанию вычислительной техники и иметь навыки настройки оборудования для работы в локальной сети.

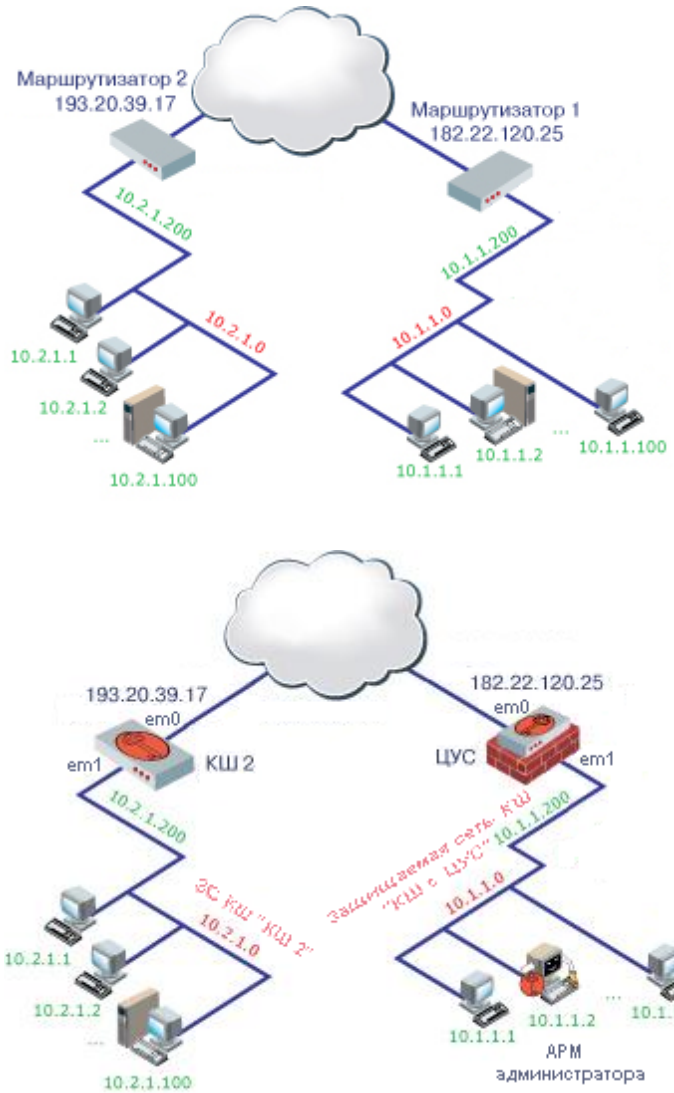
Администратор комплекса должен пройти обучение приемам администрирования комплекса и иметь следующие знания и навыки:

- навыки администрирования операционной системы MS Windows;
- навыки настройки оборудования для работы в локальной сети;
- базовые знания по техническим и криптографическим аспектам обеспечения информационной безопасности;
- навыки администрирования баз данных.

Основные сценарии ввода комплекса в эксплуатацию

Защищенное соединение между локальными сетями

На рисунке представлен пример организации действующих локальных сетей до и после подключения КШ.



Исходные данные

Для выполнения работ необходимо наличие перечисленных ниже сведений.

Данные	Описание	Примечание
Имя внешнего интерфейса ЦУС	Имя интерфейса ЦУС, подключаемого к внешней сети	См. стр.**8**. На рисунке em0
Внешний IP-адрес ЦУС	IP-адрес внешнего интерфейса ЦУС	Необходимо получить у провайдера. На рисунке 182.22.120.25
Маска внешней сети ЦУС	Маска внешней сети, к которой подключен ЦУС	Необходимо получить у провайдера. На рисунке 255.255.255.0

Данные	Описание	Примечание
IP-адрес маршрутизатора по умолчанию для ЦУС	IP-адрес маршрутизатора по умолчанию для ЦУС	Необходимо получить у провайдера. Например, 182.22.120.1
Имя внутреннего интерфейса ЦУС	Имя интерфейса ЦУС, подключаемого к защищаемой сети. К этой сети должно быть подключено АРМ администратора	См. стр.**8**. На рисунке em1
Внутренний IP-адрес ЦУС	IP-адрес внутреннего интерфейса ЦУС	На рисунке 10.1.1.200
Маска защищаемой сети ЦУС	Маска защищаемой сети, к которой подключен ЦУС	На рисунке 255.255.255.0
Имя КШ 2	Наименование КШ 2 для регистрации в БД ЦУС	На рисунке "КШ 2"
Имя внешнего интерфейса КШ 2	Имя интерфейса КШ 2, подключаемого к внешней сети	См. стр.**8**. На рисунке em0
Внешний IP-адрес КШ 2	IP-адрес внешнего интерфейса КШ 2	Необходимо получить у провайдера. На рисунке 193.20.39.17
Маска внешней сети КШ 2	Маска внешней сети, к которой подключен КШ 2	Необходимо получить у провайдера. На рисунке 255.255.255.0
IP-адрес маршрутизатора по умолчанию для КШ 2	IP-адрес маршрутизатора по умолчанию для КШ 2	Необходимо получить у провайдера. Например, 193.20.39.1
Имя внутреннего интерфейса КШ 2	Имя интерфейса КШ 2, подключаемого к защищаемой сети	См. стр.**8**. На рисунке em1
Внутренний IP-адрес КШ 2	IP-адрес внутреннего интерфейса КШ 2	На рисунке 10.2.1.200
Маска защищаемой сети КШ 2	Маска защищаемой сети, к которой подключен КШ 2	На рисунке 255.255.255.0
Строка конфигурации КШ 2	Строка символов, определяющая аппаратную конфигурацию КШ	См. паспорт из комплекта поставки
Тип и сетевое имя сервера БД	Тип и сетевое имя сервера баз данных, используемого для организации хранения регистрационных журналов	Определяется при развертывании СУБД на стадии подготовки к вводу комплекса в эксплуатацию
Имя пользователя и пароль администратора СУБД	Под этой учетной записью будет осуществляться обращение к СУБД при установке подсистемы управления	Определяется при развертывании СУБД на стадии подготовки к вводу комплекса в эксплуатацию
Имя пользователя и пароль для подключения агента	Под этой учетной записью будет осуществляться обращение агента к СУБД после его установки и запуска	Эту учетную запись можно создать в процессе установки подсистемы управления комплексом
Имя пользователя и пароль для просмотра журналов	Под этой учетной записью будет предоставляться доступ к регистрационным журналам, хранящимся в базе данных, из программы просмотра журналов	Эту учетную запись можно создать в процессе установки подсистемы управления комплексом

Данные	Описание	Примечание
Серийный номер лицензии на право использования ЦУС	Строка символов, определяющая ограничения на параметры ЦУС	Из комплекта поставки
Правила фильтрации	Правила, определяющие прохождение трафика в КИС	Примеры см. стр.**89**

Организация защищенного соединения между локальными сетями

Ввод комплекса в эксплуатацию выполняют в следующем порядке:

1. Подключение ЦУС.
2. Установка подсистемы управления.
3. Подключение сетевых устройств.
4. Настройка защищенного соединения.

Шаг 1. Подключение ЦУС

1. Получите у провайдера два IP- адреса: один для ЦУС и один для маршрутизатора по умолчанию.

   Примечание. На приведенном выше рисунке это IP-адрес 182.22.120.25 для ЦУС и IP-адрес 182.22.120.1 для маршрутизатора по умолчанию.

2. Выполните инициализацию ЦУС (см. стр.**37**). При этом укажите следующие значения параметров:

Имя внешнего интерфейса	Имя внешнего интерфейса ЦУС
Внешний IP-адрес шлюза	Внешний IP-адрес ЦУС
Маска сети внешнего IP-адреса	Маска внешней сети ЦУС
Имя внутреннего интерфейса	Имя внутреннего интерфейса ЦУС
Внутренний IP-адрес шлюза	Внутренний IP-адрес ЦУС
Маска сети внутреннего IP-адреса	Маска защищаемой сети ЦУС
Адрес маршрутизатора по умолчанию	IP-адрес маршрутизатора по умолчанию для ЦУС
Носитель для инициализации	ПАК "Соболь"

3. Подключите ЦУС к сетевым коммуникациям, как указано на рисунке выше.

Результат

- Функционирующий ЦУС.
- Идентификатор и пароль администратора комплекса на USB-флеш-накопителе.

Шаг 2. Установка подсистемы управления

1. Выполните установку и запуск ПУ ЦУС на АРМ администратора комплекса (см. стр.**46**).

   При запуске ПУ ЦУС (см. стр.**48**) выполните следующие действия:

   - Предъявите идентификатор администратора комплекса, созданный при инициализации ЦУС.
   - Заполните поля диалога "Параметры настройки ЦУС":

IP-адрес	Внутренний IP-адрес ЦУС

Время ожидания соединения, сек.	Значение по умолчанию
Считыватель ключей	Для идентификатора администратора комплекса, созданного при инициализации ЦУС на USB-флеш-накопителе, — значение "Съемный диск"

- Введите пароль для расшифровывания ключа администратора, указанный при инициализации ЦУС.
- Укажите серийный номер лицензии на право использования ЦУС.

2. Установите агент на сервер БД (см. стр.**46**).
3. Сконфигурируйте базу данных журналов. Для этого используйте Конфигуратор БД журналов ЦУС и СД (см. стр.**54**).

   При подключении к базе данных укажите следующие значения параметров (см. стр.**55**):

Тип базы данных	Тип сервера БД
Имя сервера	Сетевое имя сервера БД
Учетная запись сервера базы данных	Имя пользователя и пароль администратора СУБД

   При создании новой базы данных укажите произвольное имя (например Continent).

   Укажите имя пользователя (например ContinentAgent) и пароль для подключения агента (см. стр.**56**).

   Укажите имя пользователя (например ContinentReader) и пароль для просмотра журналов (см. стр.**56**).
4. Запустите программу создания ключевого носителя и создайте единый ключевой носитель (см. стр.**57** и стр.**58**). При этом укажите следующие значения параметров:

Ключевой носитель-источник	Идентификатор администратора комплекса, созданный при инициализации ЦУС
IP-адрес объекта	Внутренний IP-адрес ЦУС
Пароль для расшифровки ключей	Пароль, указанный при инициализации ЦУС для защиты идентификатора администратора комплекса

5. Запустите программу управления агентом и настройте параметры агента (см. стр.**60**).

   Для запуска нажмите кнопку "Пуск" и в главном меню Windows выберите "Все программы > Код Безопасности > Континент 3.7 > Программа управления агентом ЦУС и СД".

   Для единого ключевого носителя на USB-флеш-накопителе укажите значение "Съемный диск".
6. Предъявите единый ключевой носитель и запустите агент вручную. Для этого используйте команду "Запустить Агент" контекстного меню пиктограммы агента. Настройте в ПУ ЦУС расписание передачи журналов в базу данных (см. стр.**63**).

Результат

- Установленная и запущенная программа управления ЦУС (ПУ ЦУС).
- Автоматически созданные объекты, отображаемые в ПУ ЦУС:
  - криптографический шлюз "КШ с ЦУС";
  - сетевой объект "Любой";

- сервисы "Любой TCP", "Любой UDP", "Любой ICMP" и другие стандартные сервисы;
- временной интервал "Постоянно";
- класс трафика "Нормальный".

- Функционирующий агент.
- Установленная и настроенная программа просмотра журналов (ППЖ).

Шаг 3. Подключение КШ (сетевого устройства)

1. Получите у провайдера два IP- адреса: один для КШ и один для маршрутизатора по умолчанию.

Примечание. На приведенном выше рисунке это IP-адрес 193.20.39.17 для КШ 2 и IP-адрес 193.20.39.1 для маршрутизатора по умолчанию.

2. В программе управления зарегистрируйте КШ (см. стр. **69**) и запишите на носитель конфигурацию и ключи (см. стр. **69**).

   При регистрации укажите следующие значения параметров:

   - Диалог "Создание криптошлюза":

Название	Имя КШ 2
Строка конфигурации	Строка конфигурации КШ 2
Продолжить настройку параметров созданного криптошлюза в окне свойств	Установите отметку

   - Диалог "Свойства криптошлюза/ Интерфейсы", вкладка <Имя внешнего интерфейса КШ 2>:

Тип	Внешний
Режим	Автовыбор
IP-адрес	Внешний IP-адрес КШ 2
Маска	Маска внешней сети КШ 2

   - Диалог "Свойства криптошлюза/ Интерфейсы", вкладка <Имя внутреннего интерфейса КШ 2>:

Тип	Внутренний
Режим	Автовыбор
IP-адрес	Внутренний IP-адрес КШ 2
Маска	Маска защищаемой сети КШ 2

   - Диалог "Свойства криптошлюза/ Маршрутизация".

Статическая	Установите отметку
Адрес назначения	0.0.0.0
Следующий узел	IP-адрес маршрутизатора по умолчанию для КШ 2

   При записи конфигурации на носитель в поле "Режим" выберите значение "Основной".

3. Выполните инициализацию КШ (см.стр. **41**) и подключите его к сетевым коммуникациям, как указано на рисунке выше.
4. Введите КШ в эксплуатацию (см. стр. **70**).

Результат

- Функционирующий КШ.
- Автоматически созданные объекты, отображаемые в ПУ ЦУС:

- криптографический шлюз "КШ 2";
- стандартные сервисы.

Шаг 4. Настройка защищенного соединения

1. Средствами ПУ ЦУС сформируйте для ЦУС список связанных КШ (см. стр.**74**). Для этого имя КШ 2 перенесите в список "Связанные криптографические шлюзы".
2. Создайте правила фильтрации для прохождения зашифрованного трафика между защищенными сетями. Значения параметров таких правил см. стр.**89**. Процедуру создания правил фильтрации см. стр.**82**.

Результат

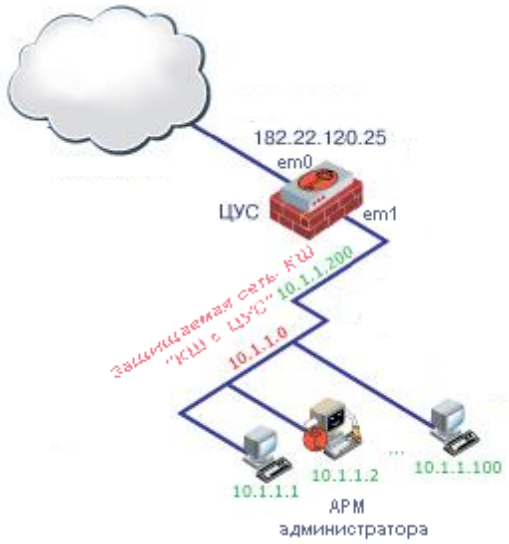
- Включенный режим шифрования.
- Правила фильтрации для прохождения зашифрованного трафика.

Результат

1. Наличие трафика между защищенными сетями.
2. Регистрация в системных журналах обоих КШ события об установке парной связи с определенным КШ.
3. Анализ трафика на промежуточном маршрутизаторе:
   - регистрация IP-пакетов, передаваемых между внешними интерфейсами КШ по протоколу UDP с порта 10000 на порт 10000;
   - отсутствие адресов хостов, обменивающихся IP-пакетами.

Межсетевое экранирование

На рисунке представлен пример организации действующих локальных сетей до и после подключения КШ:



Исходные данные

Для выполнения работ необходимо наличие перечисленных ниже сведений.

Данные	Описание	Примечание
Имя внешнего интерфейса ЦУС	Имя интерфейса ЦУС, подключаемого к внешней сети	См. стр.**8**. На рисунке em0
Внешний IP-адрес ЦУС	IP-адрес внешнего интерфейса ЦУС	Необходимо получить у провайдера. На рисунке 182.22.120.25
Маска внешней сети ЦУС	Маска внешней сети, к которой подключен ЦУС	Необходимо получить у провайдера. На рисунке 255.255.255.0
IP-адрес маршрутизатора по умолчанию для ЦУС	IP-адрес маршрутизатора по умолчанию для ЦУС	Необходимо получить у провайдера. Например, 182.22.120.1
Имя внутреннего интерфейса ЦУС	Имя интерфейса ЦУС, подключаемого к защищаемой сети. К этой сети должен быть подключен АРМ администратора	См. стр.**8**. На рисунке em1
Внутренний IP-адрес ЦУС	IP-адрес внутреннего интерфейса ЦУС	На рисунке 10.1.1.200
Маска защищаемой сети ЦУС	Маска защищаемой сети, к которой подключен ЦУС	На рисунке 255.255.255.0
Тип и сетевое имя сервера БД	Тип и сетевое имя сервера баз данных, используемого для организации хранения регистрационных журналов	Определяется при развертывании СУБД на стадии подготовки к вводу комплекса в эксплуатацию
Имя пользователя и пароль администратора СУБД	Под этой учетной записью будет осуществляться обращение к СУБД при установке подсистемы управления	Определяется при развертывании СУБД на стадии подготовки к вводу комплекса в эксплуатацию
Имя пользователя и пароль для подключения агента	Под этой учетной записью будет осуществляться обращение агента к СУБД после его установки и запуска	Эту учетную запись можно создать в процессе установки подсистемы управления комплексом

Данные	Описание	Примечание
Имя пользователя и пароль для просмотра журналов	Под этой учетной записью будет предоставляться доступ к регистрационным журналам, хранящимся в базе данных, из программы просмотра журналов	Эту учетную запись можно создать в процессе установки подсистемы управления комплексом
Серийный номер лицензии на право использования ЦУС	Строка символов, определяющая ограничения на параметры ЦУС	Из комплекта поставки
Правила фильтрации и трансляции	Правила, определяющие прохождение трафика в КИС	Примеры см. стр.**90**

Организация межсетевого экранирования

Ввод комплекса в эксплуатацию выполняют в следующем порядке:

1. Подключение ЦУС.
2. Установка подсистемы управления.
3. Настройка правил фильтрации и трансляции.

Шаг 1. Подключение ЦУС

1. Получите у провайдера два IP- адреса: один для ЦУС и один для маршрутизатора по умолчанию.

   Примечание. На приведенном выше рисунке это IP-адрес 182.22.120.25 для ЦУС и IP-адрес 182.22.120.1 для маршрутизатора по умолчанию.

2. Выполните инициализацию ЦУС (см. стр.**37**). При этом укажите следующие значения параметров:

Имя внешнего интерфейса	Имя внешнего интерфейса ЦУС
Внешний IP-адрес шлюза	Внешний IP-адрес ЦУС
Маска сети внешнего IP-адреса	Маска внешней сети ЦУС
Имя внутреннего интерфейса	Имя внутреннего интерфейса ЦУС
Внутренний IP-адрес шлюза	Внутренний IP-адрес ЦУС
Маска сети внутреннего IP-адреса	Маска защищаемой сети ЦУС
Адрес маршрутизатора по умолчанию	IP-адрес маршрутизатора по умолчанию для ЦУС
Носитель для инициализации	ПАК "Соболь"

3. Подключите ЦУС к сетевым коммуникациям, как указано на рисунке выше.

Результат

- Функционирующий ЦУС.
- Идентификатор и пароль администратора комплекса на USB-флеш-накопителе.

Шаг 2. Установка подсистемы управления

1. Выполните установку и запуск ПУ ЦУС на АРМ администратора комплекса (см. стр.**46**).

   При запуске ПУ ЦУС (см. стр.**48**) выполните следующие действия:

   - Предъявите идентификатор администратора комплекса, созданный при инициализации ЦУС.
   - Заполните поля диалога "Параметры настройки ЦУС":

IP-адрес	Внутренний IP-адрес ЦУС
Время ожидания соединения, сек.	Значение по умолчанию
Считыватель ключей	Для идентификатора администратора комплекса, созданного при инициализации ЦУС на USB-флеш-накопителе, — значение "Съемный диск"

- Введите пароль для расшифровывания ключа администратора, указанный при инициализации ЦУС.
- Укажите серийный номер лицензии на право использования ЦУС.

2. Установите агент на сервер БД (см. стр.**46**).
3. Сконфигурируйте базу данных журналов. Для этого используйте Конфигуратор БД журналов ЦУС и СД (см. стр.**54**).

   При подключении к базе данных укажите следующие значения параметров (см. стр.**55**):

Тип базы данных	Тип сервера БД
Имя сервера	Сетевое имя сервера БД
Учетная запись сервера базы данных	Имя пользователя и пароль администратора СУБД

   При создании новой базы данных укажите произвольное имя (например Continent).

   Укажите имя пользователя (например ContinentAgent) и пароль для подключения агента (см. стр.**56**).

   Укажите имя пользователя (например ContinentReader) и пароль для просмотра журналов (см. стр.**56**).
4. Запустите программу создания ключевого носителя и создайте единый ключевой носитель (см. стр.**57** и стр.**58**). При этом укажите следующие значения параметров:

Ключевой носитель-источник	Идентификатор администратора комплекса, созданный при инициализации ЦУС
IP-адрес объекта	Внутренний IP-адрес ЦУС
Пароль для расшифровки ключей	Пароль, указанный при инициализации ЦУС для защиты идентификатора администратора комплекса

5. Запустите программу управления агентом и настройте параметры агента (см. стр.**60**).

   Для запуска нажмите кнопку "Пуск" и в главном меню Windows выберите "Все программы > Код Безопасности > Континент 3.7 > Программа управления агентом ЦУС и СД".

   Для единого ключевого носителя на USB-флеш-накопителе укажите значение "Съемный диск".
6. Предъявите единый ключевой носитель и запустите агент вручную. Для этого используйте команду "Запустить Агент" контекстного меню пиктограммы агента. Настройте в ПУ ЦУС расписание передачи журналов в базу данных (см. стр.**63**).

Результат

- Установленная и запущенная программа управления ЦУС (ПУ ЦУС).
- Автоматически созданные объекты, отображаемые в ПУ ЦУС:
  - криптографический шлюз "КШ с ЦУС";
  - сетевой объект "Любой";

- сервисы "Любой TCP", "Любой UDP", "Любой ICMP" и другие стандартные сервисы;
- временной интервал "Постоянно";
- класс трафика "Нормальный".

- Функционирующий агент.
- Установленная и настроенная программа просмотра журналов (ППЖ).

Шаг 3. Настройка правил фильтрации и трансляции

- Для каждого правила фильтрации и трансляции:
  - Создайте сетевые объекты, необходимые для формирования правил (см. стр.**77**).
  - При необходимости создайте нужные сервисы (см. стр.**79**).
  - Сформируйте правила фильтрации и трансляции для прохождения разрешенного трафика (см. стр.**82**).

  Примеры таких правил см. стр.**90**.

Результат

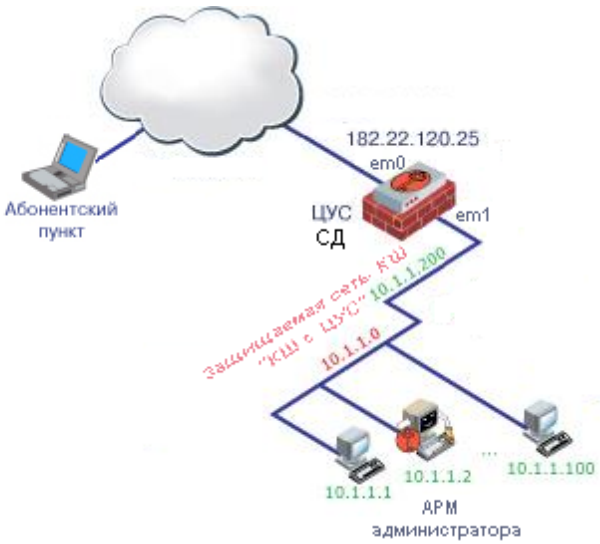
- Правила фильтрации и трансляции для прохождения разрешенного трафика.

Результат

- Наличие трафика между указанными сетевыми объектами.

Удаленный доступ сотрудников к корпоративным ресурсам

На рисунке представлен пример организации действующих локальных сетей до и после подключения КШ:



Исходные данные

Для выполнения работ необходимо наличие следующих сведений:

Данные	Описание	Примечание
Имя внешнего интерфейса ЦУС	Имя интерфейса ЦУС, подключаемого к внешней сети	См. стр.**8**. На рисунке em0
Внешний IP-адрес ЦУС	IP-адрес внешнего интерфейса ЦУС	Необходимо получить у провайдера. На рисунке 182.22.120.25
Маска внешней сети ЦУС	Маска внешней сети, к которой подключен ЦУС	Необходимо получить у провайдера. На рисунке 255.255.255.0
IP-адрес маршрутизатора по умолчанию для ЦУС	IP-адрес маршрутизатора по умолчанию для ЦУС	Необходимо получить у провайдера. Например, 182.22.120.1
Имя внутреннего интерфейса ЦУС	Имя интерфейса ЦУС, подключаемого к защищаемой сети. К этой сети должен быть подключен АРМ администратора	См. стр.**8**. На рисунке em1
Внутренний IP-адрес ЦУС	IP-адрес внутреннего интерфейса ЦУС	На рисунке 10.1.1.200
Маска защищаемой сети ЦУС	Маска защищаемой сети, к которой подключен ЦУС	На рисунке 255.255.255.0
Тип и сетевое имя сервера БД	Тип и сетевое имя сервера баз данных, используемого для организации хранения регистрационных журналов	Определяется при развертывании СУБД на стадии подготовки к вводу комплекса в эксплуатацию
Имя пользователя и пароль администратора СУБД	Под этой учетной записью будет осуществляться обращение к СУБД при установке подсистемы управления	Определяется при развертывании СУБД на стадии подготовки к вводу комплекса в эксплуатацию
Имя пользователя и пароль для подключения агента	Под этой учетной записью будет осуществляться обращение агента к СУБД после его установки и запуска	Эту учетную запись можно создать в процессе установки подсистемы управления комплексом

Данные	Описание	Примечание
Имя пользователя и пароль для просмотра журналов	Под этой учетной записью будет предоставляться доступ к регистрационным журналам, хранящимся в базе данных, из программы просмотра журналов	Эту учетную запись можно создать в процессе установки подсистемы управления комплексом
Серийный номер лицензии на право использования ЦУС	Строка символов, определяющая ограничения на параметры ЦУС	Из комплекта поставки
Серийный номер лицензии на право использования СД	Строка символов, определяющая ограничения на параметры СД	Из комплекта поставки
Характеристики сертификата ЦС	Название сертификата; название организации и подразделения, выдающих корневой сертификат; срок действия сертификата	
Характеристики сертификата сервера доступа	Имя сервера доступа; название организации и подразделения, отвечающего за эксплуатацию сервера доступа; срок действия сертификата	
Регистрационные данные удаленного пользователя	Имя сотрудника и адрес его электронной почты; название организации и подразделения, где сотрудник работает	
Правила фильтрации	Правила, определяющие прохождение трафика в КИС	Примеры см. стр.**102**

Организация удаленного доступа

Ввод комплекса в эксплуатацию выполняют в следующем порядке:

1. Подключение ЦУС и СД.
2. Установка подсистемы управления.
3. Издание сертификатов.
4. Определение пула адресов для АП.
5. Настройка правил фильтрации СД.
6. Регистрация удаленного пользователя.
7. Установка и настройка АП.
8. Установка соединения АП с СД.

Шаг 1. Подключение ЦУС и СД

1. Получите у провайдера два IP- адреса: один для ЦУС и один для маршрутизатора по умолчанию.

   Примечание. На приведенном выше рисунке это IP-адрес 182.22.120.25 для ЦУС и IP-адрес 182.22.120.1 для маршрутизатора по умолчанию.

2. Выполните инициализацию ЦУС и СД (см. стр. **37** и стр. **43**). При инициализации ЦУС укажите следующие значения параметров:

Имя внешнего интерфейса	Имя внешнего интерфейса ЦУС
Внешний IP-адрес шлюза	Внешний IP-адрес ЦУС
Маска сети внешнего IP-адреса	Маска внешней сети ЦУС
Имя внутреннего интерфейса	Имя внутреннего интерфейса ЦУС
Внутренний IP-адрес шлюза	Внутренний IP-адрес ЦУС
Маска сети внутреннего IP-адреса	Маска защищаемой сети ЦУС

Адрес маршрутизатора по умолчанию	IP-адрес маршрутизатора по умолчанию для ЦУС
Носитель для инициализации	ПАК "Соболь"

3. Подключите ЦУС к сетевым коммуникациям, как указано на рисунке выше.

Результат

- Функционирующий ЦУС и СД.
- Идентификатор и пароль администратора комплекса на USB Flash-накопителе.
- Идентификатор и пароль администратора сервера доступа на USB Flash-накопителе.

Шаг 2. Установка подсистемы управления

1. Выполните установку и запуск подсистемы управления на АРМ администратора комплекса (см. стр.**46**).

   При запуске ПУ ЦУС (см. стр.**48**) выполните следующие действия:

   - Предъявите идентификатор администратора комплекса, созданный при инициализации ЦУС.
   - Заполните поля диалога "Параметры настройки ЦУС":

IP-адрес	Внутренний IP-адрес ЦУС
Время ожидания соединения, сек.	Значение по умолчанию
Считыватель ключей	Для идентификатора администратора комплекса, созданного при инициализации ЦУС на USB Flash-накопителе, — значение "Съемный диск"

   - Введите пароль для расшифровывания ключа администратора, указанный при инициализации ЦУС.
   - Укажите серийный номер лицензии на право использования ЦУС.

