



Код безопасности

Аппаратно-программный комплекс шифрования

Континент

Версия 3.7



Руководство администратора

Централизованное управление комплексом



Код безопасности

© Компания "Код Безопасности", 2016. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

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

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

Почтовый адрес: **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	7
Введение	8
Общие сведения	9
Назначение комплекса	9
Состав комплекса	9
Основные технические характеристики	11
Принципы функционирования комплекса	11
Структура защищенной корпоративной сети	11
Обработка IP-пакетов	16
Управление криптографическими ключами	20
Аутентификация пользователей	22
Обеспечение отказоустойчивости комплекса	23
Централизованное управление сетевыми устройствами	25
Связь между КШ, управляемыми разными ЦУС	25
Контроль сетевых устройств по протоколу SNMP	25
Multicast-вещание	25
Автоматическая настройка сетевых параметров	26
Поддержка QoS	26
Поддержка IPv6	28
Организация сетей L2VPN	28
Защитные механизмы	28
Лицензирование	29
Требования к сетевым коммуникациям	29
Требования к квалификации персонала	29
Ввод комплекса в эксплуатацию	31
Порядок ввода комплекса в эксплуатацию	31
Особенности при обновлении ПО комплекса	31
Установка подсистемы управления	32
Состав и варианты размещения подсистемы управления	32
Требования к оборудованию и программному обеспечению	32
Установка компонентов подсистемы управления	34
Постановка на контроль программных модулей, подлежащих контролю целостности	37
Запуск подсистемы управления	37
Запуск программы управления ЦУС	37
Запуск агента	38
Запись конфигурации и ключей сетевого устройства на носитель	39
Запись конфигурации сетевого устройства на носитель	39
Запись ключей сетевого устройства на носитель	39
Программа управления ЦУС	41
Запуск программы	41
Интерфейс программы	41
Главное окно	41
Настройка интерфейса	43
Управление таблицами	43
Управление группами	45
Настройка программы	46
Настройка параметров соединения с ЦУС	46
Настройка параметров соединения с агентом	46
Управление лицензиями ЦУС	47
Выход из программы	47
Переустановка, исправление и удаление программы управления	47
Изменение списка установленных компонентов	47
Исправление программы управления	48
Удаление программы управления	48
Настройка комплекса	49

Организация работы администраторов комплекса	50
Управление учетными записями администраторов	50
Настройка политики аутентификации администраторов	51
Смена административного ключа	52
Копирование административного ключа	52
Централизованное управление сетевыми устройствами	54
Регистрация нового сетевого устройства	54
Ввод сетевого устройства в эксплуатацию и вывод из эксплуатации	54
Удаление сетевого устройства	55
Перезагрузка сетевого устройства	55
Выключение сетевого устройства	56
Обновление конфигурации сетевого устройства	56
Миграция на новую аппаратную платформу	56
Просмотр сведений о сетевом устройстве	56
Обновление программного обеспечения сетевого устройства	57
Удаление последнего обновления с жесткого диска ЦУС	57
Копирование файла обновления на жесткий диск ЦУС	57
Загрузка файла обновления на сетевое устройство	58
Применение файла обновления на сетевом устройстве	58
Настройка общих параметров сетевого устройства	58
Настройка интерфейсов	60
Сетевые интерфейсы	60
Изменение внешнего адреса сетевого устройства	61
Изменение внешнего адреса ЦУС	62
Модемное подключение и поддержка PPPoE	63
Подключение модема Huawei 3372h	64
VLAN-интерфейсы	66
Настройка VoIP	67
Настройка гигабитного соединения	68
Настройка Multi-WAN	68
Формирование перечня каналов связи и выбор режима	69
Настройка свойств канала связи	69
Обеспечение отказоустойчивости канала связи	70
Балансировка трафика между внешними интерфейсами сетевого устройства	73
Настройка правила распределения трафика	74
Выключение режима Multi-WAN	74
Настройки сервиса DHCP	74
Вызов окна настройки сервиса DHCP	75
Включение и настройка режима сервера	75
Включение и настройка ретранслятора	76
Отключение сервиса DHCP	76
Просмотр статистики сервера DHCP	77
Настройка параметров хранения журналов	77
Управление списком связанных сетевых устройств	78
Настройка параметров маршрутизации	79
Переход к настройке параметров	79
Переключение режима маршрутизации	79
Статическая маршрутизация	80
Динамическая маршрутизация	81
Определение классов трафика	82
Управление приоритизацией трафика	83
Вызов окна управления QoS	83
Настройка общих параметров очереди на интерфейсе	83
Настройка параметров очереди	84
Экспорт/импорт конфигурации очередей	85
Управление очередью заданий	85
Режим изолированной сети	86
Установка времени на ЦУС	87
Управление криптографической коммутируемой сетью	89

Управление пользователями	94
Управление списком пользователей	94
Настройка параметров учетной записи	95
Настройка параметров группы пользователей	95
Правила фильтрации IP-пакетов и правила трансляции сетевых адресов	97
О правилах и элементах правил	97
Управление элементами правил	98
Сетевой объект	98
Сервис	100
Временной интервал	102
Правила фильтрации	104
Управление списком правил фильтрации	104
Регулярные выражения	107
Настройка параметров правила фильтрации	112
Регистрация IP-пакетов	114
Настройка режима защиты от DoS-атак	114
Очистка таблицы состояния соединений	115
Усиленная фильтрация	115
Предварительные настройки	116
Профили усиленной фильтрации	118
Агенты усиленной фильтрации	121
Включение профиля в правило фильтрации	123
Контроль приложений	125
Профили контроля приложений	125
Включение профиля контроля приложений в правило фильтрации	127
Фильтрация пакетов по информации от системы обнаружения вторжений	127
Настройка параметров детектора атак	127
Динамические правила фильтрации	129
Правила трансляции сетевых адресов	129
Управление списком правил трансляции	129
Настройка параметров правила трансляции	130
Пример использования правила трансляции	132
Запрет доступа к ресурсам единого реестра Роскомнадзора	134
Загрузка сведений о запрещенных ресурсах	134
Виртуальная адресация	135
Управление криптографическими ключами	137
Изменение режима управления ключами	137
Базовая схема управления ключами	137
Общий порядок смены ключей	137
Генерация резервного ключевого материала	138
Смена ключей сетевого устройства с использованием резервного ключевого материала	139
Смена ключей парной связи	139
Внеплановая смена ключей сетевого устройства	140
Усиленная схема управления ключами	141
Порядок и схема распространения ключей	141
Вызов мастера управления ключами	142
Назначение комплектов ключей сетевым устройствам	144
Загрузка и активация ключей в ЦУС	146
Отправка комплектов новых ключей на узлы	148
Экспорт комплектов ключей	149
Удаление комплектов ключей	149
Просмотр текущего распределения ключей	152
Организация связи со сторонними криптографическими сетями	154
Общий порядок организации связи	154
Инфраструктура открытых ключей	154
Управление внешними сетями	156
Управление межсетевыми ключами	158
Агент Роскомнадзора	160

Установка агента	160
Программа управления агентом Роскомнадзора	161
Команды управления агентом Роскомнадзора	161
Настройка параметров агента	161
Запуск агента	162
Сообщения об ошибках	163
Мониторинг и оперативное управление	164
Мониторинг состояния комплекса	164
Общая таблица состояния компонентов комплекса	164
Отчеты о состоянии проблемных компонентов	165
Средства оповещения о событиях	166
Настройка реакции на события	167
Оперативное управление комплексом	169
Обеспечение отказоустойчивости комплекса	171
Резервное копирование и восстановление конфигурации ЦУС	171
Резервное копирование конфигурации ЦУС	171
Восстановление конфигурации ЦУС из резервной копии	172
Управление кластером	173
Условия функционирования кластера	173
Создание кластера	174
Настройка параметров резервирования	176
Добавление и удаление дополнительных интерфейсов резервирования	176
Изменение адреса на интерфейсах резервирования	177
Определение состояния кластера	177
Переключение канала связи в кластере	177
Выключение режима резервирования	178
Нештатные ситуации при работе кластера	178
Восстановление работы кластера после ремонта основного устройства	179
Приложение	180
Протоколы и порты	180
Инициализация ПАК "Соболь" перед установкой ПУ ЦУС	182
Права администраторов на управление комплексом	185
Модуль поддержки SNMP	186
Формат и примеры конфигурационных файлов	189
Формат конфигурационного файла	189
Примеры конфигурационных файлов	190
Примеры правил фильтрации	191
Метасимволы в регулярных выражениях	201
Примеры правил трансляции	202
Примеры использования VLAN в защищенных сетях	207
Пример использования групповой адресации в защищенных сетях	208
Пример использования фермы КШ для увеличения пропускной способности VPN-канала	210
Диагностика сетевого устройства	212
Программные модули, требующие контроля целостности	213
Сохранение базы данных ЦУС	217
Документация	218

Список сокращений

DCOM	Distributed Component Object Model
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
PPPoE	Point to Point Protocol over Ethernet
RAS	Remote Access Service
RPC	Remote Procedure Call
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VID	VLAN Identifier
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
АПКШ	Аппаратно-программный комплекс шифрования
АРМ	Автоматизированное рабочее место
АРМ ГК	Автоматизированное рабочее место генерации ключей
БД	База данных
ДА	Детектор (компьютерных) атак
ДСЧ	Датчик случайных чисел
КК	Криптографический коммутатор
КШ	Криптографический шлюз
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПУ	Программа управления
СД	Сервер доступа
СКЗИ	Средство криптографической защиты информации
СОВ	Система обнаружения вторжений (компьютерных атак)
СУ	Сетевое устройство (КШ, КК, ДА)
СУБД	Система управления базами данных
ЦУС	Центр управления сетью криптографических шлюзов
ЭЦП	Электронная цифровая подпись

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 ввода комплекса в эксплуатацию, централизованного управления сетевыми устройствами, а также для локального управления отдельными компонентами комплекса.

Специализированные сведения по администрированию комплекса содержатся также в [2] и [3].

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).

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

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

Общие сведения

Назначение комплекса

Современный уровень развития сетевых технологий сделал возможным появление и широкое распространение виртуальных частных сетей (Virtual Private Network — VPN). Технология VPN позволяет объединить локальные вычислительные сети (ЛВС), их сегменты или отдельные компьютеры предприятия в единую защищенную виртуальную сеть на базе общих сетей передачи данных. Переход от распределенной корпоративной сети на базе выделенных каналов к VPN позволяет существенно снизить эксплуатационные расходы. Однако использование общих сетей для организации VPN предъявляет дополнительные требования к обеспечению надежной защиты информационных ресурсов предприятия от несанкционированного доступа (НСД).

Комплекс предназначен для построения виртуальных частных сетей (VPN) на основе общих сетей передачи данных, использующих протоколы семейства TCP/IP.

Комплекс реализует следующие основные функции:

- криптографическая защита данных, передаваемых по каналам связи общих сетей передачи данных между составными частями VPN;
- межсетевое экранирование;
- скрывание внутренней структуры локальных вычислительных сетей;
- автоматическая регистрация событий, связанных с функционированием комплекса, в том числе событий НСД;
- централизованное управление компонентами комплекса.

Комплекс предназначен для работы в сетях, использующих для передачи данных протоколы семейства TCP/IP версии 4, а также в общих сетях передачи данных, поддерживающих протоколы IPv6.

Состав комплекса

Комплекс включает в свой состав следующие компоненты:

- криптографический шлюз;
- центр управления сетью;
- сервер доступа;
- детектор компьютерных атак;
- криптокоммутатор;
- программа управления комплексом;
- автоматизированное рабочее место генерации ключей;
- клиент аутентификации пользователя.

Криптографический шлюз представляет собой аппаратно-программное средство на базе компьютера с архитектурой x86, x64.

Имеются следующие варианты исполнения криптографического шлюза:

- криптографический шлюз;
- криптографический коммутатор;
- детектор атак.

Криптографический шлюз в варианте исполнения "Криптографический шлюз" обеспечивает:

- криптографическую защиту данных, передаваемых по каналам связи общих сетей передачи данных между составными частями VPN (локальными вычислительными сетями и отдельными компьютерами удаленных пользователей);

- защиту составных частей VPN от несанкционированного доступа (НСД) посредством межсетевого экранирования.

Криптографический шлюз в варианте исполнения "Криптографический коммутатор" обеспечивает защищенную передачу Ethernet-кадров (L2) через сети общего пользования между территориально разделенными сегментами сети предприятия с использованием шифрованных (L3) VPN-туннелей Континент (L2VPN).

Криптографический шлюз в варианте исполнения "Детектор атак" обеспечивает анализ сетевого трафика и обнаружение сетевых атак сигнатурным методом.

Криптографический шлюз функционирует совместно с предустановленным изделием "Программно-аппаратный комплекс "Соболь". Версия 3.0" (далее — ПАК "Соболь").

Криптографический коммутатор представляет собой аппаратно-программное средство на базе компьютеров платформ x86, x64.

Криптографический коммутатор обеспечивает криптографическую защиту данных, передаваемых по каналам связи общих сетей передачи данных между удаленными (разрозненными) сегментами одной подсети предприятия.

Центр управления сетью представляет собой предварительно устанавливаемое на одном из КШ программное средство, обеспечивающее централизованное управление работой всех сетевых устройств комплекса.

Примечание. В эксплуатационной документации термином ЦУС обозначается как программное обеспечение, устанавливаемое на одном из КШ, так и КШ с установленным программным обеспечением ЦУС.

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

Детектор компьютерных атак представляет собой программное средство, предварительно установленное на специализированной аппаратной платформе. Детектор атак обеспечивает обнаружение следующих основных угроз безопасности информации:

- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;
- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

Программа управления комплексом представляет собой программное средство, устанавливаемое на одном или нескольких компьютерах (рабочих местах администратора), которые находятся в той же сети, что и КШ с ЦУС.

Программа управления обеспечивает централизованное управление настройками и оперативный контроль состояния всех компонентов комплекса и соединений удаленных пользователей.

В состав ПУ комплексом входят:

- ПУ сетью, предназначенная для управления и мониторинга сетевых устройств;
- ПУ сервером доступа;
- агент БРП;
- агент Роскомнадзора;
- агент ЦУС и сервера доступа, необходимый для обработки регистрационных журналов на сервере баз данных.

Примечание. В эксплуатационной документации и пользовательском интерфейсе программа управления комплексом именуется подсистемой управления, а ПУ сетью — программой управления ЦУС или ПУ.

Автоматизированное рабочее место генерации ключей (АРМ ГК) предназначено для генерации главных ключей КШ и ключей связи с ЦУС при использовании усиленной схемы распределения ключей. АРМ ГК представляет собой системный блок с установленным ПО под управлением ОС FreeBSD на аппаратной платформе IPC- 10. Сгенерированные комплекты ключей записываются на отчуждаемые носители с целью дальнейшего распространения по сети.

Клиент аутентификации пользователя представляет собой устанавливаемое на компьютерах, находящихся в защищенном сегменте сети, программное средство, обеспечивающее идентификацию и аутентификацию пользователей, зарегистрированных в ПУ сетью.

Основные технические характеристики

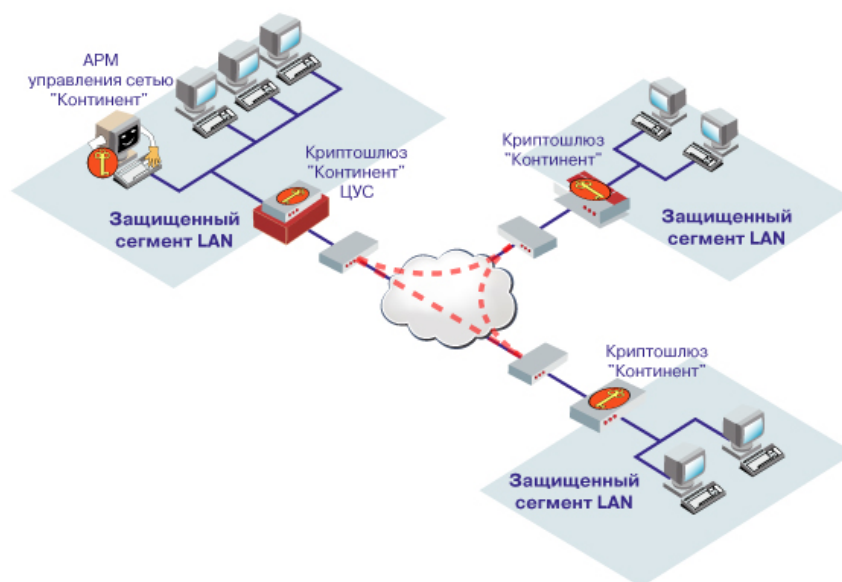
Технические характеристики приведены для комплекса в стандартной комплектации.

Алгоритм шифрования	ГОСТ 28147-89 режим гаммирования с обратной связью
Длина ключа, бит	256
Защита передаваемых данных от искажения	ГОСТ 28147-89 режим имитовставки
Фильтрация IP-пакетов	В соответствии с задаваемыми правилами фильтрации
Увеличение размера пакета с учетом дополнительного IP-заголовка, байт, не более	52
Максимальное количество КШ в сети с одним ЦУС	5000
Максимальное количество сетевых интерфейсов у одного КШ	34
Максимальное количество портов у одного виртуального криптографического коммутатора	16
Аутентификация пользователей при подключении к межсетевому экрану на КШ	По идентификатору и паролю, некриптографическим способом
Максимальное количество КШ в кластере высокой доступности	2
Количество записей в таблице состояния соединений:	
• IPC-10	3000
• IPC-25	7000
• IPC-100	250000
• IPC-400	350000
• IPC-1000	1000000
• IPC-3000	1500000
• Неопределенная	50000
Режим работы	Непрерывная работа в необслуживаемом режиме

Принципы функционирования комплекса

Структура защищенной корпоративной сети

На рисунке представлена структура защищенной корпоративной сети, состоящей из нескольких локальных вычислительных сетей (ЛВС).



Связь между данными ЛВС осуществляется по каналам связи общих сетей передачи данных. К общим сетям каждая ЛВС подключена через криптографический шлюз. Подключение ЛВС через криптографический шлюз обеспечивает скрытие внутренней структуры защищаемого сегмента сети. При этом IP-адреса компьютеров в защищаемых сегментах должны быть уникальными только в рамках данной корпоративной сети. Криптографический шлюз может содержать несколько сетевых интерфейсов, к которым можно подключить несколько независимых локальных сетей.

При подключении компьютеров к криптографическому шлюзу может осуществляться их аутентификация.

Предусмотрена поддержка виртуальных локальных сетей (VLAN), организованных в защищенных сегментах сети.

При отсутствии прямого доступа к сети передачи данных предусмотрена возможность подключения криптографического шлюза к телефонной коммутируемой или выделенной линии с помощью модема (см. стр. 15).

Криптографический шлюз осуществляет маршрутизацию проходящего через него трафика IP-пакетов, поэтому дополнительный маршрутизатор в общем случае не требуется.

При необходимости использования дополнительного маршрутизатора он может быть размещен как перед криптографическим шлюзом (в защищаемом сегменте сети), так и после (вне защищаемого сегмента сети). Если маршрутизатор находится в защищаемом сегменте сети, никаких дополнительных действий по защите маршрутизатора не требуется.