   При запуске ПУ СД (см. стр.**49**) предъявите идентификатор администратора сервера доступа, созданный при инициализации сервера доступа, и введите пароль для его расшифровывания. В ПУ СД укажите серийный номер лицензии на право использования сервера доступа (см. стр.**95**).
2. Установите агент на сервер БД (см. стр.**46**).
3. Сконфигурируйте базу данных журналов. Для этого используйте Конфигуратор БД журналов ЦУС и СД (см. стр.**54**).

   При подключении к базе данных укажите следующие значения параметров (см. стр.**55**):

Тип базы данных	Тип сервера БД
Имя сервера	Сетевое имя сервера БД
Учетная запись сервера базы данных	Имя пользователя и пароль администратора СУБД

   При создании новой базы данных укажите произвольное имя (например Continent).

   Укажите имя пользователя (например ContinentAgent) и пароль для подключения агента (см. стр.**56**).

   Укажите имя пользователя (например ContinentReader) и пароль для просмотра журналов (см. стр.**56**).

4. Запустите программу создания ключевого носителя и создайте единый ключевой носитель (см. стр.**57** и стр.**58**). При этом укажите следующие значения параметров:
   - для идентификатора администратора комплекса, созданного при инициализации ЦУС:

IP-адрес объекта	Внутренний IP-адрес ЦУС
Пароль для расшифровывания ключей	Пароль, указанный при инициализации ЦУС для защиты идентификатора администратора комплекса

   - для идентификатора администратора сервера доступа, созданного при инициализации сервера доступа:

IP-адрес объекта	Внешний IP-адрес ЦУС
Пароль для расшифровывания ключей	Пароль, указанный при инициализации сервера доступа для защиты идентификатора администратора сервера доступа

5. Запустите программу управления агентом и настройте параметры агента (см. стр.**60**).

   Для запуска нажмите кнопку "Пуск" и в главном меню Windows выберите "Все программы > Код Безопасности > Континент 3.7 > Программа управления агентом ЦУС и СД".

   Для единого ключевого носителя на USB Flash-накопителе укажите значение "Съемный диск".
6. Предъявите единый ключевой носитель и запустите агент вручную. Для этого используйте команду "Запустить Агент" контекстного меню пиктограммы агента. Настройте в ПУ ЦУС расписание передачи журналов в базу данных (см. стр.**63**).

Результат

- Установленная и запущенная программа управления ЦУС (ПУ ЦУС).
- Автоматически созданные объекты, отображаемые в ПУ ЦУС:
  - криптографический шлюз "КШ с ЦУС";
  - сетевой объект "Любой";
  - сервисы "Любой TCP", "Любой UDP", "Любой ICMP" и другие стандартные сервисы;
  - временной интервал "Постоянно";
  - класс трафика "Нормальный".
- Установленная и запущенная программа управления СД (ПУ СД).
- Функционирующий агент.
- Установленная и настроенная программа просмотра журналов (ППЖ).

Шаг 3. Издание сертификатов

1. Издайте средствами ПУ СД корневой сертификат (см. стр.**115**). При издании сертификата используйте криптопровайдер "Код Безопасности CSP".
2. Издайте средствами ПУ СД сертификат сервера доступа (см. стр.**116**).

Результат

- USB Flash-накопитель с ключами центра сертификации.
- Ключи и сертификат сервера доступа в базе данных СД.

Шаг 4. Определение пула адресов для АП

- Определите пул адресов для АП (см. стр.**96**). Для этого необходимо указать начальный адрес диапазона, из которого будут выдаваться адреса, и маску.

Маска определяет количество адресов в диапазоне. Первый адрес из диапазона назначается серверу доступа

Например, 5.5.5.1 255.255.255.248. Данный диапазон содержит адреса для шести хостов.

Результат

- Пул адресов для АП.

Шаг 5. Настройка правил фильтрации СД

- Создайте правила фильтрации для доступа пользователя к корпоративным ресурсам. Значения параметров таких правил см. стр. **102**. Процедуру создания правил фильтрации см. стр. **98**.

Результат

- Правила фильтрации для доступа пользователя к корпоративным ресурсам.

Шаг 6. Регистрация удаленного пользователя

1. Зарегистрируйте пользователя в ПУ СД. Используйте вариант регистрации пользователя с изданием сертификата (см. стр. **106**). Способ ввода регистрационной информации — вручную. При издании сертификата используйте криптопровайдер "Код Безопасности CSP".
2. Предоставьте пользователю права доступа. Для этого сформируйте индивидуальный список правил фильтрации (см. стр. **110**).

Результат

- Объект "Пользователь" с предоставленными правами, отображаемый в ПУ СД.
- USB Flash-накопитель с ключами пользователя и сертификатами пользователя и ЦС. Контейнер с ключами пользователя защищен паролем.

Шаг 7. Установка и настройка АП

1. Выполните установку АП на удаленную рабочую станцию (см. стр. **50**). При этом укажите следующие значения параметров:
   - Диалог "Выбор компонентов":

Абонентский пункт	Да
Межсетевой экран	Нет

   - Диалог "Конфигурация АП и МСЭ" (выбор способа начального конфигурирования...):

Использовать настройки по умолчанию	Выбрать

   - Диалог " Конфигурация АП и МСЭ" (параметры программного обеспечения...):

IP-адрес сервера доступа	Внешний IP-адрес ЦУС

   Для корректной работы абонентского пункта перезагрузите компьютер.
2. Зарегистрируйте сертификаты на АП (см. стр. **124**). Для этого используйте USB Flash-накопитель с ключами пользователя и сертификатами пользователя и ЦС (см. Шаг 6).
3. Проверьте параметры сетевого подключения (см. стр. **119**).

Результат

- Функционирующий и настроенный АП.

Шаг 8. Установка соединения АП с сервером доступа

- Установите соединение с сервером доступа (см. стр. **127**). Перед подключением к серверу доступа подсоедините к считывателю USB Flash-

накопитель с ключами пользователя и сертификатами пользователя и ЦС (см. Шаг 6).

Результат

- Соединение АП с сервером доступа.

Результат

- Доступ с абонентского пункта к ресурсам сети, защищаемым ЦУС.

Локальное управление: инициализация сетевого устройства

ЦУС является программным обеспечением, установленным на одном из КШ комплекса. Локальное управление такого КШ имеет некоторые отличия.

Сервер доступа является программным обеспечением, устанавливаемым на КШ, и его наличие зависит от условий поставки.

Инициализация и подключение ЦУС

При инициализации ЦУС выполняют следующие операции:

- подготовка к инициализации;
- настройка сетевых интерфейсов данного КШ;
- загрузка исходной ключевой информации;
- создание идентификатора администратора комплекса;
- настройка дополнительных параметров;
- подключение к сетевым коммуникациям.

В качестве источника исходной ключевой информации может быть использован ПАК "Соболь" или ключевой блокнот РДП-006.

В качестве идентификатора администратора комплекса при инициализации ЦУС могут использоваться устройства типа USB-флеш-накопитель.

При настройке интерфейсов указывают подключаемые к ним сети. Запомните или запишите, какой интерфейс к какой сети необходимо подключить.

Для инициализации ЦУС:

1. Выключите питание КШ. Подключите к системному блоку КШ клавиатуру и монитор.
2. Включите питание КШ и войдите в меню установки BIOS (BIOS Setup).

   Примечание. Способ входа в меню установки BIOS отображается на экране на начальной стадии загрузки компьютера. Как правило, для входа в меню используют клавиши <F2>, <F10>, <Del> или <Alt + S>.

3. Установите в BIOS Setup системное время в соответствии с текущей датой и текущим временем по Гринвичу.

   Пример. Для Москвы текущее время нужно уменьшить на три часа.

4. Закройте меню настройки BIOS с сохранением внесенных изменений.

   Компьютер перезагрузится, и на экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.

   Не дожидаясь автоматической загрузки КШ, аккуратно приложите персональный идентификатор администратора к считывателю.

   Если в течение определенного промежутка времени идентификатор не предъявлен, КШ автоматически продолжит загрузку текущей конфигурации. Время ожидания устанавливает администратор при настройке параметров ПАК "Соболь".

   После успешного считывания информации из идентификатора на экране появится запрос пароля.

5. Введите пароль администратора и нажмите клавишу <Enter>.

   На экране появится меню администратора, подобное изображенному ниже (для ПАК "Соболь" вер. 3.0).

Примечание. Все сведения, необходимые администратору для управления работой ПАК "Соболь", содержатся в документе "ПАК "Соболь". Руководство администратора" из комплекта поставки КШ.

В штатном режиме работы КШ загрузка ОС с отчуждаемого носителя для всех пользователей должна быть запрещена. Убедитесь, что режим "Запрет загрузки с внешних носителей" включен для всех пользователей.

6. Выберите с помощью клавиш со стрелками в меню администратора команду "Загрузка операционной системы" и нажмите клавишу <Enter>.

   Дождитесь появления на экране сообщения с пронумерованным списком интерфейсов данного криптографического шлюза, подобного следующему:

```
Криптографический шлюз "Континент"
Конфигурация: ЦУС
Начальная конфигурация ЦУС.
Обнаруженные интерфейсы:
Номер  Имя
1.     em0
2.     em1
3.     em2
4.     tun0
Укажите номер внешнего интерфейса:
```

Примечание. Имена интерфейсов, отображаемые на экране в строке сообщений, соответствуют именам, указанным на корпусе КШ рядом с соответствующим разъемом (кроме tun). Интерфейс tun предназначен для настройки подключения к внешним сетям по протоколу PPPoE.

7. Введите номер, соответствующий внешнему интерфейсу. Например, если к внешней сети подсоединен интерфейс с именем "em0", введите в командной строке "1". Нажмите клавишу <Enter>.

   На экране появится запрос:

```
Введите внешний IP адрес шлюза:
```

8. Введите внешний IP-адрес данного КШ. По этому адресу будут поступать IP-пакеты от внешних и сторонних абонентов. Адрес вводится в формате IPv4 или IPv6 с указанием префикса. Например, 192.0.2.5/24 (для IPv4) или 2345:02BD::5/48 (для IPv6). Нажмите клавишу <Enter>.

   На экране появится запрос:

9. Если допущена ошибка, введите "n" и нажмите клавишу <Enter>. Повторите ввод характеристик внешнего интерфейса.

   Если запись верна, введите "y" и нажмите клавишу <Enter>.

Модемное подключение. Если в п. 7 был указан интерфейс tun, то на экране появится сообщение "Настройка PPPoE" и перечень доступных интерфейсов. Укажите последовательно следующие параметры PPPoE:

- название интерфейса, через который осуществляется подключение;
- имя сервиса;
- имя пользователя;
- пароль.

После определения каждого параметра нажимайте клавишу <Enter>.

На экране появится пронумерованный список внутренних интерфейсов данного криптографического шлюза:

```
  Обнаруженные интерфейсы:
  Номер  Имя
  2.     em1
  3.     em2
Укажите номер внутреннего интерфейса.
Если их несколько — того, к которому подключается АРМ
администратора:
```

10. Введите номер соответствующего интерфейса из списка, представленного на экране. Например, если к локальной сети, в которой находится АРМ администратора, подсоединен интерфейс с именем "em1", введите "2". Если АРМ администратора находится в сети, к которой подсоединен внешний интерфейс (в случае размещения ЦУС в защищенной сети), укажите любой номер из списка. Нажмите клавишу <Enter>.

На экране появится запрос:

```
Введите внутренний IP адрес шлюза:
```

11. Введите IP-адрес данного интерфейса в локальной сети. Адрес вводится с указанием маски (префикса). Например, "10.1.1.200/29". Нажмите клавишу <Enter>.

Примечание. Внутреннему интерфейсу необходимо назначить IP-адрес, даже если подключение защищаемых сетей к этому интерфейсу не предполагается. IP-адрес должен быть уникальным для данной корпоративной сети.

На экране появится сообщение, подобное следующему:

```
Продолжить (y/n)?
```

12. Если допущена ошибка, введите "n" и нажмите клавишу <Enter>. Повторите ввод характеристик внутреннего интерфейса. Если запись верна, введите "y" и нажмите клавишу <Enter>.

После того как параметры интерфейсов определены, на экране появится запрос:

```
Введите адрес маршрутизатора по умолчанию:
```

13. Введите IP-адрес маршрутизатора по умолчанию. Этот маршрутизатор и регистрируемый КШ должны находиться в одной подсети, заданной указанными ранее IP-адресом и маской внешнего интерфейса КШ. Например, "192.0.2.1". Нажмите клавишу <Enter>.

На экране появится сообщение, подобное следующему:

```
Адрес маршрутизатора 192.0.2.1
Продолжить (y/n)?
```

14. Если допущена ошибка, введите "n" и нажмите клавишу <Enter>. Повторите ввод адреса маршрутизатора. Если запись верна, введите "y" и нажмите клавишу <Enter>.

ЦУС сохранит информацию о конфигурации в базе данных, после чего на экране появится сообщение:

```
Использовать внешний носитель для инициализации? (Y/N)
```

15. Выполните одно из следующих действий:

- при использовании в качестве источника исходной ключевой информации ПАК "Соболь" введите "n" и нажмите клавишу <Enter>. Перейдите к п.17;
- при использовании ключевого блокнота РДП-006 введите "y" и нажмите клавишу <Enter>. На экране появится сообщение:

```
Вставьте носитель с исходной ключевой информацией и
нажмите Enter
```

16. Предъявите носитель с исходной ключевой информацией и нажмите клавишу <Enter>.

    Исходный ключевой материал будет загружен в ЦУС. По окончании данной операции на экране появится сообщение:

```
Загружена ключевая информация с носителя <наименование
ключевого блокнота>
Введите пароль административного ключа
```

17. Введите пароль и нажмите клавишу <Enter>.

> **Примечание.** Длина и сложность пароля должны соответствовать политике аутентификации администраторов. По умолчанию длина пароля – не менее 4 символов. Разрешено использование любых символов, кроме кириллицы.

Внимание! Запомните пароль. Этот пароль будет использован для шифрования административного ключа и в дальнейшем понадобится для запуска программы управления ЦУС.

На экране появится сообщение:

```
Повторите пароль
```

18. Введите пароль повторно и нажмите клавишу <Enter>.

    На экране появится сообщение:

```
Вставьте носитель для записи административного ключа и
нажмите Enter
```

19. Предъявите чистый носитель и нажмите клавишу <Enter>.

    Дождитесь сообщения о завершении процедуры конфигурирования и появления главного меню:

    Пункт меню "Тестирование" предназначен для выполнения аппаратных тестов сетевого устройства до начала инициализации. Описание тестов см. на стр.**130**.

20. Для завершения процедуры инициализации ЦУС введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

    Если в течение 5 секунд после появления последнего сообщения клавиша <Enter> нажата не будет, ЦУС автоматически завершит процедуру инициализации.

    После завершения инициализации на экране появится сообщение:

```
Успешный запуск <Дата, Время>
```

> **Примечание.** Носитель, содержащий административный ключ, является идентификатором администратора комплекса. Он необходим для запуска программы управления.

21. Извлеките носитель из считывающего устройства.

    Загрузка ЦУС осуществится автоматически. С этого момента ЦУС готов к работе.

> **Примечание.** В случае каких-либо нарушений в процедуре инициализации ЦУС повторите процедуру инициализации.

22. Подключите интерфейсы КШ к сетевым коммуникациям в соответствии с настройкой. Имена интерфейсов указаны на корпусе КШ рядом с соответствующим разъемом.

Инициализация и подключение сетевого устройства

При инициализации сетевого устройства выполняют следующие операции:

- загрузка конфигурации сетевого устройства;
- загрузка ключей;
- настройка дополнительных параметров;
- подключение к сетевым коммуникациям.

Конфигурация сетевого устройства может считываться с носителей типа USB-флеш-накопитель.

Для инициализации сетевого устройства:

1. Выключите питание сетевого устройства. Подключите к системному блоку сетевого устройства клавиатуру и монитор.

   Примечание. Если конфигурация сетевого устройства записана на USB-флеш-накопителе, подсоедините его к разъему USB-порта.

2. Включите питание сетевого устройства. На экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.

   Не дожидаясь автоматической загрузки сетевого устройства, аккуратно приложите персональный идентификатор администратора к считывателю.

   Если в течение определенного промежутка времени идентификатор не предъявлен, сетевое устройство автоматически продолжит загрузку текущей конфигурации. Время ожидания устанавливает администратор при настройке параметров ПАК "Соболь".

   После успешного считывания информации из идентификатора на экране появится запрос пароля.

3. Введите пароль администратора и нажмите клавишу <Enter>.

   На экране появится меню администратора, подобное изображенному ниже (для ПАК "Соболь" вер. 3.0).

   Примечание. Все сведения, необходимые администратору для управления работой ПАК "Соболь", содержатся в документе "ПАК "Соболь". Руководство администратора" из комплекта поставки сетевого устройства.

   В штатном режиме работы сетевого устройства загрузка ОС с отчуждаемого носителя для всех пользователей должна быть запрещена. Убедитесь, что режим "Запрет загрузки с внешних носителей" включен для всех пользователей.

4. Выберите с помощью клавиш со стрелками в меню администратора команду "Загрузка операционной системы" и нажмите клавишу <Enter>.

   Дождитесь появления на экране следующего сообщения:

```
Вставьте носитель с конфигурацией и нажмите Enter
```

5. Предъявите носитель с конфигурационной информацией, сохраненной после регистрации сетевого устройства в базе данных ЦУС (см. [**1**]). Нажмите клавишу <Enter>.

   Если носитель не предъявлен, на нем отсутствуют нужные файлы или файлы повреждены, на экране появится сообщение об ошибке и предложение повторить инициализацию.

   При успешном чтении информации с носителя на экране появится сообщение:

   ```
   Введите пароль
   ```

6. Введите пароль, заданный при записи конфигурации на носитель, и нажмите клавишу <Enter>.

   На экране появится меню загрузки ключей.

   ```
   1: Загрузить активный ключ
   2: Загрузить резервный ключ
   0: Отмена
   Выберите вариант загрузки ключа:
   ```

7. Если загрузка ключей не требуется, введите номер пункта "Отмена" и нажмите клавишу <Enter>.

   На экране появится главное меню. Перейдите к п. 13.

   Если выполняется первичная инициализация, введите номер пункта "Загрузить активный ключ" и нажмите клавишу <Enter>.

   Если ранее инициализация этого сетевого устройства уже проводилась и на сетевом устройстве загружены ключи, то на экране появится следующее сообщение:

   ```
   Уже имеются ключи, установленные на устройстве.
   Осуществить замену ключей? (y/n)
   ```

8. Если замена ключей не требуется, введите "n" и нажмите клавишу <Enter>. На экране появится главное меню. Перейдите к выполнению п. 13.

   Если требуется замена ключей, введите "y" и нажмите клавишу <Enter>. На экране появится сообщение:

   ```
   Вставьте носитель с ключами и нажмите Enter
   ```

9. Вставьте носитель с ключами и нажмите клавишу <Enter>.

   На экране появится список обнаруженных на носителе комплектов ключей.

   Примечание. Если на предъявленном носителе хранятся ключи, записанные средствами ПУ ЦУС для базовой схемы распределения ключей, список будет представлен одним комплектом, содержащим один ключ. Комплекты используются для трехлетней схемы хранения ключей (подробнее о схемах хранения ключей и управлении ключами см. [**1**], [**9**]).

10. Введите номер пункта, соответствующий нужному комплекту ключей, и нажмите клавишу <Enter>.

    На экране появится список ключей выбранного комплекта.

11. Введите номер пункта, соответствующий нужному ключу, и нажмите клавишу <Enter>.

    На экране появится запрос ввода пароля.

12. Введите пароль и нажмите клавишу <Enter>.

    При правильном вводе пароля выполняется автоматическая настройка конфигурации сетевого устройства и на экране появится главное меню:

```
1: Выключить
2: Перезагрузить
3: Управление
4: Настройки безопасности
5: Настройка ДА <функция недоступна>
6: Настройка СД <функция недоступна>
7: Тестирование
0: Выход
Выберите пункт меню (0-7):
```

Примечание. Если пароль указан неверно, операция загрузки ключей будет отменена. Загрузку ключей можно повторить, используя дополнительное меню "Настройки безопасности" (см. [2]).

Пункт меню "Тестирование" предназначен для выполнения аппаратных тестов сетевого устройства до начала инициализации. Описание тестов см. на стр.**130**.

13. Для завершения процедуры инициализации сетевого устройства введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

Если в течение 5 секунд после появления последнего сообщения клавиша <Enter> нажата не будет, сетевое устройство автоматически завершит процедуру инициализации.

После завершения процедуры инициализации на экране появится сообщение:

```
Успешный запуск <Дата, Время>
```

14. Извлеките носитель из считывающего устройства.

Загрузка сетевого устройства осуществится автоматически. С этого момента сетевое устройство готово к работе.

Примечание. В случае каких-либо нарушений в процедуре инициализации сетевого устройства повторите процедуру инициализации.

15. Подключите интерфейсы сетевого устройства к сетевым коммуникациям в соответствии с настройкой. Имена интерфейсов указаны на корпусе сетевого устройства рядом с соответствующим разъемом.

Внимание! Чтобы ЦУС установил соединение с инициализированным сетевым устройством, в программе управления ЦУС в диалоге "Свойства сетевого устройства" на вкладке "Общие сведения" установите отметку в поле выключателя "Введен в эксплуатацию".

Инициализация сервера доступа

Программное обеспечение сервера доступа устанавливается на криптографическом шлюзе вместе с установкой программного обеспечения ЦУС или КШ.

При первичной инициализации сервера доступа создается идентификатор администратора сервера. В качестве идентификатора могут использоваться USB-флеш-накопители.

Для инициализации сервера доступа:

1. Выполните шаги **1– 12** процедуры первичной инициализации криптографического шлюза (см. стр. **41**) или шаги **1– 20** процедуры первичной инициализации ЦУС (см. стр.**37**).

Дождитесь появления на экране главного меню:

```
1: Выключить
2: Перезагрузить
3: Управление
4: Настройки безопасности
5: Настройка СД
6: Тестирование
0: Выход
Выберите пункт меню (0-6):
```

Пункт меню "Тестирование" предназначен для выполнения аппаратных тестов сетевого устройства до начала инициализации. Описание тестов см. стр.**130**.

2. В главном меню введите в строке ввода номер команды "Настройка СД" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Начальная конфигурация СД (версия <номер версии>)
   Введите пароль ключа администратора СД
   ```

3. Введите пароль и нажмите клавишу <Enter>.

   Примечание. Длина пароля – не менее 8 символов. Разрешено использование любых символов, кроме кириллицы.

   Внимание! Запомните пароль. Этот пароль будет использован для шифрования административного ключа и в дальнейшем понадобится для запуска программы управления сервером доступа.

   На экране появится сообщение:

   ```
   Повторите пароль
   ```

4. Введите пароль повторно и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Вставьте носитель для записи ключа ПУ СД и нажмите Enter.
   ```

5. Предъявите носитель для записи ключа.

   Примечание. Это идентификатор администратора сервера доступа. Он необходим для установки соединения программы управления с сервером доступа.

   По окончании создания и записи ключа на носитель на экране появится меню конфигурирования сервера доступа:

   ```
   Конфигурирование Сервера Доступа
   1. Переинициализировать СД
   2. Создать ключевой носитель
   3. Изменить лицензии
   4. Восстановить БД СД
   0. Вернуться в основное меню
   Выберите пункт меню:
   ```

   Процедуры настройки дополнительных параметров см. [**2**].

6. Для завершения конфигурирования сервера введите в строке ввода номер команды "Вернуться в основное меню" и нажмите клавишу <Enter>.

7. Для завершения конфигурирования КШ введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

   Примечание. Если в течение 1 минуты команда меню не выбрана, осуществляется автоматическое завершение процедуры конфигурирования сервера.

   Запуск сервера доступа осуществится автоматически. На экране появится сообщение:

   ```
   Успешный запуск <Дата> <Время>.
   ```

Извлеките носитель из считывающего устройства. С этого момента сервер доступа готов к работе.

Установка подсистемы управления и абонентского пункта

Установка компонентов подсистемы управления

Внимание! Установку и удаление компонентов подсистемы управления может выполнить только пользователь, наделенный правами локального администратора данного компьютера.

Установку компонентов подсистемы управления осуществляют в следующем порядке:

1. Запуск программы установки.
2. Выбор варианта установки.
3. Настройка криптоядра (для программы управления сервером доступа).
4. Проверка выбранных настроек.
5. Копирование файлов.
6. Завершение установки.

Перед запуском программы установки завершите работу всех приложений.

Шаг 1. Запуск программы установки

1. Поместите установочный диск в устройство чтения компакт-дисков.
2. Запустите на исполнение файл \Setup\Continent\RCP\Setup.exe.

   На экране появится диалог со списком дополнительных компонентов, которые должны быть установлены до начала установки подсистемы управления.
3. Нажмите кнопку "OK".

   Начнется установка первого компонента. После завершения его установки на экране появится запрос на установку второго компонента — средства защиты информации "Secret Net 7".

   Внимание! Компонент "Secret Net 7" устанавливается только в том случае, если программное обеспечение комплекса должно удовлетворять требованиям высокого уровня безопасности.
4. Для установки компонента "Secret Net 7" нажмите кнопку "OK", для отмены установки компонента нажмите кнопку "Отмена".

   Если была нажата кнопка "OK", запустится программа установки "Secret Net 7".

   После завершения установки дополнительных компонентов на экране появится стартовый диалог программы установки подсистемы управления.
5. Ознакомьтесь с информацией, содержащейся в стартовом диалоге, и нажмите кнопку "Далее >" для продолжения установки.

   Появится диалог с текстом лицензионного соглашения.
6. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца. Если вы согласны с условиями лицензионного соглашения, подтвердите свое согласие, нажав кнопку "Далее", и перейдите к следующему шагу установки. Если вы не согласны с условиями лицензионного соглашения, откажитесь от продолжения установки, нажав кнопку "Отмена", и подтвердите свой выбор в появившемся на экране диалоге. Установка завершится.

Шаг 2. Выбор варианта установки

На этом шаге программа установки предложит выбрать компоненты программного обеспечения, которые требуется установить на данный компьютер, а также папку установки для программных файлов.

Предусмотрено два варианта установки: типовая и выборочная.

При использовании типового варианта устанавливаются следующие компоненты:

- программа управления ЦУС;
- программа копирования ключей;
- программа просмотра журналов;
- агент ЦУС иСД.

Выборочная установка позволяет выбрать необходимые компоненты из списка.

Примечание. Компоненты "Программа создания ключевого носителя для агента ЦУС и СД" и "Конфигуратор БД журналов ЦУС и СД" устанавливаются автоматически независимо от выбранного варианта установки.

На экране появится диалог "Вид установки".

Для типовой установки:

1. Выберите вариант установки "Типовая" и нажмите кнопку "Далее >".

   На экране появится диалог "Папка назначения" для определения папки установки подсистемы управления.

2. При необходимости измените папку установки подсистемы управления и нажмите кнопку "Далее >".

   Для выбора папки в стандартном диалоге используйте кнопку "Изменить". По умолчанию программа установки копирует файлы на системный диск в папку \Program Files\Код Безопасности\Континент.

Для выборочной установки:

1. Выберите вариант установки "Выборочная" и нажмите кнопку "Далее".

   На экране появится стандартный диалог выбора компонентов программного обеспечения, которые требуется установить на данный компьютер.

2. Отметьте в списке устанавливаемые компоненты.

   Для запрета установки компонента щелкните мышью значок рядом с его названием и в раскрывшемся меню выберите пункт "Данный компонент будет недоступен".

3. При необходимости измените папку установки подсистемы управления. Для этого используйте кнопку "Изменить". По умолчанию программа установки копирует файлы на системный диск в папку \Program Files\Код Безопасности\Континент.

4. Для продолжения установки нажмите кнопку "Далее >".

Шаг 3. Настройка криптоядра "Континент"

Данный диалог появляется на экране только при наличии программы управления сервером доступа (ПУ СД) среди выбранных компонентов.

Для настройки криптоядра:

- Установите отметку в нужном поле и нажмите кнопку "Далее >".

Биологический ДСЧ	При наличии отметки криптопровайдер "Код Безопасности" использует собственный биологический датчик случайных чисел
Физический ДСЧ	При наличии отметки криптопровайдер "Код Безопасности" использует физический датчик случайных чисел ПАК "Соболь"

Шаг 4. Проверка выбранных настроек

На этом шаге перед началом копирования файлов можно проверить и откорректировать выполненные настройки.

Для проверки и корректировки настроек используйте кнопку "< Назад".

Для начала установки программы нажмите кнопку "Установить". Программа установки приступит к копированию файлов на жесткий диск компьютера.

Шаг 5. Копирование файлов

Файлы копируются в папку, выбранную для установки программы (см. Шаг 2). Ход выполнения процесса копирования отображается на экране в специальном окне.

Примечание. Если программа установки в процессе копирования не обнаружит файл, заявленный в комплекте поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. Скопируйте еще раз файлы с дистрибутивного диска и повторите установку. Если это не приведет к желаемому результату, обратитесь к поставщику комплекса.

Шаг 6. Завершение установки

После успешного выполнения предыдущих шагов на экране появится запрос на перезагрузку компьютера. Перезагрузите компьютер.

Внимание! Если в состав установленных компонентов входит программа управления сервером доступа, после перезагрузки компьютера на экране появится сообщение с инструкцией по накоплению энтропии для биологического датчика случайных чисел. Следуя инструкции, нажимайте левой кнопкой мыши на мишень, перемещающуюся по экрану, до завершения процесса накопления энтропии.

После установки компонентов подсистемы управления в меню "Программы" главного меню Windows появится программная группа "Код Безопасности" с группой "Континент 3.7". При полной установке эта группа будет содержать следующие команды:

- программа управления ЦУС (ПУ ЦУС);
- программа управления СД (ПУ СД);
- программа просмотра журналов ЦУС и СД;
- программа просмотра отчетов ЦУС;
- агент ЦУС и СД;
- агент БРП;
- агент Роскомнадзора;
- программа копирования ключей ЦУС.

Запуск подсистемы управления

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

Запуск программы управления ЦУС

Для запуска программы управления:

1. Предъявите идентификатор администратора комплекса.
2. Активируйте команду "Программы > Код Безопасности > Континент 3.7> Программа управления ЦУС (ПУ ЦУС)" в главном меню Windows или ярлык программы управления на рабочем столе.

   На экране появится диалог "Параметры соединения с ЦУС...".
3. Заполните поля этого диалога и нажмите кнопку "ОК" (см. стр.**68**).

   На экране появится запрос пароля для расшифровки ключей администратора.

Примечание. Если идентификатор администратора не предъявлен, на экране появится запрос идентификатора. Предъявите идентификатор. Если носитель испорчен или не содержит административного ключа, на экране появится сообщение об ошибке. Закройте окно сообщения и повторите попытку запуска с надлежащим носителем.

Сообщение об ошибке может содержать техническую информацию для разработчиков. При обращении в службу технической поддержки необходимо представить снимок экрана с сообщением или полный текст сообщения, включая техническую информацию.

4. Введите пароль и нажмите кнопку "ОК".

   Если при установке компонентов подсистемы управления был выбран биологический датчик случайных чисел, на экране появится сообщение с инструкцией по накоплению энтропии. Следуя инструкции, нажимайте левой кнопкой мыши на мишень, перемещающуюся по экрану, до завершения процесса накопления энтропии для датчика случайных чисел.

   При успешном чтении служебной информации с идентификатора на экране появится диалог для регистрации лицензий ЦУС.

5. Зарегистрируйте приобретенные лицензии на работу с ЦУС. Для этого выполните следующие действия:

   - для каждой лицензии укажите в поле ввода серийный номер лицензии и нажмите кнопку "Добавить";

     Примечание. При успешной регистрации лицензии ее серийный номер и краткая характеристика отображаются в списке зарегистрированных лицензий. При ошибке на экране появляется соответствующее сообщение.

   - после регистрации всех лицензий нажмите кнопку "Закрыть".

   Программа управления установит защищенное соединение с ЦУС и на экране появится главное окно программы управления (см. стр.**66**).

   Совет. Если при установке соединения произошел сбой и на экран выведено сообщение о невозможности соединения с ЦУС, проверьте работоспособность ЦУС и повторите попытку соединения с ним еще раз.

Внимание! После запуска программы управления ЦУС при необходимости можно изменить режим управления ключами. По умолчанию при установке ПО комплекса и вводе его в эксплуатацию устанавливается режим, соответствующий базовой схеме управления.

Для изменения режима управления ключами:

1. Активируйте в меню "ЦУС" команду "Свойства".

   Появится диалоговое окно "Свойства ЦУС".

2. В разделе "Режим управления ключевой информацией" выберите нужный режим и нажмите кнопку "ОК".

   Диалоговое окно "Свойства ЦУС" закроется.

Важно! После смены режима управления ключами необходимо выполнить смену ключей. Смену ключей проводят в соответствии с установленным для данной схемы порядком.

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. стр.**43**). Кроме того, необходимо правильно настроить параметры соединения программы с сервером доступа (см.стр.**94**).

Для запуска программы управления:

1. Предъявите идентификатор администратора.

2. Нажмите кнопку "Пуск" ("Start") и активируйте в меню "Программы" команду: / Код Безопасности / Континент 3.7 / Программа Управления СД (ПУ СД).

   На экране появится основное окно программы и запрос 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.

   После того как защищенное соединение с сервером доступа успешно установлено, программа управления загрузит необходимые данные и отобразит в основном окне структуру объектов управления (см. стр.**93**).

   Совет. Если при установке 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.**94**).

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

Запуск агента

В данном разделе представлен общий порядок первого запуска агента. Подробное описание процедур см. в [**3**].

Для запуска агента:

1. Создайте единый ключевой носитель.
2. Сконфигурируйте базу данных журналов. Для этого используйте конфигуратор БД журналов ЦУС и СД.
3. Запустите программу управления агентом. Для этого нажмите кнопку "Пуск" и в главном меню Windows выберите "Все программы > Код Безопасности > Континент 3.7 > Программа управления агентом ЦУС и СД".
4. Настройте параметры агента.
5. Предъявите единый ключевой носитель.
6. Запустите агент вручную. Для этого используйте команду "Запустить агент" контекстного меню пиктограммы агента.

   Примечание. Если носитель испорчен или не содержит ключевой информации, на экране появится всплывающее сообщение об остановке агента. Предъявите надлежащий носитель и повторите запуск.

Установка абонентского пункта и межсетевого экрана

Пакет установки Комплекса содержит следующие компоненты:

- абонентский пункт;
- программа установки ПО Secret Net;
- межсетевой экран.

В состав абонентского пункта входит криптопровайдер "Код Безопасности CSP".

Установка МСЭ без абонентского пункта невозможна.

Внимание! В процессе установки абонентского пункта все работающие сетевые подключения будут автоматически разорваны. Для их восстановления

необходима перезагрузка компьютера. Работа установленных компонентов Комплекса возможна также только после перезагрузки компьютера.

Примечание. Имеется возможность установки программного обеспечения Комплекса из командной строки.

Для установки программного обеспечения:

1. Войдите в систему с правами администратора компьютера.

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

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

   Примечание. Для установки с жесткого диска скопируйте файлы с установочного диска в любой рабочий каталог и запустите на исполнение файл _setup.exe.

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

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

4. Нажмите кнопку "Далее >" для продолжения установки. На экране появится диалог "Лицензионное соглашение".
5. Прочтите лицензионное соглашение и, если вы принимаете его условия, поставьте отметку в поле "Я принимаю условия лицензионного соглашения, и нажмите кнопку "Далее >".

   На экране появится диалог "Компоненты устанавливаемой программы".
6. Выберите компоненты для установки и нажмите кнопку "Далее >".

   На экране появится диалог "Выбор папки установки". По умолчанию программа установки копирует файлы на системный диск в каталог \Program Files\Security Code\.

   Примечание. Для установки программы в другую папку нажмите кнопку "Обзор..." и укажите нужную папку в диалоге, появившемся на экране.

7. Нажмите кнопку "Далее >".

   На экране появится диалог "Конфигурация АП".
8. Выберите нужный вариант конфигурационных настроек и нажмите кнопку "Далее >".

Использовать настройки по умолчанию	В последующих диалогах мастера установки будут отображены значения конфигурационных параметров по умолчанию
Использовать настройки из файла	Файл создается при удалении предыдущей версии с возможностью экспорта настроек или вручную. Для выбора файла в стандартном диалоге Windows используйте кнопку "..." Пример файла конфигурационных настроек приведен в Приложении (см. стр.**133**)

   - Если был выбран вариант "Использовать настройки по умолчанию", на экране появится диалог "Конфигурация АП" с параметрами абонентского пункта. Перейдите к следующему пункту данной процедуры.

- Если был выбран вариант "Использовать настройки из файла", начнется установка программного обеспечения, и после ее завершения появится сообщение "Установка завершена". Перейдите к **п. 12**.

9. Укажите нужные значения параметров и нажмите кнопку "Далее >".

Имя RAS-соединения	Наименование подключения к RAS-серверу (по умолчанию "Континент-АП")
Адрес сервера доступа	IP-адрес или сетевое имя сервера доступа (по умолчанию 0.0.0.0)

На экране появится диалог "Конфигурация АП" с вопросом о вхождении данного компьютера в домен.

Примечание. Если в диалоге "Компоненты устанавливаемой программы" выбран только абонентский пункт, то мастер установки приступит сразу же к копированию файлов на компьютер. Перейдите к выполнению п. **12**.

10. Выберите нужное значение и нажмите кнопку "Далее >".

На экране появится диалог "Конфигурация АП" с параметрами межсетевого экрана.

11. Укажите нужные значения параметров и нажмите кнопку "Установить".

Логин администратора	Логин и пароль для перехода МСЭ к режиму настройки (по умолчанию логин "Администратор", пароль "111111")
Пароль администратора	
Пароль пользователя	Пароль для перехода МСЭ к режиму работы пользователя (по умолчанию "111111")

Программа установки приступит к копированию файлов в указанную папку. Полоса прогресса и сообщения, появляющиеся в диалоге, отображают ход процесса установки.

Примечание. В процессе установки на экране могут появляться сообщения о том, что устанавливаемое программное обеспечение не тестировалось на совместимость с операционной системой. В окне таких сообщений следует нажимать кнопку "Все равно продолжить".
Если по какой-то причине отсутствует какой-либо из файлов, входящих в комплект поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. В этом случае проверьте компьютер на наличие вирусов и повторите установку. Если в дальнейшем данная ошибка будет повторяться, обратитесь к поставщику Комплекса.

По окончании процесса копирования в верхней части диалога появится сообщение "Установка завершена", а кнопка "Далее >" станет активной.

12. Нажмите кнопку "Далее >".

На экране появится заключительное окно мастера установки с запросом на перезагрузку компьютера.

Внимание! Работа установленных компонентов возможна только после перезагрузки компьютера.

13. Выберите вариант перезагрузки компьютера и нажмите кнопку "Готово".

Внимание! Для уровня безопасности "Низкий" после перезагрузки и автоматического запуска абонентского пункта появится диалоговое окно встроенного криптопровайдера "Код Безопасности CSP". В этом диалоге выполняют набор энтропии, необходимой для дальнейшей работы криптопровайдера. Следуйте указаниям, отображаемым в данном диалоге.

После установки абонентского пункта и перезагрузки компьютера:

- в элементе управления Windows "Панель управления \ Сетевые подключения" появится новое сетевое подключение "Континент-АП";
- в меню "Все программы" главного меню Windows появится подменю "Код Безопасности \ Континент- АП ", которое содержит пункты "", "Код Безопасности CSP", "Контроль целостности", "", "Удаление Континент-АП";

- на панели задач Windows появится пиктограмма абонентского пункта (в случае полной установки дополнительно появятся пиктограмма межсетевого экрана и сообщение об ограничении доступа к сети).

Установка из командной строки

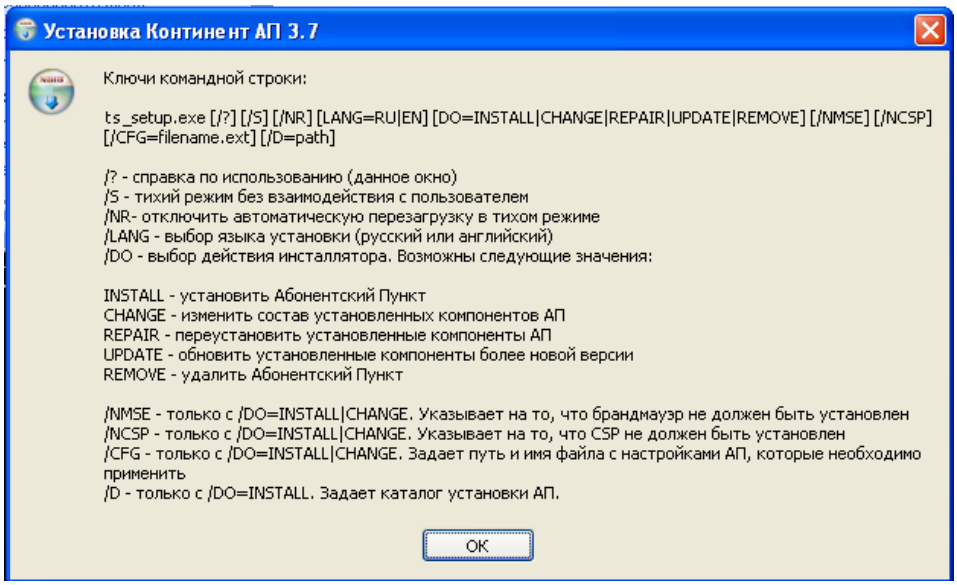
Внимание! Из командной строки можно установить программное обеспечение Комплекса, соответствующее только низкому и среднему уровням безопасности.

Для установки программного обеспечения Комплекса из командной строки используется команда ts_ setup.exe. Формат команды и описание ключей представлены в справочной системе.

Для вызова справочного окна:

- Введите в командной строке "ts_setup.exe /?" (без кавычек).

  На экране появится окно справочной системы с описанием формата и ключей команды.



Предусмотрена возможность выполнить установку в фоновом режиме без взаимодействия с пользователем.

Для задания фонового режима установки:

1. В меню "Пуск" вызовите контекстное меню для пункта "Мой компьютер" и выберите команду "Свойства".

   На экране появится стандартный диалог "Свойства системы".

2. Перейдите на вкладку "Оборудование" и в разделе "Драйверы" нажмите кнопку "Подписывание драйверов".

   На экране появится диалог "Параметры подписывания драйвера".

3. Выберите пункт "Пропускать" и нажмите кнопку "ОК".

Для установки программного обеспечения из командной строки:

- Введите в командной строке:

  ts_setup.exe /S /LANG=RU /DO=INSTALL

  и нажмите клавишу <ENTER>.

  Начнется установка программного обеспечения Комплекса и после ее завершения будет выполнена перезагрузка компьютера. При этом значения настраиваемых параметров устанавливаются по умолчанию.

Конфигурирование базы данных журналов

Агент в соответствии с расписанием сохраняет регистрационные журналы в базе данных. Администраторы комплекса получают доступ к содержимому журналов с помощью программы просмотра журналов.

Конфигуратор предназначен для решения следующих задач:

- настройка параметров подключения агента к СУБД;
- обеспечение доступа администраторов комплекса к БД журналов.

Конфигуратор предоставляет администратору СУБД следующие возможности:

- дистанционно подключиться к серверу СУБД;
- сконфигурировать базу данных для хранения журналов;
- записать сведения, необходимые агенту для подключения к БД, в реестр компьютера.

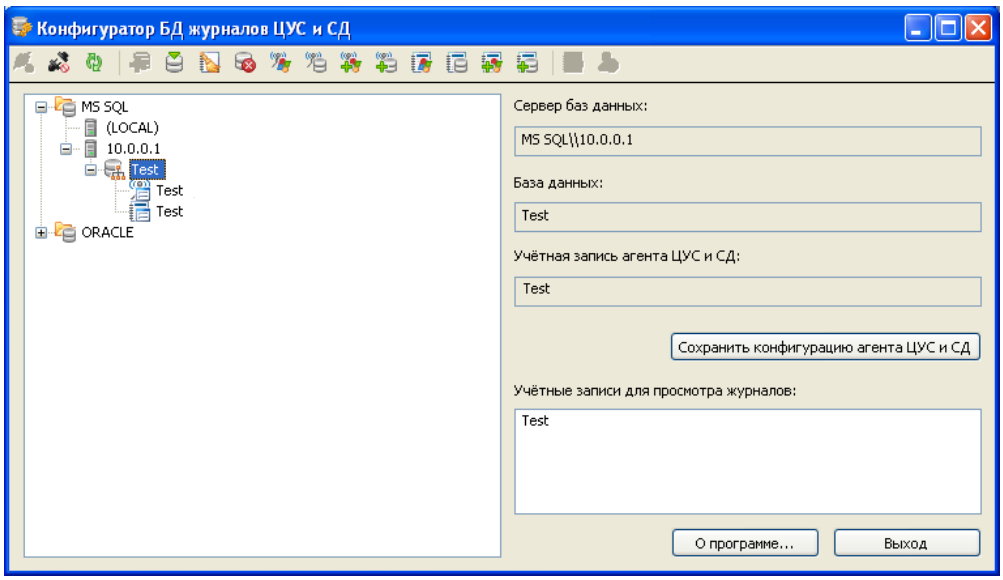
Запуск конфигуратора

Для запуска конфигуратора:

- Нажмите кнопку "Пуск" и выберите в главном меню Windows команду "Программы\ Код Безопасности\ Континент 3.7\ Конфигуратор БД журналов ЦУС и СД".

  На экране появится окно конфигуратора (см. стр.**54**).

Интерфейс конфигуратора



В левой части окна отображается иерархический список объектов. В верхней правой части окна — настройки агента для подключения к СУБД. В нижней правой части окна — перечень учетных записей администраторов комплекса для доступа к БД журналов.

Управление объектами осуществляют с помощью команд контекстного меню и кнопок на панели инструментов (см. таблицу ниже).

Табл.5 Команды управления объектами

Кнопка	Команда	Описание
	Подключиться к серверу СУБД...	Запускает процедуру подключения конфигуратора к серверу БД с правами администратора
	Отключить соединение	Отключает соединение с выбранным сервером БД

Кнопка	Команда	Описание
	Обновить	Обновляет в иерархическом списке отображаемые сведения о выбранном объекте
	Создать базу данных...	Запускает процедуру создания базы данных
	Выбрать	Отображает в правой части окна настройки агента, необходимые для подключения к выбранной в иерархическом списке базе данных
	Очистить журналы ЦУС	Выполняет очистку выбранной базы данных
	Удалить	Удаляет выбранную базу данных
	Назначить учетную запись для агента > Пользователь Windows...	Запускает стандартную процедуру выбора зарегистрированной учетной записи Windows для доступа агента к базе данных
	Назначить учетную запись для агента > Пользователь СУБД...	Запускает процедуру выбора зарегистрированной учетной записи СУБД для доступа агента к базе данных
	Назначить учетную запись для агента > Создать нового пользователя Windows...	Запускает стандартную процедуру создания новой учетной записи Windows для доступа агента к базе данных
	Назначить учетную запись для агента > Создать нового пользователя СУБД...	Запускает процедуру создания новой учетной записи СУБД для доступа агента к базе данных
	Назначить учетную запись для ППЖ > Пользователь Windows...	Запускает стандартную процедуру выбора зарегистрированной учетной записи Windows для доступа пользователя программы просмотра журналов к базе данных
	Назначить учетную запись для ППЖ > Пользователь СУБД...	Запускает процедуру выбора зарегистрированной учетной записи СУБД для доступа пользователя программы просмотра журналов к базе данных
	Назначить учетную запись для ППЖ > Создать нового пользователя Windows...	Запускает стандартную процедуру создания новой учетной записи Windows для доступа пользователя программы просмотра журналов к базе данных
	Назначить учетную запись для ППЖ > Создать нового пользователя СУБД...	Запускает процедуру создания новой учетной записи СУБД для доступа пользователя программы просмотра журналов к базе данных
	Отменить доступ пользователя к журналам ЦУС	Отменяет доступ выбранного пользователя к базе данных без удаления учетной записи
	Удалить пользователя СУБД	Удаляет учетную запись выбранного пользователя из СУБД

Подключение конфигуратора к серверу БД

Для подключения к серверу БД:

1. Вызовите на экран окно конфигуратора (см. стр.**54**).
2. В иерархическом списке объектов выберите нужный объект (см. стр.**54**).
3. Вызовите контекстное меню элемента и активируйте команду "Подключиться к серверу СУБД...".

   На экране появится диалог "Подключение к серверу БД...".
4. Заполните поля диалога и нажмите кнопку "ОК".

Тип базы данных	Тип базы данных (поле не редактируется)

Имя сервера	Сетевое имя сервера БД
Учетная запись текущего пользователя	При наличии отметки подключение к СУБД выполняется под текущей учетной записью Windows
Учетная запись сервера базы данных	При наличии отметки подключение к СУБД выполняется под учетной записью, указанной ниже
Имя пользователя	Имя пользователя, зарегистрированного в СУБД
Пароль	Пароль пользователя, зарегистрированного в СУБД

Настройка параметров подключения агента к СУБД

Для настройки параметров подключения:

1. Вызовите на экран окно конфигуратора (см. стр.**54**).
2. В иерархическом списке объектов выберите нужный сервер БД (см. стр.**54**).
3. С помощью команд контекстного меню и кнопок панели инструментов выполните следующие действия:
   - Выберите/создайте базу данных для хранения журналов.

     Примечание. При создании новой базы данных на диске резервируется 4 ГБ дискового пространства.

   - Выберите/создайте учетную запись, под которой агент будет обращаться к базе данных.

     Внимание! Для доступа агента к базе данных под учетной записью пользователя Windows данный пользователь должен входить в группу локальных администраторов.

     Примечание. При выборе/создании новой учетной записи доступ предыдущей учетной записи к БД автоматически отменяется.

   Описание команд см.в Табл.5.
4. Активируйте в контекстном меню нужной базы данных команду "Выбрать" для отображения в правой части окна настроек агента, необходимых для подключения к этой базе данных.
5. Нажмите кнопку "Сохранить конфигурацию агента ЦУС и СД", расположенную в правой части главного окна конфигуратора.

   На экране появится запрос пароля учетной записи агента.
6. Введите пароль и нажмите кнопку "ОК".

   На экране появится сообщение о сохранении конфигурации.
7. Нажмите кнопку "ОК" для закрытия окна сообщения.

   Сведения, необходимые агенту для подключения к БД, будут внесены в реестр компьютера.

Обеспечение доступа администраторов комплекса к БД журналов

Для обеспечения доступа администраторов комплекса к БД:

1. Вызовите на экран окно конфигуратора (см. стр.**54**).
2. В иерархическом списке объектов выберите нужную базу данных (см. стр.**54**).
3. С помощью команд контекстного меню и кнопок панели инструментов сформируйте перечень учетных записей, под которыми администраторы комплекса будут обращаться к базе данных (см. Табл.5).

Настройка агента

Агент ЦУС и СД обеспечивает:

- установление защищенного соединения с ЦУС для получения содержимого журналов регистрации в соответствии с установленным расписанием;
- установление защищенного соединения с СД для получения содержимого журналов регистрации в соответствии с установленным расписанием;
- очистку журналов регистрации в соответствии с установленным расписанием;
- автоматическое сохранение в зашифрованном виде резервной копии конфигурации ЦУС в соответствии с установленным расписанием.

При настройке агента определяют следующие параметры:

- расписание получения журналов от ЦУС;
- расписание очистки журналов;
- пароль для зашифрования резервной копии конфигурации ЦУС;
- расписание сохранения резервной копии конфигурации ЦУС и папку для архивных копий.

Кроме того, требуется создать единый ключевой носитель (ЕКН) для подключения агента к ЦУС и СД.

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

Управление единым ключевым носителем

Агент забирает журналы с ЦУС и всех СД комплекса. Для подключения к каждому объекту агенту требуется:

- указать сетевой адрес объекта;
- предъявить специальный ключ, индивидуальный для каждого объекта.

Ключи создаются при инициализации объекта и записываются в файле contkey.str на отдельный отчуждаемый носитель – идентификатор администратора.

Единый ключевой носитель содержит ключевую информацию и адреса всех объектов также в файле contkey.str. Для создания и обновления ЕКН используют программу создания ключевого носителя для агента ЦУС и СД.

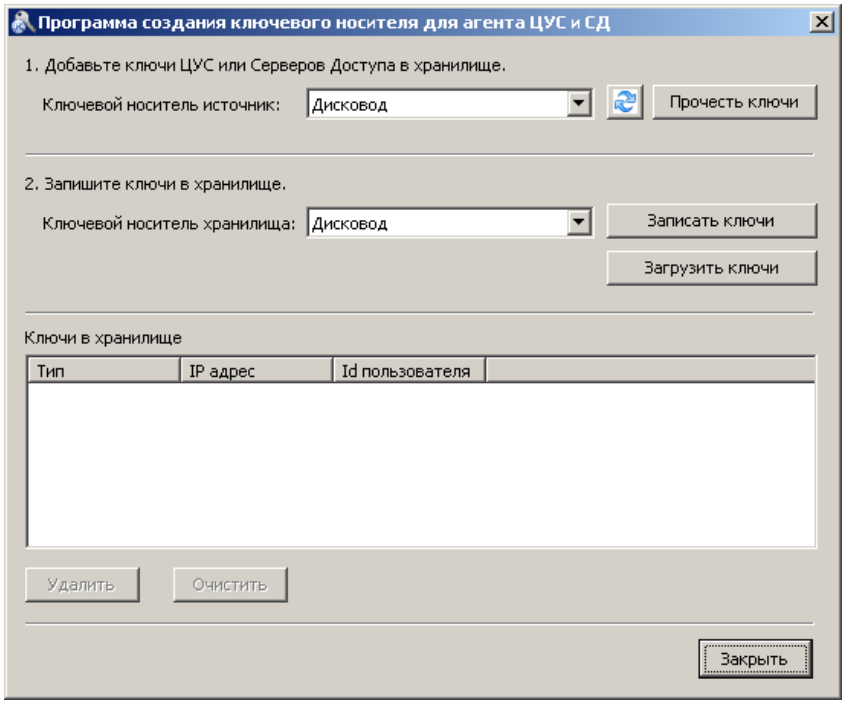
IP-адреса и ключи записываются в специальное хранилище (контейнер). На период работы программы на компьютере создается временное хранилище. Затем это хранилище записывают на носитель. При закрытии программы временное хранилище удаляется.

Запуск программы создания ключевого носителя

Для запуска программы:

1. Выполните одно из следующих действий:
   - Нажмите кнопку "Пуск" на панели задач и в главном меню Windows активируйте команду "Программы (Все программы)/ Код Безопасности/ Континент 3.7/ Программа создания ключевого носителя для агента ЦУС и СД".
   - В программе управления ЦУС активируйте в меню "ЦУС" команду "Создание ключевого носителя агента…".

   На экране появится главное окно программы.



Создание и обновление ЕКН выполняют в данном окне.

Создание единого ключевого носителя

Для создания ЕКН:

1. Вызовите на экран окно программы создания ключевого носителя (см. стр.**57**).
2. Сформируйте содержимое ЕКН. Для каждого объекта выполните следующие действия:
   - Подключите носитель с ключами к считывателю.
   - В поле "Ключевой носитель-источник" укажите нужный считыватель и нажмите кнопку "Прочесть ключи".
   - В появившемся диалоге "Ключи" укажите IP-адрес объекта, пароль для расшифровки ключей и нажмите кнопку "OK".

   В поле "Ключи в хранилище" отобразится новая запись.
3. Сохраните сформированный перечень ключей на ЕКН. Для этого:
   - Подключите ЕКН к считывателю.
   - В поле "Ключевой носитель хранилища" укажите нужный считыватель и нажмите кнопку "Записать ключи".
   - Дождитесь сообщения о завершении создания хранилища и нажмите кнопку "OK".

Локальное управление агентом

Запуск агента

Запуск программы управления агентом осуществляется автоматически при включении и перезагрузке компьютера, на котором агент установлен. Процедура запуска агента при первом включении описана в [**1**].

Внимание! Запуск агента возможен только при предъявлении единого ключевого носителя (ЕКН) и пароля, заданного в настройках агента (см. стр.**60**).

Запуск программы управления агентом на компьютере под управлением ОС Windows Vista и выше необходимо выполнять под учетной записью, наделенной правами локального администратора.

Для автоматического запуска агента:

- Включите питание компьютера, на котором установлен агент, и предъявите ЕКН до окончания загрузки операционной системы.

  При успешном чтении ключевой информации агент будет запущен, а в правом углу панели задач появится пиктограмма "Программы управления агентом", отображающая состояние связи между агентом и ЦУС.

  Примечание. Если носитель испорчен или не содержит административного ключа, на экране появится всплывающее сообщение об ошибке. Предъявите надлежащий носитель и запустите агент вручную.

Если агент был остановлен, запуск агента можно осуществить вручную.

Для запуска агента вручную:

1. Предъявите ЕКН.
2. Вызовите контекстное меню пиктограммы "Программа управления агентом" и активируйте команду "Запустить агент".

   При успешном чтении ключевой информации агент будет запущен.

   Примечание. Если носитель испорчен или не содержит административного ключа, на экране появится всплывающее сообщение об ошибке. Предъявите надлежащий носитель и запустите агент вручную.

Интерфейс агента

После запуска программы управления агентом в правом углу панели задач появляется пиктограмма "Программа управления агентом ЦУС и СД ". Пиктограмма отображает текущее состояние агента, а также наличие события НСД на каком-либо КШ/ДА/КК. Используемые для этой цели пиктографические изображения, а также сведения о командах контекстного меню данной пиктограммы представлены в таблицах ниже.

Оповещение об ошибках в работе агента осуществляется с помощью всплывающих сообщений в правой нижней части экрана. Более подробные сведения об ошибках фиксируются в регистрационном журнале ОС "Просмотр событий> Приложение".