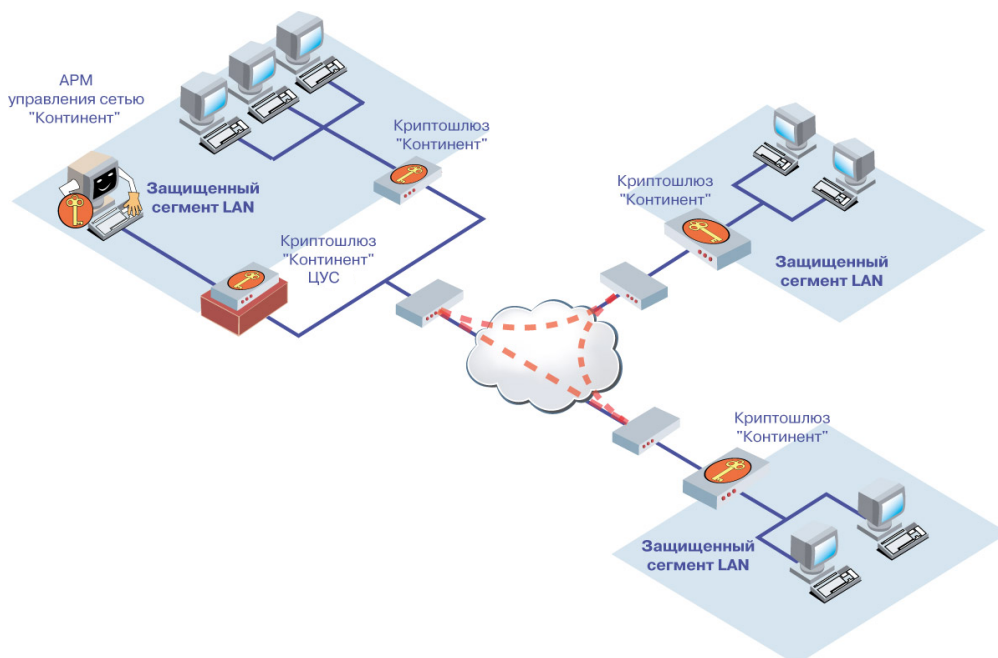
Если же маршрутизатор находится вне защищаемого сегмента сети, то предусмотрена возможность защищенного управления маршрутизатором (см. стр. 15).

Кроме маршрутизации трафика криптографический шлюз осуществляет обработку входящих и исходящих IP-пакетов: фильтрацию и криптографическое преобразование данных, передаваемых по общим каналам связи. Для организации доступа пользователей корпоративной сети к узлам общей сети используется механизм трансляции сетевых адресов (Network Address Translation — NAT).

Автоматическое управление криптографическими шлюзами осуществляет ЦУС, размещающийся на одном из криптографических шлюзов. Этот криптографический шлюз можно использовать как любой другой рядовой шлюз в корпоративной сети для приема и передачи IP-пакетов, их фильтрации, маршрутизации и криптографического преобразования.

Администратор комплекса управляет криптографическими шлюзами через ЦУС с помощью программы управления. Программа управления устанавливается на выделенном компьютере, входящем в состав защищаемого сегмента корпоративной сети (АРМ управления сетью КШ).

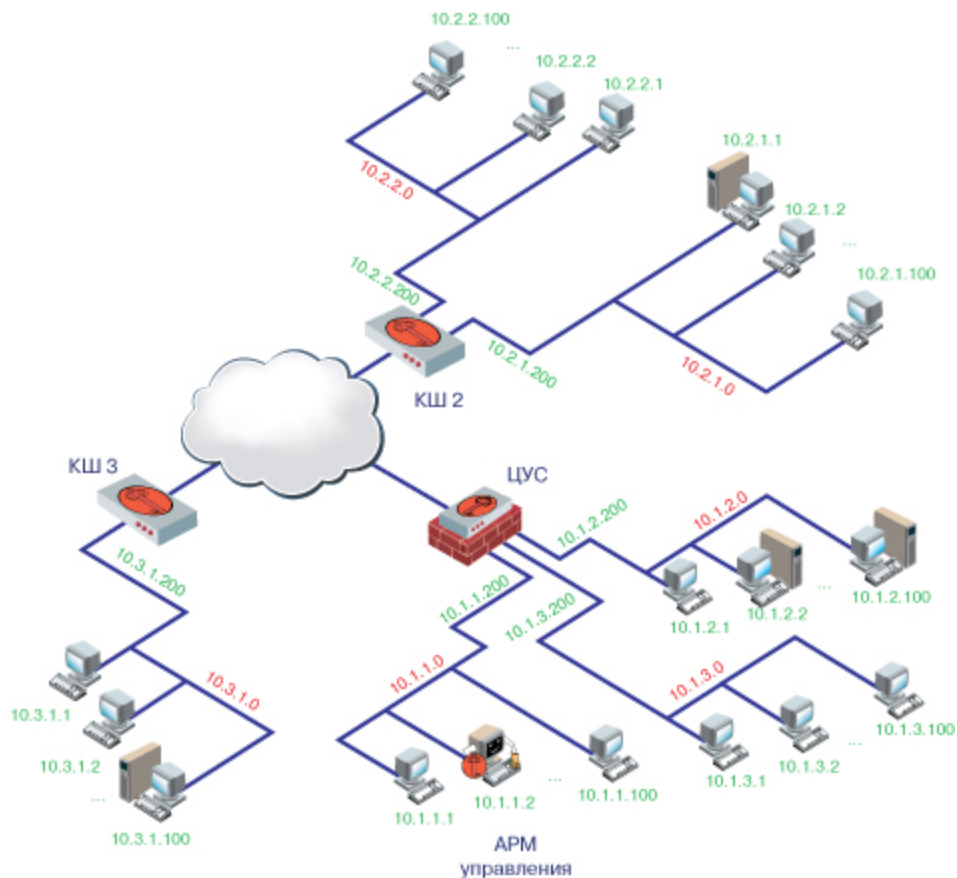
Представленный выше вариант использования комплекса применим только для небольших сетей (2–5 КШ). При использовании в комплексе более пяти КШ рекомендуется ЦУС и АРМ управления сетью КШ вынести в отдельный защищаемый сегмент (см. рисунок ниже). В этом случае ЦУС используется только для управления сетью КШ.



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. [180](#).

Пример организации защищенной корпоративной сети

Ниже на рисунке представлен пример организации защищенной корпоративной сети, объединяющей локальные сети центрального офиса и двух филиалов. Криптографический шлюз центрального офиса КШ 1 (ЦУС) защищает три локальные сети, криптографические шлюзы филиалов КШ 2 и КШ 3 — две и одну соответственно.



Взаимодействие с сетевыми устройствами, поддерживающими NAT

Обеспечена совместная работа криптографических шлюзов с сетевыми устройствами, поддерживающими трансляцию сетевых адресов (NAT). Имеется ограничение: на пути трафика между двумя КШ не должно быть более одного сетевого устройства с поддержкой динамической трансляции адресов. Криптографический шлюз, на который установлен ЦУС, должен всегда иметь публичный адрес.

Подключение КШ к нескольким внешним сетям (Multi-WAN)

Криптографический шлюз может быть одновременно подключен к нескольким внешним сетям (например, принадлежащим разным провайдерам). Имеются следующие режимы Multi-WAN:

- передача трафика в соответствии с таблицей маршрутизации;
- обеспечение отказоустойчивости канала связи;
- балансировка трафика между внешними интерфейсами КШ.

Криптографический шлюз может функционировать только в одном из выбранных режимов.

Режим "Передача трафика в соответствии с таблицей маршрутизации" предоставляет возможность администратору контролировать внешние каналы связи при использовании статической маршрутизации.

В режиме "Обеспечение отказоустойчивости канала связи" КШ при выходе из строя основного канала связи автоматически переключается на резервный. Статус канала (основной или резервный) определяется назначенным ему приоритетом (см. стр. 70). Обратное переключение осуществляется после восстановления работоспособности основного канала в соответствии с выбранным алгоритмом:

- немедленно;
- через указанное время;

- после завершения всех активных соединений.

В режиме "Балансировка трафика между внешними интерфейсами КШ" исходящий трафик автоматически распределяется в соответствии с указанными правилами (см. стр. 73). Одному классу трафика соответствует одно правило.

В системном журнале регистрируются следующие события:

- переключение каналов;
- изменение состояния неактивного канала.

Примечание. В режиме Multi-WAN в качестве каналов связи между криптошлюзами могут использоваться выделенные каналы, исключающие пересечение между собой и с сетями общего пользования (Internet и пр.).

Подключение КШ к телефонной коммутируемой или выделенной линии

Подключение КШ к телефонной коммутируемой или выделенной линии осуществляют с помощью модема. Модем к криптографическому шлюзу подключают через COM-порт или USB-разъем. Подключение КШ с помощью модема возможно только к внешней сети.

Выбор варианта подключения к внешней сети осуществляют при регистрации КШ. Изменение варианта подключения возможно только с последующей инициализацией КШ.

Примечание. У ЦУС возможность модемного подключения отсутствует.

При подключении к коммутируемой линии соединение устанавливается автоматически при поступлении на КШ IP-пакета, предназначенного для отправки через внешний интерфейс. При подключении к выделенной линии соединение устанавливается автоматически при включении КШ. Имеется возможность установки модемного соединения с КШ по инициативе сервера удаленного доступа (RAS). Для этого у сервера должен быть включен режим дозвона по запросу (demand-dial). См. [2].

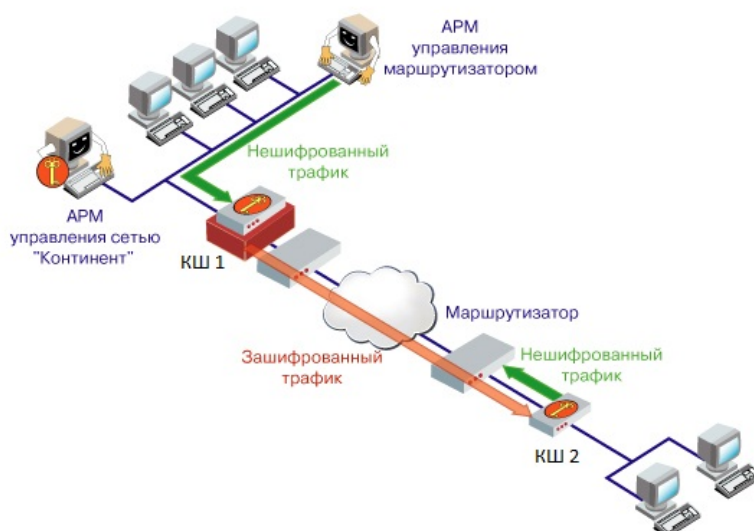
Управление настройками модемного подключения может осуществляться как централизованно из программы управления, так и локально на КШ. Настройки модемного подключения, выполненные локально, в программе управления не отображаются.

Для подключения КШ к внешним сетям с помощью xDSL-сервисов предусмотрена поддержка PPPoE (Point-to-point protocol over Ethernet).

Защищенное управление маршрутизатором

Защищенное управление маршрутизатором, размещенным после криптографического шлюза (вне защищаемого сегмента сети), организуется следующим образом (см. рисунок ниже):

- на криптографическом шлюзе КШ 2 определяют защищенную сеть из одного маршрутизатора;
- на криптографических шлюзах КШ 1 и КШ 2 создают правила фильтрации, разрешающие прохождение управляющего трафика;
- на маршрутизаторе добавляют правило маршрутизации для отсылки IP-пакетов к консоли управления через криптографический шлюз КШ 2.

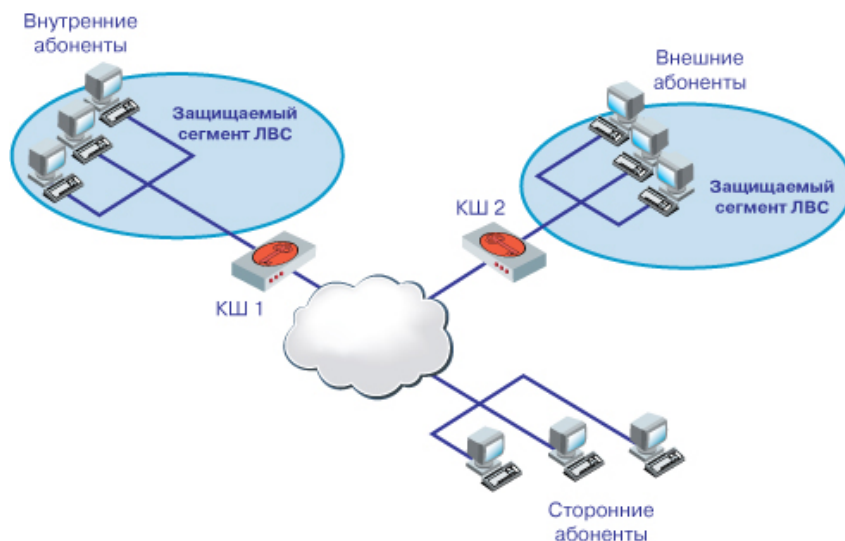


Таким образом, исходный управляющий трафик от консоли управления зашифровывается криптографическим шлюзом КШ 1 и по общей сети передается в зашифованном виде на КШ 2. Криптографический шлюз КШ 2 расшифровывает трафик и передает его в открытом виде на маршрутизатор. IP-пакеты, отсылаемые маршрутизатором к консоли управления, идут тем же путем в обратном порядке.

Защищенное управление маршрутизатором возможно только при прямом подключении КШ 2 к общим сетям. Защищенное управление маршрутизатором при подключении КШ 2 через модем не поддерживается.

Обработка IP-пакетов

Обработка IP-пакетов осуществляется криптографическими шлюзами. Режим обработки зависит от статуса абонента сети по отношению к данному криптографическому шлюзу (см. рисунок).



Абонент — любой компьютер, отправляющий и получающий IP- пакеты. Абоненты IP- сети классифицируются следующим образом (на рисунке — по отношению к КШ 1):

- внутренний абонент, если он входит в состав сегмента сети, защищаемого данным КШ;
- внешний абонент, если он относится к сегменту сети, защищаемому любым другим (отличным от данного) КШ комплекса;

- сторонний абонент — любой абонент IP-сети, не входящий в состав защищаемых сегментов.

Фильтр IP-пакетов

Все IP-пакеты, проходящие через криптографический шлюз, подвергаются фильтрации. Каждый КШ имеет два фильтра. Фильтрация выполняется дважды, до и после обработки IP-пакетов блоком криптографической защиты.

Фильтрация IP- пакетов осуществляется в соответствии с правилами, сформированными на основе IP- адресов отправителя и получателя, названия протокола, номеров портов UDP/TCP и имен сетевых интерфейсов. Проверяются также время, факт аутентификации (для защищаемого сегмента), а при фильтрации прикладных протоколов — содержимое пакетов. По умолчанию прохождение любого IP- пакета запрещено, если это не разрешено явно соответствующим правилом фильтрации.

Правила фильтрации IP-пакетов подразделяются на два типа:

- правила, сформированные комплексом автоматически;
- правила, заданные администратором.

Автоматическое формирование правил фильтрации для данного КШ осуществляется при инициализации ЦУС и КШ. Правила этого типа не отображаются на экране и не могут быть удалены или изменены администратором.

Правила, сформированные комплексом автоматически, разрешают соединения:

- ЦУС с программой управления и агентом;
- ЦУС с зарегистрированными сетевыми устройствами;
- основного и резервного КШ.

Для всех остальных соединений в рамках корпоративной сети правила фильтрации формирует администратор.

Кроме того, администратор может сформировать правила фильтрации для разрешения незашифрованных соединений со сторонними абонентами (веб-сайтами, ftp-серверами).

Внимание! При разрешении незашифрованных соединений общий уровень защищенности корпоративной сети снижается, поэтому для обеспечения максимального уровня защиты информации рекомендуется отказаться от разрешения таких соединений.

Имеется функция автоматической оптимизации правил фильтрации. Оптимизация позволяет уменьшить количество правил фильтрации, загружаемых на сетевое устройство.

Оптимизации подлежат однотипные правила, отличающиеся только отправителями и получателями. Отправители и получатели, указанные в таких правилах, автоматически объединяются в соответствующие группы. Для этих групп создается единое правило.

Группы, созданные для оптимизации, отображаются в технологических отчетах под именем `ipset<порядковый номер группы>`.

Созданные при оптимизации правила фильтрации отображаются в консоли локального компьютера в списке загруженных. В общем списке правил фильтрации в программе управления такие правила не отображаются.

При общем количестве групп более 1000 оптимизацию включать не рекомендуется. Также не рекомендуется включать оптимизацию при наличии групп с количеством элементов более 200000. При превышении указанных значений (групп или элементов в группе) оптимизация автоматически отключается.

Существуют два режима работы фильтра: основной и мягкий. При основном режиме работы фильтра IP- пакеты, прохождение которых запрещено, отбрасываются с регистрацией этого события в журнале НСД. При мягком режиме такие пакеты только регистрируются в журнале НСД, но пропускаются фильтром. Мягкий режим предназначен для настройки криптографического шлюза при вводе его в эксплуатацию.

Если пакет не удовлетворяет установленным правилам фильтрации, он отвергается без уведомления отправителя.

Запрет доступа к ресурсам единого реестра Роскомнадзора

С помощью правил фильтрации, сформированных администратором, может быть реализован автоматический запрет на доступ к ресурсам, включенным Роскомнадзором в единый реестр.

Сведения, содержащиеся в едином реестре Роскомнадзора, позволяют идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено.

Информацию о запрещенных ресурсах получают на сайте Роскомнадзора в виде выгрузки из единого реестра, включающей в себя IP-адреса запрещенных сайтов, и затем средствами программы управления ЦУС помещают в БД ЦУС. При этом предусмотрено автоматическое получение выгрузки и запись ее в БД ЦУС с помощью специального агента, входящего в состав подсистемы управления комплексом.

В программе управления ЦУС IP-адреса запрещенных сайтов, хранящиеся в БД ЦУС, отображаются как группа сетевых объектов с именем "Реестр запрещенных ресурсов".

Для установления запрета на доступ к запрещенным ресурсам администратор должен создать правило фильтрации и в качестве адреса получателя (или отправителя) указать группу сетевых объектов "Реестр запрещенных ресурсов". На КШ, для которого было создано данное правило, фильтрация пакетов будет осуществляться только по IP-адресам указанной группы, т.е. по IP-адресам запрещенных сайтов.

При наличии агента, обеспечивающего получение выгрузки с сайта Роскомнадзора и запись ее в БД ЦУС, поддерживается автоматическое обновление списка запрещенных ресурсов.

Блок криптографической защиты

IP-пакет, успешно прошедший фильтр IP-пакетов, поступает на обработку блоком криптографической защиты.

Если IP-пакет поступил от внутренних абонентов защищаемого сегмента, блок криптографической защиты обеспечивает его сжатие, шифрование и имитозащиту.

Для сжатия IP-пакетов используется алгоритм сжатия deflate. Предусмотрена возможность выбора степени сжатия, а также отключения этого режима.

Применение сжатия позволяет увеличить скорость передачи IP-пакетов по низкоскоростным каналам связи. Так, при пропускной способности линии 64 Кбит/с скорость передачи IP-пакетов после сжатия возрастает в 1,5 раза. Кроме того, сжатие IP-пакетов обеспечивает дополнительную защиту при попытке их несанкционированного перехвата во время передачи по общим каналам связи.

Сжатые IP-пакеты шифруются и инкапсулируются в новый IP-пакет, в котором в качестве IP-адреса источника выступает внешний IP-адрес КШ-отправителя, а в качестве IP-адреса приемника — внешний IP-адрес КШ-получателя. Список адресов, для которых осуществляется шифрование пакетов, определяется списком связанных КШ и их защищаемых сетей.

Если IP-пакет получен от стороннего абонента, обработка этого пакета блоком криптографической защиты не требуется. Если пакет получен от внешнего абонента, блок криптографической защиты проверяет целостность пакета и осуществляет его криптографическое преобразование (расшифровывает).

Трансляция сетевых адресов

Трансляцию сетевых адресов (NAT) используют для преобразования IP-адреса транзитных пакетов. Характеристики IP-пакетов, для которых используется трансляция адресов, определяют с помощью правил трансляции.

Описание правил трансляции адресов представлено в [Табл.1](#), задачи, которые решают с помощью данного механизма, — в [Табл.2](#).

Табл.1 Правила трансляции адресов

Правило	Описание
Исходящие	Инициатор соединения — абонент защищенной сети. В исходящих IP-пакетах внутрисетевой IP-адрес отправителя заменяется на указанный публичный. Имеется возможность динамического выбора из диапазона публичных адресов. Во входящих IP-пакетах, соответствующих данному соединению, публичный адрес получателя заменяется на соответствующий внутрисетевой
Входящие	Инициатор соединения — сторонний абонент, которому известен только публичный IP-адрес получателя. Во входящих IP-пакетах публичный IP-адрес получателя заменяется на указанный внутрисетевой. Порт назначения у входящих IP-пакетов можно также переопределить. В исходящих IP-пакетах, соответствующих данному соединению, внутрисетевой адрес отправителя заменяется на соответствующий публичный
1:1	Инициатор соединения — любая сторона. В исходящих IP-пакетах внутрисетевой IP-адрес отправителя заменяется на указанный публичный. Во входящих IP-пакетах публичный IP-адрес получателя заменяется на указанный внутрисетевой

Табл.2 Задачи, решаемые с помощью трансляции адресов

Задача	Правило
Скрытие структуры внутренней сети за одним публичным адресом	Исходящие
Предоставление пользователям с неуникальными внутрисетевыми адресами доступа к внешним сетям общего пользования	Исходящие
Обеспечение доступа извне к внутрисетевым сервисам:	
• по определенным портам	Входящие
• с переопределением портов	Входящие
• по всем портам (обычно используют для предоставления доступа к серверам, находящимся в демилитаризованной зоне)	1:1

Трансляция сетевых адресов выполняется перед применением правил фильтрации. При обработке IP- пакетов блоком криптографической защиты трансляция сетевых адресов не применяется.

Защита от DoS-атак

Для правила фильтрации, разрешающего TCP-соединение, можно включить режим защиты от DoS-атак типа SYN-флуд.

При обращении клиента к серверу криптографический шлюз сначала устанавливает TCP-соединение с клиентом от имени сервера, а затем с сервером от имени клиента. После этого клиент с сервером могут беспрепятственно обмениваться сетевыми пакетами. Полуоткрытые соединения с просроченным временем ожидания автоматически удаляются из очереди.

Для настройки режима используют следующие параметры:

- максимальное количество соединений, которое может быть установлено по указанному правилу фильтрации;
- время, по истечении которого неактивное соединение будет автоматически разорвано;
- количество новых соединений, регистрируемых для данного правила, в секунду.

Поддержка SPAN

Имеется возможность осуществлять проверку всего трафика, проходящего через КШ, на наличие попыток неавторизованного доступа (сетевых атак). Для этого к одному из сетевых интерфейсов КШ подключают выделенный компьютер с установленной на нем системой обнаружения атак, и этот интерфейс определяется как SPAN-порт (Switched Port Analyzer). Через этот порт система обнаружения атак получает копии всех IP-пакетов, проходящих через КШ, и анализирует их на наличие неавторизованных или подозрительных действий. Копии IP-пакетов, отправляемых или поступивших по защищенному каналу, передаются на SPAN-порт соответственно до их зашифрования или после расшифрования.

Возможный набор ответных действий зависит от используемой системы. Например, у ISS RealSecure Network Sensor существуют следующие варианты автоматического реагирования на атаки:

- запись факта атаки в регистрационном журнале RealSecure;
- уведомление об атаке администратора через консоль управления средствами RealSecure;
- уведомление об атаке по электронной почте;
- аварийный разрыв соединения с атакующим узлом;
- запись IP-пакетов, вызвавших срабатывание системы обнаружения атак, в отдельный файл для дальнейшего анализа;
- посылка управляющих SNMP-последовательностей.



Передача управляющих пакетов системы обнаружения атак в контролируруемую сеть (сетевой сегмент) осуществляется либо в обратном порядке через SPAN-порт, либо через дополнительный специально настроенный сетевой интерфейс системы обнаружения атак.

Следует учитывать, что 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.

Описание управления системой обнаружения атак см. [10].

Управление криптографическими ключами

Схема обмена информацией по защищенным каналам связи в корпоративной сети, обслуживаемой комплексом, представлена ниже.

Управление криптографическими ключами осуществляется централизованно из ЦУС. Средствами ЦУС выполняются следующие операции:

- Ключи парной связи генерируются для каждого КШ сети в ЦУС. Передача ключей с ЦУС на КШ производится по защищенному каналу связи на ключе связи с ЦУС. Парные ключи связи, зашифрованные на главном ключе КШ, хранятся на жестком диске КШ.

Главные ключи и ключи парной связи генерирует ЦУС из исходного ключевого материала ("исходная ключевая информация"). В качестве источника исходной ключевой информации может быть использован ПАК "Соболь" или ключевой блокнот РДП-006.

Для защиты соединения программы управления с ЦУС используется специальный административный ключ. Этот ключ хранится на идентификаторе администратора комплекса. Ключ администратора зашифровывается с использованием пароля по ГОСТ 28147-89 в режиме гаммирования с обратной связью.

Каждому зарегистрированному администратору присваивается уникальный ключ.

Смена ключей шифрования осуществляется периодически в соответствии с принятым планом смены ключей, а также в случае компрометации ключей. Смену ключей на ЦУС выполняют с помощью программы управления. Смену ключей на КШ — средствами локального управления.

Имеется возможность средствами программы управления создать резервный ключевой материал. При необходимости на основе этого ключевого материала можно сгенерировать ключ связи с ЦУС для любого КШ.

Табл.3 Перечень ключей, используемых комплексом

Наименование ключа	Назначение	Место хранения
Ключ шифрования пакета	Шифрование IP-пакетов	ОЗУ КШ
Ключ парной связи	Формирование ключей шифрования пакетов	Жесткий диск КШ
Главный ключ КШ	Шифрование ключей парной связи для хранения на диске	Жесткий диск ЦУС, энергонезависимая память ПАК "Соболь" КШ
Ключ связи с ЦУС	Формирование ключей шифрования команд для связи с ЦУС	Жесткий диск ЦУС, энергонезависимая память ПАК "Соболь" КШ
Ключ хранения	Шифрование ключевого материала в БД ЦУС	Энергонезависимая память ПАК "Соболь" ЦУС
Административный ключ	Защита соединения программы управления с ЦУС	Идентификатор администратора

Предусмотрено два режима управления криптографическими ключами, различающихся способами генерации ключей и сроками их хранения:

- по базовой схеме;
- по усиленной схеме.

По базовой схеме генерация ключей КШ и их распределение осуществляются средствами ЦУС. Срок действия/хранения ключей определяется Правилами пользования.

По усиленной схеме генерация ключей выполняется на отдельном, не имеющем сетевых соединений АРМ ГК. Средствами АРМ ГК сгенерированные ключи записываются на отчуждаемые USB-носители. Ключевые носители передаются администраторам для загрузки в БД ЦУС и КШ. В качестве ключевых носителей используются устройства "Рутокен ЭЦП". Срок действия/хранения ключей составляет три года.

Режим управления выбирается в ПУ ЦУС. В зависимости от выбранного режима администратору ПУ ЦУС становятся доступны или блокируются те или иные операции, выполняемые с ключевой информацией.

Если в состав комплекса входит хотя бы один КШ версии ниже 3.7, режим управления ключами по усиленной схеме становится недоступным.

Аутентификация пользователей

Идентификация и аутентификация пользователей предназначены для более тонкой настройки доступа сотрудников к корпоративным ресурсам.

Идентификация и аутентификация пользователей, работающих на компьютерах в защищенной сети КШ, выполняются с помощью специальной программы "Клиент аутентификации пользователя", установленной на компьютере пользователя.

Регистрацию пользователя выполняют средствами централизованного управления комплексом. При регистрации пользователю присваивают имя и пароль. Эти имя и пароль пользователь указывает при аутентификации на своем компьютере.

Доступ предоставляют группам пользователей с помощью правил фильтрации IP-пакетов и правил трансляции сетевых адресов. Группа пользователей связана с определенным сетевым объектом. Доступ, предоставляемый этой группе, действует только на компьютерах, относящихся к этому сетевому объекту.

Информация о зарегистрированных пользователях и группах хранится в базе данных ЦУС. Информация о пользователях, прошедших аутентификацию, — на КШ.

Для выполнения идентификации и аутентификации пользователей необходимо включение на КШ режима "Аутентификация пользователей" (см. стр. 58).

Возможна аутентификация только на тех компьютерах, которые подключены к внутренним интерфейсам КШ. Аутентификация пользователя на компьютерах, подключенных к внешнему интерфейсу КШ, не выполняется.

Аутентификация пользователей при подключении к межсетевому экрану на КШ выполняется по идентификатору и паролю, некриптографическим способом.

Обмен данными между КШ и подключаемым компьютером осуществляется по протоколу TCP.

Установка и настройка программы "Клиент аутентификации пользователя" представлены в [4].

Обеспечение отказоустойчивости комплекса

Резервное копирование и восстановление базы данных ЦУС

Резервное копирование и восстановление базы данных ЦУС предназначены для быстрого восстановления работы сети в случае выхода из строя штатного ЦУС.

Резервное копирование базы данных ЦУС выполняется автоматически по заданному расписанию. Рекомендуется после очередного изменения настроек комплекса сохранять резервную копию вручную.

В случае выхода ЦУС из строя осуществляется замена криптографического шлюза, на котором функционирует ЦУС, на работоспособный. После этого администратор запускает процедуру восстановления базы данных ЦУС из ранее сохраненной резервной копии. Сохранение резервной копии и восстановление базы данных осуществляются администратором с помощью программы управления.

Аппаратное резервирование

Аппаратное резервирование предназначено для обеспечения бесперебойной работы комплекса в случае выхода из строя какого-либо из криптографических шлюзов или криптокоммутаторов.

Примечание. Возможность аппаратного резервирования отсутствует у следующих криптографических шлюзов:

- ЦУС;
- КШ, подключенные к телефонным линиям с помощью модема.

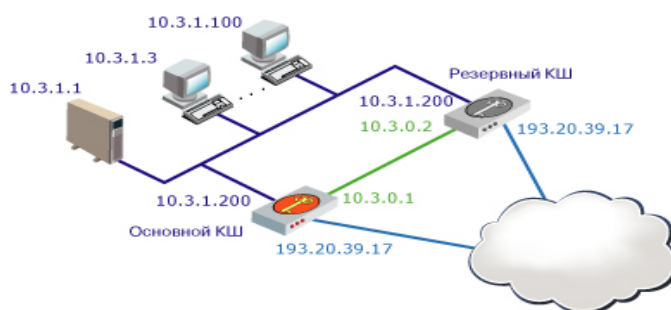
Аппаратное резервирование осуществляется путем подключения к основному криптографическому шлюзу (или криптокоммутатору) резервного устройства — создается кластер. Любое из устройств такого кластера может быть как основным, так и резервным. IP- и MAC-адреса внешнего и внутренних интерфейсов у основного и резервного устройства совпадают. При подключении сетевого оборудования к данным интерфейсам необходимо выполнить его настройку, исключаящую обнаружение "петель".

Для обмена служебными данными между основным и резервным КШ используются специально выделенные интерфейсы (таких интерфейсов резервирования у КШ может быть несколько). Прием и передача шифруемых

данных или обмен данными с ЦУС через эти интерфейсы невозможны. IP-адреса интерфейсов резервирования должны быть уникальными для данной корпоративной сети и различаться для основного и резервного КШ. На рисунке представлен пример использования резервного КШ в корпоративной сети.

Если оба КШ расположены в одной серверной стойке, для их соединения используется сетевой кросс-кабель. В остальных случаях соединение криптографических шлюзов осуществляется через IP-сеть.

В штатном режиме работы основной КШ обрабатывает проходящие через него IP-пакеты и осуществляет связь с ЦУС. Кроме этого он периодически передает на резервный КШ текущие значения счетчиков пакетов. Изменения в конфигурационной информации, полученной от ЦУС, передаются на резервный КШ по мере поступления.



Резервный КШ принимает только данные синхронизации от основного КШ. Его внутренние и внешний интерфейсы отключены, обработка IP-пакетов не производится. Отсутствие сигнала от основного КШ воспринимается как его отключение, и резервный КШ автоматически переходит в активный режим. Время перехода резервного КШ в активный режим составляет около 30 сек. после переключения. При этом в основном окне программы управления изменится вид пиктограммы, отображающей вышедший из строя КШ.

Обратное переключение канала связи с резервного КШ на основной может осуществляться как вручную администратором из программы управления, так и автоматически. В автоматическом режиме резервный КШ (который в данный момент является активным) отслеживает наличие сообщений от основного КШ и при их поступлении в течение установленного времени осуществляет обратное переключение. Настройка автоматического режима осуществляется с помощью программы управления.

Автоматическое переключение криптографических шлюзов в кластере осуществляется также при потере соединения на каком-либо из используемых сетевых интерфейсов. Переключение выполняется по следующему алгоритму:

- Проверяются внешние интерфейсы. Активным становится КШ, у которого большее количество работоспособных внешних интерфейсов.
- При одинаковом состоянии внешних интерфейсов проверяется количество функционирующих внутренних интерфейсов. Активным становится КШ, у которого количество работоспособных внутренних интерфейсов больше.
- При одинаковом состоянии внешних интерфейсов и при одинаковом количестве работоспособных внутренних интерфейсов:
 - при включенном автоматическом режиме активным становится основной КШ;
 - при выключенном автоматическом режиме переключения не происходит.

Механизм работы нескольких интерфейсов резервирования следующий. Для обмена трафиком между основным и резервным КШ всегда используется только один интерфейс. При выходе этого интерфейса из строя выполняется автоматическое переключение на следующий интерфейс. Сбой на отдельном интерфейсе в системе не отображается. Регистрируется в журнале и

отображается в программе управления только выход из строя всех интерфейсов резервирования.

Централизованное управление сетевыми устройствами

Управление сетью КШ осуществляется с помощью программы управления, установленной на одном или нескольких компьютерах защищенного сегмента сети (АРМ управления сетью "Континент" или АРМ администратора). Ограничение на количество АРМ администратора отсутствует.

Эти компьютеры должны входить в защищенную сеть, к которой подключен один из интерфейсов ЦУС. Обычное местоположение АРМ администратора — в сети, защищаемой таким КШ (см. стр. 11).

Программа управления устанавливает защищенное соединение с ЦУС и позволяет в диалоговом режиме через ЦУС контролировать все сетевые устройства комплекса. Запуск программы управления возможен только при предъявлении идентификатора администратора комплекса.

Связь между КШ, управляемыми разными ЦУС

Имеется возможность организации защищенного соединения между КШ, принадлежащими разным криптографическим сетям и управляемыми разными ЦУС.

Для этого администраторы этих сетей регистрируют каждый в своей программе управления внешнюю криптографическую сеть и обмениваются конфигурационными файлами со списком разрешенных к доступу ресурсов. Перед отправкой конфигурационный файл подписывают электронной подписью и зашифровывают. При получении выполняется проверка ЭЦП и целостности, а также расшифровка конфигурационного файла.

Информационный обмен между КШ, принадлежащими разным сетям, регулируют с помощью правил фильтрации. Ключи парной связи КШ генерируются на основе специального межсетевого ключа.

Для генерации межсетевого ключа, а также для формирования ЭЦП и зашифровывания конфигурационных файлов используется собственная инфраструктура открытых ключей. Генерацию ключевой пары и издание сертификата открытого ключа для своей сети выполняет ЦУС. Администраторы обмениваются этими сертификатами до начала процедуры организации связи между сетями.

Контроль сетевых устройств по протоколу SNMP

Имеется возможность контролировать работу сетевых устройств с помощью средств управления объектами сети по протоколу SNMP. Например, таким образом можно контролировать следующие параметры:

- время работы сетевого устройства с момента включения;
- количество полученных/переданных пакетов;
- состояние интерфейсов (Up/Down) и пр.

Реализовано обслуживание запросов "на чтение" к сетевому устройству. Имеется возможность рассылки служебных сообщений (traps). Эти сообщения рассылаются при возникновении следующих событий:

- "холодный запуск" (coldStart);
- физическое нарушение связи на интерфейсе (linkDown);
- восстановление связи на интерфейсе (linkUp).

Подробное описание модуля см. стр. 186.

Настройку модуля выполняют средствами локального управления сетевым устройством (см. [2]).

Multicast-вещание

Комплекс поддерживает следующие методы рассылки пакетов:

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

Метод рассылки определяется типом сетевого объекта (см. стр.98).

Multicast- вещание используют для организации мультимедиа-трансляций, видеоконференций, видеонаблюдения и т.п.

Для групповой рассылки используется специально выделенный диапазон сетевых адресов от 224.0.0.0 до 239.255.255.255.

Автоматическая настройка сетевых параметров

Криптографический шлюз может использоваться в качестве DHCP-сервера или DHCP-ретранслятора. Это позволяет компьютерам при загрузке автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

Сервис DHCP доступен только для компьютеров, расположенных в защищенных (внутренних) сегментах КШ. При этом за одним внутренним интерфейсом КШ может располагаться только один домен.

Сервис DHCP на КШ может быть отключен или работать в одном из двух режимов:

- сервер;
- ретранслятор.

Режим ретранслятора используется в тех случаях, когда компьютер не может подключиться к DHCP-серверу напрямую. DHCP-ретранслятор обрабатывает стандартный широковещательный DHCP-запрос и перенаправляет его на DHCP-сервер в виде целенаправленного (unicast) пакета, а полученный от DHCP-сервера ответ, в свою очередь, перенаправляет DHCP-клиенту.

По умолчанию сервис DHCP на КШ отключен.

Управление сервисом DHCP осуществляется удаленно средствами ПУ ЦУС.

Поддержка QoS

Комплекс поддерживает работу следующих механизмов управления QoS:

- классификация трафика;
- маркировка IP-пакетов;
- управление перегрузками с помощью очередей;
- предупреждение перегрузок.

Классификация трафика

Классы трафика определяют в специальном справочнике. Максимальное количество классов – 32. Принадлежность конкретных IP-пакетов данному классу указывают в правилах фильтрации и трансляции.

Маркировка IP-пакетов

Маркировка IP-пакета определяется значением поля ToS в заголовке IP-пакета. Правила маркировки задают при определении класса. Имеются следующие возможности автоматической обработки поля ToS:

- сохранение имеющегося значения;
- заполнение классификатором DSCP;
- заполнение классификатором IPP.

Управление перегрузками с помощью очередей (распределение по очередям)

Комплекс предоставляет возможности по управлению очередями следующих типов:

- очередь на обработку IP-пакетов блоком криптографической защиты;
- очередь на отправку IP-пакетов сетевым интерфейсом.

Обработка IP-пакетов блоком криптографической защиты выполняется в соответствии с приоритетом, указанным для данного класса трафика. Приоритет указывают непосредственно в свойствах класса. Возможные значения 0–31. Большему значению соответствует более высокий приоритет.

Методы обработки очередей (планировщики) на отправку IP-пакетов сетевыми интерфейсами представлены в Табл.4. На сетевом интерфейсе можно организовывать очереди только с одинаковым методом обработки. Максимальное количество очередей – 16 для PRIQ и 8 для CBQ и HFSC. IP-пакеты, для которых очередь явным образом не определена, поступают в очередь по умолчанию.

Табл.4 Методы обработки очередей

Метод	Описание
PRIQ	Priority Queuing. Последовательная обработка очередей в соответствии с их приоритетами. Возможна монополизация канала высокоприоритетными очередями
CBQ	Class Based Queuing. Обработка очередей в соответствии с выделенной на очередь долей общей полосы пропускания. Имеется возможность учитывать приоритеты очередей, а также включать для очереди механизм заимствования общей полосы пропускания в случае неиспользования ее другими очередями (borrow)
HFSC	Hierarchical Fair Service Curve. Дополнительно к возможностям CBQ предлагается два типа управления очередью: realtime и linkshare (см. Табл.5). Параметры Service Curve в данной версии не поддерживаются

Табл.5 Дополнительные параметры HFSC

Метод	Описание
realtime	Полоса пропускания, гарантируемая для данной очереди независимо от потребностей других очередей. При необходимости указанное значение может быть превышено, если определено значение параметра upperlimit
linkshare	Доля общей полосы пропускания, выделенная для данной очереди. При необходимости указанное значение может быть превышено, если определено значение параметра upperlimit
upperlimit	Максимальная полоса пропускания, устанавливаемая для данной очереди. Значение параметра должно быть больше или равно значению, указанному для параметра realtime или linkshare. Необязательный параметр

Предупреждение перегрузок

Механизмы защиты от перегрузок, поддерживаемые комплексом, представлены в Табл.6. Включение нужного механизма выполняют при настройке очереди на сетевом интерфейсе.