Табл.6 Пиктографические обозначения состояний агента

Пиктограмма	Описание
	Связь между агентом и ЦУС установлена
	Связь между агентом и ЦУС отсутствует
	На одном из устройств зафиксировано событие несанкционированного доступа

Табл.7 Команды контекстного меню программы управления агентом

Название команды	Описание
Запустить агент	Осуществляет запуск агента
Остановить агент	Осуществляет остановку агента
Параметры агента...	Открывает диалог программы управления агентом, предназначенный для просмотра и настройки параметров агента
Отключить уведомления об ошибках	Отключает/включает вывод всплывающих сообщений об ошибках в работе агента

Название команды	Описание
Журнал приложений системы	Вызывает на экран журнал приложений Windows
О программе…	Открывает окно, содержащее сведения о номере версии программы управления агентом, а также сведения об авторских правах на программный продукт
Выход	Осуществляет выход из программы управления агентом и удаляет пиктограмму с панели задач. **Внимание!** При удалении пиктограммы агент не выключается!

Настройка агента

Настройка агента предусматривает:

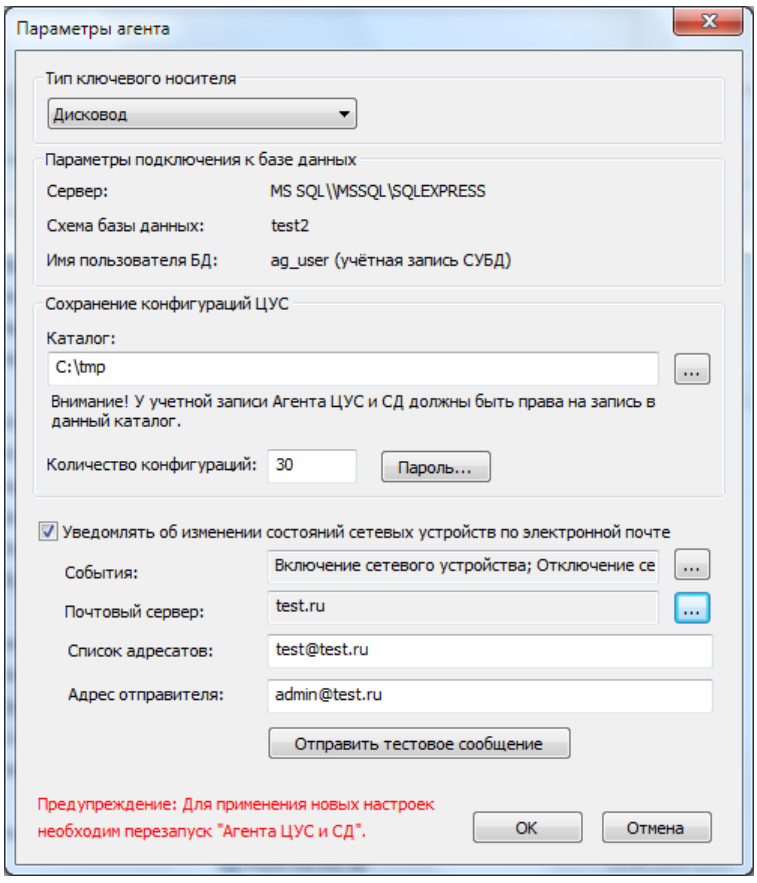
- выбор типа ЕКН;
- просмотр параметров соединения с базой данных для хранения журналов;
- выбор папки архива;
- настройку рассылки уведомлений по электронной почте.

Определение параметров работы агента выполняют в окне настройки.

Вызов окна настройки

Для вызова окна настройки агента:

1. Активируйте команду "Параметры агента…" в контекстном меню пиктограммы агента, расположенной в системной области панели задач. На экране появится диалог для настройки агента.



   Просмотр параметров соединения с базой данных и настройку параметров работы агента выполняют в этом окне.

2. Для сохранения изменений нажмите кнопку "OK".

3. Для применения новых настроек остановите агент и заново вручную запустите его (см.стр.**62** и стр.**58**).

Выбор типа ЕКН

Для выбора типа ЕКН:

- В поле "Тип ключевого носителя" выберите в раскрывающемся списке нужное значение и нажмите кнопку "ОК".

Выбор папки архива

В эту папку агент автоматически сохраняет зашифрованную резервную копию конфигурации ЦУС в соответствии с заданным расписанием. Имя файла резервной копии Save_at_yy_mm_dd_yy-hh_mm.dat. В папке одновременно хранится указанное количество резервных копий. При сохранении очередной копии сверх указанного количества самая старая копия удаляется.

Примечание. По умолчанию это папка %PUBLIC%\Documents\Continent3\<имя_базы_данных>. Имейте в виду, что в MS Windows имя папки Documents может отображаться как Shared documents.

Для выбора папки архива:

- В группе полей "Сохранение конфигураций ЦУС" укажите нужные значения параметров и нажмите кнопку "ОК".

Каталог	Полное имя папки архива. Для выбора папки в стандартном диалоге нажмите кнопку "Обзор..."
Количество конфигураций	Максимальное количество хранимых резервных копий
Пароль	Назначение пароля для зашифрования резервной копии конфигурации ЦУС. Пароль не должен быть простым и его длина должна составлять не менее 8 символов. Этот пароль потребуется для загрузки сохраненных БД

Настройка рассылки

Агент автоматически рассылает уведомления по указанным адресам электронной почты о заданных событиях из следующего списка:

- Включение КШ/ДА/КК;
- Выключение КШ/ДА/КК ;
- Канал WAN стал неработоспособен;
- Канал WAN стал работоспособен;
- Появление НСД;
- Отключение основного КШ/КК кластера;
- Включение основного КШ/КК кластера;
- Изменение состояния ключей КШ/ДА/КК;
- Задание находится в очереди более указанного времени.

Внимание! На почтовом сервере, через который будут рассылаться уведомления, должен быть включен один из следующих типов аутентификации:

- Anonymous access;
- Basic authentication.

Для настройки рассылки:

- Установите отметку в поле "Уведомлять об изменении состояний КШ/ДА/КК по электронной почте", укажите нужные значения параметров и нажмите кнопку "ОК".

События	Перечень событий, требующих уведомлений. Для выбора из списка нажмите кнопку "..." справа от поля. В открывшемся диалоге укажите также период проверки состояния КШ/ДА/КК

Почтовый сервер	Сетевое имя или IP-адрес почтового сервера, через который будут рассылаться уведомления. Для ввода данных нажмите кнопку "..." справа от поля. В открывшемся диалоге укажите имя почтового сервера и, при необходимости, имя и пароль для аутентификации агента на этом сервере
Список адресатов	Список адресов электронной почты получателей уведомлений (через ";")
Адрес отправителя	Произвольный адрес электронной почты для отображения в поле "Отправитель" сообщения с уведомлением

Примечание. Для проверки правильности настроек используйте кнопку "Отправить тестовое сообщение". Тестовое сообщение будет отправлено по указанным адресам.

Остановка агента

Остановку агента можно осуществить:

- из программы управления агентом;
- из консоли "Службы".

Для остановки агента из программы управления агентом:

- Вызовите контекстное меню пиктограммы "Программа управления агентом" и активируйте команду "Остановить агент".

  Агент будет остановлен.

Для остановки агента из консоли "Службы":

1. Нажмите кнопку Пуск, активируйте в главном меню Windows команду "Настройка\ Панель управления" и откройте окно элемента "Администрирование\ Службы".
2. Остановите службу "Агент ЦУС и СД". Для остановки службы выберите в списке нужное название, вызовите контекстное меню и выберите команду "Остановить".

   Агент будет остановлен, а его пиктограмма изменит вид.
3. Закройте окно "Службы".

Управление агентом с помощью программы управления ЦУС

Настройка параметров соединения с агентом

Для настройки параметров соединения с агентом:

1. Активируйте в меню "ЦУС" команду "Параметры соединения с агентом...". На экране появится одноименный диалог.
2. Заполните поля данного диалога и нажмите кнопку "ОК":

IP-адрес	IP-адрес компьютера, на котором установлен агент. Если агент и программа управления установлены на одном и том же компьютере — IP-адрес данного компьютера или 127.0.0.1
Время ожидания соединения, сек.	Время ожидания соединения в секундах (от 10 до 600 сек.)

Программа управления устанавливает соединение с агентом автоматически каждый раз, когда это необходимо, поэтому никакие дополнительные действия после изменения параметров соединения не требуются.

Вызов окна настройки агента

Определение параметров работы агента выполняют в окне настройки.

Внимание! Перед настройкой свойств агента из программы управления убедитесь, что служба "Агент ЦУС и СД" работает. При остановленной службе "Агент ЦУС и СД" настройка агента из программы управления невозможна.

Для вызова окна настройки агента:

- Активируйте в программе управления ЦУС в меню "ЦУС" команду "Настройка агента...".

  На экране появится диалог "Настройка агента ЦУС и СД".

  Настройку параметров работы агента выполняют в этом окне.

Настройка расписания автоматической передачи журналов в базу данных

Передача журналов из буфера ЦУС и буфера СД в базу данных осуществляется агентом одновременно по заданному расписанию.

Примечание. По команде администратора (аудитора) может осуществляться внеочередная передача журналов криптографических шлюзов (см. стр.65).

Для настройки расписания передачи журналов:

1. Вызовите на экран диалоговое окно "Настройка агента ЦУС и СД" (см. стр.62).
2. Перейдите к вкладке "Получение журналов".
3. Выберите тип расписания и определите его параметры:

Периодическое расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется через равные промежутки времени. Продолжительность промежутка задается количеством минут или часов. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране диалоге введите нужные значения. Способы выбора и редактирования значений в этом диалоге аналогичны стандартным способам, принятым в ОС Windows для установки даты и времени
Еженедельное расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется в моменты времени, заданные специальным расписанием. Расписание представлено в виде таблицы, разделенной, для оптимального отображения, на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Для установки отметки поместите указатель в ячейку и нажмите левую кнопку мыши. Повторное нажатие кнопки приводит к удалению отметки. Действие расписания повторяется еженедельно

4. Нажмите кнопку "ОК".

Настройка параметров автоматической очистки журналов в базе данных

В базе данных записи журналов хранятся определенное время до установленного срока устаревания записей. Очистка журналов от устаревших записей осуществляется агентом по заданному расписанию.

Для настройки параметров очистки журналов:

1. Вызовите на экран диалоговое окно "Настройка агента ЦУС и СД" (см. стр.62).
2. Перейдите к вкладке "Очистка журналов".

3. В группе полей "Срок устаревания записей" для каждого журнала укажите срок хранения записей. При автоматической очистке журналов записи, которые хранятся в базе данных менее указанного срока, удалены не будут.
4. Выберите тип расписания и определите его параметры:

Периодическое расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется через равные промежутки времени. Продолжительность промежутка задается количеством минут или часов. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране диалоге введите нужные значения. Способы выбора и редактирования значений в этом диалоге аналогичны стандартным способам, принятым в ОС Windows для установки даты и времени
Еженедельное расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется в моменты времени, заданные специальным расписанием. Расписание представлено в виде таблицы, разделенной, для оптимального отображения, на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Для установки отметки поместите указатель в ячейку и нажмите левую кнопку мыши. Повторное нажатие кнопки приводит к удалению отметки. Действие расписания повторяется еженедельно

5. Нажмите кнопку "ОК".

Настройка расписания автоматического копирования конфигурации ЦУС

Предусмотрена возможность сохранения конфигурации ЦУС в файл. Резервная копия позволяет быстро восстановить работу сети при выходе из строя штатного ЦУС. Агент сохраняет резервную копию конфигурации ЦУС в соответствии с заданным расписанием в папку, которую можно указать средствами локального управления агентом (см. стр. **61**) . По умолчанию это папка %PUBLIC% \Documents\Continent3\<имя_ базы данных>. В папке одновременно хранится указанное количество резервных копий. При сохранении очередной копии сверх указанного количества самая старая копия удаляется.

Для настройки расписания автоматического сохранения:

1. Вызовите на экран диалоговое окно "Настройка агента ЦУС и СД" (см. стр.**62**).
2. Перейдите к вкладке "Сохранение конфигурации ЦУС".
3. Выберите тип расписания и определите его параметры:

Периодическое расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется через равные промежутки времени. Продолжительность промежутка задается количеством минут или часов. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране диалоге введите нужные значения. Способы выбора и редактирования значений в этом диалоге аналогичны стандартным способам, принятым в ОС Windows для установки даты и времени

Еженедельное расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется в моменты времени, заданные специальным расписанием. Расписание представлено в виде таблицы, разделенной, для оптимального отображения, на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Для установки отметки поместите указатель в ячейку и нажмите левую кнопку мыши. Повторное нажатие кнопки приводит к удалению отметки. Действие расписания повторяется еженедельно

4. Нажмите кнопку "ОК".

Агент будет автоматически создавать резервную копию конфигурации ЦУС в соответствии с заданным расписанием.

Внеочередная передача журналов в базу данных

Автоматическая передача регистрационных журналов в базу данных осуществляется агентом в соответствии с заданным расписанием (описание процедуры настройки расписания см.стр.**63**). При необходимости администратор (аудитор) может выполнить внеочередной запуск процесса передачи журналов. Запуск осуществляется в программе управления ЦУС.

Для запуска передачи журналов:

- В главном меню ПУ ЦУС активируйте команду "Объекты > Сбор журналов".

  На экране появится сообщение об отправке команды на исполнение. Через некоторое время, необходимое для передачи журналов в базу данных, полученные записи могут быть загружены в программу просмотра журналов.

ПУ ЦУС: централизованное управление сетевыми устройствами

Интерфейс программы

Главное окно

После того как соединение программы управления с ЦУС успешно установлено и необходимые данные из базы данных ЦУС загружены, на экране появится главное окно программы управления.

В главном окне отображаются характеристики зарегистрированных объектов, а также сведения об их текущем состоянии.

Для выбора отображаемой в главном окне информации предназначено окно объектов. По умолчанию окно объектов расположено в левой части главного окна. В окне объектов отображаются папки объектов, используемых в базе данных ЦУС. Папки представлены в виде иерархического списка. Содержимое папок представлено в Табл.8 и Табл.9. При выборе папки в главном окне отображается перечень соответствующих зарегистрированных объектов и их свойства. Сведения об объектах представлены в табличном виде. Часть сведений о выбранном объекте отображается на вкладках дополнительного окна. По умолчанию дополнительное окно расположено в нижней части главного окна.

Окно объектов и дополнительное окно можно перетаскивать, а также изменять их размеры с помощью мыши.

Управление объектами осуществляют с помощью команд главного и контекстных меню, а также панели инструментов информационного и дополнительного окон.

Табл.8 Объекты папки "Центр управления сетью"

Объект	Описание
Сетевые объекты	Содержат списки соответствующих элементов правил фильтрации IP-пакетов и трансляции сетевых адресов (см. стр.**77**). Сетевые объекты и сервисы можно объединять в группы
Группы сетевых объектов	
Сервисы	
Временные интервалы	
Пользователи	Перечень зарегистрированных пользователей и групп пользователей. Группы пользователей используют в правилах фильтрации IP-пакетов и трансляции сетевых адресов для более тонкой настройки доступа сотрудников к ресурсам
Классы трафика	Справочник классов трафика (используются для гибкого управления трафиком)
Реакции на события	Перечень автоматических реакций агента ЦУС и СД на события
Сертификаты	Перечень собственных сертификатов открытых ключей, зарегистрированных в комплексе. Эти сертификаты предназначены для установки защищенного соединения с внешними криптографическими сетями
Правила фильтрации	Перечень всех правил фильтрации IP-пакетов, установленных администратором
Администраторы	Перечень учетных записей администраторов комплекса
Сетевые устройства Континент	Перечень зарегистрированных в системе сетевых устройств (криптографические шлюзы, криптографические коммутаторы, детекторы атак)

Объект	Описание
База решающих правил	Список групп загруженных в БД ЦУС решающих правил (см. [**10**])
Виртуальные коммутаторы	Список виртуальных коммутаторов, используемых для управления криптографической коммутируемой сетью
Отчеты	Для каждого отчета перечень проблемных сетевых устройств, отфильтрованных по определенному параметру

Табл.9 Объекты папки "Внешние криптографические сети" (для каждой сети)

Объект	Описание
Сертификаты	Перечень сертификатов открытых ключей данной внешней сети. Эти сертификаты предназначены для установки защищенного соединения с данной внешней сетью
Межсетевые ключи	Перечень межсетевых ключей, предназначенных для установки защищенного соединения с данной внешней сетью
Сетевые объекты	Видимые сетевые объекты данной внешней сети
Криптошлюзы	Видимые криптографические шлюзы данной внешней сети
Ресурсы для внешней сети\ Сетевые объекты	Собственные сетевые объекты, видимые из внешней сети
Ресурсы для внешней сети\ Криптошлюзы	Собственные криптографические шлюзы, видимые из внешней сети

Управление группами

Для удобства просмотра и управления объекты можно объединять в группы. Возможность группировки предусмотрена для следующих объектов:

- сетевые объекты;
- сервисы;
- пользователи;
- детекторы атак;
- криптографические коммутаторы;
- криптографические шлюзы.

Имеется возможность создавать иерархию групп криптографических шлюзов.

При удалении группы объекты, входящие в нее, не удаляются.

Для создания группы:

1. Вызовите в окне объектов контекстное меню нужной папки и выберите команду "Создать группу <название объекта>…".

   На экране появится диалоговое окно для создания группы.

   Примечание. Диалоговое окно для создания группы можно вызвать нажатием на панели инструментов кнопки "Создать группу <название объекта>".

2. Заполните поля данного диалога и нажмите кнопку "ОК":

Название	Наименование группы объектов
Описание	Дополнительные сведения (необязательный параметр)
<Название объекта>	Перечень объектов, входящих в группу. Для формирования используйте кнопки "Добавить…" и "Удалить"

В окне объектов появится новая папка с указанным названием группы. При выборе этой папки в главном окне будет отображен перечень объектов, входящих в данную группу.

Для редактирования свойств группы:

1. Вызовите в окне объектов контекстное меню нужной группы и выберите команду "Свойства…".

   На экране появится диалоговое окно для редактирования свойств группы.

2. Внесите необходимые изменения и нажмите кнопку "ОК":

Название	Наименование группы объектов
Описание	Дополнительные сведения (необязательный параметр)
<Название объекта>	Перечень объектов, входящих в группу. Для формирования используйте кнопки "Добавить…" и "Удалить"

Для удаления группы:

1. Вызовите в окне объектов контекстное меню нужной группы и выберите команду "Удалить группу <название объекта>".

   На экране появится запрос на удаление.

2. Нажмите кнопку "Да".

Примечание. При удалении группы сетевых объектов, которые используются в правилах фильтрации или трансляции, на экране появится предупреждение об удалении правил для этой группы. Нажмите кнопку "Да" для удаления группы вместе с правилами. Кнопка "Нет" отменяет удаление группы.

Группа будет удалена из списка немедленно, а сведения о ней — из базы данных ЦУС без возможности восстановления. При этом объекты, которые входили в эту группу, не будут удалены.

Настройка программы

Настройка программы осуществляется с помощью команд меню "ЦУС" и заключается в настройке параметров соединения с ЦУС и агентом, а также в выборе режима идентификации администратора.

Настройка параметров соединения с ЦУС

Внимание! Чтобы измененные параметры вступили в силу, необходимо разорвать соединение программы управления с ЦУС и заново установить его.

Для настройки параметров соединения с ЦУС:

1. Активируйте в меню "ЦУС" команду "Параметры соединения с ЦУС…". На экране появится одноименный диалог.
2. Заполните поля данного диалога и нажмите кнопку "ОК":

IP-адрес	IP-адрес того интерфейса ЦУС, который подключен к сегменту сети, содержащему данный компьютер
Время ожидания соединения, сек.	Время ожидания соединения в секундах (от 10 до 600 сек.)
Считыватель ключей	Устройство для считывания ключа администратора ЦУС. Список содержит названия тех устройств идентификации, драйверы которых установлены на компьютере

Регистрация нового сетевого устройства

Регистрация сетевых устройств осуществляется с помощью программы управления после установки соединения с ЦУС и появления на экране основного окна этой программы.

Для регистрации сетевого устройства:

1. Вызовите меню "Объекты" и в подменю "Создать" активируйте команду с названием сетевого устройства (криптошлюз/детектор атак/криптокоммутатор).

   На экране появится диалог "Создание <сетевого устройства>".

2. Заполните поля диалога и нажмите кнопку "ОК":

Название	Имя сетевого устройства, под которым оно будет зарегистрировано в базе данных ЦУС. Это имя будет определять данное устройство в списке объектов, отображаемом программой управления. Максимальная длина имени — 39 символов
Описание	Дополнительная информация, которая будет отображаться программой управления в списке сетевых устройств. Максимальная длина записи в этом поле — 79 символов
Строка конфигурации	Строка символов, определяющая аппаратную конфигурацию сетевого устройства. Строка аппаратной конфигурации сетевого устройства указана в его паспорте
Часовой пояс	Смещение зимнего времени относительно Гринвича в часах для того региона, в котором будет эксплуатироваться данное сетевое устройство
Продолжить настройку параметров созданного сетевого устройства в окне свойств	При наличии отметки мастер регистрации после завершения своей работы открывает диалог "Свойства <сетевого устройства>" для настройки параметров зарегистрированного сетевого устройства

Окно мастера регистрации закроется, а в список сетевых устройств в основном окне программы управления будет добавлен объект с заданным именем.

Примечание. Если установлена отметка в поле "продолжить настройку параметров созданного сетевого устройства в окне свойств", то после нажатия кнопки "ОК" на экране появится диалог "Свойства <сетевого устройства>" для настройки параметров зарегистрированного сетевого устройства (в том числе параметров сетевых интерфейсов, см. стр. 72). Если отметка не установлена, то у зарегистрированного сетевого устройства все сетевые интерфейсы будут иметь статус "Не определен".

Запись конфигурации и ключей сетевого устройства на носитель

При инициализации сетевого устройства информация о его зарегистрированной в программе управления конфигурации переносится с помощью USB-флеш-накопителя. Файл конфигурации записывают на USB-флеш-накопитель под именем "gate.cfg".

Кроме того, для функционирования сетевого устройства требуются главный ключ и ключ связи с ЦУС. Эти ключи предъявляют при инициализации сетевого устройства на отдельном USB-флеш-накопителе под именем keyset (или под именами main.key и backup.key для ключей более ранних версий).

Запись конфигурации сетевого устройства на носитель

Конфигурацию сетевого устройства записывают на носителе в файл "gate.cfg".

Для записи конфигурации:

1. Предъявите носитель для записи конфигурации.
2. В основном окне программы управления в контекстном меню зарегистрированного сетевого устройства активируйте команду "Сохранить конфигурацию".

   На экране появится диалог "Сохранение конфигурации ".
3. Заполните поля диалога и нажмите кнопку "ОК".

Пароль	Пароль, с помощью которого будет ограничен доступ к сохраняемой конфигурации сетевого устройства. Этот пароль запрашивается при считывании конфигурации сетевым устройством. Пароль должен удовлетворять требованиям политики аутентификации администраторов. В противном случае кнопка "ОК" в диалоге назначения пароля будет неактивной
Подтверждение	Подтверждение пароля
Режим	Режим работы устройства в кластере (основной, резервный). Для одиночного устройства доступно только значение "Основной"
Имя файла	Полное имя файла gate.cfg. Для вызова стандартного диалога сохранения файла используйте кнопку "..." **Внимание!** Файл должен быть записан в папку верхнего уровня. При этом в одну папку может быть записан только один файл

После успешного завершения записи конфигурации сетевого устройства на экране появится сообщение об этом. Закройте окно этого сообщения.

Запись ключей сетевого устройства на носитель

Для записи ключей:

1. Предъявите носитель для записи ключей.
2. В основном окне программы управления в контекстном меню зарегистрированного сетевого устройства активируйте команду "Сохранить текущие ключи на носитель".

   На экране появится диалог назначения пароля.
3. Введите и подтвердите пароль.

   Внимание! Пароль должен удовлетворять требованиям политики аутентификации администраторов. В противном случае кнопка "ОК" в диалоге назначения пароля будет неактивной.

   На экране появится стандартный диалог выбора каталога для хранения ключей.
4. Укажите в качестве каталога предъявленный носитель.

   В результате успешной записи ключей на носитель появится сообщение "Текущие ключи сетевого устройства сохранены".

Ввод сетевого устройства в эксплуатацию и вывод из эксплуатации

Ввод сетевого устройства в эксплуатацию осуществляется после его инициализации и подключения. Вывод из эксплуатации требуется для выполнения некоторых настроек.

Пока сетевое устройство не введено в эксплуатацию, для него не могут быть установлены парные связи. При этом в программе управления такое сетевое устройство отображается с соответствующим статусом.

Для ввода сетевого устройства в эксплуатацию/вывода сетевого устройства из эксплуатации:

1. Вызовите контекстное меню объекта с именем нужного устройства и активируйте команду "Свойства…".

   На экране появится окно настройки свойств данного сетевого устройства.
2. Установите/удалите отметку в поле "Введен в эксплуатацию".
3. Нажмите кнопку "ОК".

Примечание. Данную операцию можно выполнить для группы сетевых устройств. Для этого выделите группу в списке, вызовите контекстное меню и выберите команду "Ввести в эксплуатацию" или "Вывести из эксплуатации".

Обновление конфигурации сетевого устройства

Обновление конфигурации сетевого устройства требуется для согласования взаимодействия ЦУС с устройством в случае возникновения сбоев в работе программного обеспечения.

Для обновления конфигурации сетевого устройства:

- Вызовите контекстное меню объекта с именем нужного устройства и активируйте команду "Обновить конфигурацию".

  По этой команде все настройки сетевого устройства будут приведены в соответствие настройкам, хранящимся в базе данных ЦУС. В течение интервала времени до обновления конфигурации на сетевом устройстве это сетевое устройство будет отображаться в списке с индикатором  .

Настройка общих параметров сетевого устройства

Настройку общих параметров выполняют в диалоговом окне "Свойства <сетевого устройства>".

Для настройки общих параметров:

1. Вызовите контекстное меню объекта с именем устройства, параметры которого требуется изменить, и активируйте команду "Свойства…".

   На экране появится окно "Свойства <сетевого устройства>".

   Общие параметры сетевого устройства настраивают на вкладке "Общие сведения".
2. Внесите необходимые изменения в поля вкладки и нажмите кнопку "ОК".

Идентификатор	Информационное поле, отображающее заводской идентификационный номер сетевого устройства. Изменению средствами ПУ ЦУС не подлежит
Название	Имя сетевого устройства, под которым оно зарегистрировано в базе данных ЦУС и значится в списке объектов, отображаемом программой управления. Максимальная длина имени — 39 символов
Описание	Дополнительные сведения. Максимальная длина записи в этом поле — 79 символов
Часовой пояс	Смещение зимнего времени относительно Гринвича в часах для того региона, в котором эксплуатируется сетевое устройство
Введен в эксплуатацию	При наличии отметки ЦУС устанавливает управляющее соединение с данным сетевым устройством, при отсутствии отметки — не устанавливает. Для КШ, на котором находится ЦУС, выключатель заблокирован
Режимы работы эвристик	Только для ДА. Задание режима работы: обнаружение или обучение. Если выбран режим обучения, необходимо указать IP-адрес обучающего компьютера

Сигнатурный анализатор	Только для ДА. Включение/выключение сигнатурного анализатора
Мягкий режим	Установка отметки включает мягкий режим работы КШ и КК, который предназначен для настройки устройства. В этом режиме нарушения правил фильтрации регистрируются в журнале НСД, однако IP-пакеты, не удовлетворяющие правилам фильтрации, не отбрасываются
Аутентификация пользователей	Только для КШ. При наличии отметки выполняется процедура аутентификации пользователей на данном КШ
Оптимизация правил фильтрации	Только для КШ. При наличии отметки ЦУС оптимизирует список правил фильтрации, загружаемых на сетевое устройство
Минимальный размер сжимаемого пакета, байт	Размер IP-пакета в байтах, при превышении которого IP-пакеты подвергаются сжатию, если режим сжатия для данного сетевого устройства включен (см. стр.**74**). IP-пакеты меньшего размера сжатию не подвергаются
Период контроля целостности файлов, мин.	Периодичность в минутах, с которой на сетевом устройстве осуществляется проверка целостности объектов, заданных шаблонами контроля целостности. Проверка осуществляется средствами программного обеспечения сетевого устройства. Сведения о результатах проверки сохраняются в журналах регистрации
Размер проверяемого сегмента данных, байт (только для КШ)	Объем проверяемых данных в байтах, относящихся к одному соединению. В зависимости от задаваемого значения может составлять от доли пакета до нескольких пакетов. Если в сегменте указанного размера заданное регулярное выражение обнаружено, дальнейшая проверка по данному правилу прекращается. Все пакеты, относящиеся к данному соединению, пропускаются. Если выражение не обнаружено, соединение разрывается. Распространяется только на разрешающие правила фильтрации с заданным регулярным выражением и контролем состояния соединения
Автоматический поиск MTU в канале управления	Включение/отключение режима принудительной установки флага DF (Don't fragment) в канале управления. По умолчанию режим включен
Автоматический поиск MTU в канале VPN	Включение/отключение режима принудительной установки флага DF (Don't fragment) в канале VPN. По умолчанию режим включен
MSS пользовательского трафика	"Не менять" – значение MSS устанавливается автоматически. "Установить" – ввод вручную значения из диапазона 536-1408

Настройка интерфейсов

Сетевые интерфейсы

Имена интерфейсов, отображаемые в окне диалога, соответствуют именам, указанным на корпусе сетевого устройства рядом с каждым разъемом.