Табл.6 Механизмы управления переполнением очередей

Механизм	Описание
RED	Random Early Detection. Предупреждение перегрузок путем отбрасывания пакетов из случайно выбранных сессий. При использовании RED невозможно разделение по классам QoS
RIO	RED In/Out. Разновидность алгоритма RED, позволяющая использовать классы QoS
ECN	Explicit Congestion Notification. Предупреждение перегрузок путем уведомления отправителя посредством ECN-сессии

Поддержка IPv6

Комплекс поддерживает работу с каналами связи общих сетей передачи данных, использующих протоколы IPv6. При этом действуют приведенные ниже правила и ограничения.

- Протокол IPv6 поддерживается только внешними интерфейсами КШ/КК/ДА и используется только для зашифрованного трафика.
- Связь между двумя КШ может быть установлена только при совпадении версий IP на их внешних интерфейсах.
- В защищенных подсетях комплекса используется адресное пространство IPv4.
- Взаимодействие программы управления с ЦУС, а также абонентского пункта, сервера доступа и программы управления сервером доступа осуществляется по протоколу IPv4.
- Управляющий трафик ЦУС–КШ может осуществляться как по протоколу IPv6, так и по протоколу IPv4 (в зависимости от версии IP на внешних интерфейсах КШ).
- Рабочие станции защищаемой криптошлюзом подсети не могут обращаться к ресурсам IPv6 в открытой сети и наоборот – запрещен доступ из открытой сети с адреса IPv6 к ресурсам подсети, защищенной криптошлюзом.
- Не поддерживается динамическое назначение IPv6-адресов.
- Для PPP-интерфейсов адресация IPv6 не используется.

Организация сетей L2VPN

Сети L2VPN используют для объединения разрозненных ЛВС в единую одноранговую сеть масштаба предприятия. В этом случае отдельные ЛВС подключают к сетям общего пользования с помощью криптографических коммутаторов (КК), входящих в комплект поставки комплекса.

Преимущества сетей L2VPN:

- сохранение существующего адресного пространства ЛВС;
- использование в ЛВС любых сетевых протоколов, совместимых с Ethernet;
- использование дополнительных полей кадров Ethernet;
- простота управления объединенной сетью.

Управляют сетью L2VPN из программы управления с помощью виртуального коммутатора, который содержит перечень используемых КК. Порт виртуального коммутатора — интерфейс КК, к которому подключают ЛВС. Максимальное количество портов виртуального коммутатора — 16.

Подключение КК к сетям общего пользования аналогично подключению КШ. Ethernet- кадры между двумя КК передаются в зашифрованном виде инкапсулированными в UDP-пакеты.

Защитные механизмы

В состав программного обеспечения комплекса входят защитные механизмы, позволяющие реализовать следующие функции:

- создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера (замкнутой программной среды);
- разграничение доступа пользователей к ресурсам файловой системы и устройствам компьютера;
- контроль целостности защищаемых ресурсов;
- регистрация событий безопасности.

Настройку и управление защитными механизмами выполняют средствами системы Secret Net, устанавливаемой в составе программного обеспечения комплекса. Описание настройки и управления защитными механизмами приведены в

эксплуатационной документации Secret Net, поставляемой на установочном диске АПКШ "Континент".

Лицензирование

Имеется ряд ограничений на использование комплекса, связанных с политикой лицензирования данного продукта.

Ограничение на параметры ЦУС:

- максимальное количество сетевых устройств, имеющих статус "Введен в эксплуатацию".

Ограничение на параметры сервера доступа:

- максимальное количество клиентов, находящихся в базе СД.

Ограничения на использование комплекса определяются приобретенными лицензиями на использование данного продукта.

Лицензии разделяются по типам. Предусмотрены следующие типы лицензий:

Тип лицензии	Описание
Ввод в эксплуатацию	Используется при создании сети ЦУС и вводе сетевого устройства в эксплуатацию
Обновление	Используется при локальном и дистанционном обновлении ПО сетевого устройства, а также при централизованном управлении локально обновленным КШ. При обновлении ПО КШ проверяется наименование аппаратной платформы КШ и его соответствие наименованию, указанному в лицензии. При отсутствии в базе ЦУС лицензии на обновление для аппаратной платформы локально обновленного КШ такой КШ обслуживаться не будет и будет отображаться в ПУ ЦУС как отключенный
Обновление базы решающих правил	Используется при загрузке базы решающих правил с сервера обновлений. При отсутствии лицензии ручная загрузка файла обновлений базы решающих правил в ЦУС запрещена

Лицензии на максимальное количество введенных в эксплуатацию сетевых устройств и активных клиентов сервера доступа являются накопительными. Общее количество разрешенных к использованию объектов определяется суммой объектов, указанных в каждой лицензии.

Первоначальная регистрация лицензий для ЦУС выполняется при первом запуске программы управления ЦУС. Первоначальная регистрация лицензий для сервера доступа выполняется в любое время после инициализации. Доступ удаленных пользователей к ресурсам защищаемой сети возможен только после регистрации лицензий сервера доступа.

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. [180](#).

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.

Ввод комплекса в эксплуатацию

Порядок ввода комплекса в эксплуатацию

Ввод комплекса в эксплуатацию осуществляют в следующем порядке:

1. Инициализация и подключение ЦУС. См. [2].
2. Инициализация и настройка параметров ПАК "Соболь" на АРМ администратора комплекса (см. стр.182).
3. Установка подсистемы управления (см. стр.32).
4. Постановка на контроль программных модулей, подлежащих контролю целостности (см. стр.37).
5. Конфигурирование базы данных журналов. См. [3].
6. Запуск подсистемы управления (см. стр.37) и выбор режима управления ключевой информацией.
7. Настройка агента. См. [3].
8. Регистрация сетевых устройств, входящих в комплекс (см. стр.54).
9. Запись конфигураций сетевых устройств на отчуждаемые носители (см. стр.39).
10. Запись ключей сетевых устройств на отчуждаемые носители.

В зависимости от выбранного режима управления ключевой информацией (см. п.6) запись ключей выполняют в соответствии с приведенным ниже описанием.

Режим управления	Описание
Базовая схема	Ключи сетевого устройства, сгенерированные при его регистрации, записывают на USB-флеш-накопитель в ПУ ЦУС (см. стр.39)
Усиленная схема	На АРМ ГК ключи сетевого устройства изготавливают при выпуске серии ключевых документов и записывают на USB-ключи Rutoken ЭЦП (см. [9])

11. Инициализация и подключение зарегистрированных сетевых устройств. См. [2], [10].
12. Ввод в эксплуатацию инициализированных сетевых устройств (см. стр.54).
13. Настройка комплекса (см. стр.49).

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.180.

Особенности при обновлении ПО комплекса

При обновлении программного обеспечения комплекса более ранних версий на текущую версию имеется возможность использовать конфигурацию (базу данных) ЦУС предыдущей версии. Для загрузки конфигурации ЦУС в программу управления необходимо выполнить следующую последовательность действий:

1. До установки программного обеспечения текущей версии выполнить сохранение (резервное копирование) конфигурации ЦУС (см. стр.171).
2. Установить программное обеспечение текущей версии.
3. Выполнить восстановление конфигурации ЦУС из файла резервной копии в формате текущей версии (см. стр.172).

Установка подсистемы управления

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.7](#) и в [Табл.8](#).

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).

Требования к оборудованию и программному обеспечению

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

Компьютер, на который устанавливается программа 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 устанавливается программа управления, должен содержать средства, обеспечивающие контроль целостности програм-

много обеспечения (например ПАК "Соболь"). Перечень программных модулей и ключей реестра Windows, требующих контроля целостности, см. стр. **213**.

Размещение ПУ и сервера баз данных на одном компьютере

Требования к конфигурации АРМ администратора представлены в [Табл.7](#).

Табл.7 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	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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.8](#) и [Табл.9](#) соответственно.

Табл.8 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	

Элемент	Минимально	Рекомендуется
Сетевой адаптер	Ethernet	
Операционная система	<ul style="list-style-type: none"> 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 и Home Edition) 	
Установленное ПО	Версии СУБД для хранения журналов: <ul style="list-style-type: none"> 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.9 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	
Операционная система	<ul style="list-style-type: none"> 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.

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 "ОК".

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 "ОК", для отмены установки компонента нажмите кнопку "Отмена".

Если была нажата кнопка "ОК", 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 и СД.

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 криптодра "Континент"

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

Для настройки криптодра:

- 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.

Постановка на контроль программных модулей, подлежащих контролю целостности

После установки компонентов подсистемы управления на компьютере, на котором они были установлены, необходимо выполнить постановку на контроль программных модулей, подлежащих контролю целостности. Перечень программных модулей и ключей реестра Windows, подлежащих контролю целостности, приведен в Приложении (см. стр. **213**).

Постановка модулей на контроль осуществляется средствами, обеспечивающими контроль целостности программного обеспечения и установленными на данном компьютере. Если для контроля целостности используется ПАК "Соболь", постановку программных модулей на контроль следует выполнять в соответствии с описанием процедур, приведенных в документах "Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство администратора".

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. **46**).

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 "Закреть".

Программа управления установит защищенное соединение с ЦУС и на экране появится главное окно программы управления (см. стр. 41).

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 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.

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 (см. стр. 51)
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".

Программа управления ЦУС

Централизованное управление сетевыми устройствами осуществляется с помощью специальной программы управления, устанавливаемой на одном или нескольких компьютерах, находящихся в защищенном сегменте сети (АРМ администратора). Программа управления устанавливает защищенное соединение с ЦУС и позволяет в диалоговом режиме контролировать все сетевые устройства, а также редактировать данные, содержащиеся в базе данных ЦУС.

Работа программы управления возможна только при предъявлении идентификатора администратора комплекса. Права пользователя на администрирование комплекса в зависимости от предоставленной ему роли см. стр. **185**. Не рекомендуется одновременное управление сетевыми устройствами с нескольких компьютеров, на которых установлена программа управления.

Запуск программы

При запуске ПУ ЦУС осуществляется аутентификация администратора. Аутентификация выполняется в соответствии с политикой, заданной по умолчанию или измененной главным администратором комплекса (настройку параметров политики аутентификации см. стр. **51**).

Для запуска программы управления:

1. Нажмите на панели задач кнопку "Пуск" и активируйте в главном меню Windows команду "Программы > Код Безопасности > Континент 3.7 > Программа управления ЦУС (ПУ ЦУС)". На экране появится запрос идентификатора администратора.

2. Предъявите идентификатор администратора.

На экране появится запрос пароля для расшифровки ключей администратора.

3. Введите пароль и нажмите кнопку "ОК".

При успешном чтении служебной информации с идентификатора программа управления установит защищенное соединение с ЦУС и агентом, загрузит данные, необходимые для ее работы, и отобразит на экране главное окно (см. стр. **41**).

Если носитель испорчен или не содержит административного ключа, соединение с ЦУС установлено не будет и на экране появится сообщение об ошибке. В этом случае закройте окно сообщения и повторите процедуру запуска с надлежащим носителем.

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. 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.

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.10 и Табл.11. 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.10 Объекты папки "Центр управления сетью"

Объект	Описание
Сетевые объекты	Содержат списки соответствующих элементов правил фильтрации IP-пакетов и трансляции сетевых адресов (см. стр.98). 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 (см. стр.167)
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 (см. стр.50)
Сетевые устройства Континент	Перечень зарегистрированных в системе сетевых устройств (криптографические шлюзы, криптографические коммутаторы, детекторы атак)
База решающих правил	Список групп загруженных в БД ЦУС решающих правил (см. [10])
Виртуальные коммутаторы	Список виртуальных коммутаторов, используемых для управления криптографической коммутируемой сетью (см. стр.89)
Отчеты	Для каждого отчета перечень проблемных сетевых устройств, отфильтрованных по определенному параметру (см. стр.165)

Табл.11 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

Объект	Описание
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

Настройка интерфейса

Настройка интерфейса программы управления осуществляется с помощью меню "Вид".


Для отображения/скрытия на экране элемента главного окна:

- Откройте меню "Вид" и установите/удалите отметку у названия нужного элемента окна.

Для восстановления исходного расположения окон:

- Откройте меню "Вид" и активируйте команду "Восстановить расположение окон".

Для обновления отображаемой информации:

- Выберите в окне объектов нужный объект и выполните одно из следующих действий:
 - нажмите на панели инструментов кнопку "Обновить" ();
 - нажмите клавишу F5.

Информация об этом объекте будет обновлена.

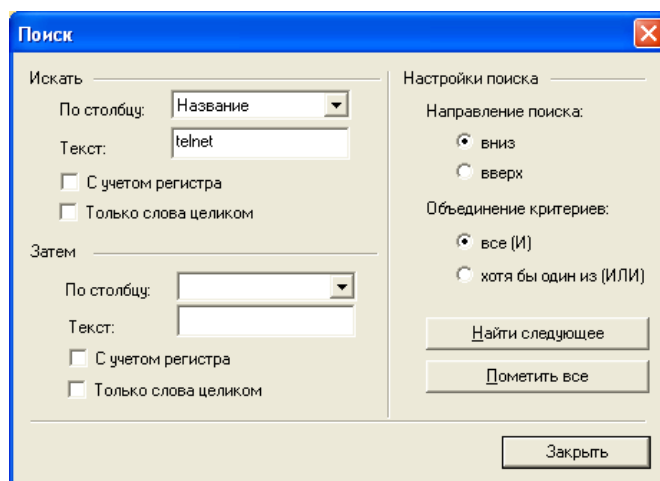
Управление таблицами

Сведения о выбранном объекте представлены в главном окне в табличном виде. Программа управления снабжена развитым инструментарием для работы с таблицами:

- поиск нужной записи;
- отбор (фильтрация);
- сортировка записей;
- перемещение столбцов;
- выбор отображаемых полей.

Для поиска нужной записи:

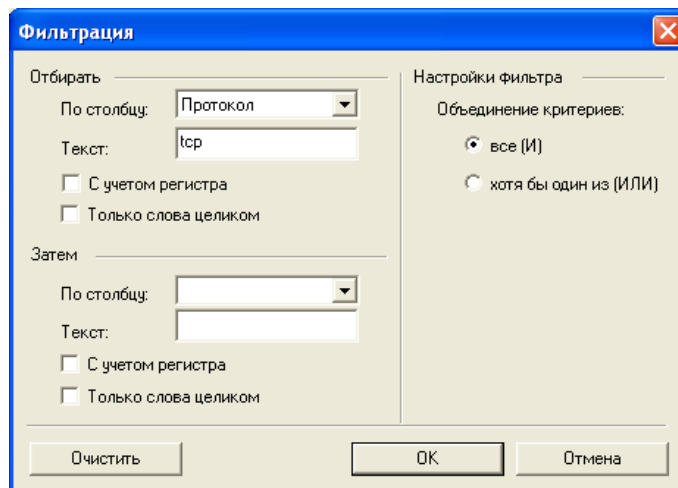
- Нажмите на панели инструментов кнопку "Поиск...".
На экране появится диалоговое окно "Поиск".



2. В полях диалога укажите условия поиска.
3. Для поиска нужных записей нажмите одну из кнопок:
 - "Найти следующее" — для поиска очередной записи, удовлетворяющей заданным условиям;
 - "Пометить все" — для выделения всех записей, удовлетворяющих заданным условиям.
4. Нажмите кнопку "Закрыть" после завершения процедуры поиска.

Для отбора нужных записей:

1. Нажмите на панели инструментов кнопку "Включить фильтрацию списка".
На экране появится диалоговое окно "Фильтрация".



2. Определите критерии отбора.
3. Нажмите кнопку "ОК" для выполнения отбора.
Диалоговое окно закроется, а в таблице будут отображены только те записи, которые удовлетворяют заданным условиям отбора.

Для отключения фильтрации:

1. Нажмите на панели инструментов кнопку "Включить фильтрацию списка".
На экране появится диалоговое окно "Фильтрация".
2. Нажмите кнопку "Очистить".
Действующие условия отбора будут удалены из полей диалога.
3. Нажмите кнопку "ОК".
Диалоговое окно закроется, а в таблице будут отображены все записи.

Примечание. Отключить фильтрацию можно другим способом: нажмите на панели инструментов кнопку "Отключить фильтрацию списка".

Для сортировки записей:

- Наведите курсор мыши на заголовок столбца и нажмите левую кнопку мыши. Список будет отсортирован по данному полю в алфавитном порядке. Повторное нажатие кнопки мыши изменяет порядок сортировки.

Для перемещения столбцов:

- Наведите курсор мыши на заголовок перемещаемого столбца и нажмите левую кнопку мыши. Не отпуская кнопку, перетащите поле в нужное место. Отпустите кнопку. Столбец займет указанное место.

Для добавления/удаления полей:

1. Нажмите на панели инструментов кнопку "Выбор полей отображения".
На экране появится диалоговое окно для определения перечня отображаемых полей.
2. Сформируйте перечень отображаемых полей. Для этого используйте кнопки ">>", ">", "<", "<<".
3. Укажите порядок отображения полей. Для этого в списке "Отображаемые поля" выберите нужное поле и с помощью кнопок "Вперед" и "Назад" переместите поле в нужное место списка.
4. Нажмите кнопку "ОК".

Диалоговое окно закроется, а в таблице будут отображены указанные поля.

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

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.

Управление лицензиями ЦУС

Ограничения на параметры ЦУС определяются приобретенными лицензиями (см. стр. 29). Управление лицензиями осуществляют в диалоговом окне "Управление лицензиями ЦУС" программы управления.

Для вызова окна:

1. Активируйте в меню "ЦУС" команду "Лицензии...". На экране появится диалоговое окно для управления лицензиями.

В верхней части окна отображается перечень зарегистрированных лицензий. Под списком лицензий отображаются итоговые результаты регистрации всех лицензий. В список можно добавлять новые лицензии.

Примечание. Лицензии, зарегистрированные в более ранних версиях комплекса, отображаются в списке с отметкой "Ввод <устройства> в эксплуатацию". При этом действие таких лицензий сохраняется.

2. После завершения работы с окном нажмите кнопку "Закрыть".

Для регистрации лицензий:

- 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.

Выход из программы

Для завершения работы с программой управления активируйте в меню "Объекты" команду "Выход". При этом защищенное управляющее соединение программы с ЦУС будет разорвано, а основное окно программы исчезнет с экрана.

Переустановка, исправление и удаление программы управления

Перед выполнением обновления, переустановки или удаления обязательно завершите работу программы управления (см. стр. 47), иначе появится сообщение с предложением закрыть программу управления для продолжения установки.

Обновление, переустановка или удаление агента, установленного с программой управления на одном компьютере, осуществляются автоматически при выполнении этих процедур над программой управления.

Изменение списка установленных компонентов

Изменение списка установленных компонентов выполняют при изменении архитектуры развертывания комплекса.

Для изменения списка установленных компонентов:

1. Запустите программу установки Setup.exe (см. стр. 35).

На экране появится сообщение программы установки о выполнении подготовительных действий. После завершения подготовки на экране появится диалог "Обслуживание программ".

С помощью данного диалога можно выполнить следующие процедуры:

- изменить список установленных компонентов программы управления;
- переустановить установленные компоненты программы управления;
- полностью удалить программу управления с компьютера.

2. Установите отметку в поле "Изменить" и нажмите "Далее >".

На экране появится диалог выбора компонентов программы.

3. Отметьте в списке нужные компоненты и нажмите кнопку "Далее>".

Примечание. В сети под управлением одного ЦУС может быть установлен только один агент.

4. Выполните [Шаг 4 – Шаг 6](#) процедуры установки подсистемы управления (см. стр. [34](#)).

Исправление программы управления

Исправление программы управления обычно выполняется в следующих случаях:

- после неудачного завершения установки;
- при нарушении работоспособности программного обеспечения.

Для исправления программы:

1. Запустите программу установки Setup.exe (см. стр. [35](#)).

На экране появится сообщение программы установки о выполнении подготовительных действий. После завершения подготовки на экране появится диалог "Обслуживание программ".

2. Установите отметку в поле "Исправить" и нажмите "Далее >".

3. Выполните [Шаг 4 – Шаг 6](#) процедуры установки подсистемы управления (см. стр. [34](#)).

Удаление программы управления

Для удаления программы управления:

1. Нажмите кнопку "Пуск" ("Start") и активируйте в главном меню команду "Настройка> Панель управления". В открывшемся окне выберите значок "Установка и удаление программ".

На экране появится стандартный диалог "Установка и удаление программ".

2. Выберите в списке установленных программ элемент "Континент. Подсистема управления" и нажмите кнопку "Изменить". На экране появится сообщение программы установки о выполнении подготовительных действий.

После завершения подготовки на экране появится диалог "Обслуживание программ".

3. Поставьте отметку в поле "Удалить" и нажмите кнопку "Далее >".

На экране появится диалог "Удаление конфигураций ЦУС".

4. Установите отметку в диалоге и нажмите кнопку "Далее>".

Начнется процесс удаления и по его завершении появится сообщение "Удаление завершено".

5. Нажмите кнопку "Готово".

На экране появится сообщение о необходимости перезагрузки компьютера.

6. Выберите вариант завершения удаления:

- нажмите кнопку "Да" для немедленной перезагрузки компьютера;
- нажмите кнопку "Нет", чтобы продолжить работу без перезагрузки компьютера. В этом случае завершите текущий сеанс работы и самостоятельно перезагрузите компьютер.

Настройка комплекса

На начальном этапе настройки комплекса могут быть использованы мастера для настройки VoIP и гигабитного Ethernet-соединения между КШ (см. стр. [67](#) и стр. [68](#)).

Для настройки комплекса:

1. Создайте для каждого зарегистрированного КШ исходное правило фильтрации.

Примечание. Параметры исходного правила и его элементов см. стр. [192](#). Создание элементов правила см. стр. [98](#), создание правила см. стр. [112](#).

2. Проведите опытную эксплуатацию комплекса в течение нескольких дней.
3. Проанализируйте журналы сетевого трафика для каждого КШ:
 - выделите из общего списка пакеты, разрешенные к хождению в сети политикой безопасности вашего предприятия;
 - определите для этих пакетов перечень подсетей, протоколов и портов.
4. Создайте необходимые элементы правил (см. стр. [98](#)) и сами правила фильтрации (см. стр. [112](#)). Примеры правил см. стр. [191](#).
5. Отключите исходное правило фильтрации (см. стр. [106](#)). Трафик в сети будет определяться вновь созданными правилами фильтрации.
6. Проведите контрольную эксплуатацию комплекса в течение нескольких дней:
 - контролируйте работу каждого КШ по журналу НСД;
 - при необходимости внесите изменения в список правил фильтрации.

Примечание. Если при контрольной эксплуатации будет нарушена работа какой-либо службы, включите на время отладки работы этой службы мягкий режим работы КШ (см. стр. [58](#)).

Организация работы администраторов комплекса

Управление учетными записями администраторов

После установки комплекс будет содержать только одну учетную запись администратора — "Встроенный администратор". Этому пользователю-администратору присвоена роль "Главный администратор" и он обладает всеми правами на администрирование комплекса.

Идентификатор администратора, предназначенный для идентификации главного администратора, создается при инициализации ЦУС. Идентификатор содержит служебную информацию, необходимую для запуска программы управления.

Главный администратор может назначать себе помощников — других администраторов, наделенных специфическими правами на администрирование комплекса. Перечень ролей администраторов и соответствующих им прав см. стр. [185](#). При добавлении новой учетной записи создается идентификатор данного администратора.

Для просмотра списка зарегистрированных администраторов:

- Выберите в окне объектов папку "Центр управления сетью > Администраторы".

В главном окне будет отображен перечень зарегистрированных администраторов.

Имеется возможность создания, изменения, блокировки и удаления учетных записей администраторов.

Примечание. Если в системе зарегистрирован единственный действующий администратор с правами главного администратора, изменить, заблокировать или удалить его учетную запись невозможно.

Для создания учетной записи администратора:

1. Активируйте в меню "Операции" команду "Создать администратора...". На экране появится диалог "Администратор".
2. Заполните поля диалога и нажмите кнопку "ОК".

Название	Имя администратора (не более 59 символов)
Роль	Наименование роли. Роль определяет права администратора на администрирование системы. Перечень ролей и соответствующих им прав см. стр. 185
Действительна до	Срок действия данной учетной записи. Максимальный срок действия учетной записи — до 01.01.2038
Заблокирована	При наличии отметки запуск программы управления и агента данным администратором невозможен

На экране появится запрос пароля, на котором будет зашифрован ключ администратора.

3. Введите пароль и нажмите кнопку "ОК". На экране появится диалог "Параметры соединения".
4. Выберите в раскрывающемся списке устройство идентификации администратора и сохраните изменения, нажав кнопку "ОК".

Примечание. Список содержит названия тех устройств идентификации, драйверы которых установлены на компьютере.

На экране появится запрос носителя для сохранения административного ключа. Это будет идентификатор администратора.

5. Предъявите носитель для сохранения ключа.

После успешного завершения записи ключевой информации на носитель на экране появится сообщение об этом. Закройте окно сообщения. В перечне пользователей-администраторов появится новая запись.

Для изменения учетной записи администратора:

1. Выберите в списке нужную учетную запись администратора.
2. Активируйте в контекстном меню команду "Свойства".
На экране появится диалог "Администратор".
3. Внесите необходимые изменения и нажмите кнопку "ОК".

Примечание. Если в системе зарегистрирован единственный действующий администратор с правами главного администратора, изменить его учетную запись невозможно.

Для блокировки учетной записи администратора:

1. Выберите в списке учетную запись администратора, которую необходимо заблокировать.
2. Активируйте в контекстном меню команду "Свойства".
На экране появится диалог "Администратор".
3. Установите отметку в поле "Заблокирована" и нажмите кнопку "ОК".
Выбранная учетная запись администратора будет заблокирована.

Примечание. Если в системе зарегистрирован единственный действующий администратор с правами главного администратора, заблокировать его учетную запись невозможно.

Для удаления учетной записи администратора:

1. Выберите в списке учетную запись администратора, которую необходимо удалить.
2. Активируйте в контекстном меню команду "Удалить администратора".
На экране появится запрос на удаление учетной записи.
3. Нажмите кнопку "ОК".
Окно запроса закроется, а выбранная учетная запись администратора будет удалена из списка.

Примечание. Если в системе зарегистрирован единственный действующий администратор с правами главного администратора, удалить его учетную запись невозможно.

Настройка политики аутентификации администраторов

Параметрами политики аутентификации администраторов при запуске ПУ ЦУС являются:

- минимальная длина пароля;
- количество неудачных попыток входа до блокировки;
- время блокировки при превышении количества неудачных попыток входа;
- контроль слабых паролей.

Настройка параметров выполняется главным администратором комплекса. Остальным администраторам параметры политики доступны только для просмотра.

Внимание! Политика аутентификации распространяется на вход в локальное меню сетевого устройства.

Для просмотра и настройки политики аутентификации:

1. Активируйте в меню "ЦУС" команду "Свойства".
Появится диалоговое окно "Свойства ЦУС".
2. Перейдите на вкладку "Политика аутентификации".

На вкладке представлены значения параметров политики аутентификации.

3. Установите нужные значения параметров и нажмите кнопку "ОК".

Смена административного ключа

Смена ключей осуществляется периодически в соответствии с требованиями политики безопасности предприятия, а также при утере носителя с административным ключом.

При записи административного ключа на новый носитель старый административный ключ становится недействительным.

Для смены ключа:

1. Выберите в списке учетную запись администратора, которому необходимо сменить ключ.
2. Вызовите контекстное меню и активируйте команду "Сменить ключ".
На экране появится запрос для подтверждения обновления ключа.
3. Нажмите кнопку "Да".
На экране появится диалог для ввода пароля.
4. Введите пароль для шифрования ключей и нажмите кнопку "ОК".
На экране появится диалог для определения параметров соединения.
5. Выберите в раскрывающемся списке устройство идентификации администратора и нажмите кнопку "ОК".

Примечание. Список содержит названия тех устройств идентификации, драйверы которых установлены на компьютере.

На экране появится запрос носителя для сохранения нового административного ключа.

6. Предъявите носитель для сохранения ключа.
После успешного завершения записи ключевой информации на носитель на экране появится сообщение об этом. Закройте окно сообщения.

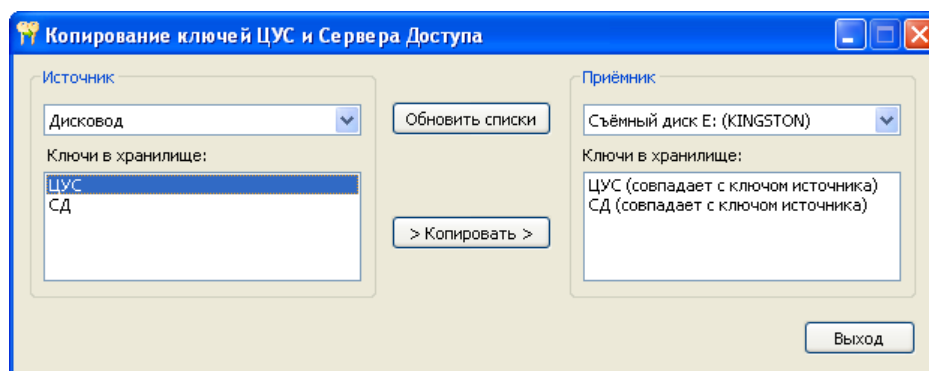
Копирование административного ключа

Данная процедура позволяет создать дубликат административного ключа, с помощью которого осуществляется идентификация администратора. Программа копирования ключей является одним из компонентов подсистемы управления и устанавливается на компьютер с установочного диска совместно с другими компонентами.

Примечание. Ключевой носитель может содержать один ключ ЦУС и произвольное количество ключей серверов доступа.

Для копирования ключа:

1. Предъявите носитель с ключом и носитель для записи дубликата.
2. Нажмите на панели задач кнопку "Пуск" и активируйте в главном меню Windows команду "Программы > Код Безопасности > Континент 3.7 > Программа копирования ключей".
На экране появится окно "Копирование ключей ЦУС и сервера доступа".



3. Выберите из раскрывающихся списков:

- в группе полей "Источник" — название устройства, с которого будет копироваться ключ;
- в группе полей "Приемник" — название устройства, на которое будет копироваться ключ.

Примечание. Списки содержат названия тех устройств идентификации, драйверы которых установлены на компьютере. Для обновления списков используйте кнопку "Обновить списки".

В поле "Ключи в хранилище" отобразится перечень ключей, хранящихся на данном носителе.

4. В поле "Ключи в хранилище" группы полей "Источник" выберите ключи для копирования и нажмите кнопку "> Копировать >".

Выбранные ключи будут скопированы на новый носитель, и перечень скопированных ключей отобразится в поле "Ключи в хранилище" группы полей "Приемник".

5. Закройте окно программы с помощью кнопки "Выход".

Централизованное управление сетевыми устройствами

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. 60). Если отметка не установлена, то у зарегистрированного сетевого устройства все сетевые интерфейсы будут иметь статус "Не определен".

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".

Удаление сетевого устройства

Внимание! Запрещено удалять криптографический шлюз, на котором находится ЦУС.

Для удаления сетевого устройства:

1. Вызовите контекстное меню объекта с именем устройства, которое требуется удалить, и активируйте команду "Удалить <сетевое устройство>". Используйте также кнопку панели инструментов "Удалить криптошлюз", предварительно выбрав удаляемый объект.
На экране появится запрос на подтверждение удаления.
2. Нажмите кнопку "ОК" (<Enter>) в окне запроса.
На экране появится диалог "Режимы удаления криптошлюза".

Примечание. Диалог отображается только в том случае, если существуют сетевые объекты, привязанные к данному сетевому устройству. Если такие объекты отсутствуют, то сетевое устройство будет удалено сразу после подтверждения запроса.

3. Выберите режим удаления и нажмите кнопку "ОК".

Удалить объекты	Удаляет сетевые устройства, а также все сетевые объекты, привязанные к этому сетевому устройству
Снять привязку к объектам	Удаляет сетевое устройство. Сетевые объекты данного сетевого устройства сохраняются

Перезагрузка сетевого устройства

Программа управления позволяет проводить дистанционную перезагрузку сетевых устройств. Перезагрузка выполняется при обнаружении сбоев в работе программного обеспечения сетевого устройства.

Для перезагрузки сетевого устройства:

1. Вызовите контекстное меню объекта с именем сетевого устройства, который требуется перезагрузить, и активируйте команду "Перезагрузить <сетевое устройство>".

Примечание. Возможен множественный выбор объектов.

На экране появится запрос на перезагрузку сетевого устройства.

2. Нажмите кнопку "Да".

При перезагрузке сетевого устройства осуществляется проверка целостности файлов программного обеспечения и загрузочных секторов. Сведения о нарушении целостности этих объектов помещаются в журнал НСД данного сетевого устройства.

Выключение сетевого устройства

Программа управления позволяет проводить дистанционное выключение сетевых устройств. При выключении сетевого устройства происходит корректное завершение работы операционной системы, после чего отключается питание устройства.

Внимание! После выключения сетевого устройства защищаемый им сегмент сети отключается от общей сети и связь с внешними и сторонними абонентами из этого сегмента становится невозможной.

Для выключения сетевого устройства:

1. В окне объектов выделите папку соответствующих сетевых устройств.
2. В главном окне вызовите контекстное меню объекта с именем сетевого устройства, которое требуется выключить, и активируйте команду "Выключить <сетевое устройство>".

Примечание. Возможен множественный выбор объектов.

На экране появится запрос на выключение устройства.


3. Нажмите кнопку "Да".

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 .

Миграция на новую аппаратную платформу

При необходимости можно заменить аппаратную платформу ЦУС или сетевого устройства, например, более производительной.

Для проведения работ, связанных с переходом на новую аппаратную платформу, отличающуюся количеством и типами сетевых адаптеров от исходной, необходимо предварительно связаться со службой технической поддержки компании "Код Безопасности" и получить соответствующие инструкции.

Внимание! Самостоятельная замена аппаратной платформы запрещена.

Просмотр сведений о сетевом устройстве

В программе управления ЦУС можно просмотреть следующие сведения о сетевом устройстве:

- состояние программного обеспечения – наличие в БД ЦУС обновления ПО, готового для установки на данное сетевое устройство;
- текущая версия программного обеспечения, установленного на сетевом устройстве;
- контрольная сумма установленного программного обеспечения;
- аппаратная платформа;
- статус автозагрузки сетевого устройства (отключена или включена); задается настройками ПАК "Соболь".

Для просмотра сведений о сетевом устройстве:

1. Вызовите контекстное меню нужного сетевого устройства и активируйте команду "Свойства...".

На экране появится окно настройки свойств данного сетевого устройства.

2. Перейдите на вкладку "Версия ПО".

На вкладке отобразятся сведения о сетевом устройстве.

Примечание. В нижней части вкладки расположена группа полей "Время загрузки ПО", предназначенная для загрузки файла обновления на данное сетевое устройство" (см. далее).

Обновление программного обеспечения сетевого устройства

Дистанционное обновление программного обеспечения сетевого устройства осуществляется для смены версии ПО. При этом используются два файла обновления, входящие в состав установочного ПО комплекса:

- preupdate.tar;
- update_all_release.tar.

Внимание! Версия обновления ПО сетевого устройства должна соответствовать версии ПО ЦУС.

При обновлении ПО сетевого устройства последовательно выполняют следующие процедуры:

1. Удаление последнего обновления ПО с жесткого диска ЦУС.
2. Копирование файла обновления preupdate.tar на жесткий диск ЦУС.
3. Загрузка файла обновления preupdate.tar на сетевое устройство.
4. Применение файла preupdate.tar на сетевом устройстве.
5. Удаление файла preupdate.tar с жесткого диска ЦУС.
6. Копирование файла обновления update_all_release.tar на жесткий диск ЦУС.
7. Загрузка файла обновления update_all_release.tar на сетевое устройство.
8. Применение файла обновления update_all_release.tar на сетевом устройстве с заменой файлов текущей версии на файлы новой версии.

Обновление ПО кластера:

- при обновлении ПО должны функционировать и основное, и резервное устройство;
- параметр "Режим обратного переключения" должен иметь значение "Автоматический" (см. стр. 176).

Удаление последнего обновления с жесткого диска ЦУС

Для удаления последнего обновления ПО с жесткого диска ЦУС:

1. Вызовите контекстное меню папки "Центр управления сетью" и активируйте команду "Свойства...".

На экране появится диалог "Свойства ЦУС".

2. Нажмите кнопку "Удалить ПО".

На экране появится запрос для подтверждения операции удаления ПО.

3. Нажмите кнопку "Да" для удаления текущей версии ПО.

Копирование файла обновления на жесткий диск ЦУС

Описанную ниже процедуру используют для копирования файлов обновления (preupdate.tar или update_all_release.tar) при обновлении ПО сетевых устройств.

Для копирования файла обновления на жесткий диск ЦУС:

1. Вызовите контекстное меню папки "Центр управления сетью" и активируйте команду "Свойства...".

На экране появится диалог "Свойства ЦУС".

2. Нажмите кнопку "Загрузить ПО".

На экране появится стандартный диалог выбора файла.

3. Откройте нужную папку, укажите файл обновления (preupdate.tar или update_all_release.tar) и нажмите кнопку "Открыть".

Файл обновления будет скопирован на жесткий диск ЦУС. По окончании копирования на экран будет выведено сообщение об этом.

4. Закройте окно сообщения, нажав кнопку "ОК".

В поле "Текущая версия" диалога "Свойства ЦУС" будет показан номер версии ПО, содержащегося в файле обновления.

5. Нажмите кнопку "ОК" для закрытия диалога "Свойства ЦУС".

Загрузка файла обновления на сетевое устройство

Для загрузки файла обновления на сетевое устройство:

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

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

2. Перейдите к вкладке "Версия ПО".

3. В группе полей "Время загрузки ПО" укажите нужное время и нажмите кнопку "Загрузить ПО".

Примечание. При установке отметки в поле "Сейчас" загрузка файла обновления на устройство выполняется немедленно после закрытия диалога.

Задание на загрузку файла обновления на сетевое устройство будет передано в ЦУС, а на экране появится сообщение об этом.

4. Закройте окно сообщения для возврата в диалог "Свойства < сетевого устройства >".

5. Закройте диалог "Свойства < сетевого устройства >", нажав кнопку "ОК".

В указанное время файл обновления будет загружен на сетевое устройство, а в поле "Состояние" диалога "Свойства > Версия ПО" станет доступной кнопка "Обновить ПО".

Применение файла обновления на сетевом устройстве

Приведенную ниже процедуру выполняют после загрузки на сетевое устройство файлов обновления preupdate.tar и update_all_release.tar.

Для применения файла обновления:

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

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

2. Перейдите к вкладке "Версия ПО" и нажмите кнопку "Обновить ПО".

На экране появится подтверждение о проведении обновления в указанный срок.

3. Закройте окно сообщения для возврата в диалог "Свойства < сетевого устройства >".

4. Закройте диалог "Свойства < сетевого устройства >", нажав кнопку "ОК".