Любой интерфейс может иметь несколько IP-адресов.

Интерфейс, определенный как SPAN-порт, должен использоваться только для целей анализа сетевого трафика. Подключать его к любым сетям запрещается, так как это может привести к лавинообразному росту трафика и выходу сети из строя.

Для настройки интерфейсов сетевого устройства:

1. Вызовите контекстное меню объекта с именем сетевого устройства, параметры которого требуется изменить, и активируйте команду "Свойства…".

   На экране появится окно "Свойства <сетевого устройства>".

2. Перейдите к вкладке "Интерфейсы".

Примечание. Имена интерфейсов, отображаемые на ярлыках вкладок, соответствуют именам, указанным на корпусе сетевого устройства рядом с каждым разъемом.

3. Определите параметры интерфейсов сетевого устройства. Для этого перейдите к нужной вкладке и внесите необходимые изменения в поля диалога:

Тип	Тип интерфейса: • Внешний — интерфейс, подключаемый к сетям общего пользования. • Внутренний — интерфейс, подключаемый к защищаемой сети (только для КШ). • Резервирование <сетевого устройства>— интерфейс для обмена служебной информацией между основным и резервным устройством в кластере (интерфейс резервирования). • SPAN — интерфейс для подключения компьютера с установленной на нем системой обнаружения сетевых атак. • Управление (только для ДА) – интерфейс для связи с ЦУС. • Мониторинг (только для ДА) – интерфейс, подключаемый к span-порту для анализа зеркального трафика. • Порт криптокоммутатора (только для КК) – интерфейс, используемый в составе виртуального коммутатора для создания криптографической коммутируемой сети. • Не определен — интерфейс при работе сетевого устройства не используется
Режим	Режим работы сетевой карты
Регистрация	Задание правила регистрации событий в журналах. Значения: • определяется сетевым устройством (правило наследуется из свойств сетевого устройства); • первые 64 байта; • тело пакета
MTU	Максимальная единица передачи данных (в байтах). Допустимые значения: 576 - 1600. Если типом интерфейса является "порт криптокоммутатора", по умолчанию устанавливается значение 1500, которое изменять не рекомендуется
IP-адреса	Список IP-адресов интерфейса. Для добавления нового адреса нажмите кнопку "Добавить", укажите IP-протокол (IPv4 или IPv6; IPv6 используется только для внешних интерфейсов) и далее введите адрес и маску (префикс для IPv6). Для удаления выбранного IP-адреса используйте кнопку "Удалить"

4. Нажмите кнопку "ОК" для сохранения внесенных изменений.

Настройка параметров хранения журналов

Настройку параметров хранения журналов сетевого устройства осуществляют в диалоговом окне "Свойства <сетевого устройства>".

Для настройки параметров хранения журналов:

1. Вызовите контекстное меню объекта с именем сетевого устройства, параметры которого требуется изменить, и активируйте команду "Свойства…".

   На экране появится окно "Свойства <сетевого устройства>".

2. Перейдите к вкладке "Журналы".

   Поля этого диалога определяют индивидуальные параметры хранения журналов регистрации на сетевом устройстве, а также параметры регистрации IP-пакетов в Журнале НСД и Журнале сетевого трафика.

3. Укажите в поле с названием журнала размер пространства на жестком диске сетевого устройства, которое отводится для хранения содержимого этого журнала. Размер пространства указывается в килобайтах.

Внимание! Суммарный размер пространства на жестком диске сетевого устройства, отводящегося для хранения журналов, не может превышать 32 Мбайта. Это конструктивное ограничение введено для поддержки высокого быстродействия системы.

Примечание. Если при добавлении новых записей размер журнала превысит указанное значение, новые записи заместят записи, помещенные в журнал ранее других (самые старые записи), т. е. осуществится автоматическая очистка журнала. Сведения об автоматической очистке журнала добавляются в системный журнал сетевого устройства.

Необходимо учитывать, что журналы хранятся на сетевом устройстве непродолжительное время, а затем передаются на ЦУС. Поэтому переполнение журналов на сетевом устройстве и их автоматическая очистка обычно происходит при отсутствии связи сетевого устройства с ЦУС.

4. В группе полей "Регистрировать в журнале сетевого трафика пакеты" укажите IP-пакеты, сведения о которых следует сохранять в журналах регистрации. Для этого отметьте соответствующие поля выключателей этой группы.

Примечание. IP- пакеты, переданные получателям, регистрируются в журнале сетевого трафика. IP-пакеты, отброшенные фильтром или не соответствующие ни одному правилу, — в журнале НСД и в журнале сетевого трафика.

Внимание! Если включить регистрацию пропущенных пакетов (поле "Переданные получателям"), то журнал при интенсивном трафике будет периодически переполняться с последующей автоматической очисткой и, как следствие, часть информации будет утеряна. Чтобы этого не произошло, рекомендуется осуществлять выборочную регистрацию пропущенных пакетов с помощью правил фильтрации (см. стр.**85**).

5. Нажмите кнопку "ОК" или "Применить" для сохранения внесенных изменений.

Управление списком связанных сетевых устройств

Перечень криптографических шлюзов и криптокоммутаторов, с которыми данное устройство должно устанавливать защищенные соединения, определяется списком связанных сетевых устройств . В этом случае трафик между сетевыми устройствами зашифровывается, в противном случае нет.

Количество защищенных соединений (VPN- каналов) для каждой пары связанных сетевых устройств соответствует количеству зарегистрированных в системе классов трафика. Состояние защищенных соединений отображается в разделе "Каналы VPN" вкладки "Состояние <сетевого устройства>" общей таблицы состояния <сетевого устройства>.

Для формирования списка связанных сетевых устройств:

1. Вызовите контекстное меню объекта с именем нужного устройства и активируйте команду "Свойства...".

   На экране появится окно настройки свойств данного устройства.

2. Перейдите к вкладке "Связи".

   В этом диалоге осуществляют формирование списка связанных сетевых устройств, а также настройку параметров соединений с ними. В поле "Время" отображается время установки ключа парной связи, на котором осуществляется криптографическое соединение с этим устройством.

   Изменения в данном диалоге вступают в силу сразу после их внесения.

3. Сформируйте список связанных сетевых устройств.

   Чтобы переместить имя устройства из одного списка в другой, выберите его с помощью мыши в исходном списке. Для выбора нескольких элементов используйте клавиши <Shift> и <Ctrl>. Перемещайте выбранные элементы из списка в список с помощью кнопок "<", "<<" и ">", ">>".

4. Укажите нужный режим сжатия передаваемых IP-пакетов. Для этого выберите в перечне связанных устройств нужное устройство и заполните поле:

Степень сжатия пакетов	Содержит значения от "1" до "9" и "Выключено". При переходе от режима "1" к режиму "9" степень сжатия IP-пакетов увеличивается и, соответственно, увеличивается время сжатия. При выборе значения "Выключено" сжатие IP-пакетов не осуществляется. Данная настройка к криптокоммутаторам не применяется

5. Нажмите кнопку "ОК" для сохранения изменений.

Аналогичная запись автоматически дополнит список связанных сетевых устройств другого — добавленного — устройства. С этого момента данные сетевые устройства могут устанавливать между собой защищенное соединение.

Внимание! Параметры сжатия IP-пакетов каждого из двух устройств, составляющих пару взаимодействующих устройств, настраиваются отдельно и могут не совпадать.

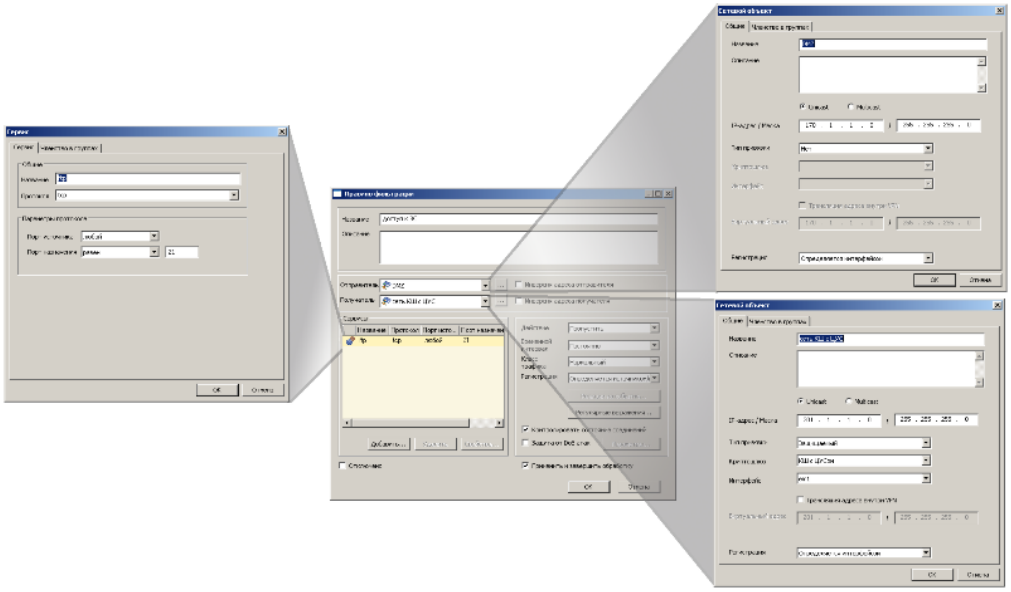
ПУ ЦУС: правила фильтрации IP-пакетов для КШ

О правилах и элементах правил

Правила фильтрации ( ) устанавливают порядок действий над IP-пакетами с заданными характеристиками при их обработке фильтром IP- пакетов криптографического шлюза.

Правила трансляции ( ) определяют характеристики IP-пакетов, для которых используется трансляция адресов.

Параметры правила, использующиеся при проверке соответствия IP-пакета правилу, а также расписание действия правила определяются параметрами объектов более низкого уровня — элементами правил.



К элементам правил относятся следующие объекты:

- сетевой объект ( )— используется в правилах фильтрации и трансляции для определения отправителя или получателя IP-пакетов. Содержит IP-адрес объекта и маску подсети;
- сервис ( ) — используется в правилах фильтрации и трансляции для определения характеристик IP-пакетов, к которым следует применять правило. К этим характеристикам относятся протокол (TCP, UDP, ICMP или номер протокола), диапазоны портов отправителя и получателя (для TCP и UDP), тип и код ICMP-сообщения;
- временной интервал ( ) — определяет расписание действия правила фильтрации.

Список правил фильтрации создается один на всю систему. Распределение правил фильтрации по КШ осуществляется автоматически.

Списки правил трансляции создаются индивидуальными для каждого КШ.

Списки элементов правил являются общими для всех КШ.

Внимание! У новых криптографических шлюзов, входящих в поставку, список правил фильтрации пуст и прохождение любых IP-пакетов через данный КШ запрещено.

Прежде чем приступить к составлению списков правил фильтрации или правил трансляции, создайте все необходимые элементы правил.

Управление элементами правил

Сетевой объект

Сетевые объекты подразделяются на следующие типы:

- Unicast — однонаправленная передача данных (сетевой пакет направляется одному адресату).
- Multicast — групповая передача данных (сетевой пакет одновременно направляется определенной группе адресатов).

Сетевые объекты типа Unicast привязывают к КШ. Привязка определяет КШ, на котором будут выполняться правила фильтрации с упоминанием этих сетевых объектов. Параметры привязки будут учитываться при функционировании правил фильтрации.

Внимание! Сетевой объект, относящийся к внутреннему интерфейсу КШ, должен быть обязательно привязан к этому же КШ. Обмен IP-пакетами с объектами, не имеющими привязки к данному КШ, разрешен только через внешний интерфейс.

Если сетевой объект входит в состав другого сетевого объекта, имеющего тип привязки "Защищаемый", то для дочернего объекта можно использовать только тип привязки "Внутренний".

Для сетевых объектов типа Multicast определяют перечень КШ, которые участвуют в групповой рассылке. На этих КШ будет включен режим ip multicast-routing. Адреса сетевых объектов этого типа должны принадлежать диапазону от 224.0.0.0 до 239.255.255.255.

Управление группами сетевых объектов см. стр.**67**.

Для вызова списка сетевых объектов:

- В левой части окна программы управления выберите папку "Центр управления сетью> Сетевые объекты".

  В правой части окна отобразится перечень сетевых объектов.

Табл.10 Перечень полей списка сетевых объектов

Поле	Описание
Название	Уникальное наименование сетевого объекта
Описание	Дополнительные сведения
IP-адрес	IP-адрес сегмента сети или отдельного компьютера
Маска	Маска сети
Криптошлюз	Имя того КШ, на котором выполняются правила фильтрации с упоминанием этого сетевого объекта (только для типов привязки "Внутренний" и "Защищаемый")
Тип привязки	Тип привязки для Unicast-объектов
Интерфейс	Имя интерфейса, через который проходят пакеты, подвергающиеся фильтрации
Виртуальный адрес	Виртуальный IP-адрес, назначенный данному сетевому объекту
Регистрация	Задание правила регистрации событий в журналах. Значения: • определяется интерфейсом; • первые 64 байта; • тело пакета

Создание и удаление сетевых объектов, а также настройка их параметров осуществляются в этом окне.

Объект "Любой", имеющий IP-адрес "0.0.0.0" и определяющий сеть в диапазоне всех известных IP-адресов, создается автоматически при инициализации ЦУС. Объект используется для доступа к ресурсам внешних сетей.

Для создания сетевого объекта:

1. Вызовите список сетевых объектов.
2. Вызовите меню "Операции" и активируйте команду "Создать сетевой объект".

   На экране появится окно настройки параметров сетевого объекта.
3. Настройте параметры создаваемого объекта, как это описано ниже.
4. Нажмите кнопку "ОК".

   В списке появится имя нового объекта, а сведения о нем будут сохранены в базе данных ЦУС.

Для настройки параметров сетевого объекта:

1. Вызовите список сетевых объектов.
2. Вызовите контекстное меню нужного сетевого объекта и активируйте команду "Свойства".

   На экране появится окно настройки параметров сетевого объекта. Перечень отображаемых полей зависит от выбора типа сетевого объекта.
3. Заполните поля на вкладке "Общие".

Название	Уникальное наименование сетевого объекта
Описание	Дополнительные сведения (необязательный параметр)
Unicast	Однонаправленная передача данных (сетевой пакет направляется одному адресату)
Multicast	Групповая передача данных (сетевой пакет одновременно направляется определенной группе адресатов)
IP-адрес	IP-адрес сегмента сети или отдельного компьютера
Маска	Маска сети. Все значимые биты адреса должны покрываться маской. Например, если поле "IP-адрес" содержит значение "134.17.11.0", то значение маски может равняться "255.255.255.0", но не может быть равно "255.255.0.0". Если указано значение "255.255.255.255" — задана сеть из одного компьютера, IP-адрес которого определяется значением поля "IP-адрес"
Тип привязки	Тип привязки (только unicast): • Нет — Привязка сетевого объекта к КШ отсутствует. • Внутренний — Сетевой объект привязан к КШ. Шифрование трафика не требуется. • Защищаемый — Сетевой объект привязан к КШ. Требуется шифрование трафика. **Внимание!** Шифрование трафика будет выполняться только при включении данного КШ в список связанных КШ (см. стр.**74**)
Криптошлюз	Имя того КШ, на котором должны выполняться правила фильтрации с упоминанием этого сетевого объекта (только для типов привязки "Внутренний" и "Защищаемый")
Интерфейс	Имя интерфейса. Фильтрации будут подвергаться только те IP-пакеты, которые проходят через этот интерфейс указанного криптошлюза (только для типов привязки "Внутренний" и "Защищаемый"). При выборе значения "Любой" фильтрации будут подвергаться IP-пакеты, проходящие через любой интерфейс
Получатели	Перечень КШ, которые должны участвовать в групповой передаче (только multicast)
Трансляция адреса внутри VPN	Включение/выключение виртуальной адресации. Поле доступно только в том случае, если в поле "Тип привязки" установлено значение "Защищаемый"

Виртуальный адрес	Виртуальный IP-адрес, назначенный данному сетевому объекту. Поле доступно, если установлена отметка в поле "Трансляция адреса внутри VPN"
Регистрация	Задание правила регистрации событий в журналах. Значения: • определяется интерфейсом; • первые 64 байта; • тело пакета

4. Перейдите к вкладке "Членство в группах" и сформируйте список групп, членом которых будет являться данный объект. Используйте кнопки:

Добавить	Вызывает на экран перечень зарегистрированных групп сетевых объектов
Удалить	Удаляет выбранную в списке группу

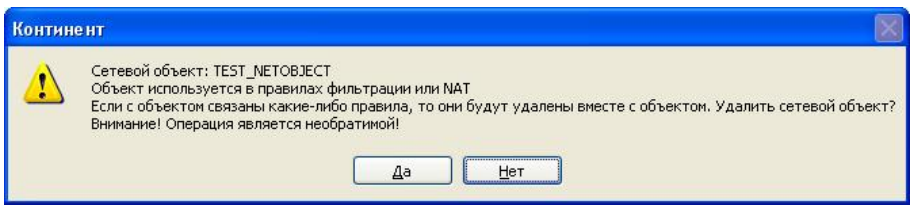
5. Нажмите кнопку "ОК".

Для удаления сетевого объекта:

1. Вызовите список сетевых объектов.
2. Вызовите контекстное меню удаляемого сетевого объекта и активируйте команду "Удалить".

   На экране появится запрос на удаление объекта.
3. Нажмите кнопку "Да".

   На экране появится предупреждение об удалении правил фильтрации для этого объекта.



Примечание. При подтверждении удаления будут удалены только те правила фильтрации и правила трансляции, которые используют этот объект непосредственно. Правила фильтрации для групп, содержащих удаляемый объект, удалены не будут.

4. Нажмите кнопку "Да".

   Объект будет удален из списка немедленно, а сведения о нем — из базы данных ЦУС без возможности восстановления.

Сервис

Для вызова списка сервисов:

- В левой части окна программы управления выберите папку "Центр управления сетью> Сервисы".

  В правой части окна отобразится перечень сервисов.

Создание и удаление сервисов, а также настройка их параметров осуществляются в этом окне.

Управление группами сервисов см. стр.**67**.

Для создания сервиса:

1. Вызовите список сервисов.
2. Вызовите меню "Операции" и активируйте команду "Создать сервис".

   На экране появится окно настройки параметров сервиса.
3. Настройте параметры создаваемого сервиса, как это описано ниже.
4. Нажмите кнопку "ОК".

   В списке появится имя нового сервиса, а сведения о нем будут сохранены в базе данных ЦУС.

Для настройки параметров сервиса:

1. Вызовите список сервисов.
2. Вызовите контекстное меню нужного сервиса и активируйте команду "Свойства".

   На экране появится окно настройки параметров сервиса. Перечень отображаемых полей зависит от выбора протокола.
3. Укажите или отредактируйте параметры сервиса.

Название	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
Протокол	Выберите из раскрывающегося списка название нужного протокола. Если требуется указать номер протокола, введите его в это поле с клавиатуры
Параметры протокола	Настройте параметры, специфичные для выбранного протокола: • для протоколов TCP или UDP укажите порты отправителя и получателя IP-пакетов. Для этого выберите нужный оператор и в появившихся полях укажите номер порта или диапазон номеров; • для протокола ICMP укажите тип ICMP-сообщения. Кроме этого, для ICMP-сообщений Destination Unreachable, Redirect и Time Exceeded укажите код

4. Перейдите к вкладке "Членство в группах" и сформируйте список групп, членом которых будет являться данный сервис. Используйте кнопки:

Добавить	Вызывает на экран перечень зарегистрированных групп сервисов
Удалить	Удаляет выбранную в списке группу

5. Нажмите кнопку "ОК".

   Новые значения параметров сервиса будут сохранены в базе данных ЦУС.

Для удаления сервиса:

Удаление элемента правила, использующегося в одном или нескольких правилах фильтрации или трансляции, невозможно.

1. Вызовите список сервисов.
2. Вызовите контекстное меню удаляемого сервиса и активируйте команду "Удалить".

   На экране появится запрос на удаление сервиса.
3. Нажмите кнопку "Да".

   Сервис будет удален из списка немедленно, а сведения о нем — из базы данных ЦУС без возможности восстановления.

Временной интервал

Для вызова списка временных интервалов:

- В левой части окна программы управления выберите папку "Центр управления сетью> Временные интервалы".

  В правой части окна отобразится перечень временных интервалов.

Создание и удаление временных интервалов, а также настройка их параметров осуществляются в этом окне.

Для создания временного интервала:

1. Вызовите список временных интервалов.
2. Вызовите меню "Операции" и активируйте команду "Создать временной интервал".

   На экране появится окно настройки параметров временного интервала.

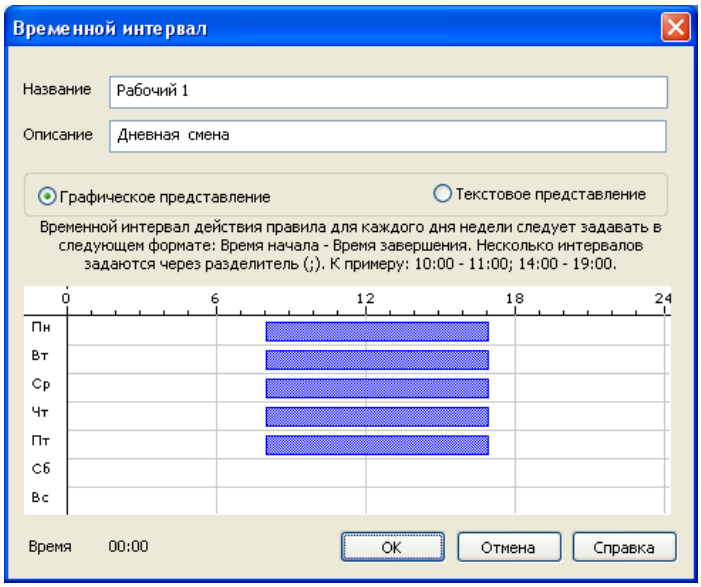
3. Настройте параметры создаваемого временного интервала, как это описано ниже.
4. Нажмите кнопку "ОК".

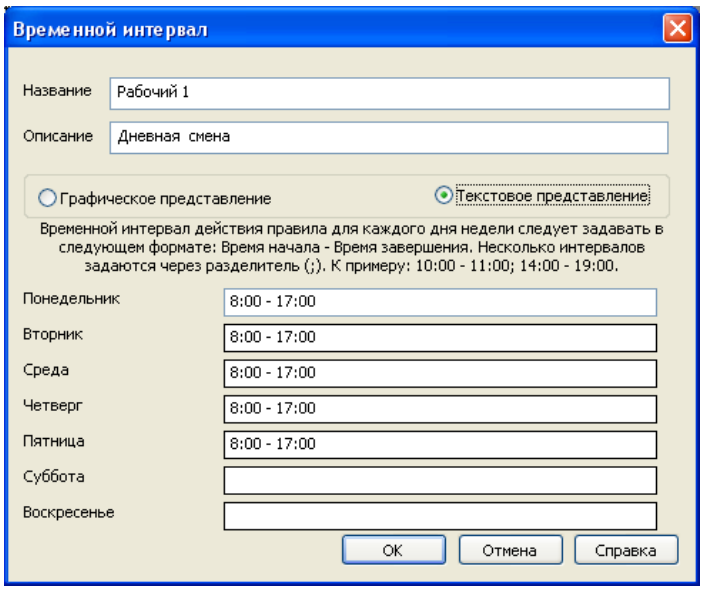
   В списке появится имя нового временного интервала, а сведения о нем будут сохранены в базе данных ЦУС.

Для настройки параметров временного интервала:

1. Вызовите список временных интервалов.
2. Вызовите контекстное меню нужного временного интервала и активируйте команду "Свойства".

   На экране появится окно настройки параметров временного интервала.





3. Укажите в поле "Название" наименование данного расписания, а в поле "Описание" — дополнительную информацию о нем.

   Совет. По возможности давайте расписаниям осмысленные названия, так как при настройке параметров правил фильтрации выбор этого элемента правила осуществляется только по его названию.

4. Выберите режим представления — графический или текстовый и определите время действия правила в течение суток. Для этого укажите один или несколько интервалов времени.

Примечание. При графическом представлении выберите нужный интервал мышью, при текстовом представлении введите нужные интервалы с клавиатуры. Несколько интервалов в течение дня разделяют символом ";".

5. Нажмите кнопку "ОК".

   Новые значения параметров временного интервала будут сохранены в базе данных ЦУС.

Для удаления временного интервала:

Удаление элемента правила, использующегося в одном или нескольких правилах фильтрации, невозможно.

1. Вызовите список временных интервалов.
2. Вызовите контекстное меню удаляемого временного интервала и активируйте команду "Удалить".

   На экране появится запрос на удаление временного интервала.
3. Нажмите кнопку "Да".

   Временной интервал будет удален из списка немедленно, а сведения о нем — из базы данных ЦУС без возможности восстановления.

Правила фильтрации

Управление списком правил фильтрации

Проверка соответствия IP-пакетов параметрам правил фильтрации осуществляется последовательно, в порядке их отображения в списке правил фильтрации. Если IP-пакет соответствует параметрам правила, над ним осуществляется действие, заданное этим правилом. Если таких правил несколько, то осуществляется действие, заданное последним из этих правил.

Правилу может быть присвоен признак немедленного применения. Это означает, что если IP-пакет соответствует параметрам этого правила, то действие, заданное правилом, осуществляется немедленно, а проверка последующих правил не выполняется.

Внимание! Правило может оказаться недействующим в следующих случаях:

- если отменяющее его правило находится ниже по списку;
- если отменяющее его правило находится выше по списку и имеет признак немедленного действия.

При формировании списка правил фильтрации учитывайте, что прохождение любого IP-пакета запрещено, если это не разрешено явно соответствующим правилом фильтрации.

Для управления списком правил фильтрации используются команды контекстного меню или кнопки панели инструментов.

Для вызова списка:

- В левой части окна программы управления выберите папку "Центр управления сетью> Правила фильтрации".

  В правой части окна отобразится список правил фильтрации IP-пакетов.

Список правил фильтрации отображается в форме таблицы, каждая строка которой соответствует одному правилу. Перечень полей, отображаемых в списке, и их описание, а также пиктографические обозначения правил фильтрации представлены в таблицах ниже.

Табл.11 Перечень полей списка правил фильтрации

Поле	Описание
Действие	Пропустить или отбросить IP-пакет и пиктографическое обозначение типа правила фильтрации (см. Табл.12)

Поле	Описание
Контроль состояния	Пиктографическое обозначение значения параметра правила фильтрации "Контролировать состояние соединения" (см. Табл.12). Если контроль состояния включен, то автоматически создаются правила фильтрации, которые разрешают прохождение всех пакетов, относящихся к этому соединению
№	Порядковый номер правила фильтрации в списке
Название	Название правила
Описание	Описание правила
Отправитель	Имя сетевого объекта или группы сетевых объектов. Определяет IP-адреса абонентов-отправителей, для которых будет действовать правило
Получатель	Имя сетевого объекта или группы сетевых объектов. Определяет IP-адреса абонентов-получателей, для которых будет действовать правило
Временной интервал	Временной интервал действия правила
Класс трафика	Класс трафика, которому будут принадлежать IP-пакеты с заданными характеристиками
Регистрация	Наличие и вид регистрации IP-пакета
Сервисы	Перечень сервисов или групп сервисов. Определяет характеристики IP-пакетов, для которых будет действовать правило
Реакции на события	Назначение определенной реакции правилу фильтрации IP-пакетов

Табл.12 Пиктографические обозначения правил фильтрации

Пиктограмма	Описание
	Правило, разрешающее прохождение IP-пакетов
	Правило, запрещающее прохождение IP-пакетов
	Контроль состояния соединения выключен
	Контроль состояния соединения включен
	Инверсия адреса

Если правило отключено, оно отображается в таблице серым цветом.

Для создания правила:

1. Вызовите контекстное меню в любом месте списка правил и активируйте команду "Создать правило фильтрации" или нажмите одноименную кнопку на панели инструментов ().

   На экране появится диалог "Правило фильтрации".
2. Настройте и сохраните параметры создаваемого правила. Порядок настройки параметров правила см. стр.**85**.

Созданное правило фильтрации будет добавлено в конец списка.

Для удаления правила:

- Выберите одно или несколько правил в списке и нажмите кнопку "Удалить" на панели инструментов (клавишу <Delete>). Для выбора нескольких элементов используйте клавиши <Shift> и <Ctrl>.

Для изменения местоположения правила в списке:

- Выберите одно или несколько правил в списке и с помощью кнопок панели инструментов "Переместить элемент вверх" () и "Переместить элемент вниз" () переместите правило или выбранную группу правил в нужное

место списка. Для выбора нескольких элементов используйте клавиши <Shift> и <Ctrl>.

Примечание. Изменить местоположение правила в списке можно также перетаскиванием или использованием команд контекстного меню. При выполнении операции перетаскивания поддерживается множественное выделение правил.

Для изменения параметров правила:

1. Выберите нужное правило и выполните одно из следующих действий:
   - подведите курсор мыши к соответствующей строке списка правил и дважды нажмите левую кнопку мыши;
   - активируйте в контекстном меню команду "Свойства...";
   - нажмите на панели инструментов кнопку "Свойства правила фильтрации" ().