В указанное время система приступит к обновлению ПО. В процессе обновления дважды автоматически выполняется перезагрузка сетевого устройства. По окончании обновления в ПУ в диалоге свойств изменится версия ПО.

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. 78). 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

Изменение внешнего адреса сетевого устройства

Внимание! При изменении внешнего адреса КШ с включенным режимом динамической маршрутизации работа динамической маршрутизации может быть нарушена.

Изменение внешних адресов на нескольких устройствах выполняют последовательно. Приступать к процедуре изменения адреса на следующем устройстве можно только после успешного завершения процедуры изменения адреса на предыдущем устройстве. Завершение процедуры определяют по пустой очереди заданий для этого устройства (см. стр. **85**).

Процедура изменения внешнего адреса сетевого устройства зависит от включенного на нем режима Multi-WAN (см. стр. **68**). Ниже приведены отдельные процедуры для сетевого устройства, работающего в режиме отключенного Multi-WAN ("Передача трафика в соответствии с таблицей маршрутизации") и в режиме включенного Multi-WAN ("Обеспечение отказоустойчивости канала связи" или "Балансировка трафика между внешними интерфейсами").

Для изменения внешнего адреса сетевого устройства с выключенным Multi-WAN:

1. Выберите в списке сетевое устройство, вызовите контекстное меню и активируйте команду "Свойства".

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

2. Перейдите на вкладку "Интерфейсы" и для внешнего интерфейса добавьте новый адрес.

Внимание! Новый адрес должен принадлежать другой подсети.

3. Нажмите кнопку "Применить" и перейдите на вкладку "Маршрутизация".
4. Измените маршрут по умолчанию. Маршрутизатор должен быть доступен с нового IP-адреса.
5. Перейдите на вкладку "Интерфейсы" и удалите старый IP-адрес.

Для изменения внешнего адреса сетевого устройства с включенным Multi-WAN:

1. Выберите в списке сетевое устройство, вызовите контекстное меню и активируйте команду "Свойства".

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

2. Перейдите на вкладку "Multi-WAN" и удалите все записи в таблице "Каналы WAN".
3. Установите в поле "Режим Multi-WAN" значение "Передача трафика в соответствии с таблицей маршрутизации" и нажмите кнопку "Применить".
4. Перейдите на вкладку "Интерфейсы", укажите новый IP-адрес внешнего интерфейса и нажмите кнопку "Применить".
5. Перейдите на вкладку "Маршрутизация" и при необходимости измените маршруты.
6. Перейдите на вкладку "Интерфейсы" и удалите старый адрес внешнего интерфейса.
7. Перейдите на вкладку "Multi-WAN" и восстановите настройки WAN.

8. Нажмите кнопку "Применить".

Изменение внешнего адреса ЦУС

Процедура изменения внешнего адреса ЦУС состоит из двух этапов:

- Назначение альтернативного адреса ЦУС.
- Замена действующего адреса ЦУС на альтернативный.

Изменение внешнего адреса ЦУС выполняют в диалоговом окне "Изменение адреса ЦУС".

На первом этапе введенный альтернативный адрес автоматически рассылается на сетевые устройства. Список сетевых устройств, которые еще не получили альтернативный адрес, отображается в соответствующем поле диалога.

На втором этапе осуществляется замена адреса ЦУС.

Вызов диалога "Изменение адреса ЦУС"

Для вызова диалога:

- Вызовите контекстное меню объекта с именем ЦУС и активируйте команду "Изменить внешний адрес ЦУС...".

На экране появится диалог "Изменение адреса ЦУС". В этом диалоге выполняют ввод альтернативного адреса ЦУС, контроль за рассылкой альтернативного адреса на сетевые устройства и замену действующего адреса на альтернативный.

Назначение альтернативного адреса ЦУС

Для назначения альтернативного адреса ЦУС:

1. Вызовите на экран диалог "Изменение адреса ЦУС" (см. выше).
2. В поле "Альтернативные адреса ЦУС" сформируйте перечень альтернативных адресов. Для формирования списка используйте кнопки "Добавить..." и "Удалить".

При вводе альтернативного адреса укажите протокол (IPv4 или IPv6).

Система приступит к рассылке альтернативных адресов на сетевые устройства. Перечень устройств, еще не получивших альтернативных адресов, отображается в центральной части диалога. Обновление этого списка осуществляется автоматически. После получения оповещения всеми сетевыми устройствами значок "Внимание!" справа от поля изменится на значок "Выполнено".

3. После завершения работы нажмите кнопку "Закрыть".

Замена действующего адреса ЦУС на альтернативный

Для замены адреса ЦУС:

1. Вызовите на экран диалог "Изменение адреса ЦУС" (см. выше).
2. В поле "Адреса ЦУС" выберите адрес, который требуется заменить, и нажмите кнопку "Изменить...".

На экране появится диалог "Ввод адреса".

3. Заполните поля диалога и нажмите кнопку "ОК".

Адрес ЦУС	Альтернативный адрес для замены
Маска/Префикс	Маска (префикс) сети, к которой подключен внешний интерфейс ЦУС
Следующий узел	IP-адрес маршрутизатора по умолчанию

Система автоматически сменит внешний адрес ЦУС на указанный.

4. После завершения работы нажмите кнопку "Закрыть".

Модемное подключение и поддержка PPPoE

Подключение сетевого устройства с помощью модема возможно только к внешней сети. В качестве протокола аутентификации используется протокол CHAP. Протоколы MS-PAP и MS-CHAP не поддерживаются.

При использовании выделенной линии необходимо выполнить дополнительную настройку модема заранее, до подключения его к сетевому устройству. См. [2].

Добавление или удаление PPP-интерфейса, а также изменение параметра "Режим работы" возможно только в том случае, если сетевое устройство выведено из эксплуатации. После изменения режима работы необходимо выполнить инициализацию сетевого устройства.

При локальной настройке модемного подключения ее результаты в программе управления не отображаются.

При регистрации 3G-модема укажите для параметра "Режим работы" значение "Dialup (Исходящий)". Остальные параметры настройки модема необходимо получить у провайдера.

Вызов списка PPP-интерфейсов

Для вызова списка PPP-интерфейсов:

1. Вызовите контекстное меню объекта с именем сетевого устройства, параметры которого требуется изменить, и активируйте команду "Свойства...".
2. В появившемся окне перейдите к вкладке "Интерфейсы" и активируйте закладку "PPP".

В поле "PPP-интерфейсы" отобразится список зарегистрированных модемных подключений.

Регистрация нового PPP-интерфейса

Для регистрации нового PPP-интерфейса:

1. Нажмите кнопку "Добавить".

На экране появится диалог "PPP-интерфейс". Набор отображаемых полей зависит от выбранного значения в поле "Режим работы".

2. Определите параметры модемного подключения и нажмите кнопку "ОК":

Название	Наименование PPP-интерфейса. Присваивается автоматически (tun0, tun1 и т.д.)
Тип	Тип интерфейса: Внешний — интерфейс, подключаемый к сетям общего пользования
MTU	Максимальная единица передачи данных (в байтах)
Режим работы	Dialup (Входящий), Dialup (Исходящий), Выделенная линия или PPPoE (Исходящий). Поле доступно, если сетевое устройство выведено из эксплуатации (см. стр. 54)
IP-адрес	IP-адрес RAS-клиента для подключения к серверу удаленного доступа (для режимов Dialup)
Имя пользователя, пароль	Имя пользователя, зарегистрированного у провайдера, и его пароль
Скорость	Скорость передачи данных через COM-порт (для режимов Dialup и Выделенная линия). Примечание. При подключении модема через USB-порт в данном поле необходимо выбрать значение "USB-модем".
Тайм-аут	Время ожидания соединения в секундах (для режимов Dialup)
Строка инициализации	Значение строки инициализации модема (для режимов Dialup)

Номер телефона	Список номеров телефонов модемного пула (только для режима Dialup (Исходящий)). Для добавления нового номера введите номер телефона в одноименное поле и нажмите кнопку "Добавить". Для удаления выбранного номера используйте кнопку "Удалить".
Имя сервиса	Имя сервиса (только для режима PPPoE (Исходящий))
Интерфейс	Название интерфейса, через который осуществляется подключение (только для режима PPPoE (Исходящий))
Регистрация	Задание правила регистрации событий в журналах. Значения: <ul style="list-style-type: none"> • определяется сетевым устройством (правило наследуется из свойств сетевого устройства); • первые 64 байта; • тело пакета

Настройка параметров PPP-интерфейса

Для настройки параметров PPP-интерфейса:

1. Выберите нужную запись в списке PPP-интерфейсов и нажмите кнопку "Свойства".
На экране появится диалог "PPP-интерфейс" (см. выше).
2. Внесите необходимые изменения в поля данного диалога и нажмите кнопку "ОК".

Удаление PPP-интерфейса

Для удаления PPP-интерфейса:

- Выберите удаляемую запись в списке и нажмите кнопку "Удалить".

Подключение модема Huawei 3372h

В данном подразделе приводится описание настроек, которые должны быть выполнены при использовании модема Huawei 3372h.

Внимание!

- Модем Huawei 3372h работает только с криптошлюзами версии 3.7.6 и выше.
- Подключение модема к КШ с ЦУС не предусмотрено.
- Подключение и отключение модема выполняют только при выключенном КШ.

Ниже приведен общий порядок подключения модема и настройки КШ. Предполагается, что КШ, к которому должен быть подключен модем, не проинициализирован. Порядок подключения и настройки для проинициализированного КШ приведен в конце подраздела.

Для подключения модема и настройки КШ:

1. Зарегистрируйте КШ в ПУ ЦУС, если до этого он не был зарегистрирован (см. стр. 54).
2. Выключите КШ и подсоедините к USB-разъему модем.
3. В ПУ ЦУС выберите в списке КШ с подключенным модемом, вызовите контекстное меню и выберите пункт "Свойства".
На экране появится диалог "Свойства КШ".
4. Перейдите на вкладку "Интерфейсы" и активируйте закладку "PPP", далее на вкладке "PPP" нажмите кнопку "Добавить".
На экране появится диалог "PPP-интерфейс".
5. В поле "Режим работы" укажите CDCE, выбрав его из раскрывающегося списка.
Поле "IP-адрес" автоматически заполнится значением 192.168.8.100.

Внимание! Менять данное значение на IP-адрес, находящийся вне диапазона 192.168.8.2-192.168.8.254, не рекомендуется.

6. Нажмите кнопку "OK".

Диалог "PPP-интерфейс" закрывается.

7. Задайте для КШ с модемом маршрут по умолчанию. Для этого в диалоге "Свойства КШ" перейдите на вкладку "Маршрутизация" и нажмите кнопку "Добавить".

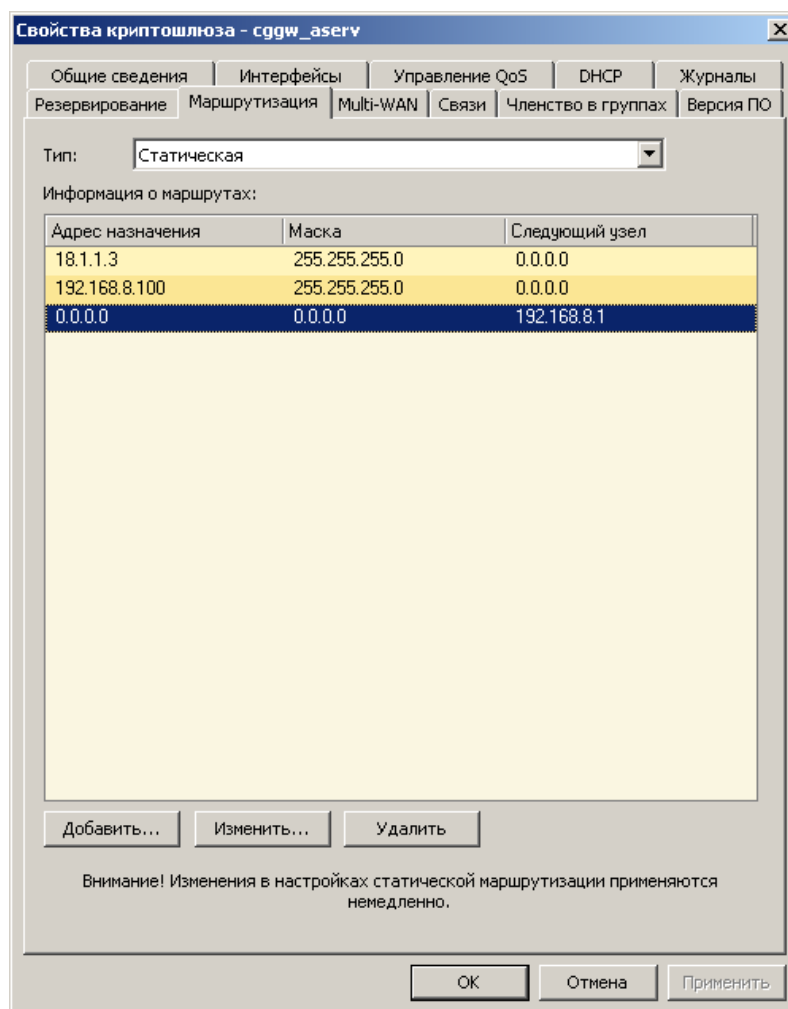
На экране появится диалог "Ввод адреса".

8. Укажите значения параметров:

Параметр	Значение
Адрес	0.0.0.0
Маска	0
Следующий узел	192.168.8.1

Нажмите кнопку "OK".

Диалог "Ввод адреса" закрывается и в списке появится добавленный маршрут по умолчанию.



9. Запишите конфигурацию и комплект ключей КШ на USB-флеш-накопитель (см. стр.39).
10. Включите КШ с модемом и средствами локального управления выполните его инициализацию (см. [2]). При выполнении инициализации КШ загрузите конфигурацию и комплект ключей, сохраненные на USB-флеш-накопителе.
11. Введите КШ с модемом в эксплуатацию (см. стр.54).

Для подключения модема к ранее проинициализированному КШ:

1. Выведите КШ из эксплуатации (см. стр.54).
2. В ПУ ЦУС в свойствах КШ добавьте CDCE- интерфейс (см. выше).
3. Введите КШ в эксплуатацию (см. стр.54).
4. Сохраните конфигурацию КШ на USB-флеш-накопителе (см. стр.39).
5. Выключите КШ и подсоедините к USB-разъему модем.
6. Включите КШ, перейдите к режиму настройки сетевого устройства и в меню "Управление" выполните загрузку конфигурации, сохраненной на USB-флеш-накопителе (см. [2]).

VLAN-интерфейсы

Комплекс поддерживает работу с виртуальными локальными сетями (VLAN).

Вызов списка VLAN-интерфейсов

Для вызова списка VLAN-интерфейсов:

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" и активируйте закладку "VLAN".

В поле "VLAN-интерфейсы" отобразится список зарегистрированных VLAN-интерфейсов.

Регистрация нового VLAN-интерфейса

Для регистрации нового VLAN-интерфейса:

1. Нажмите кнопку "Добавить".

На экране появится диалог "Свойства VLAN-интерфейса".

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

Название	Наименование VLAN-интерфейса. Присваивается автоматически (vlan0, vlan1 и т.д.)
Тип	Тип интерфейса: <ul style="list-style-type: none"> Внешний — интерфейс, подключаемый к сетям общего пользования. Внутренний — интерфейс, подключаемый к защищаемой сети (для КШ) Порт криптокоммутатора (для КК)
MTU	Максимальная единица передачи данных (в байтах)
VLAN-идентификатор	Идентификатор виртуальной локальной сети (VID)
Родительский интерфейс	Выберите в раскрывающемся списке родительский интерфейс
IP-адреса	Список IP-адресов интерфейса (до 16). 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"
Регистрация	Задание правила регистрации событий в журналах. Значения: <ul style="list-style-type: none"> определяется сетевым устройством (правило наследуется из свойств сетевого устройства); первые 64 байта; тело пакета

Настройка параметров VLAN-интерфейса

Для настройки параметров VLAN-интерфейса:

1. Выберите нужную запись в списке VLAN-интерфейсов и нажмите кнопку "Свойства".

На экране появится диалог "Свойства VLAN-интерфейса".

2. Внесите необходимые изменения в поля данного диалога и нажмите кнопку "ОК". Описание полей см. выше.

Удаление VLAN-интерфейса

Для удаления VLAN-интерфейса:

• Выберите удаляемую запись в списке и нажмите кнопку "Удалить".

Настройка VoIP

Предусмотрена автоматическая настройка криптошлюзов для работы VoIP, которая выполняется на начальном этапе настройки комплекса. В результате настройки:

- создаются защищенные сегменты для внутренних интерфейсов КШ;
- создаются правила фильтрации;
- устанавливаются связи между КШ.

Внимание! Если в сети уже были созданы защищенные объекты, правила фильтрации и установлены связи, корректная настройка не гарантируется.

Настройка выполняется с помощью мастера. Для настройки необходимо указать КШ, участвующие в работе VoIP, и схему их подключения (полносвязная матрица или звезда).

Для настройки VoIP:

1. Запустите мастер одним из следующих способов:

- в окне объектов вызовите контекстное меню папки "Криптошлюзы" и выберите в нем "Настройка криптошлюзов > VoIP";
- в окне объектов выделите папку "Криптошлюзы" и выберите в меню "Операции > Настройка криптошлюзов > VoIP".

Появится стартовый диалог мастера.

2. Нажмите кнопку "Далее".

Появится очередной диалог мастера "Настройка параметров".

3. Выберите схему подключения и нажмите кнопку "Далее".

Полносвязная матрица	В списке "Криптошлюзы" отметьте КШ, которые должны участвовать в работе VoIP
Звезда	В поле "Центр звезды" укажите центральный КШ. В списке "Криптошлюзы" отметьте остальные КШ, которые должны участвовать в работе VoIP

Мастер приступит к настройке. Ход настройки отображается в следующем диалоге мастера "Завершение настройки". При нарушении условий корректной настройки результаты выполнения операций выделяются красным цветом.

4. Дождитесь завершения работы мастера и проанализируйте результаты.

- Если настройка выполнена успешно, нажмите кнопку "Готово".
- Если в процессе настройки имели место ошибки, нажмите кнопку "Отмена", устраните причины их возникновения и повторите процедуру.

Настройка гигабитного соединения

Гигабитное соединение устанавливается между парами КШ. Настройка выполняется с помощью мастера. В результате настройки устанавливается связь между КШ и отключается регистрация сетевого трафика.

Для настройки соединения:

1. Раскройте папку "Криптошлюзы" и в главном окне программы выберите КШ, для которого необходимо настроить гигабитное соединение.

2. Выберите в меню "Операции > Настройка криптошлюзов > Гигабитный Ethernet".

Появится стартовый диалог мастера.

3. Нажмите кнопку "Далее".

Появится следующий диалог мастера "Выбор криптошлюза".

4. Выберите в раскрывающемся списке парный КШ и нажмите кнопку "Далее".

Начнется настройка соединения, ход которой отображается в следующем диалоге мастера "Завершение настройки".

При обнаружении мастером уже имеющейся связи между КШ результат выполнения операции выделяется красным цветом.

5. Дождитесь завершения работы мастера и нажмите кнопку "Готово".

Настройка Multi-WAN

Данные настройки предоставляют возможность сконфигурировать сеть при одновременном подключении КШ или криптокоммутатора к нескольким

внешним сетям. Имеются следующие режимы Multi-WAN:

- передача трафика в соответствии с таблицей маршрутизации;
- обеспечение отказоустойчивости канала связи;
- балансировка трафика между внешними интерфейсами КШ или криптокоммутатора.

Настройку режимов выполняют на вкладке "Multi- WAN" диалогового окна "Свойства <сетевого устройства>". Настройку каждого канала — в диалоговом окне "Свойства канала связи".

Примечание. Для сетевого устройства с включенным режимом динамической маршрутизации данная функция не поддерживается.