   После выполнения любого из указанных действий на экране появится диалог "Правило фильтрации".
2. Внесите необходимые изменения и сохраните их. Порядок настройки параметров правила см. стр.**85**.

Для временного отключения правила:

1. Выберите нужное правило и выполните одно из следующих действий:
   - подведите курсор мыши к соответствующей строке списка правил и дважды нажмите левую кнопку мыши;
   - активируйте в контекстном меню команду "Свойства...";
   - нажмите на панели инструментов кнопку "Свойства правила фильтрации" ().

   После выполнения любого из указанных действий на экране появится диалог "Правило фильтрации".
2. Установите отметку в поле "Отключено".
3. Нажмите кнопку "ОК".

   Выбранное правило фильтрации будет отключено. Для того чтобы разрешить использование отключенного правила, удалите отметку из данного поля.

Для сохранения изменений:

- Нажмите кнопку "Сохранить изменения" () на панели инструментов.

  В результате отредактированный список правил фильтрации будет сохранен в базе данных ЦУС и передан на соответствующий КШ.

Примечание. Если при несохраненных изменениях выбрать в окне объектов любой другой объект (папку), то на экране появляется запрос на сохранение внесенных изменений. Для сохранения изменений нажмите кнопку "Да", для отказа от сохранения изменений и возврата к редактированию правил фильтрации нажмите кнопку "Нет".

При сохранении внесенных изменений выполняется автоматическая проверка их корректности. При некорректных изменениях выводится сообщение об ошибке, а процесс сохранения прерывается. При очередном переходе к другому объекту вновь появится запрос на сохранение правил фильтрации и при команде на сохранение — сообщение об ошибке. Ликвидируйте ошибку или откажитесь от сохранения изменений.

Внимание! После внесения изменений в правила фильтрации с контролем состояния или изменения их порядка в списке администратор должен выполнить очистку соединений на задействованных в правилах криптошлюзах.

Для отказа от внесенных изменений:

- Нажмите на панели инструментов кнопку "Отказаться от изменений" ().

  Изменения, внесенные в правила фильтрации, будут отменены.

Для группировки правил фильтрации:

- Выберите правило фильтрации, под которым необходимо вставить разделитель, и в контекстном меню активируйте команду "Добавить разделитель".

  Разделитель объединяет в группу правила фильтрации, заключенные между этим и следующим разделителем.

Для управления разделителем:

- Используйте кнопки панели инструментов и команды контекстного меню.

Кнопка	Команда	Описание
Свернуть все		Скрывает детали списка
Развернуть все		Отображает детали списка
Список		Скрывает разделители
Группировка		Отображает разделители
	Переименовать разделители	Включает режим редактирования имени выбранного разделителя
	Удалить разделитель	Удаляет выбранный разделитель из списка

Настройка параметров правила фильтрации

Для настройки параметров правила фильтрации:

1. Вызовите на экран диалог для редактирования правила фильтрации. Описание процедуры вызова диалога при добавлении нового правила или изменении существующего см. стр.**82**.
2. Заполните поля диалога и нажмите кнопку "OK".

Поле/Кнопка	Описание
Название	Наименование правила
Описание	Дополнительные сведения (необязательный параметр)
Отправитель	Имя одного из следующих объектов: • группа пользователей; • сетевой объект; • группа сетевых объектов. Определяет абонентов-отправителей, для которых будет действовать правило
Инверсия адреса отправителя*	При наличии отметки правило будет действовать для всех абонентов-отправителей, кроме указанного
Получатель	Имя одного из следующих объектов: • группа пользователей; • сетевой объект; • группа сетевых объектов. Определяет абонентов-получателей, для которых будет действовать правило
Инверсия адреса получателя*	При наличии отметки правило будет действовать для всех абонентов-получателей, кроме указанного
Сервисы	Перечень сервисов или групп сервисов. Определяет характеристики IP-пакетов, для которых будет действовать правило. Для формирования списка используйте кнопки в нижней части поля

Поле/Кнопка	Описание
Действие	• Пропустить — разрешить прохождение пакета; • Отбросить — запретить прохождение пакета; • Усиленная фильтрация; • Контроль приложений
Временной интервал	Имя временного периода, который будет определять расписание действия правила
Класс трафика	Класс трафика, которому будут принадлежать IP-пакеты с заданными характеристиками. Класс трафика используется для формирования очереди на обработку блоком криптографической защиты, а также очереди на отправку на сетевом интерфейсе
Регистрация**	• Определяется источником/получателем. • Первые 64 байта — регистрировать в журнале сетевого трафика первые 64 байта пакета. • Тело пакета — регистрировать заголовок и первые 128 байт содержания пакета после заголовка. • Только первый пакет в соединении — регистрировать заголовок и первые 128 байт содержания пакета после заголовка только первого пакета, открывающего соединение
Профиль усиленной фильтрации	Выбираемый из списка профиль усиленной фильтрации или профиль запрещенных ресурсов
Профиль контроля приложений	Выбираемый из списка профиль контроля приожений
Пропускать фрагментированные пакеты	Запрет или разрешение пропускать фрагментированные пакеты
Кнопка "Реакция на события..."	Вызывает на экран список зарегистрированных реакций на события. Отметьте нужные и нажмите кнопку "ОК". Кнопка доступна только при выборе в поле "Регистрация" значения "Только первый пакет соединения"
Кнопка "Регулярные выражения..."	Вызывает на экран список зарегистрированных регулярных выражений. Отметьте нужные и нажмите кнопку "ОК"
Отключено	Установка отметки отключает данное правило без удаления его из списка
Контролировать состояние соединения	Отметку устанавливают для пакетов, открывающих соединение. В этом случае автоматически создаются правила фильтрации, которые разрешают прохождение всех пакетов, относящихся к этому соединению. Автоматически созданные правила сохраняются в таблице состояния соединений и на экране не отображаются
Защита от DoS-атак	Включает для данного правила режим защиты от DoS-атак. Для настройки параметров нажмите кнопку "Параметры..." справа (см. стр.**86**)
Применить и завершить обработку	Установка отметки присваивает данному правилу признак немедленного применения

* Для групп сетевых объектов возможна некорректная работа в режиме инверсии адреса. Используйте инверсию адреса только для одиночных сетевых объектов.

** Для регистрации пакетов в журнале сетевого трафика необходимо дополнительно установить отметки в соответствующих полях диалога "Журналы" свойств КШ (см. стр.**73**).

Настройка режима защиты от DoS-атак

Включение и настройку режима защиты от DoS-атак выполняют в диалоговом окне для редактирования правила фильтрации. Этот режим действует для данного правила при наличии следующих условий:

- поле "Действие" содержит значение "Пропустить";

- поле "Сервисы" содержит только сервисы TCP;
- установлена отметка в поле "Контролировать состояние соединения".

Для настройки параметров правила фильтрации:

1. Вызовите на экран диалог для редактирования правила фильтрации. Описание процедуры вызова диалога при добавлении нового правила или изменении существующего см. стр.**82**.
2. Установите отметку в поле "Защита от DoS-атак" и нажмите кнопку "Параметры...".

   На экране появится диалог "Параметры защиты от DoS-атак".
3. Заполните поля диалога и нажмите кнопку "OK".

Поле	Описание
Ограничить количество соединений	Максимальное количество соединений, которое может быть установлено по указанному правилу фильтрации
Тайм-аут соединений	Время, по истечении которого неактивное соединение будет автоматически разорвано
Ограничить интенсивность соединений/сек.	Количество новых соединений, регистрируемых для данного правила, в секунду

Правила трансляции сетевых адресов

Управление списком правил трансляции

Управление списком правил трансляции осуществляют с помощью команд контекстного меню или кнопок панели инструментов. Для настройки правил трансляции используют элементы правил: сетевые объекты и сервисы (см. стр.**76**).

Внимание! До начала работы с правилами трансляции создайте нужные элементы правил (см. стр.**77**).

Для вызова списка:

- В левой части окна программы управления выберите папку "Криптошлюзы", выберите в перечне нужный КШ и перейдите к вкладке "Правила трансляции".

Список правил трансляции отображается в форме таблицы, каждая строка которой соответствует одному правилу. Поля таблицы соответствуют параметрам правила трансляции.

Для создания правила:

1. Вызовите контекстное меню в любом месте списка правил и активируйте команду "Создать правило трансляции".

   На экране появится диалог "Правило трансляции адресов (NAT)".
2. Настройте и сохраните параметры создаваемого правила. Порядок настройки параметров правила см. стр.**88**.

Для удаления правила:

1. Выберите одно или несколько правил в списке и нажмите кнопку "Удалить правило трансляции" на панели инструментов (клавишу <Delete>).

   Примечание. Используйте также команду контекстного меню "Удалить правило", установив курсор мыши перед вызовом меню в выделенную область списка. Для выбора нескольких элементов используйте клавиши <Shift> и <Ctrl>.

   На экране появится запрос на удаление правила.
2. Нажмите кнопку "Да".

Для изменения параметров правила:

1. Выберите нужное правило и активируйте в контекстном меню команду "Свойства".

   На экране появится диалог "Правило трансляции адресов (NAT)".

2. Внесите необходимые изменения и сохраните их. Порядок настройки параметров правила см. стр.**88**.

Для временного отключения правила:

1. Выберите нужное правило и активируйте в контекстном меню команду "Свойства".

   На экране появится диалог "Правило трансляции адресов (NAT)".

2. Установите отметку в поле "Отключено".
3. Нажмите кнопку "OK".

   Выбранное правило трансляции будет отключено. Для того чтобы разрешить использование отключенного правила, удалите отметку из данного поля.

Настройка параметров правила трансляции

Трансляция адресов осуществляется для IP-пакетов, которые соответствуют параметрам правил трансляции.

Для настройки параметров правила трансляции:

1. Вызовите на экран диалог для редактирования правила трансляции (см. стр.**87**).
2. Заполните поля диалога и нажмите кнопку "OK":

Поле	Описание
Название	Наименование правила трансляции сетевых адресов
Описание	Дополнительные сведения (необязательный параметр)
Направление	Тип правила фильтрации (Входящие, Исходящие, 1:1). Определяет доступность полей диалога
Источник	Имя одного из следующих объектов: • группа пользователей; • сетевой объект. Определяет абонентов-отправителей, для которых будет действовать правило
Получатель	Имя одного из следующих объектов: • группа пользователей; • сетевой объект. Определяет абонентов-получателей, для которых будет действовать правило
Интерфейс*	Интерфейс КШ, на котором выполняется правило трансляции. Обычно — внешний интерфейс
IP-адрес	IP-адрес и маска сетевого объекта, для которого будет действовать данное правило трансляции. Поле "IP-адрес" заполняется вручную при выборе значения в поле "Источник" (для Исходящие и 1:1) или "Получатель" (для Входящие). Поле "Маска" заполняется автоматически
Маска	
Изменить на	IP-адрес и маска сети, присваиваемые сетевому объекту — отправителю (для Исходящие и 1:1) или получателю (для Входящие)

Поле	Описание
Сервисы и трансляция портов**	Перечень сервисов или групп сервисов, для которых действует правило фильтрации. Для формирования списка используйте кнопки внизу. Кнопка "Порт трансляции" вызывает на экран диалог для переопределения порта (только для Входящие). Отметку в поле "Трансляция FTP" устанавливают для обеспечения корректной трансляции адресов источника для правила NAT 1:1 при передаче данных по протоколу FTP. **Внимание!** При добавлении правила трансляции (1:1), отличающегося от уже имющегося только наличием отметки в поле "Трансляция FTP", работа ftp не гарантируется
Временной интервал	Название временного периода, который будет определять расписание действия правила
Класс трафика	Класс трафика, которому будут принадлежать IP-пакеты с заданными характеристиками. Класс трафика используется для формирования очереди на обработку блоком криптографической защиты, а также на отправку на сетевом интерфейсе
Регистрация	Вид регистрации: • Нет — определяется источником/получателем. • Первые 64 байта — регистрировать в журнале сетевого трафика первые 64 байта пакета. • Тело пакета — регистрировать заголовок и первые 128 байт содержания пакета после заголовка. • Только первый пакет в соединении — регистрировать заголовок и первые 128 байт содержания пакета после заголовка только первого пакета, открывающего соединение
Кнопка "Реакция на события..."	Вызывает на экран список зарегистрированных реакций на события. Отметьте нужные и нажмите кнопку "OK". Кнопка доступна только при выборе в поле "Регистрация" значения "Только первый пакет соединения"
Отключено	Установка отметки отключает данное правило без удаления его из списка

* Трансляция сетевых адресов для зашифрованных пакетов возможна только в том случае, если для правила трансляции указан интерфейс КШ, через который трафик проходит в открытом виде. При этом для адресов самого КШ правило не будет применяться.

** Для настройки входящего правила трансляции можно использовать сервисы только со следующими параметрами:

- протокол — TCP или UDP;
- порт источника — любой (определяется с помощью оператора "Любой");
- порт назначения — конкретное значение одного порта (определяется с помощью оператора "==").

Процедуру настройки параметров сервиса см. стр.79.

Для регистрации пакетов в журнале сетевого трафика необходимо дополнительно установить отметки в соответствующих полях диалога "Журналы" свойств КШ (см. стр.73).

Примеры правил фильтрации и трансляции для КШ

Защищенное соединение

Информационный обмен между подсетями, защищенными разными КШ

Необходимо обеспечить взаимный обмен информацией между рабочими станциями и серверами локальной сети "Защищаемая сеть КШ «КШ с ЦУС»" (IP-адрес 10.1.1.0, ЦУС) и рабочими станциями и серверами "ЗС КШ «КШ 2»" (IP-адрес 10.2.1.0, КШ 2). Инициатор соединения — любая рабочая станция любой локальной сети.

Табл.13 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	**Сетевой объект 2**
Название	Защищаемая сеть КШ "КШ с ЦУС"	ЗС КШ "КШ"
Описание	Локальная сеть	Локальная сеть
IP-адрес	10.1.1.0	10.2.1.0
Маска	255.255.255.0	255.255.255.0
Тип привязки	Защищаемый	Защищаемый
Криптошлюз	КШ с ЦУС	КШ
Интерфейс	Любой	Любой

Табл.14 Параметры правил фильтрации

Параметр	Значение	
	Правило 1	**Правило 2**
Отправитель	Защищаемая сеть КШ "КШ с ЦУС"	ЗС КШ "КШ"
Инверсия адреса	—	—
Получатель	ЗС КШ "КШ"	Защищаемая сеть КШ "КШ с ЦУС"
Инверсия адреса	—	—
Сервисы	Любой TCP, Любой UDP, Любой ICMP	Любой TCP, Любой UDP, Любой ICMP
Действие	Пропустить	Пропустить
Регистрировать	Нет	Нет
Временной интервал	Постоянно	Постоянно
Контролировать состояние соединения	Установить отметку	Установить отметку
Отключено	—	—

Межсетевое экранирование

Доступ рабочих станций из защищенной подсети к узлам общей сети

Необходимо обеспечить круглосуточный доступ к узлам общей сети с рабочих станций, входящих в состав подсети 10.1.1.0, защищаемой КШ 1 . Публичный IP-адрес отправителя — 198.23.75.100. В этом случае на КШ 1 нужно создать исходящее правило трансляции.

Табл.15 Параметры сетевого объекта

Параметр	Значение	
	Сетевой объект 1	**Сетевой объект 2**
Название	LAN 1-1-0	Любой*
Описание	Локальная сеть	Любой
IP-адрес	10.1.1.0	0.0.0.0
Маска	255.255.255.0	0.0.0.0
Тип привязки	Защищаемый	Нет
Криптошлюз	КШ 1	—
Интерфейс	em0	—

* Объект "Любой", имеющий IP-адрес "0.0.0.0" и определяющий сеть в диапазоне всех известных IP-адресов, создается автоматически при инициализации ЦУС.

Табл.16 Параметры исходящего правила трансляции для КШ 1

Параметр	Значение
Направление	Исходящие
Источник	LAN 1-1-0
Получатель	Любой
Интерфейс	em0
Изменить на	198.23.75.100
	255.255.255.255
Сервисы	http

Доступ к почтовому серверу из открытой сети

Необходимо обеспечить доступ к почтовому серверу Post, находящемуся в защищенной сети (IP-адрес 10.1.2.100, КШ с ЦУС, интерфейс em1), от любого сетевого объекта "Любой" в открытой сети.

Табл.17 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2*
Название	Post	Любой
Описание	Почтовый сервер	Любой объект в открытой сети за внешним интерфейсом КШ1
IP-адрес	10.1.2.100	0.0.0.0
Маска	255.255.255.255	0.0.0.0
Тип привязки	Внутренний	Нет
Криптошлюз	КШ с ЦУС	—
Интерфейс	em1	—

* Создается автоматически.

Табл.18 Параметры сервиса

Параметр	Значение
Название	smtp*
Протокол	tcp
Порт источника	Любой
Порт назначения	25

* Создается автоматически.

Табл.19 Параметры правила фильтрации

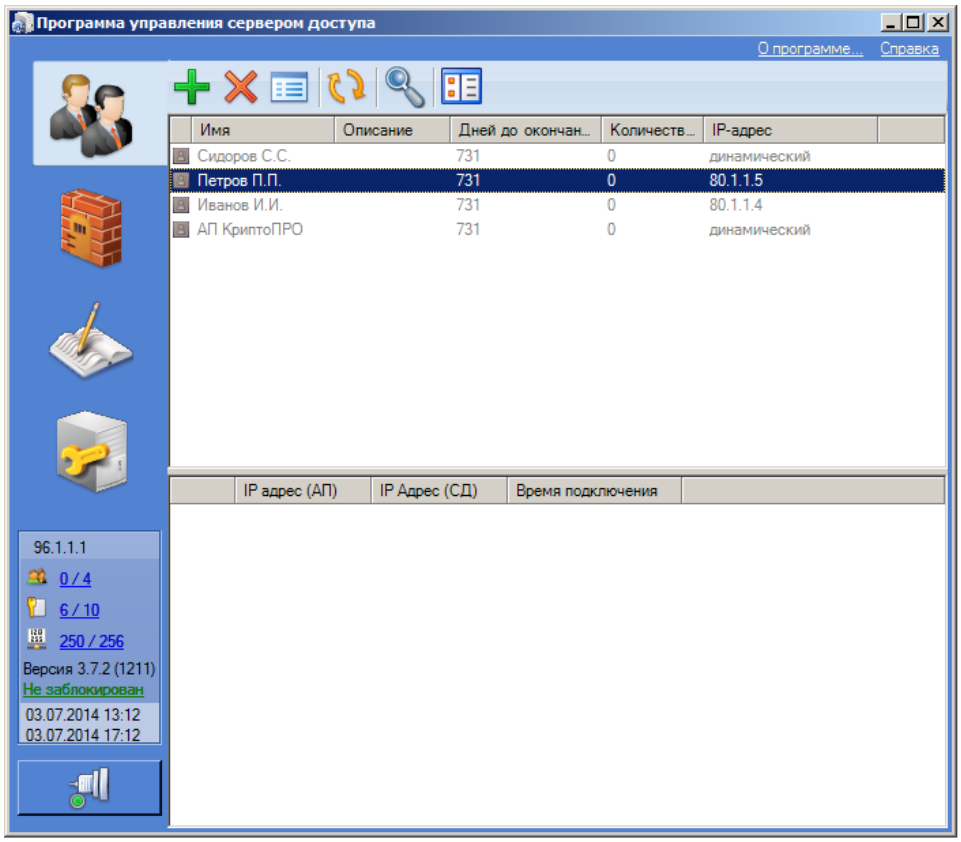
Параметр	Значение
Отправитель	Любой
Инверсия адреса	—
Получатель	Post
Инверсия адреса	—
Сервисы	smtp

Параметр	Значение
Действие	Пропустить
Регистрировать	Нет
Временной интервал	Постоянно
Контролировать состояние соединения	Установить отметку
Отключено	—

ПУ СД: управление сервером доступа

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.20 Элементы управления основного окна

Элемент	Описание
Панель переходов	Содержит ярлыки для доступа к объектам управления (см. Табл.21)
Информационное окно	Отображает выбранные на панели переходов объекты управления
Панель инструментов	Содержит кнопки для управления записями в информационном окне
Окно состояния (под панелью переходов)	Содержит следующую информацию (для просмотра подробной информации активируйте соответствующую ссылку): • подключено пользователей/всего пользователей; • доступно лицензий/всего лицензий; • свободно IP-адресов/всего IP-адресов в пуле
Кнопка для управления соединением с сервером	Предназначена для установки или разрыва связи с сервером доступа

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

Табл.21 Объекты управления

Ярлык	Объект	Содержимое информационного окна
	Учетные записи	Список пользователей, зарегистрированных в базе данных сервера доступа (см. стр.**103**)
	Журналы	Регистрационные журналы сервера доступа
	Правила фильтрации	Переход к настройкам групп правил фильтрации IP-пакетов (см. стр.**101**). Настройка защищенных подсетей" (см. стр.**98**) и сервисов (см. стр.**99**), необходимых для формирования правил фильтрации
	Настройки сервера	Параметры соединения с сервером доступа, список сертификатов и лицензий

Настройка параметров соединения с сервером доступа

Для настройки параметров соединения:

1. Перейдите к объекту управления "Настройки сервера".

   В информационном окне появится диалог для настроек параметров программы управления.

2. Настройте параметры соединения с сервером доступа:

Адрес сервера	IP-адрес внутреннего интерфейса криптографического шлюза, через который будет осуществляться 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 сек. Для изменения введите новое значение вручную (от 30 до 600 сек.)

3. Нажмите кнопку "Сохранить настройки".

   Применение новых настроек будет осуществлено 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 запрос 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 установке 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.

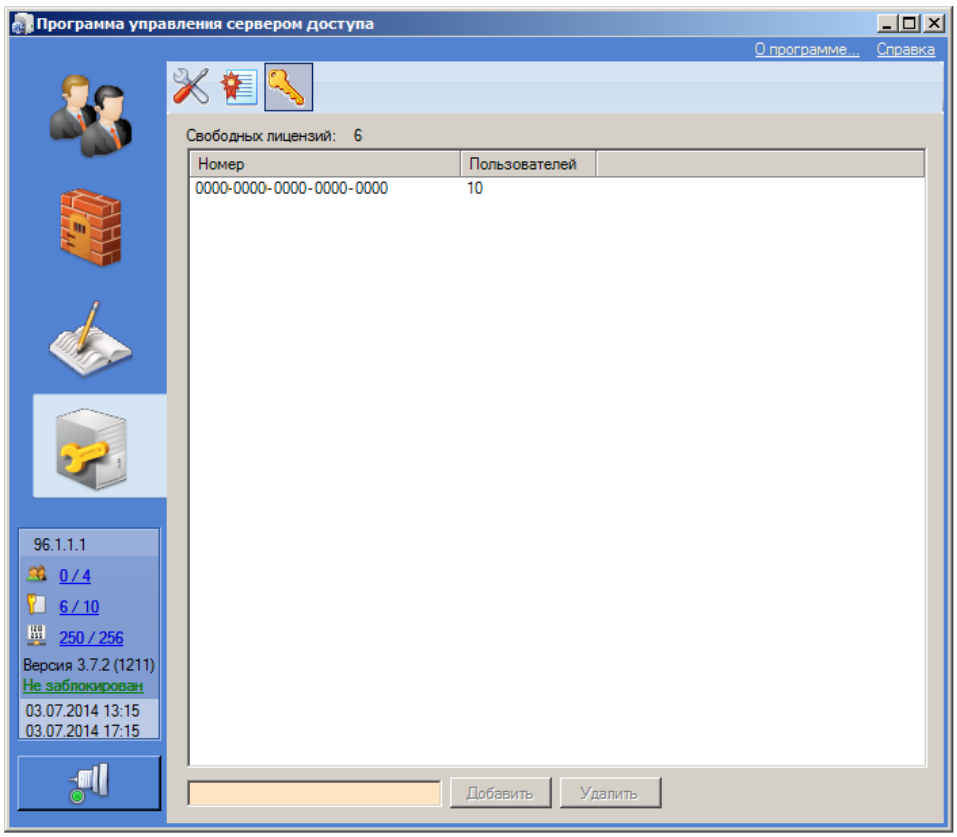
Регистрация лицензий

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

Для регистрации лицензий:

1. На панели переходов основного окна выберите ярлык "Настройки сервера", а затем в панели инструментов нажмите кнопку "Лицензии".

   В информационном окне отобразится перечень 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.**109**).

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

2. 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. На панели переходов основного окна выберите ярлык "Настройки сервера", а затем в панели инструментов нажмите кнопку "Настройка сервера".

   В информационном окне отобразится перечень 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 (см. [])
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

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

3. Нажмите кнопку "Сохранить настройки".

ПУ СД: правила фильтрации IP-пакетов для сервера доступа

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.**110**).

Примечание. Изменения в правилах фильтрации вступают в силу только в следующем сеансе пользователя. При необходимости отключите пользователя от сервера доступа принудительно (см. стр.**112**).

Управление списками объектов

Просмотр списка объектов

Для просмотра списка объектов:

1. На панели переходов основного окна программы выберите ярлык "Правила фильтрации"  .

   В информационном окне появится содержимое вкладки "Правила" — список всех правил фильтрации.

2. Для перехода к другим объектам воспользуйтесь закладками:

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 нужному списку объектов и нажмите на панели инструментов кнопку "Добавить"  .

   На экране появится окно настройки параметров объекта.
2. Настройте параметры создаваемого объекта:
   - "Защищенная подсеть" (см. стр.**98**);
   - "Сервис" (см. стр.**99**);
   - "Правило фильтрации" (см. стр.**99**);
   - "Группа правил фильтрации" (см. стр.**101**).
3. Нажмите кнопку "ОК".

   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 нажмите на панели инструментов кнопку "Удалить"  или клавишу <Delete>.

   На экране появится окно запроса.
2. Подтвердите удаление выбранного объекта, нажав кнопку "Да".

   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. Вызовите окно настройки (см. стр.**98**).
2. Укажите или отредактируйте 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 будет осуществляться без шифрования трафика

Настройка сервисов

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

Автоматически при инициализации СД создается набор наиболее часто используемых сервисов (pop-3, smtp, imap4, http, ftp, ftp-data и пр.).

Для настройки параметров сервиса:

1. Вызовите окно настройки (см. стр.**98**).
2. Укажите или отредактируйте параметры сервиса и нажмите кнопку "ОК".

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

Настройка правил фильтрации

Эти объекты размещаются во вкладке "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:

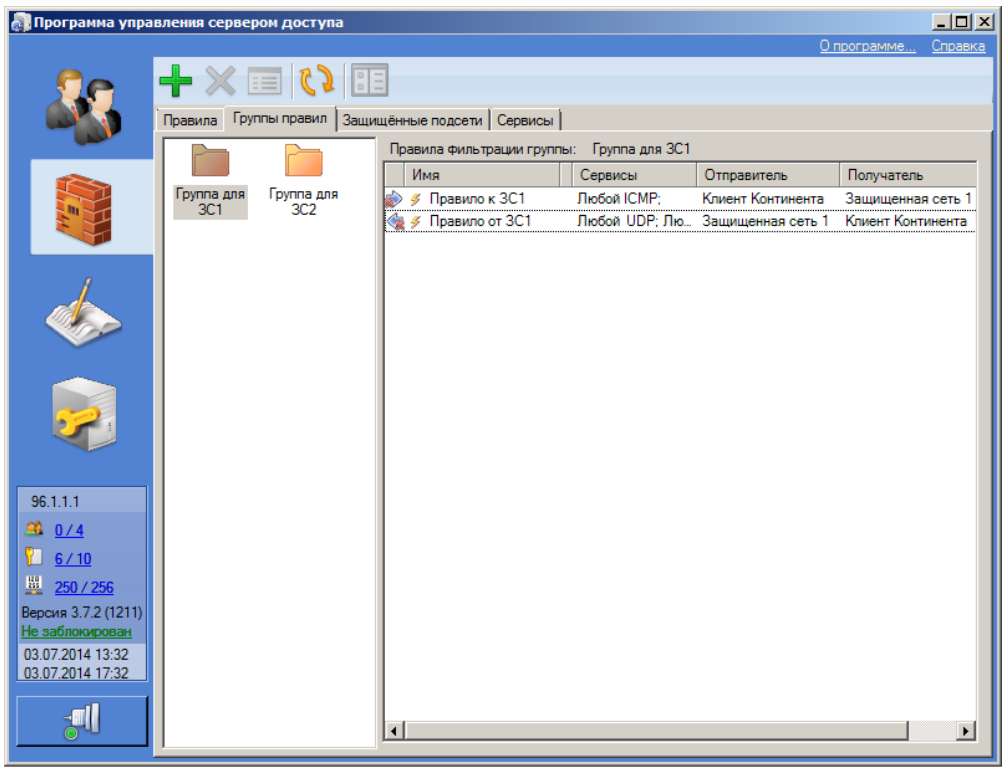
1. Вызовите окно настройки (см. стр.**98**).
2. Укажите или отредактируйте параметры правила фильтрации и нажмите кнопку "ОК".

Имя	Введите название правила фильтрации
Описание	Введите дополнительную информацию о правиле фильтрации
Отправитель Получатель	Выберите из раскрывающегося списка имя нужного объекта "Подсеть". Правило фильтрации будет применяться 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 будет указываться IP-адрес компьютера, с которого он подключился к серверу доступа. Одно из этих двух полей обязательно должно содержать значение "Клиент Континента"
Сервисы	Сформируйте перечень сервисов, используемых в правиле фильтрации. Для формирования списка используйте кнопки "Добавить" и "Удалить". Правило фильтрации будет применяться 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; • "Отбросить пакет с уведомлением" — запретить прохождение пакета и уведомить об этом отправителя.
Протоколирование	Выберите из раскрывающегося списка режим регистрации IP-пакета. При этом 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 (см. [**3**])
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

Настройка групп правил фильтрации

Эти объекты размещаются на вкладке "Группы правил".

Примечание. Редактирование свойств правил внутри группы невозможно.



Для настройки параметров группы правил:

1. Вызовите окно настройки (см. стр.**98**).
2. Укажите или отредактируйте параметры группы правил фильтрации и нажмите кнопку "ОК".

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 диалоге 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" (см. ниже).
Удалить	Нажмите для удаления выбранного правила из группы

Примеры правил фильтрации для сервера доступа

Удаленный доступ

Доступ к ресурсам защищенной сети

Необходимо обеспечить доступ сотрудника с удаленной рабочей станции (абонентский пункт) к ресурсам локальной сети "Защищаемая сеть КШ «КШ с ЦУС»" (IP-адрес 10.1.1.0, ЦУС).

Табл.22 Параметры подсети

Параметр	Значение
Имя	Защищаемая сеть КШ «КШ с ЦУС» (10.1.1.200)
Описание	Защищаемая сеть КШ «КШ с ЦУС»
IP-адрес	10.1.1.0
Маска	255.255.255.0
Защищенная сеть	Да

Табл.23 Параметры правила фильтрации

Параметр	Значение
Имя	Доступ в ЗС КШ с ЦУС
Описание	Разрешение любого трафика от АП в ЗС
Отправитель	Континент-АП
Получатель	Защищаемая сеть КШ «КШ с ЦУС» (10.1.1.200)
Сервис	Любой TCP, любой UDP, любой ICMP
Действие	Пропустить пакет
Протоколирование	Не записывать в журнал
Контроль состояния соединения	Да
Применить и завершить обработку	Нет

ПУ СД: 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.**103**).
2. Составить для пользователя индивидуальный список правил фильтрации (см. стр.**110**).
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:

- На панели переходов основного окна программы выберите ярлык "Учетные записи".

  Список учетных записей пользователей появится в правой части окна.

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.

При регистрации пользователя имеется возможность 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.

Внимание! При регистрации пользователей необходимо учитывать, что количество активных (не заблокированных администратором) учетных записей пользователей, которое может содержаться в базе данных сервера доступа, ограничено зарегистрированными лицензиями на использование сервера доступа. Когда это количество исчерпано, регистрация новых пользователей невозможна, о чем будет свидетельствовать сообщение об ошибке, появляющееся на экране при попытке регистрации нового пользователя.

В этом случае для регистрации новых пользователей нужно приобрести и добавить новые лицензии (см. стр. **95**) либо удалить или заблокировать необходимое количество имеющихся учетных записей (см. стр. **109** и стр. **109**). Сведения о лицензиях, зарегистрированных в базе данных сервера доступа, можно получить в программе управления (см. стр. **95**).

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 диалог "Добавление нового пользователя".

2. Активируйте ссылку "импортируйте сертификат из файла".

   На экране появится стандартный диалог Windows для выбора файлов.

3. Укажите 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 диалога "Добавление нового пользователя" будет отображена регистрационная информация о пользователе, содержащаяся в сертификате.

   При необходимости уточните информацию: внесите изменения в поле "Имя учетной записи" и заполните поле "Описание". 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 перечисленные ниже ограничения учетной записи пользователя и нажмите кнопку "Далее >".

Ограничение по времени работы	Установите отметку, затем нажмите ссылку "Настройка" и в появившемся диалоге установите расписание работы пользователя (см. стр. **110**)
Разрешить множественные подключения	Установите отметку для подключения под данной учетной записью одновременно с нескольких компьютеров
Отключена	Установите отметку для блокировки учетной записи (см. стр. **109**)
Действия по результату проверки наличия ПАК "Соболь"	Укажите действия по результату проверки наличия ПАК "Соболь" на компьютере пользователя (см. стр. **110**)

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 будет 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)

На экране появится диалог добавления пользователю правил фильтрации.

5. Нажмите кнопку "Добавить"

   На экране появится список групп и правил фильтрации.

6. Выберите из списка назначаемые пользователю группы или правила.

   Выбранные правила отобразятся в диалоге добавления правил пользователя.

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

8. Нажмите кнопку "Далее>".

   На экране появится диалог выбора варианта продолжения процедуры:

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

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

   Если необходимо экспортировать только файлы сертификатов, выберите вариант "Экспорт сертификатов" и перейдите к **п. 11**.

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

    Если пользователь был создан в программе управления сервером доступа по имеющимся сведениям, в конфигурационный файл вместе с шаблоном настроек будут также включены все сертификаты и ключевой контейнер сертификата пользователя.

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

    Нажмите кнопку "Далее".

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

    Перейдите к **п. 12**.

11. Укажите каталог, в который будут экспортированы файлы сертификатов, и нажмите кнопку "Далее".

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

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

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

    Внимание! Набор энтропии выполняется один раз в сутки после первого запуска мастера создания пользователя, а также при запуске мастера после перезагрузки компьютера.

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

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

14. 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.

15. Нажмите кнопку "ОК" в окне предупреждения.

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

16. 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. 18**.

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

17. Задайте 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.

18. Нажмите кнопку "Готово".

Процедура регистрации пользователя будет 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 диалог "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 нужные поля в диалоге и перейдите к п. **4**.

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

Появится стандартный диалог выбора файла.

3. Укажите нужный файл запроса.

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

4. При необходимости установите перечисленные ниже ограничения учетной записи пользователя и нажмите кнопку "Далее >".

Ограничение по времени работы	Установите отметку, затем нажмите ссылку "Настройка" и в появившемся диалоге установите расписание работы пользователя (см. стр.**110**)

Разрешить множественные подключения	Установите отметку для подключения под данной учетной записью одновременно с нескольких компьютеров
Отключена	Установите отметку для блокировки учетной записи (см. стр.**109**)
Действия по результату проверки наличия ПАК "Соболь"	Укажите действия по результату проверки наличия ПАК "Соболь" на компьютере пользователя (см. стр.**110**)
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 будет 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)

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.

5. Нажмите кнопку в окне сообщения:

Да	Будет создан новый пользователь
Нет	Пользователю будет добавлен новый сертификат

Окно сообщения закроется.

6. Нажмите кнопку "Далее >".

В диалоге "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".

7. Нажмите кнопку "Далее >".

На экране появится диалог добавления пользователю правил фильтрации.

8. Нажмите кнопку "Добавить"

На экране появится список групп и правил фильтрации.

9. Выберите из списка назначаемые пользователю группы или правила.

Выбранные правила отобразятся в диалоге добавления правил пользователя.

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

11. Нажмите кнопку "Далее >".

На экране появится диалог выбора варианта продолжения процедуры:

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

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

Если необходимо экспортировать только файлы сертификатов, выберите вариант "Экспорт сертификатов" и перейдите к **п. 14**.

13. 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 редактирования шаблона можно указать новое место его хранения. При создании нового шаблона он сохраняется в папке по умолчанию.

Нажмите кнопку "Далее".

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

Перейдите к **п. 15**.

14. Укажите каталог, в который 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.

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

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

Внимание! Набор энтропии выполняется один раз в сутки после первого запуска мастера создания пользователя, а также при запуске мастера после перезагрузки компьютера.

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

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

17. 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.

18. Нажмите кнопку "ОК" в окне предупреждения.

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

19. 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. 21**.

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

20. Задайте 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.

21. Нажмите кнопку "Готово".

Процедура регистрации пользователя будет 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, удаляются из базы данных сервера доступа. После этого установить соединение с сервером под именем этого пользователя невозможно.

Для удаления пользователя (пользователей):

1. 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.

2. Подтвердите удаление выбранного пользователя (пользователей), нажав кнопку "Да".

   Ярлык пользователя (пользователей) будет немедленно 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. Вызовите окно настройки свойств пользователя (см. стр.**109**).
2. В диалоге "Основные" установите отметку в поле "Отключена".
3. Нажмите кнопку "OK".

   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. Вызовите окно настройки свойств пользователя (см. стр.**109**).

   Совет. Пользователей с заблокированной учетной записью можно отличить по пиктограмме  .

2. В диалоге "Основные" удалите отметку из поля "Отключена".
3. Нажмите кнопку "OK".

   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. Вызовите окно настройки свойств пользователя (см. стр.**109**).
2. В диалоге "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 диалог "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" определите 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, а затем с двух часов дня до шести часов вечера, то следует ввести: "9-00–13-00; 14-00–18-00".
   - нажмите кнопку "ОК".
4. Нажмите кнопку "ОК" в окне настройки свойств пользователя.

   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. Вызовите окно настройки свойств пользователя (см. стр.**109**).
2. В диалоге "Основные" в поле "Действие по результату проверки наличия ПАК Соболь" выберите из раскрывающегося списка нужное значение:

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

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.**112**).

Для составления индивидуального списка правил:

1. Вызовите окно настройки свойств пользователя (см. стр.**109**) и перейдите к диалогу "Правила фильтрации".
2. 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.

3. Нажмите кнопку "OK".

Просмотр прав доступа пользователя

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

Для просмотра прав доступа пользователя:

1. Вызовите окно настройки свойств пользователя (см. стр.**109**) и перейдите к диалогу "Подсети".

   Диалог 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.
2. Завершите работу с диалогом, нажав кнопку "OK".

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. **109**) и перейдите к диалогу "Незащищенные соединения".
2. Укажите режим работы абонентского пункта:

Разрешено	Разрешить сторонние соединения
Запрещено	Запретить сторонние соединения

3. 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 удаления выбранной подсети из списка нажмите кнопку "Удалить".

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

Принудительное отключение абонентов

Имеется возможность отключить одного или нескольких абонентов, подключенных под одной учетной записью пользователя.

Для отключения абонента:

1. Выберите нужную учетную запись. В нижней части основного окна появится список абонентов, подключенных под выбранной учетной записью. В контекстном меню нужного абонента активируйте команду "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 запроса.
2. Нажмите кнопку "Да" для подтверждения отключения абонента (или всех абонентов).

   Выбранный абонент или все подключенные 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 какому-либо пользователю доступ к ресурсам защищенной сети, вначале заблокируйте его учетную запись (см. стр. **109**), а затем, если он в данный момент подключен к серверу, отключите его.

ПУ СД: управление сертификатами

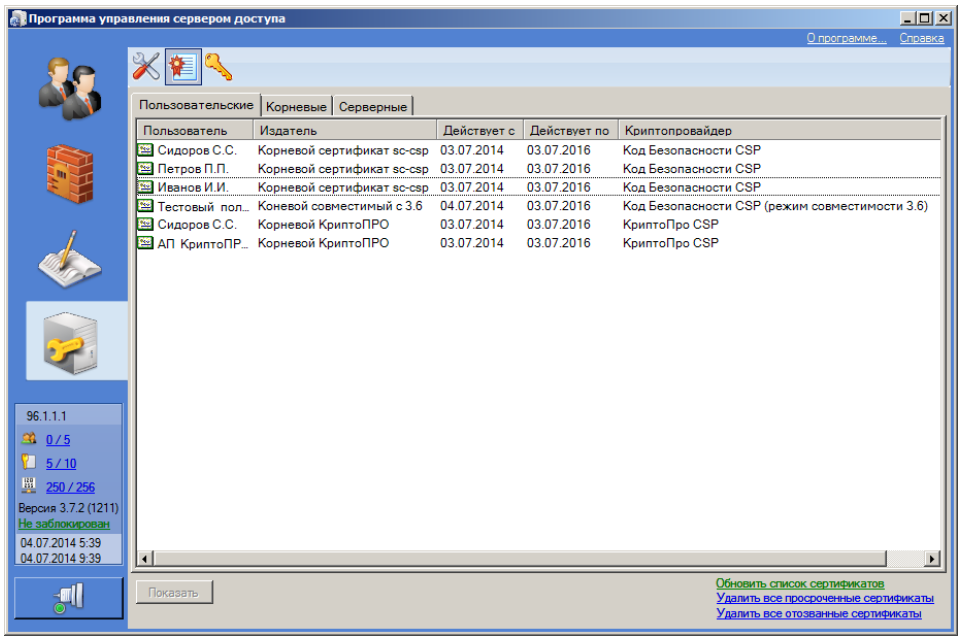
Регистрация корневого сертификата и сертификата сервера доступа обязательна при первом запуске программы управления. Без корневого сертификата невозможна регистрация пользователей, без сертификата сервера доступа невозможно соединение пользователей с сервером.

Управление списками сертификатов

Вызов списков сертификатов

Для вызова списка сертификатов:

1. На панели переходов основного окна выберите ярлык "Настройки сервера", а затем в панели инструментов нажмите кнопку "Сертификаты".



   В информационном окне отобразятся перечни сертификатов, зарегистрированных в системе.

2. Перейдите к вкладке с нужным перечнем сертификатов.

Каждая вкладка содержит в табличном представлении перечень соответствующих 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.114).

Табл.24 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

Поле	Описание
Срок действия	Дата начала и окончания срока действия сертификата
Криптопровайдер	Имя поставщика услуг криптографии

Табл.25 Управляющие элементы списка сертификатов

Управляющий элемент	Описание
Добавить	Выводит на экран стартовый диалог 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

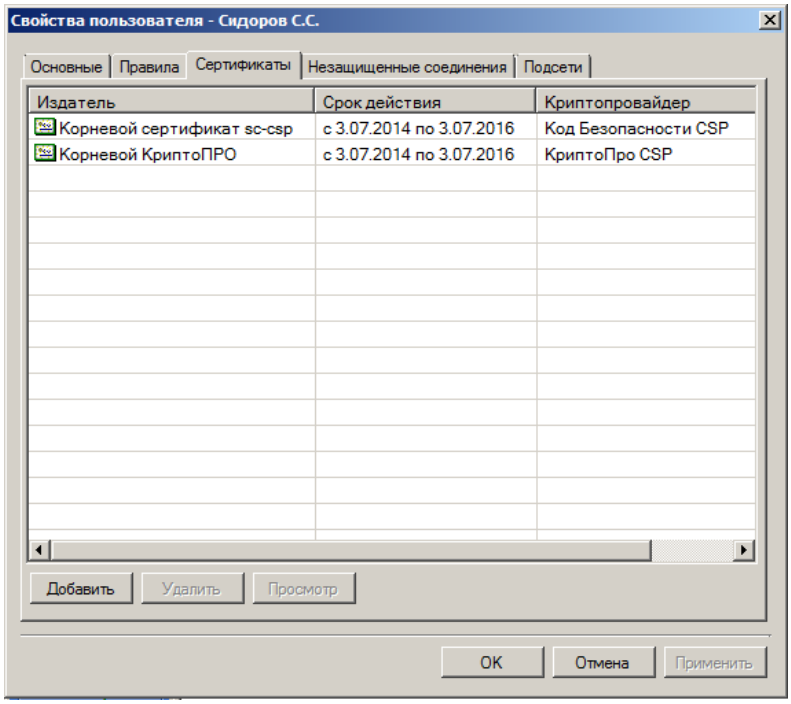
Вызов списка сертификатов пользователя

Для вызова списка сертификатов пользователя:

1. На панели переходов основного окна выберите ярлык "Пользователи".

   В информационном окне отобразится перечень пользователей.

2. Вызовите окно настройки свойств пользователя (см. стр. **109**) командой контекстного меню "Свойства" и перейдите к диалогу "Сертификаты".



Диалог "Сертификаты" содержит в табличном представлении перечень зарегистрированных в системе сертификатов данного пользователя и их характеристики. Описание полей списка сертификатов представлено в Табл.24, управляющих элементов — в Табл.25.

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 (см. таблицу ниже).

Табл.26 Криптопровайдер для создания корневого сертификата

Абонентский пункт		Криптопровайдер для создания корневого сертификата
Криптопровайдер	**Версия АП**	
Код Безопасности CSP	3.6	Код Безопасности CSP (режим совместимости 3.6)
	3.7	Код Безопасности CSP
	4.0	Код Безопасности CSP
КриптоПро CSP	3.5, 3.6 и выше	КриптоПро CSP

Издание корневого сертификата

Для издания корневого сертификата:

1. Вызовите на экран список корневых сертификатов (см. стр.**113**) и нажмите кнопку "Добавить".
2. В появившемся диалоге "Добавление корневого сертификата" выполните следующие действия:
   - Установите отметку в поле "Создать по имеющимся сведениям".
   - В поле "Поставщик услуг криптографии" выберите нужный криптопровайдер (см. Табл.26 на стр.**115**).
   - Укажите сведения, необходимые для издания корневого сертификата.

     Введите в соответствующих полях название сертификата, а также названия организации и подразделения, выдающих корневой сертификат. 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 диалоговое окно криптопровайдера. Необходимо выполнить следующие операции:
   - сформировать закрытый ключ с помощью датчика случайных чисел;
   - выбрать тип ключевого носителя для записи закрытого ключа;
   - ввести пароль для ограничения доступа к ключевому контейнеру.

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

   Порядок действий зависит от используемого криптопровайдера, датчика случайных чисел и ключевого носителя, выбранного для хранения ключевой информации (см. стр.**116**). Следуйте указаниям, появляющимся на экране.

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

   При успешном завершении процедуры в перечне 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. Вызовите на экран список сертификатов сервера доступа (см. стр.**113**) и нажмите кнопку "Добавить".
2. В появившемся диалоге "Добавление сертификата сервера" выполните следующие действия:
   - Установите отметку в поле "По имеющимся сведениям".
   - Укажите сведения, необходимые для издания сертификата сервера.

     Пояснение. Введите в соответствующих полях имя сервера доступа, название организации и подразделения, отвечающего за эксплуатацию сервера. Для продолжения данной процедуры необходимо заполнить все поля этого диалога.
   - 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.
3. Нажмите кнопку "ОК".

   На экране появится запрос на ввод пароля.

   Примечание. Данный диалог не появится, если при издании корневого сертификата была установлена отметка в поле "Запомнить пароль".
4. Введите пароль, которым был ограничен доступ к ключевой информации при издании корневого сертификата (см. стр.**115**), и нажмите кнопку "ОК".

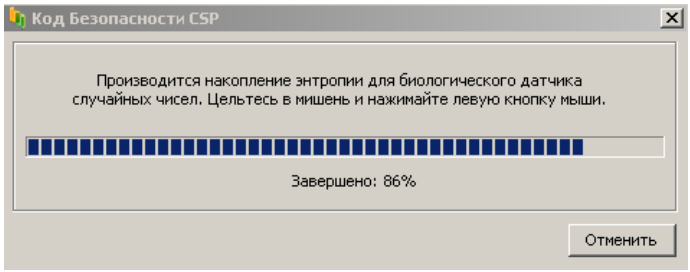
   При успешном чтении закрытого ключа корневого сертификата сертификат сервера доступа заверяется этим ключом и сохраняется в базе данных сервера.

Варианты использования криптопровайдера при формировании закрытого ключа пользователя

Код Безопасности CSP

Для формирования закрытого ключа:

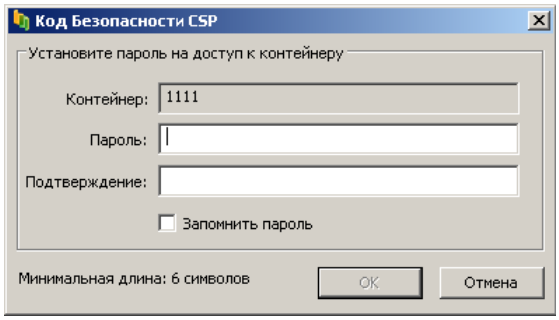
1. После нажатия в окне создания запроса кнопки "ОК" на экране появится окно накопления энтропии для биологического датчика случайных чисел.



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

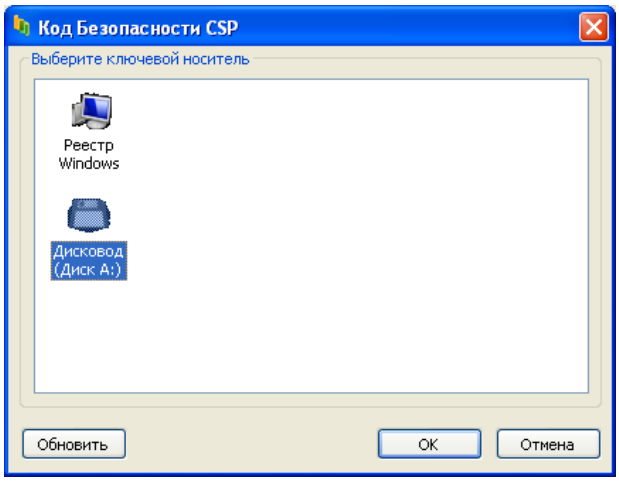
2. Следуйте отображаемой в окне инструкции и дождитесь завершения операции.

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



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

   На экране появится окно выбора ключевого носителя.



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

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

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

АП: Настройка параметров

Вызов меню управления абонентским пунктом

Управление абонентским пунктом выполняется с помощью специального меню.

Для вызова меню управления абонентским пунктом:

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

  На экране появится меню управления абонентским пунктом.

  Внимание! Состав меню, отображаемого на экране, зависит от прав пользователя, вошедшего в систему, и от уровня безопасности, выбранного при установке абонентского пункта (см. стр.**134**).

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

Пиктограмма	Цвет	Пояснение
	Серый	Соединение не установлено
	Зеленый	Соединение установлено

Табл.27 Команды меню управления абонентским пунктом

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

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

Запуск программы управления абонентским пунктом вручную

Для запуска программы управления абонентским пунктом вручную:

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

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

Настройка параметров сетевого подключения

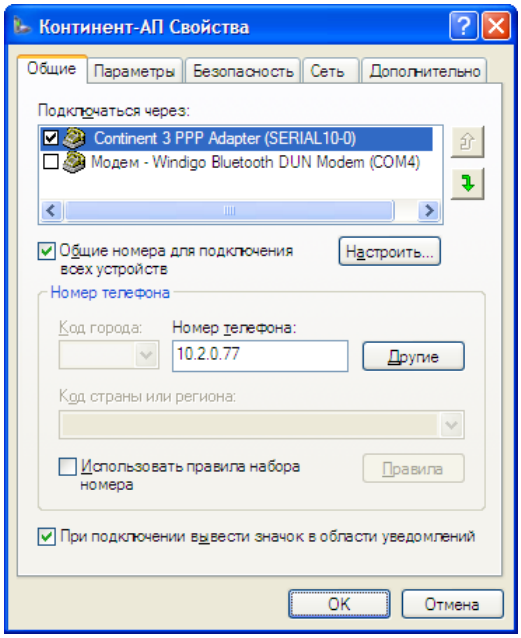
Перед тем как устанавливать соединение с сервером доступа, рекомендуется проверить и при необходимости выполнить настройку параметров сетевого подключения, посредством которого устанавливается соединение.

Примечание. Значения параметров сетевого подключения задаются при установке программного обеспечения абонентского пункта автоматически или при создании нового соединения с применением настроек из конфигурационного файла. При необходимости значения параметров могут быть изменены в соответствии с приведенной ниже процедурой.

Для настройки сетевого подключения:

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

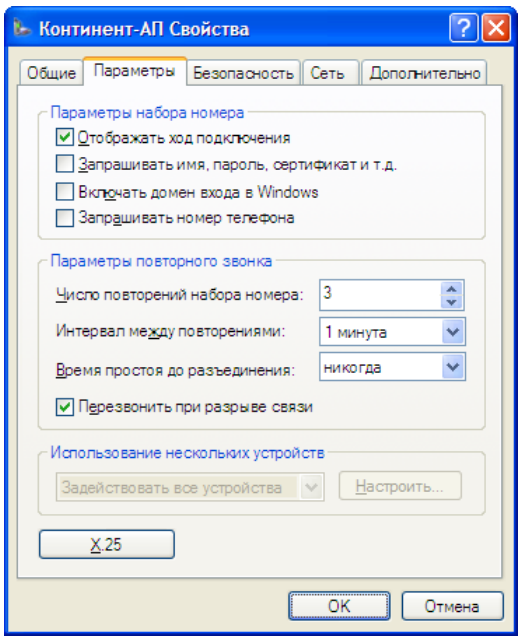
   На экране появится диалог для настройки выбранного сетевого подключения.



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

     Примечания:
     - По умолчанию в поле "Номер телефона" указан IP-адрес (сетевое имя), который был задан при установке абонентского пункта (см. стр. 50). В случае необходимости измените его. IP-адрес (сетевое имя) сервера доступа можно уточнить у администратора.
     - По умолчанию номер порта сервера доступа, на котором ожидается соединение от абонентского пункта, имеет значение 4433. Если в программе управления сервера доступа задан другой номер порта, то заданный номер необходимо указать через двоеточие после сетевого имени или значения IP-адреса. Например, 10.2.0.77:4434.

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

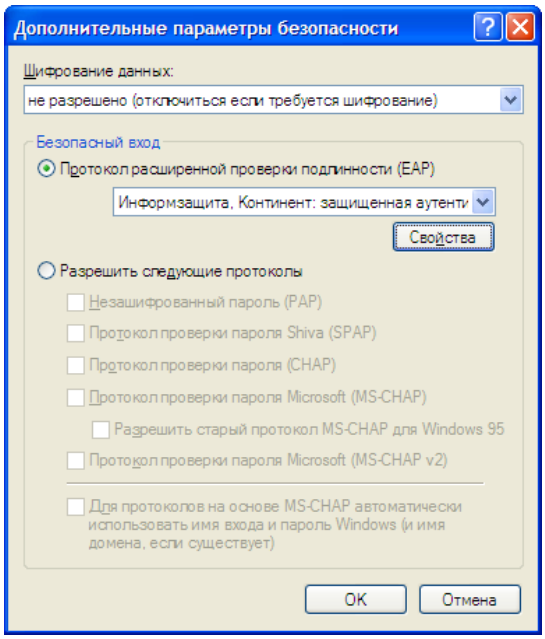


5. Установите отметку в поле "Отображать ход подключения", чтобы процесс соединения с сервером доступа отображался на экране.
6. В группе "Параметры повторного звонка" оставьте значения по умолчанию или укажите нужные значения параметров:

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

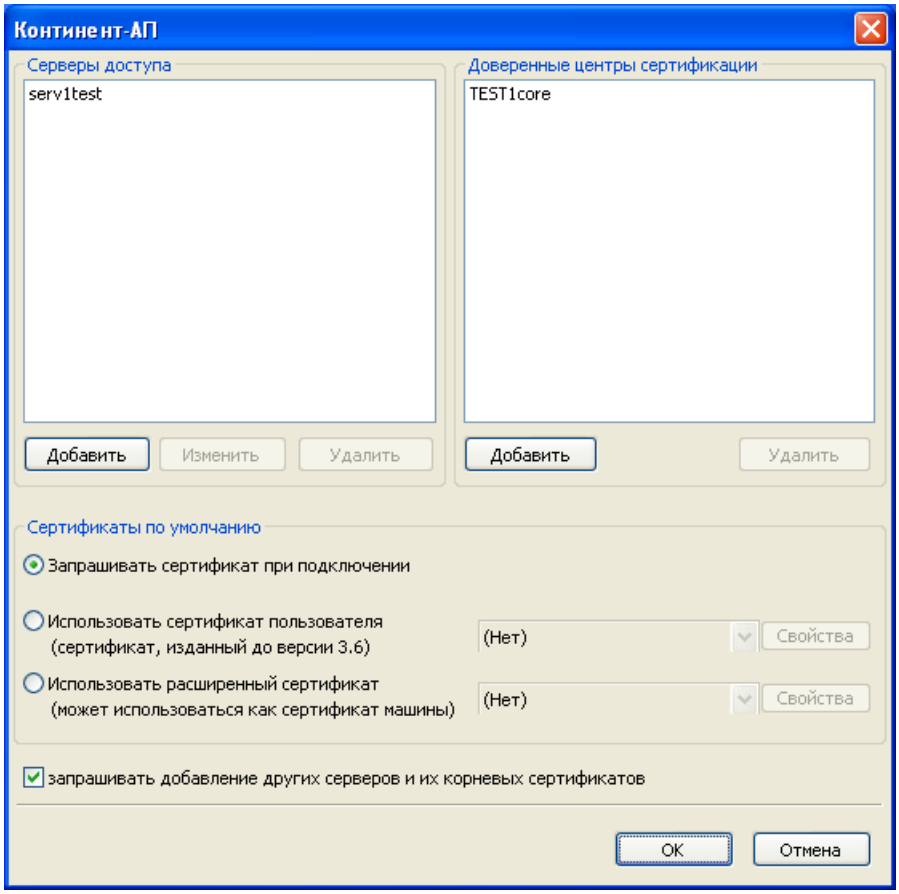
7. Перейдите к вкладке "Безопасность", установите отметку в поле "Дополнительные" и нажмите кнопку "Параметры".

   На экране появится диалог "Дополнительные параметры безопасности".