Формирование перечня каналов связи и выбор режима

Перечень внешних каналов связи формируют на вкладке "Multi- WAN" диалогового окна "Свойства <сетевого устройства>". В этом же диалоге выбирают нужный режим Multi-WAN.

Для формирования перечня каналов:

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 "Multi- WAN". Вид диалога зависит от выбранного значения в поле "Режим Multi- WAN". Режим по умолчанию "Передача трафика в соответствии с таблицей маршрутизации".
3. В поле "Каналы WAN" сформируйте перечень используемых внешних каналов. Для формирования списка используйте кнопки:

Добавить...	Вызывает на экран диалог "Свойства канала связи" для создания в списке новой записи
Удалить	Удаляет из списка выбранную запись
Изменить...	Вызывает на экран диалог "Свойств канала связи" для редактирования выбранной записи

Процедуру настройки свойств канала связи см. стр. [69](#).

4. В поле "Режим Multi- WAN" выберите в раскрывающемся списке нужный режим и заполните остальные поля диалога.

Передача трафика в соответствии с таблицей маршрутизации	Не требует дополнительной настройки
Обеспечение отказоустойчивости канала связи	См. стр. 70
Балансировка трафика между внешними интерфейсами сетевого устройства	См. стр. 73

5. Нажмите кнопку "ОК".

Настройка свойств канала связи

Для настройки свойств канала связи:

1. Вызовите диалог "Свойства канала связи" (см. стр. [69](#)).
2. Заполните поля диалога и нажмите кнопку "ОК".

Внешний интерфейс сетевого устройства	Наименование настраиваемого интерфейса сетевого устройства
IP-адрес маршрутизатора к провайдеру	IP-адрес маршрутизатора, обеспечивающий связь с внешней сетью. Маршрутизатор должен находиться в той же сети, к которой подключен настраиваемый интерфейс

Диагностика работоспособности канала	Включает режим диагностики работоспособности канала. При отключенной диагностике канал будет считаться безусловно доступным
IP-адрес контрольной точки	IP-адрес хоста во внешней сети, наличие соединения с которым будет проверяться
Метод тестирования	<ul style="list-style-type: none"> Ping — проверка доступности контрольной точки с помощью команды ping. TCP — проверка доступности контрольной точки по протоколу TCP. Необходимо указать порт, через который будет устанавливаться соединение
Интервал диагностики, сек.	Промежуток времени в секундах между попытками установления соединения с контрольной точкой
Количество успешных попыток для признания канала работоспособным	Количество последовательных успешных попыток установления соединения с контрольной точкой после восстановления работоспособности канала для присвоения каналу статуса "работоспособный"
Количество неудачных попыток для признания канала неработоспособным	Количество неудачных попыток установления соединения с контрольной точкой для присвоения каналу статуса "неработоспособный"
Регистрация в журнале	При наличии отметки в системном журнале регистрируются события, связанные с изменением статуса канала

Обеспечение отказоустойчивости канала связи

Для настройки режима обеспечения отказоустойчивости:

1. Сформируйте перечень каналов и выберите режим "Обеспечение отказоустойчивости канала связи" (см. стр. 69).
2. Укажите приоритет каналов. Для этого используйте кнопки со стрелками слева под списком каналов.

Примечание. Кнопки со стрелками перемещают выбранную запись в списке на одну позицию в выбранном направлении.

Последовательность записей в списке соответствует приоритету данного канала.

Удаление отметки в левой части записи отключает использование данного канала без удаления записи из списка.

3. Заполните поля диалога и нажмите кнопку "ОК" или "Применить".

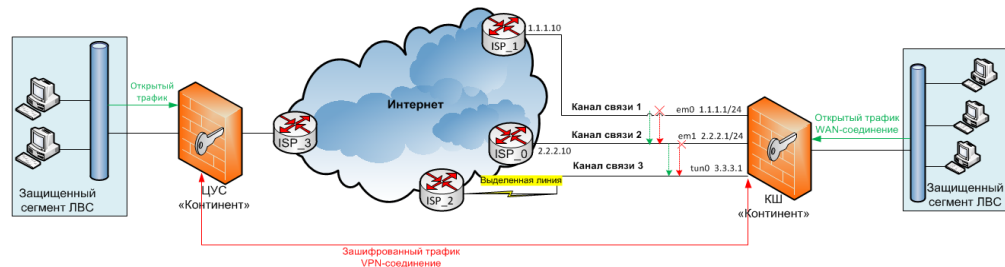
Режим Multi-WAN	Выберите значение "Обеспечение отказоустойчивости канала связи (Failover)"
Каналы WAN	Перечень используемых внешних каналов
Немедленно	Обратное переключение на канал с более высоким приоритетом будет выполнено немедленно после восстановления его работоспособности независимо от наличия активных соединений
Переключать активные соединения через	Обратное переключение на канал с более высоким приоритетом будет выполнено через указанное время после восстановления работоспособности канала
Не переключать активные соединения	Обратное переключение на канал с более высоким приоритетом будет выполнено после закрытия всех активных соединений

Автоматический исходящий NAT	При наличии отметки автоматически создаются правила трансляции, которые для всего исходящего трафика подменяют адрес отправителя на адрес активного в данный момент внешнего интерфейса. Правила трансляции, заданные администратором, отменяются
------------------------------	---

Примечание. При переключении между WAN-каналами шлюз по умолчанию автоматически устанавливается в соответствии с IP-адресом маршрутизатора, заданным в настройках свойств канала. Изменение IP-адреса шлюза по умолчанию при переключении между каналами в диалоге "Свойства криптошлюза" на вкладке "Маршрутизация" не отображается. Для просмотра текущего значения IP-адреса маршрутизатора используется команда "Вывести таблицы маршрутизации" в меню локального управления сетевого устройства (см. [2]). В таблице IP-адрес маршрутизатора отображается как шлюз по умолчанию.

Ниже приведен пример настройки режима отказоустойчивости для КШ, имеющего три внешних канала (см. рисунок):

- канал связи 1 (провайдер ISP_1);
- канал связи 2 (провайдер ISP_0);
- канал связи 3 (провайдер ISP_2, модемное подключение).



При нарушении работоспособности канала связи 1 будет выполнено переключение на канал связи 2. После восстановления работоспособности канала 1 будет выполнено обратное переключение.

Если при неработоспособном канале 1 нарушается работоспособность канала 2, будет выполнено переключение на канал 3. При восстановлении работоспособности каналов 1 и 2 будет выполнено переключение на канал, имеющий более высокий приоритет.

Параметры настройки свойств одного из каналов (для канала 2) приведены на рисунке ниже.

Свойства канала связи

Внешний интерфейс КШ:

IP-адрес маршрутизатора к провайдеру:

☒ Диагностика работоспособности канала

IP-адрес контрольной точки:

Метод тестирования: ☒ Ping ☐ TCP

Порт:

Интервал диагностики, сек:

Количество успешных попыток для признания канала работоспособным:

Количество неудачных попыток для признания канала неработоспособным:

☐ Регистрация в журнале

OK Отмена

Параметры настройки, устанавливаемые на вкладке "Multi-WAN", приведены на рисунке ниже.

Свойства криптошлюза - Москва (IPC-1000)

Общие сведения | Интерфейсы | Управление QoS | DHCP | Журналы
 Резервирование | Маршрутизация | Multi-WAN | Связи | Членство в группах | Версия ПО

Режим Multi-WAN:

Каналы WAN (в порядке убывания приоритета)

Приоритет	Интерфейс	Маршрут	Метод	Адрес
<input checked="" type="checkbox"/> 1	igb0	1.1.1.100	Ping	1.1.1.100
<input checked="" type="checkbox"/> 2	igb1	1.1.2.100	Ping	8.8.8.8
<input checked="" type="checkbox"/> 3	tun0	0.0.0.0	Ping	8.8.8.8

↓ ↑ Добавить... Удалить Изменить...

Режим обратного переключения на работоспособный канал с высшим приоритетом

☒ Немедленно

☐ Переключать активные соединения через минут

☐ Не переключать активные соединения

☒ Автоматический исходящий NAT

OK Отмена Применить

Балансировка трафика между внешними интерфейсами сетевого устройства

В режиме балансировки трафика распределение нагрузки на внешние интерфейсы осуществляется в соответствии с назначенными для внешних каналов весами.

Вес канала – количество последовательных соединений для данного класса исходящего трафика. По достижении заданного количества соединений исходящий трафик перенаправляется на другой внешний канал. Вес канала может составлять от 0 до 10.

Примечание. При установке веса канала равным 0 и при наличии каналов с весом больше 0 открытый трафик будет перенаправляться в эти каналы (режим round robin), минуя канал с весом 0, и будет распределяться согласно их весам. Если активен только канал с весом 0, трафик будет направлен в этот канал. При активности нескольких каналов с весом 0 трафик будет последовательно распределяться между этими каналами.

Для настройки режима балансировки нагрузки:

1. Сформируйте перечень каналов и выберите режим "Балансировка трафика между внешними интерфейсами <сетевого устройства>" (см. стр. 69).
2. В поле "Каналы WAN" укажите вес канала. Вес выбранного канала устанавливаются с помощью ползунка, расположенного слева под списком каналов.

Удаление отметки в левой части записи отключает использование данного канала без удаления записи из списка.

3. В поле "Политики балансировки трафика" сформируйте перечень правил распределения трафика. Для формирования списка используйте кнопки:

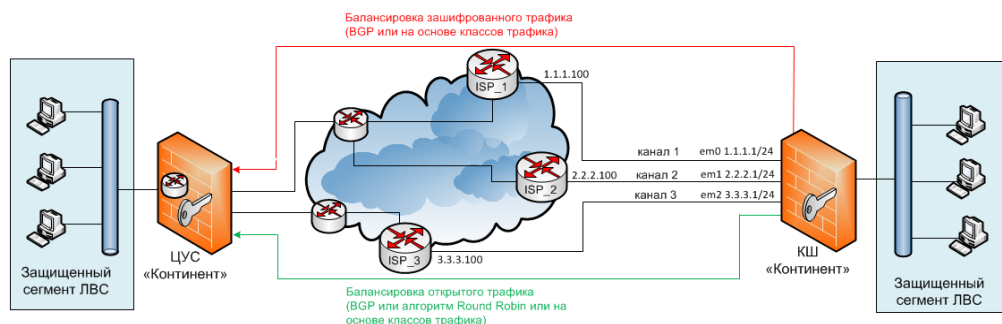
Добавить...	Вызывает на экран диалог "Параметры политики балансировки трафика" для создания в списке новой записи
Удалить	Удаляет из списка выбранную запись
Изменить...	Вызывает на экран диалог "Параметры политики балансировки трафика" для редактирования выбранной записи

Процедуру настройки правил распределения трафика см. стр. 74.

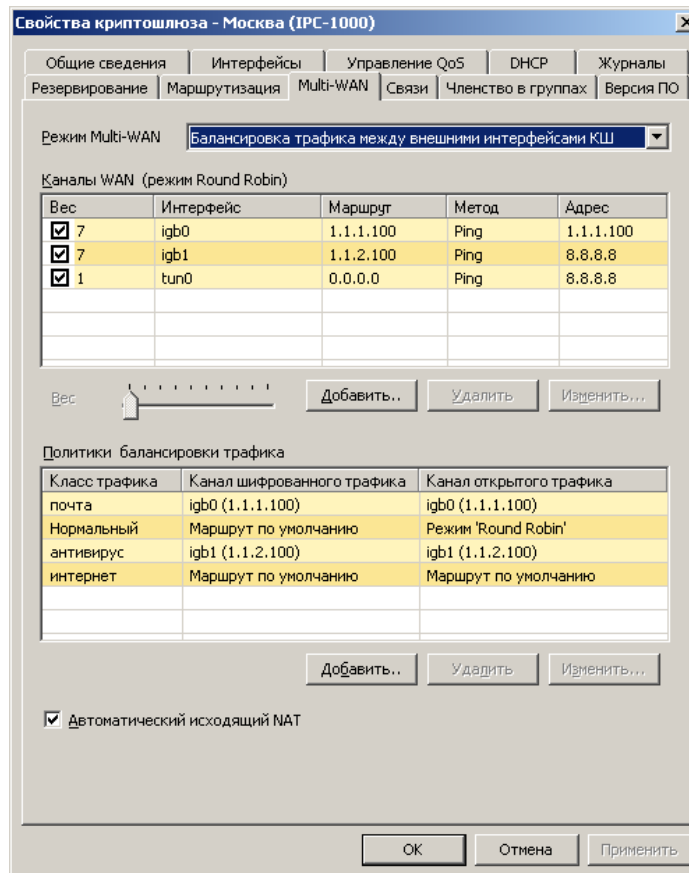
4. При необходимости установите отметку в поле "Автоматический исходящий NAT". При наличии отметки автоматически создаются правила трансляции, которые для всего исходящего трафика подменяют адрес отправителя на адрес указанного в настройках балансировки внешнего интерфейса. Правила трансляции, заданные администратором, отменяются.

5. Нажмите кнопку "ОК".

Ниже приведен пример настройки режима балансировки для КШ, имеющего три внешних канала (см. рисунок ниже).



Параметры настройки, устанавливаемые на вкладке "Multi-WAN", приведены на рисунке ниже.



Настройка правила распределения трафика

Для настройки правила распределения трафика:

1. Вызовите диалог "Параметры политики балансировки трафика" (см. стр. 73).
2. Заполните поля диалога и нажмите кнопку "OK".

Класс трафика	Зарегистрированный в справочнике класс трафика (см. стр. 82)
Канал WAN для передачи зашифрованного трафика	Внешний канал для передачи зашифрованного трафика
Канал WAN для передачи открытого трафика	<ul style="list-style-type: none"> • Внешний канал для передачи открытого трафика. • Режим Round Robin (распределение трафика между каналами в соответствии с их весами)

Выключение режима Multi-WAN

Для выключения режима:

1. Вызовите контекстное меню объекта с именем нужного сетевого устройства и активируйте команду "Свойства...".
На экране появится окно "Свойства <сетевого устройства>".
2. Перейдите к вкладке "Multi-WAN".
3. Удалите все каналы из списка и выберите режим "Передача трафика в соответствии с таблицей маршрутизации".
4. Нажмите кнопку "OK".

Настройки сервиса DHCP

По умолчанию после установки и инициализации КШ режим DHCP отключен.

Настройки сервиса DHCP на КШ выполняют в диалоговом окне "Свойства криптошлюза".

Вызов окна настройки сервиса DHCP

Для вызова окна настройки:

1. Вызовите контекстное меню объекта с именем КШ, на котором требуется выполнить или изменить настройку сервиса DHCP, и активируйте команду "Свойства...".

На экране появится окно "Свойства криптошлюза".

2. Перейдите к вкладке "DHCP".

На вкладке отображается установленный для данного устройства один из трех возможных режимов работы сервиса DHCP:

- Отключено;
- Сервер;
- Ретранслятор.

При установленном режиме "Сервер" на вкладке отображаются его настройки в виде списка профилей. Профиль сервера – это пара "внутренний интерфейс – сетевой объект", для которой администратором заданы параметры сервиса DHCP.

При установленном режиме "Ретранслятор" на вкладке отображаются IP-адрес сервера DHCP и профили ретранслятора. Профиль ретранслятора – это внутренний интерфейс сетевого устройства, на котором должен работать сервис, и соответствующие данному интерфейсу параметры ретранслятора. Параметрами ретранслятора являются:

- Relay Agent Information;
- Remote ID;
- Circuit ID.

Включение и настройка режима сервера

Для включения и настройки:

1. На вкладке "DHCP" установите отметку в поле "Сервер".
Станут доступны кнопки управления списком профилей.
2. Для добавления нового профиля нажмите кнопку "Добавить".
На экране появится диалог "Профиль DHCP-сервера".

Заполните поля диалога.

Внутренний интерфейс	Внутренний интерфейс сетевого устройства, на котором должен работать DHCP-сервис. Для выбора внутреннего интерфейса из детализированного списка используйте кнопку, расположенную справа
Сетевой объект	Сетевой объект, привязанный к указанному внутреннему интерфейсу, который должен ограничивать область раздачи адресов. Для выбора объекта из детализированного списка используйте кнопку, расположенную справа. При выборе из детализированного списка можно выбрать объект и просмотреть его свойства
Пулы IP-адресов	Один или несколько диапазонов адресов, ограниченные начальным и конечным IP-адресом
Постоянные адреса	Назначаемые вручную постоянные IP-адреса, не входящие в указанные пулы адресов и привязанные к MAC-адресам
Время аренды	По умолчанию 24 часа
Маска подсети	В маску должны попадать пулы адресов и маршрутизатор

Основной шлюз	IP-адрес шлюза не должен попадать в пулы адресов
Имя домена	Необязательный параметр
DNS-серверы	Адреса DNS-серверов

Нажмите кнопку "ОК".

Диалог "Профиль DHCP-сервера" закроется и на вкладке "DHCP" в списке появится новый профиль.

3. При необходимости добавления профиля для другого внутреннего интерфейса выполните **п.2**.

Для редактирования списка профилей используйте кнопки "Добавить", "Удалить" и "Изменить".

4. Для сохранения изменений и завершения настройки нажмите кнопку "ОК".

Примечание. После включения режима у данного сетевого устройства в списке устройств появится отметка о включенном режиме сервера DHCP.

Включение и настройка ретранслятора

Для включения и настройки:

1. На вкладке "DHCP" установите отметку в поле "Ретранслятор".

Станут доступны поле "Адрес сервера DHCP" и кнопки управления списком профилей ретранслятора.

2. В поле "Адрес сервера DHCP" введите IP-адрес сервера, на который сетевое устройство будет перенаправлять запросы клиентов.

3. Для добавления нового профиля нажмите кнопку "Добавить".

На экране появится диалог "Профиль ретранслятора DHCP".

4. Заполните поля диалога. Для выбора внутреннего интерфейса из детализированного списка используйте кнопку, расположенную справа.

После выбора внутреннего интерфейса остальные поля профиля заполняются автоматически.

5. Нажмите кнопку "ОК".

Диалог "Профиль ретранслятора DHCP" закроется и на вкладке "DHCP" в списке появится новый профиль ретранслятора.

6. При необходимости добавления профиля для другого внутреннего интерфейса выполните **пп. 3-5**.

- Для изменения адреса сервера DHCP введите в соответствующем поле его IP-адрес.
- Для редактирования списка профилей используйте кнопки "Добавить", "Удалить" и "Изменить".

7. Для сохранения изменений и завершения настройки нажмите кнопку "ОК".

Внимание! После включения режима ретранслятора настройки для режима сервера DHCP будут сброшены.

Примечание. После включения режима у данного сетевого устройства в списке устройств появится отметка о включенном режиме ретранслятора DHCP.

Отключение сервиса DHCP

Для отключения сервиса:

1. На вкладке "DHCP" установите отметку в поле "Отключен".

Кнопки управления списками профилей для режимов "Сервер" и "Ретранслятор" станут недоступны.

2. Для сохранения изменений и завершения настройки нажмите кнопку "ОК".

Внимание! После отключения сервиса DHCP все настройки, выполненные ранее для сервиса, будут сброшены.

Просмотр статистики сервера DHCP

При включенном на сетевом устройстве режиме сервера DHCP в ПУ ЦУС можно просмотреть статистику сервера и таблицу арендованных адресов. Статистика и арендованные адреса отображаются на вкладке "DHCP" дополнительного окна.

Для просмотра статистики:

- В главном окне ПУ ЦУС выберите в списке сетевое устройство, работающее в режиме сервера DHCP.

На вкладке "DHCP" дополнительного окна отобразятся статистика сервера и таблица арендованных адресов.

Примечание. Если вкладка "DHCP" скрыта, настройте ее отображение с помощью меню "Вид" (см. стр. 43).

Статистика включает в себя следующие сведения:

- имя внутреннего интерфейса сетевого устройства;
- общее количество адресов пула;
- количество используемых адресов пула;
- количество доступных адресов пула.