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

   На экране появится диалог свойств протокола проверки подлинности.



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

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

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

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

Выход из программы управления

При завершении работы программы управления абонентский пункт продолжает свою работу.

Для выхода из программы:

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

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

АП: Управление сертификатами

Получение пользователем сертификатов

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

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

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

Предусмотрены следующие варианты получения пользователем сертификатов:

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

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

  От пользователя в этом случае не требуется никаких предварительных действий;

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

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

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

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

После получения сертификатов пользователь должен выполнить процедуру регистрации сертификатов на компьютере (см. стр.**124**).

Регистрация сертификатов

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

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

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

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

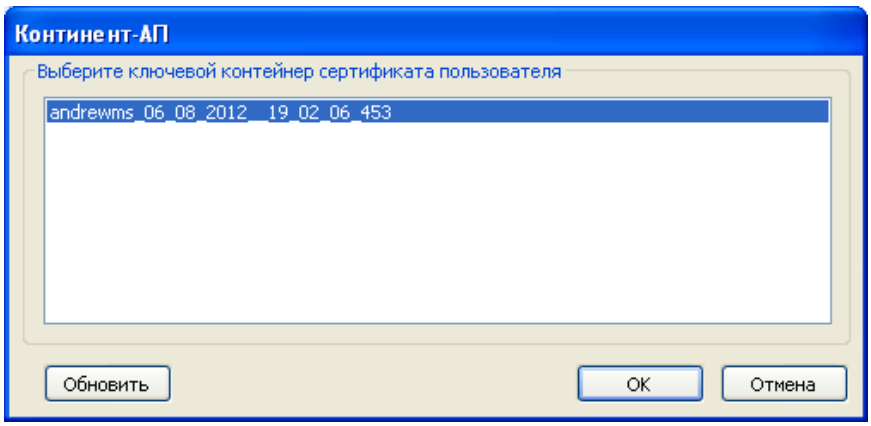
Для регистрации сертификатов:

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

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

   На экране появится диалог выбора ключевого контейнера для чтения закрытого ключа сертификата пользователя.
4. Вставьте в устройство ключевой носитель и нажмите кнопку "Обновить".

   В диалоге появится список ключевых контейнеров.



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

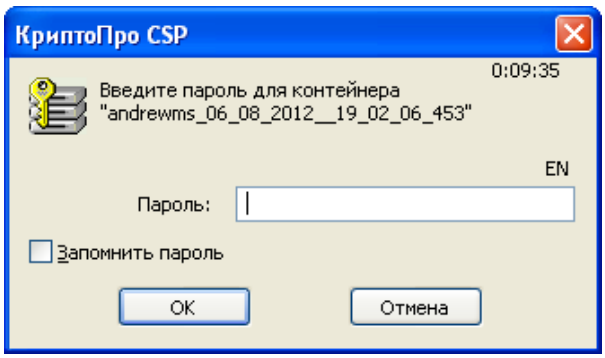
5. Выберите нужный ключевой контейнер и нажмите кнопку "OK".

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

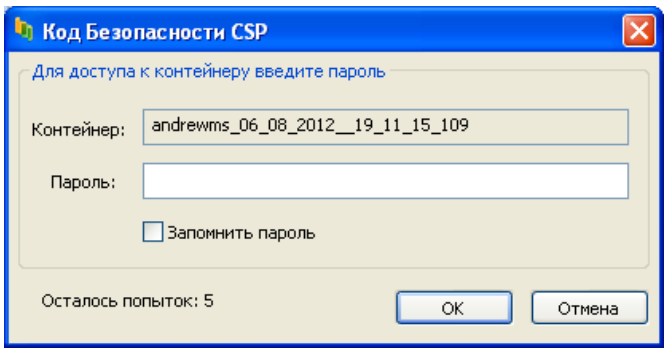
Внимание! Если сертификат должен использоваться как сертификат компьютера, установите отметку в поле "Запомнить PIN".

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

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



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

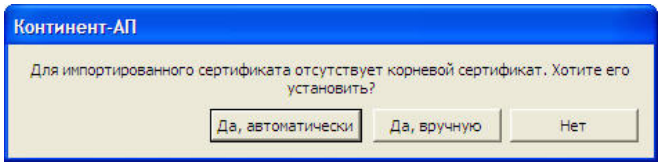


Примечание. При использовании криптопровайдера "Код Безопасности CSP" предусмотрено 5 попыток ввода пароля. После 5-ой неудачной попытки ввода пароля необходимо заново начать процедуру регистрации.

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

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

На экране появится запрос на установку корневого сертификата.



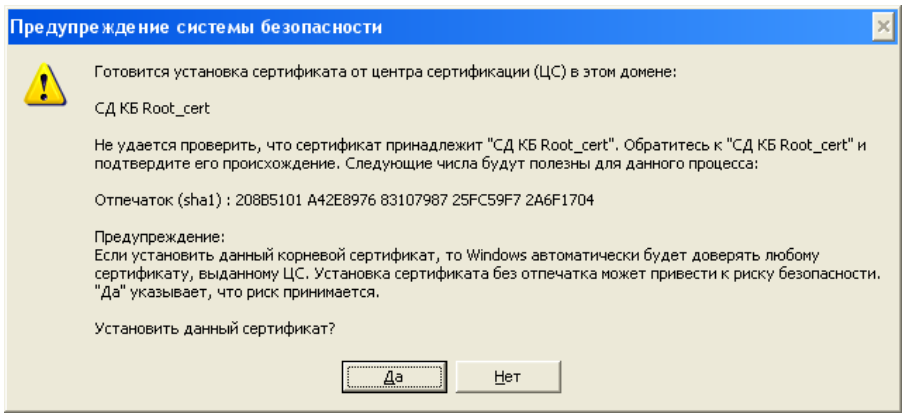
7. Для регистрации корневого сертификата нажмите кнопку:
   - "Да, автоматически" — в случае если корневой сертификат хранится в одной папке с сертификатом пользователя. Будет выполнен автоматический поиск сертификата;

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

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

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

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



8. Нажмите кнопку "Да".

   На экране появится сообщение об успешном завершении импорта пользовательского сертификата.

9. Нажмите кнопку "ОК".

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

АП: Соединение с сервером доступа

Установка соединения с сервером доступа

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

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

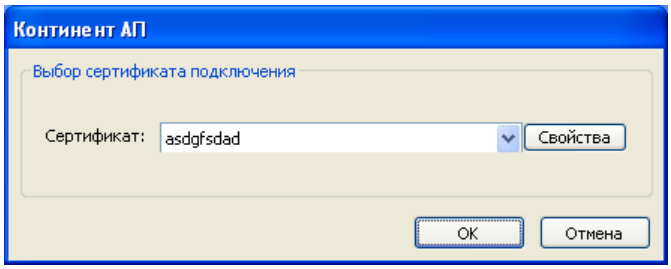
Перед подключением к серверу доступа подсоедините к считывателю ключевой носитель с закрытым ключом пользователя.

Для установки соединения с сервером доступа:

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

   На экране появится диалог выбора сертификата.

   Внимание! Данный диалог появляется только в том случае, если при выборе режима аутентификации указано значение "Запрашивать сертификат при подключении".



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

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

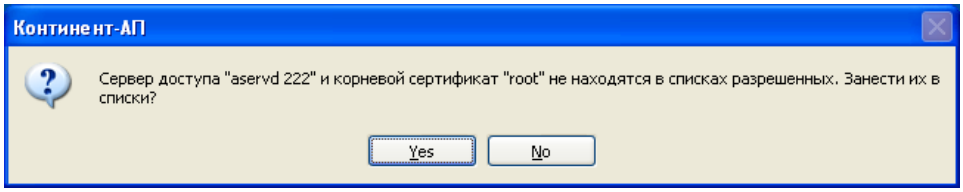
   Нажмите кнопку "OK".

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

   Примечание. Появление системных сообщений зависит от настроек абонентского пункта.

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

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



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

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

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

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

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

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

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

Примечание. Если ранее при вводе пароля доступа к данному ключевому контейнеру было отмечено поле "Запомнить пароль" (см. стр. 124), то этот диалог на экране не появится. Начнется подключение к серверу доступа.

Срок действия пароля криптопровайдера "Код Безопасности CSP" 180 дней. Если этот срок истек, то на экране появится сообщение с предложением сменить пароль, в противном случае соединение с сервером доступа установлено не будет. Для смены пароля выполняйте указания, появляющиеся на экране.

5. Заполните поля диалога:

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

6. Нажмите кнопку "OK".

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

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

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

параметров подключения абонентских пунктов и в настройках свойств пользователя (параметр "Разрешенный канал связи с СД").

Разрыв соединения с сервером доступа

Для разрыва соединения с сервером доступа:

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

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

Приложение

Аппаратное тестирование сетевого устройства

Аппаратное тестирование может выполняться в процессе установки ПО сетевого устройства, в ходе инициализации, а также при настройке параметров средствами локального управления сетевым устройством.

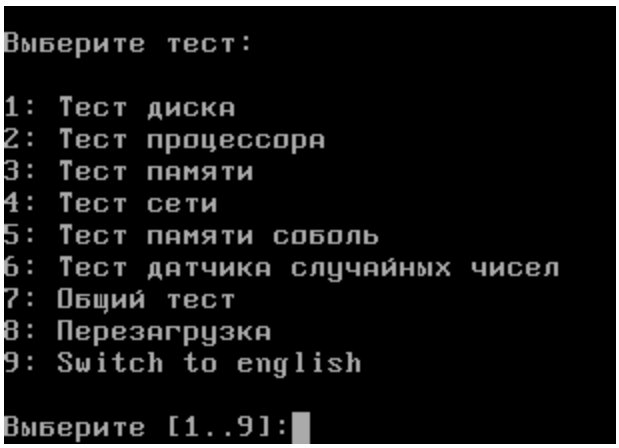
Для аппаратного тестирования применяется набор тестов, с помощью которых проверяются:

- жесткий диск;
- процессор;
- оперативная память;
- память ПАК "Соболь";
- датчик случайных чисел ПАК "Соболь";
- сетевые интерфейсы.

Для запуска теста:

1. Введите в главном локальном меню номер команды "Тестирование" и нажмите клавишу <Enter>.

   На экране появится меню выбора теста.



   - Команда "Перезагрузка" используется для выхода из режима тестирования и продолжения процедуры установки ПО. В режиме инициализации сетевого устройства команда имеет вид: "Выход".
   - Команда "Switch to english" используется для отображения данного меню на английском языке. При отображении меню на английском языке команда имеет вид: "Переключиться на русский". В режиме инициализации сетевого устройства команда не используется.

2. Введите номер команды требуемого теста и нажмите клавишу <Enter>.

   В зависимости от выбранного теста на экране появятся инструкции по выполнению дополнительных действий для проведения теста.

Тест	Описание
Тест диска	Проверка наличия сбойных секторов жесткого диска
Тест процессора	Проверка работы процессора. Необходимо задать время тестирования – от 1 до 99 минут
Тест памяти	Проверка оперативной памяти
Тест сети	Проверка работы сетевых интерфейсов. Перед запуском теста необходимо присоединить сетевые интерфейсы к общему коммутатору и соединить оптические интерфейсы в пары

Тест	Описание
Тест памяти "Соболь"	Тестирование памяти ПАК "Соболь" на чтение и запись
Тест датчика случайных чисел	Проверка работоспособности датчика случайных чисел ПАК "Соболь"
Общий тест	Последовательное выполнение всех перечисленных выше тестов с предварительным выполнением соответствующих дополнительных действий

3. Дождитесь сообщения о завершении теста и нажмите клавишу <Enter>.

   Будет выполнен возврат в меню выбора теста.
4. Для выхода из режима тестирования введите номер команды "Перезагрузка" и нажмите клавишу <Enter>.

Протоколы и порты

В данном разделе представлены сведения о протоколах и портах, используемых для связи между компонентами комплекса.

Если на пути зашифрованного трафика находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать для них правила, разрешающие прохождение служебных пакетов комплекса по протоколам и портам, указанным в таблице (см..список сокращений).

Протокол/порт	Описание	Источник/получатель	Примечание
TCP/443	Обмен сообщениями между СД и АП. При включенном на АП режиме защищенного соединения "Потоковое подключение (TCP)" или "Подключение через прокси-сервер"	АП / СД. СД / АП	АПКШ "Континент" 3.7
TCP/4431, 49152-65535	Обмен сообщениями между СД и ПУ СД. ПУ СД устанавливает подключение со случайного порта из диапазона 49152-65535 к СД на порт 4431. СД отвечает с порта 4431 на тот порт компьютера с ПУ СД, с которого пришло подключение	ПУ СД / СД. СД / ПУ СД	АПКШ "Континент" 3.2.21 и более поздние версии
TCP/4444	Передача сообщений от ПУ ЦУС к ЦУС; обмен сообщениями между ЦУС и агентом ЦУС; обмен сообщениями между агентом обновлений БРП и ЦУС. ПУ ЦУС, Агент ЦУС и СД, Агент обновлений БРП, Агент РКН устанавливают подключение со случайного порта 1024-65535 на порт ЦУС 4444. ЦУС отвечает на тот порт, с которого было обращение	ПУ ЦУС / ЦУС. Агент ЦУС и СД / ЦУС. ЦУС / агент ЦУС и СД. Агент обновления БРП / ЦУС	

Протокол/порт	Описание	Источник/получатель	Примечание
TCP/4445	Передача обновлений ПО от ПУ ЦУС к ЦУС и обмен сообщениями между ПУ ЦУС и агентом ЦУС. ПУ ЦУС устанавливает подключение со случайного порта 1024-65535 на порт ЦУС 4445. ЦУС отвечает на тот порт, с которого было обращение	ПУ ЦУС / ЦУС. ПУ ЦУС / агент ЦУС и СД. Агент ЦУС и СД / ПУ ЦУС	АПКШ "Континент" 3.1.18 и более поздние версии
TCP/4446	Аутентификация пользователей в защищенном сегменте сети. Клиент аутентификации устанавливает подключение со случайного порта 1024-65535 на порт ЦУС 4446. ЦУС отвечает на тот порт, с которого было обращение	Компьютер с установленной программой "Клиент аутентификации пользователя" / СУ	АПКШ "Континент" 3.6 и более поздние версии
TCP/5100	Передача сообщений от ЦУС к СУ и обмен сообщениями между СУ в кластере. Узел кластера обращается к парному с порта 10000-65535 на порт 5100. Парный отвечает на тот порт, с которого было обращение	ЦУС / СУ. Основное СУ / резервное СУ. Резервное СУ / основное СУ	АПКШ "Континент" 3.0 и более поздние версии
TCP/5101	Передача сообщений от СУ к ЦУС. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУСа 5101. ЦУС отвечает на тот порт, с которого было обращение	СУ / ЦУС	АПКШ "Континент" 3.0 и более поздние версии
TCP/5102	Передача файлов от ЦУС к СУ. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5102. ЦУС отвечает на тот порт, с которого было обращение	ЦУС / СУ	АПКШ Континент версии 3.5 АПКШ "Континент" 3.5
TCP/5103	Передача файлов от ЦУС к СУ. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУСа 5103. ЦУС отвечает на тот порт, с которого было обращение	ЦУС / СУ	АПКШ "Континент" 3.6 и более поздние версии
UDP/5101	Передача сообщений от СУ к ЦУС. Узел обращается с порта 5100 на порт ЦУСа 5101. ЦУС отвечает с порта 5101 на порт 5100	СУ (исходящий порт 5100) / ЦУС	АПКШ "Континент" 3.0 и более поздние версии

Протокол/ порт	Описание	Источник/получатель	Примечание
UDP/5106 UDP/5107	Поддержка работы СУ за NAT. В зависимости от используемых классов трафика, узлы отправляют пакеты с портов 10000-10031 на порты ЦУС 5106-5107	СУ / ЦУС	АПКШ "Континент" 3.6 и более поздние версии
UDP/5557	Передача сообщений об активности между СУ в кластере. Узлы кластера обмениваются пакетами с порта 5557 на порт 5557	ОсновноеСУ / резервное СУ. Резервное СУ / основное СУ	АПКШ "Континент" 3.0 и более поздние версии
UDP/4433	Обмен сообщениями между СД и АП. Номер порта по умолчанию; изменяется в программе управления СД	АП / сервер доступа	АПКШ "Континент" 3.2.21 и более поздние версии
UDP/7500	Обмен сообщениями между СД и АП. Номер порта по умолчанию; изменяется в настройках виртуального адаптера Continent 3 PPP Adapter	Сервер доступа / АП	АПКШ "Континент" 3.2.21 и более поздние версии
UDP/10000	Передача зашифрованного трафика. Узлы обмениваются пакетами с порта 10000 на порт 10000	СУ / СУ. СУ / ЦУС	АПКШ "Континент" 3.5
UDP/10000-10031	Передача зашифрованного трафика. В зависимости от используемых классов трафика, узлы обмениваются пакетами с портов 10000-31 на соответствующие порты 10000-31	СУ / СУ. СУ / ЦУС	АПКШ "Континент" 3.6 и более поздние версии

Пример конфигурационного файла

Ниже приведен пример файла конфигурационных настроек, используемого при установке ПО абонентского пункта.

```
[config]
version=3.7
vpn=1
firewall=1
upd_state=0
upd_path=
[vpn]
defcsp=90
kclevel=1
conns_num=1
[connection#0]
name=Континент АП
ip=172.17.7.101
addunksrv=1
depend=
idmode=0
lastid=W7_Aviales_06062015_1959.cer
calist=172.17.6.191_25032015_2059.cer,root_172.17.7.101_
06062015_1959.cer,root_172.17.7.101_31052015_1959.cer
sdlist=srv172.17.6.191,srv_172.17.7.101
userproxy=0
proxyaddress=0.0.0.0
proxyport=0
proxyauthtype=None
proxyuser=
proxypassword=
default=1
[firewall]
notify=0
log_user=log_user.txt
log_appl=log_appl.txt
adm_
login=hex:7849f6369eeae40cb31b9cadcaea7fb01bfa093305e02d32360-
b16d67aa46826
adm_
pass=hex:071a2f3162a5913613ac885c56e5883cf2506a292aed015ef16f-
a94bc84b135b
user_
pass=hex:071a2f3162a5913613ac885c56e5883cf2506a292aed015ef16f-
a94bc84b135b
rules_base=pass:udp port 67;pass:udp port 68;
rules_user=pass :tcp port 80;pass :tcp port 3389;pass :udp
port 445;sched=2 log :icmp;log :tcp dst host
192.168.170.100:; pass:;
rules_appl=pass::;
rules_sched=1 daily 11:30-12:45;2 daily 9:00-17:00;3 daily
8:45-18:00;
```

Разделение прав пользователей и администраторов АП

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

Функция АП	Пользователь	Администратор
Создание, удаление, изменение соединения с СД	Нет	Да
Создание личного запроса на сертификат и ключевого контейнера	Да	Да

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

Пункт меню АП	**Пользователь**	**Администратор**
Подключить <Название соединения>	Да	Да
Выбор соединения по умолчанию	Да	Да
Выбор криптопровайдера по умолчанию	Да	Да
Установить/Разорвать соединение	Да	Да
Создать новое соединение	Нет	Да
Удалить соединение	Нет	Да
Настройка соединения	Нет	Да
Настройка аутентификации	Нет	Да
Настройка зависимости между соединениями	Нет	Да
Журнал	Нет	Да
Сертификаты/Создать запрос на пользовательский сертификат	Да	Да
Сертификаты/Установить сертификат пользователя	Да	Да
Загружать автоматически	Нет	Да
Настройка автоматического обновления	Нет	Да
Справка	Да	Да
О программе	Да	Да
Выход	Да	Да

Программные модули, требующие контроля целостности

Компьютер, на который устанавливают компоненты подсистемы управления, должен содержать средства, обеспечивающие контроль целостности программного обеспечения (например ПАК "Соболь"). В данном разделе представлен перечень программных модулей, требующих контроля целостности. Программные модули находятся в папке, указанной на шаге 2 установки программы управления или агента. В таблице указывается папка, предлагаемая мастером установки по умолчанию.

Табл.28 Программные модули программы управления ЦУС

Имя	Папка
Configurator.exe	\Program Files\Код Безопасности\Континент\RCP Agent
RCPAgent.exe	\Program Files\Код Безопасности\Континент\RCP Agent
RCPTray.exe	\Program Files\Код Безопасности\Континент\RCP Agent
RCPSupport.dll	\Program Files\Код Безопасности\Континент\RCP Agent
MailSender.dll	\Program Files\Код Безопасности\Континент\RCP Agent
uc.dll	\Program Files\Код Безопасности\Континент\RCP Agent
XmlDocument.dll	\Program Files\Код Безопасности\Континент\RCP Agent
DbHelperMSSQL.dll	\Program Files\Код Безопасности\Континент\RCP Agent
DbHelperOracle.dll	\Program Files\Код Безопасности\Континент\RCP Agent

Табл.29 Программа просмотра отчетов ЦУС

Имя	Папка
DbWrapper.dll	\Program Files\Код Безопасности\Континент\Report Viewer
Interop.KEY_APICLib.dll	\Program Files\Код Безопасности\Континент\Report Viewer
IPAddressControlLib.dll	\Program Files\Код Безопасности\Континент\Report Viewer
ReportViewer.exe	\Program Files\Код Безопасности\Континент\Report Viewer
RfcCryptoLib.dll	\Program Files\Код Безопасности\Континент\Report Viewer

Табл.30 Программа управления ЦУС (ПУ ЦУС и ППЖ)

Имя	Папка
LogViewer.exe	\Program Files\Код Безопасности\Континент\RCP
LogViewer.chm	\Program Files\Код Безопасности\Континент\RCP
Rcp.exe	\Program Files\Код Безопасности\Континент\RCP
Rcp.chm	\Program Files\Код Безопасности\Континент\RCP
KeyClusterCreator.exe	\Program Files\Код Безопасности\Континент\RCP
OneLookFeatRes.dll	\Program Files\Код Безопасности\Континент\RCP
RCPAgentTuning.dll	\Program Files\Код Безопасности\Континент\RCP
DbHelperMSSQL.dll	\Program Files\Код Безопасности\Континент\RCP
DbHelperOracle.dll	\Program Files\Код Безопасности\Континент\RCP
uc.dll	\Program Files\Код Безопасности\Континент\RCP
XmlDocument.dll	\Program Files\Код Безопасности\Континент\RCP

Табл.31 Программа управления сервером доступа

Имя	Папка
RCAS3.exe	\Program Files\Код Безопасности\Континент\RCAS
CryptoWrapper.dll	\Program Files\Код Безопасности\Континент\RCAS
Interop.KEY_APICLib.dll	\Program Files\Код Безопасности\Континент\RCAS
IPAddressControlLib.dll	\Program Files\Код Безопасности\Континент\RCAS
sd_keys_new.dll	\Program Files\Код Безопасности\Континент\RCAS
Infragistics2.Shared.v6.2.dll	\Program Files\Код Безопасности\Континент\RCAS
Infragistics2.Shared.v6.2.xml	\Program Files\Код Безопасности\Континент\RCAS
Infragistics2.Win.UltraWinEditors.v6.2.dll	\Program Files\Код Безопасности\Континент\RCAS
Infragistics2.Win.UltraWinEditors.v6.2.xml	\Program Files\Код Безопасности\Континент\RCAS
Infragistics2.Win.UltraWinListView.v6.2.dll	\Program Files\Код Безопасности\Континент\RCAS
Infragistics2.Win.UltraWinListView.v6.2.xml	\Program Files\Код Безопасности\Континент\RCAS
Infragistics2.Win.v6.2.dll	\Program Files\Код Безопасности\Континент\RCAS
Infragistics2.Win.v6.2.xml	\Program Files\Код Безопасности\Континент\RCAS

Табл.32 Вспомогательные модули программы управления

Имя	Папка
ASKeyDuplicator.exe	\Program Files\Код Безопасности\Континент\KeyDuplicator
etsdk.dll	\Program Files\Код Безопасности\Континент\Hardware
ikey.dll	\Program Files\Код Безопасности\Континент\Hardware
SneToken.dll	\Program Files\Код Безопасности\Континент\Hardware
SnHwAPIExp.dll	\Program Files\Код Безопасности\Континент\Hardware
snhwapiexp.ini	\Program Files\Код Безопасности\Континент\Hardware
SnRuToken.dll	\Program Files\Код Безопасности\Континент\Hardware
SnEtokenEx.dll	\Program Files\Код Безопасности\Континент\Hardware
SnSable.dll	\Program Files\Код Безопасности\Континент\Hardware
SnEtokenSC.dll	\Program Files\Код Безопасности\Континент\Hardware
SniKey.dll	\Program Files\Код Безопасности\Континент\Hardware
SnTmCard.dll	\Program Files\Код Безопасности\Континент\Hardware
KEY_APIC.exe	\Program Files\Код Безопасности\Континент\Hardware
cspservice.exe	\Program Files\Код Безопасности\Континент\CSP
csp_uninst.exe	\Program Files\Код Безопасности\Континент\CSP

Имя	Папка
etsdk.dll - на Windows x86 etsdkx64.dll - на Windows x64	\Program Files\Код Безопасности\Континент\CSP
ikey.dll	\Program Files\Код Безопасности\Континент\CSP
SneToken.dll	\Program Files\Код Безопасности\Континент\CSP
SnEtokenEx.dll	\Program Files\Код Безопасности\Континент\CSP
SnEtokenSC.dll	\Program Files\Код Безопасности\Континент\CSP
SnHwAPIExp.dll	\Program Files\Код Безопасности\Континент\CSP
SnHwApiExp.ini	\Program Files\Код Безопасности\Континент\CSP
SniKey.dll	\Program Files\Код Безопасности\Континент\CSP
SnRuToken.dll	\Program Files\Код Безопасности\Континент\CSP
SnSable.dll	\Program Files\Код Безопасности\Континент\CSP
SnTmCard.dll	\Program Files\Код Безопасности\Континент\CSP

Табл.33 Общие модули Windows

Имя	Папка
Windows XP (32 бит), Windows 2003 Server (32 бит)	
boot.ini	%System Drive%
ntdetect.com	%System Drive%
ntldr	%System Drive%
acgenral.dll	%System Drive%\windows\apppatch
explorer.exe	%System Drive%\windows
*.sys, *.dll, *.exe	%System Drive%\windows\system32 и все вложенные папки
Windows Vista (32 бит), Windows 2008 Server (32 бит), Windows 7 (32 бит), Windows 8 (32 бит)	
*.sys, *.dll, *.exe	%System Drive%\windows\system32 и все вложенные папки
.	%Boot Drive%\boot или %System Drive%\windows\boot и все вложенные папки
bootmgr	%Boot Drive% или %System Drive%\windows\boot\PCAT
Windows 2003 Server (64 бит)	
boot.ini	%System Drive%
ntdetect.com	%System Drive%
ntldr	%System Drive%
acgenral.dll	%System Drive%\windows\apppatch
explorer.exe	%System Drive%\windows
*.sys, *.dll, *.exe	%System Drive%\windows\system32 и все вложенные папки
*.sys, *.dll, *.exe	%System Drive%\windows\sysWOW64 и все вложенные папки
Windows Vista (64 бит), Windows 2008 Server (64 бит), Windows 7 (64 бит), Windows 8 (64 бит)	
*.sys, *.dll, *.exe	%System Drive%\windows\system32 и все вложенные папки
.	%Boot Drive%\boot или %System Drive%\windows\boot и все вложенные папки
*.sys, *.dll, *.exe	%System Drive%\windows\sysWOW64 и все вложенные папки

Имя	Папка
bootmgr	%Boot Drive% или %System Drive%\windows\boot\PCAT

Табл.34 Элементы системного реестра Windows на ПК с установленной ПУ ЦУС

Ключ	Ветка реестра
RestrictAnonymous AuditBaseObjects FullPrivilegeAuditing	HKLM\System\CurrentControlSet\Control\LSA
CachedLogonsCount	HKLM\Software\Microsoft\WindowsNT\CurrentVersion\-Winlogon
RestrictGuestAccess	HKLM\System\CurrentControlSet\Services\Eventlog\<LogName> (LogName – имя журнала, для которого следует ограничить доступ пользователям группы Everyone)
ClearPageFileAtShutDown	HKLM\System\CurrentControlSet\Control\SessionManager\Memory Managment
Все ключи (включая вложенные ветки)	HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg\
EnablePlainTextPassword (только для Windows XP/2000)	HKLM\SYSTEM\CurrentControlSet\Services\MRxSmb\Parameters
EnableSecuritySignature RequareSecuritySignatureAutoShareWks AutoShareServerNullSessionPipes	HKLM\System\CurrentControlSet\Services\LanManServer\Parameters
Shell Userinit VmApplet UIHost (только для Windows XP)	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Все ключи	HKEY_LOCAL_MACHINE\SYSTEM\Select
Ключи Start из всех подразделов ветви	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services

Документация

1.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Централизованное управление комплексом
2.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Локальное управление сетевыми устройствами
3.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аудит
4.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аутентификация пользователя
5.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Сервер доступа
6.	Аппаратно-программный комплекс шифрования "Континент". Руководство пользователя. Программа мониторинга КШ
7.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Тестирование каналов связи
8.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Обновление программного обеспечения
9.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Автоматизированное рабочее место генерации ключей
10.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Система обнаружения вторжений

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