В таблице арендованных адресов приводятся следующие сведения:

- IP-адрес, выданный клиенту из пула адресов;
- MAC-адрес клиента;
- сетевое имя клиента;
- дата и время начала аренды;
- дата и время окончания аренды.

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. [112](#)).

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 (см. стр. [82](#)). Состояние защищенных соединений отображается в разделе "Каналы VPN" вкладки "Состояние <сетевого устройства>" общей таблицы состояния <сетевого устройства> (см. стр. [164](#)).

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.

Настройка параметров маршрутизации

Переход к настройке параметров

Режимы работы сетевого устройства:

- динамическая маршрутизация;
- статическая маршрутизация.

Просмотр и настройка параметров режима работы осуществляются в окне свойств сетевого устройства на вкладке "Маршрутизация".

Для просмотра и настройки параметров режима работы:

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

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

2. Перейдите к вкладке "Маршрутизация".

Вид вкладки и ее содержание зависят от режима, в котором работает в данный момент сетевое устройство.

Примечание. Если настройка режимов не производилась, по умолчанию вкладка будет соответствовать режиму статической маршрутизации.

Переключение режима маршрутизации

Ниже приведены процедуры переключения режима работы сетевого устройства со статической маршрутизации на динамическую и наоборот.

Для переключения со статической на динамическую маршрутизацию:

1. Перейдите к настройке параметров маршрутизации (см. стр.79).




Вкладка "Маршрутизация" отображает настройки статической маршрутизации. На вкладке представлен список правил для данного сетевого устройства и кнопки, с помощью которых выполняется настройка.

2. В поле "Тип" измените значение на "Динамическая (поддержка протоколов OSPF, RIP, BGP)".

Вид вкладки изменится и станет соответствовать режиму динамической маршрутизации. На вкладке будут отображаться раздел с информацией о маршрутах и разделы с конфигурациями для данного сетевого устройства.

Примечание. При переключении вида вкладки информация о конфигурациях в соответствующих разделах не отображается.

Справа от каждого раздела расположены кнопки.

 <p>Прервать обновление</p>	<p>Прерывает процесс обновления отображаемых сведений о маршрутах, поступающих от ЦУС. После открытия вкладки "Маршрутизация" кнопка недоступна в течение примерно 50 секунд. После завершения загрузки информации о маршрутах кнопка заменяется кнопкой "Обновить список маршрутов" (см. ниже)</p>
 <p>Обновить список маршрутов</p>	<p>Запускает процесс обновления отображаемых сведений о маршрутах. Если сетевое устройство в данный момент выключено, кнопка недоступна</p>
 <p>Загрузить конфигурацию из файла</p>	<p>Запускает стандартную процедуру загрузки файла. Используется для загрузки конфигурационного файла zebra и конфигураций для поддерживаемых протоколов</p>



Сохранить маршруты/конфигурацию в файл

Запускает стандартную процедуру сохранения содержимого соответствующего раздела в текстовый файл

3. Выполните процедуру настройки динамической маршрутизации (см. стр. **81**).

Для переключения с динамической маршрутизации на статическую:

1. Перейдите к настройке параметров маршрутизации (см. стр. **79**).

Вкладка "Маршрутизация" отображает настройки динамической маршрутизации. Кнопка "Прервать обновление" недоступна.

2. В поле "Тип" измените значение на "Статическая".

Вид вкладки изменится и станет соответствовать режиму статической маршрутизации.

3. Нажмите кнопку "Применить".

В поле "Информация о маршрутах" появятся правила, сформированные автоматически, и станут доступными кнопки <Добавить>, <Изменить> и <Удалить>.

4. При необходимости измените список правил (см. стр. **81**).

Статическая маршрутизация

Правила маршрутизации подразделяются на два типа:

- правила, сформированные комплексом автоматически;
- правила, заданные администратором.

Правила, сформированные автоматически, предусматривают взаимодействие только между сегментами сети, подключенными непосредственно к интерфейсам сетевого устройства. Формирование таких правил происходит при добавлении очередного адреса сетевого интерфейса. Правила этого типа действуют постоянно и не могут быть удалены или изменены администратором. Начальное заполнение поля "Правила маршрутизации" осуществляется на этапе подключения сетевого устройства.

На основе правил маршрутизации постоянного действия комплекс автоматически формирует временные правила. Временное правило формируется при поступлении на сетевое устройство IP- пакета, адресованного одному из абонентов защищаемой сети. Такое правило имеет ограниченное время действия, и если за это время на данный адрес не поступает новый пакет, правило уничтожается. Если пакет поступает, отсчет времени действия правила начинается заново. Кроме приведенного примера временные правила создаются также при наличии на пути прохождения IP-пакета сетей, характеризующихся значением MTU меньшим, чем у интерфейса сетевого устройства. Правила этого типа не могут быть удалены или изменены администратором. Они не отображаются на экране.

Если защищаемая сеть подсоединена к сетевому устройству через маршрутизатор, правила маршрутизации для абонентов этой сети задаются администратором. Эти правила действуют постоянно.

Внимание! Не изменяйте настройки в диалоге "Маршрутизация" без крайней необходимости. При некорректном вводе правил маршрутизации сетевое устройство работать не будет.

Список правил маршрутизации отображается в виде таблицы, каждая строка которой соответствует одному правилу. Перечень полей таблицы правил маршрутизации и их описание представлены в таблице ниже.

Табл.12 Поля таблицы правил маршрутизации

Поле	Описание
------	----------

Адрес	IP-адрес подсети абонента-получателя
Маска	Маска подсети абонента-получателя
Следующий узел	IP-адрес следующего узла, через который должны проходить IP-пакеты для абонента-получателя

Правило маршрутизации с нулевыми маской и адресом назначения отображает маршрут по умолчанию.

Внимание! Если маршрут по умолчанию связывает сетевое устройство с ЦУС, то после его изменения соединение устройства с ЦУС становится невозможным. В этом случае требуется запись новой конфигурации на носитель и повторная инициализация сетевого устройства.

Нулевой адрес в столбце "Следующий узел" указывает, что данная подсеть доступна напрямую через интерфейс, без промежуточных маршрутизаторов.

Для настройки правил маршрутизации:

1. Перейдите к настройке параметров маршрутизации (см. стр. 79)

При необходимости переключите вкладку на соответствие режиму статической маршрутизации (см. стр. 79).

2. Определите параметры правил.

- Чтобы добавить запись в список правил маршрутизации, нажмите кнопку "Добавить", укажите протокол (IPv4 или IPv6) и введите адрес и маску (префикс) для данной сети. Если защищаемая сеть подсоединена к сетевому устройству через маршрутизатор, в поле "Следующий узел" укажите адрес этого маршрутизатора. Затем нажмите кнопку "ОК".

Введенные данные появятся в списке правил маршрутизации.

- Для изменения записи в списке правил маршрутизации выберите нужную строку. Параметры выбранного правила будут отображены в полях, расположенных под списком. Внесите необходимые изменения и нажмите кнопку "Изменить".
- Чтобы удалить запись из списка правил маршрутизации, выберите нужную строку и нажмите кнопку "Удалить". Выбранная запись будет удалена немедленно.

Изменения в настройках таблицы маршрутизации применяются немедленно.

Динамическая маршрутизация

Динамическая маршрутизация не поддерживается в следующих случаях:

- включен режим привязки маршрутизаторов к MAC-адресам (см. [2]);
- включен один из режимов Multi-WAN (см. стр. 68).

Для поддержки протоколов динамической маршрутизации необходимо сформировать конфигурационный файл `zebra.conf`, а также конфигурационные файлы используемых протоколов (`ospfd.conf`, `bgpd.conf`, `ripd.conf`).

Внимание! Поддерживаются следующие версии протоколов:

- OSPF — версия 2;
- BGP — версия 4;
- RIP — версия 1, версия 2.

Настройку динамической маршрутизации выполняют в следующем порядке:

- создание конфигурационного файла (см. стр. 189);
- настройка параметров динамической маршрутизации (см. ниже).

Для настройки параметров:

1. Перейдите к настройке параметров маршрутизации (см. стр. 79) и при необходимости переключите вкладку на соответствие режиму динамической маршрутизации (см. стр. 79).
2. Определите параметры правил маршрутизации:

- Загрузите конфигурационный файл zebra.conf. Для этого используйте кнопку "Открыть" справа от поля "Конфигурация zebra" или введите в поле текст конфигурационного файла вручную.
- Откройте вкладку нужного протокола и загрузите для него конфигурационный файл. Для этого используйте кнопку "Открыть", расположенную справа, или введите текст конфигурационного файла вручную.

3. Нажмите кнопку "Применить".

Сетевому устройству будет отправлена команда на загрузку в ЦУС списка маршрутов, и в ЦУС начнется обновление информации о сетевом устройстве.

Примечание. Подтверждение о ходе выполнения команды отображается в очереди заданий (см. стр. 85).

После завершения обновления из ЦУС в ПУ поступит список маршрутов данного сетевого устройства, который отобразится в разделе "Информация о маршрутах". Кнопка "Прервать обновление" заменится на кнопку "Обновить список маршрутов".

Внимание! При достаточно большом количестве маршрутов обновление информации на ЦУС может потребовать дополнительного времени. При этом кнопка "Прервать обновление" в течение примерно 50 секунд будет недоступна. Если в просмотре информации о маршрутах нет необходимости, откажитесь от обновления. Для этого нажмите кнопку "Прервать обновление".

4. Если необходимо сохранить в виде текстового файла информацию о маршрутах или конфигурациях, используйте кнопку "Сохранить", расположенную справа от соответствующего раздела.

Примечание. После закрытия окна "Свойства <сетевого устройства>" информация о маршрутах, отображаемая на вкладке "Маршрутизация", не сохраняется. При следующем открытии окна на вкладке "Маршрутизация" раздел "Информация о маршрутах" будет пустым.

Внимание! Для стабильной работы сетевого устройства рекомендуется настройку параметров динамической маршрутизации оптимизировать таким образом, чтобы количество маршрутов в таблице маршрутизации не превышало лимит, указанный в паспорте сетевого устройства.

Определение классов трафика

Для определения класса трафика:

1. В левой части окна программы управления выберите папку "Центр управления сетью > Классы трафика".

В правой части окна отобразится перечень классов трафика.

Примечание. Класс трафика "Нормальный" создается автоматически при инициализации ЦУС.

2. В списке классов трафика вызовите контекстное меню и активируйте нужную команду:

Создать	Вызывает диалог для регистрации нового класса трафика
Свойства	Вызывает диалог свойств класса для редактирования выбранной записи

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

Название	Наименование класса трафика
Описание	Произвольный текстовый комментарий (необязательный параметр)
Приоритет шифрования	Очередность обработки IP-пакета, отнесенного к данному классу, блоком криптографической защиты. Возможные значения 0–31. Большшему значению соответствует более высокий приоритет

Порт внешнего интерфейса для зашифрованного трафика	Порт внешнего интерфейса, с которого отправляются IP-пакеты данного класса
Не менять	Сохраняет значение поля ToS у исходящего IP-пакета таким же, как у входящего
Установить значение	Назначает исходящему IP-пакету значение поля ToS, указанное ниже
Bin/Hex	Отображает назначаемое значение поля ToS в двоичном или шестнадцатеричном виде
Код DSCP (биты 1 – 6)	Определяет значение поля ToS по шестибитному классификатору DSCP. Возможные значения 0–63
Приоритет (биты 1 – 3)	Определяет первые три бита значения поля ToS по классификатору IPP. Возможные значения 0–7
Низкая задержка	Определяет четвертый бит значения поля ToS. Наличие отметки указывает режим низкой задержки
Высокая пропускная способность	Определяет пятый бит значения поля ToS. Наличие отметки указывает режим высокой пропускной способности
Высокая надежность	Определяет шестой бит значения поля ToS. Наличие отметки указывает режим высокой надежности

Управление приоритизацией трафика

Вызов окна управления QoS

Настройку очереди на отправку для КШ и криптокоммутаторов выполняют в диалоге "Управление QoS".

Для вызова окна управления QoS:

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 "Управление QoS".

На вкладке отображается иерархический список сетевых интерфейсов данного устройства и действующих на них очередей. Для формирования очередей используйте кнопки:

Импорт...	Запускает процедуру импорта конфигурации очередей из XML-файла
Экспорт...	Формирует XML-файл для переноса конфигурации очередей на другое устройство
Добавить очередь...	Вызывает на экран диалог для настройки параметров новой очереди
Удалить очередь	Удаляет выбранную очередь
Изменить...	<ul style="list-style-type: none"> • Вызывает на экран диалог для настройки параметров выбранного интерфейса. • Вызывает на экран диалог для настройки параметров выбранной очереди

Настройка общих параметров очереди на интерфейсе

Для настройки общих параметров очереди:

1. Перейдите к вкладке "Управление QoS" (см. стр. [83](#)).

2. Выберите нужный сетевой интерфейс и нажмите кнопку "Изменить...".
На экране появится диалог "Параметры интерфейса".
3. Заполните поля диалога и нажмите кнопку "ОК":

Тип приоритизации	Метод обработки очереди
Полоса пропускания, Кбит/с	Общая пропускная способность данного интерфейса. 0 — максимально возможная

Настройка параметров очереди

Для настройки очереди:

1. Перейдите к вкладке "Управление QoS" (см. стр. [83](#)).
2. Выполните одно из следующих действий:
 - для создания новой очереди выберите нужный интерфейс и нажмите кнопку "Добавить очередь...";
 - для редактирования выберите нужную очередь и нажмите кнопку "Изменить...".

На экране появится диалог для настройки свойств очереди. Вид диалога зависит от значения в поле "Тип приоритизации".

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

<Сетевое устройство>	Наименование сетевого устройства (недоступно для изменений)
Интерфейс	Наименование интерфейса (недоступно для изменений)
Общая полоса пропускания, Кбит/с	Общая пропускная способность данного интерфейса. 0 — максимально возможная (недоступно для изменений)
Тип приоритизации	Метод обработки очереди (недоступно для изменений)
Название очереди	Наименование очереди
Очередь по умолчанию	При наличии отметки данная очередь назначается очередью по умолчанию. В эту очередь будут попадать IP-пакеты, для которых очереди не определены
Приоритет	Последовательность обработки очередей. Возможные значения 0–7 для CBQ и HFSC, 0–15 для PRIQ. Большее значение соответствует более высокому приоритету
Классы трафика	Перечень классов трафика, включаемых в данную очередь. Для формирования списка используйте кнопки "Добавить..." и "Удалить"
Защита от перегрузок	Установка отметки включает указанный механизм защиты от перегрузок (RED, RIO, ECN)
Полоса пропускания, %	Доля общей полосы пропускания, выделенная для данной очереди, в процентах (только для CBQ)
Увеличить по возможности (borrow)	Установка отметки включает механизм заимствования общей полосы пропускания в случае неиспользования ее другими очередями (только для CBQ)
realtime, %	Доля общей полосы пропускания, выделенная для режима realtime, в процентах (только для HFSC)
upperlimit, %	Максимальная доля общей полосы пропускания, в процентах (только для HFSC)
linkshare, %	Доля общей полосы пропускания, выделенная для режима linkshare, в процентах (только для HFSC)

Экспорт/импорт конфигурации очередей

Для переноса настроек на другие сетевые устройства имеется возможность экспорта/ импорта конфигурации очередей на сетевых интерфейсах с помощью файла XML.

Для экспорта конфигурации:

1. Перейдите к вкладке "Управление QoS" (см. стр. [83](#)).
2. Нажмите кнопку "Экспорт...".

На экране появится стандартный диалог Windows для сохранения файла.

3. Выберите папку, укажите название файла и нажмите кнопку "Сохранить".

Для импорта конфигурации:

1. Перейдите к вкладке "Управление QoS" (см. выше).
2. Нажмите кнопку "Импорт...".

На экране появится стандартный диалог Windows для открытия файла.

3. Выберите нужные папку и файл и нажмите кнопку "Открыть".

На экране появится диалог "Импорт настроек QoS".

В левой части диалога представлен перечень интерфейсов сетевого устройства, в правой части отображается импортируемая конфигурация очередей.

4. Сопоставьте интерфейсам сетевого устройства названия интерфейсов импортируемой конфигурации. С этой целью для каждого значения в поле "Интерфейс на <сетевом устройстве>" выберите нужное значение из раскрывающегося списка в поле "Интерфейс из XML".

5. Нажмите кнопку "ОК".

На вкладке "Управление QoS" отобразится импортированная конфигурация очередей.

Управление очередью заданий

С помощью программы управления можно просмотреть и изменить очередь заданий любого сетевого устройства комплекса. Очередь заданий сетевого устройства содержит список текущих заданий, которые сформированы для устройства, но еще не выполнены.

Для просмотра очереди заданий:

- Выберите в главном окне нужное устройство и перейдите к вкладке "Очередь заданий" дополнительного окна.

На этой вкладке отображается список текущих заданий данного сетевого устройства. Этот список будет пуст, если все текущие задания выполнены.

Список заданий, составляющих очередь, отображается в форме таблицы, каждая строка которой соответствует одному заданию. Перечень полей, отображаемых в списке заданий, и их описание представлены в таблице ниже.

Табл.13 Перечень полей списка заданий

Поле	Описание
Описание	Наименование задания
Время ожидания	Интервал времени, прошедший с момента формирования задания

В случае необходимости из очереди могут быть удалены выбранные задания, а также может быть очищена вся очередь. Для удаления заданий или очистки очереди используйте кнопки, расположенные на вкладке, или команды контекстного меню.

Режим изолированной сети

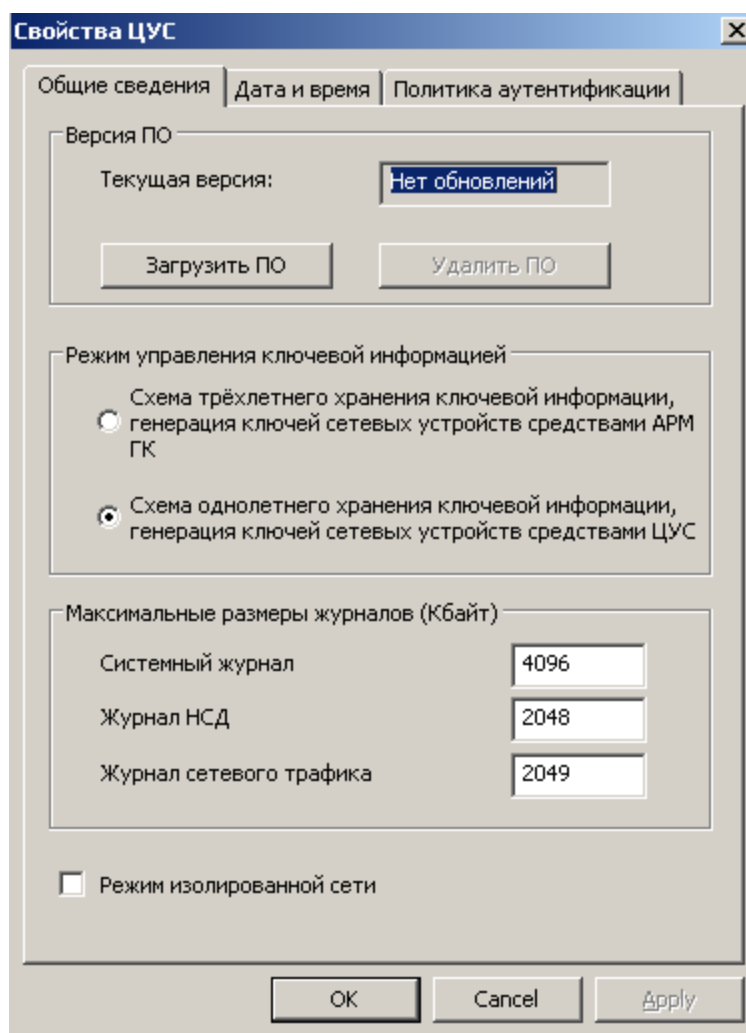
Предусмотрен режим изоляции криптошлюзов от внешней среды, при котором ни одно из сетевых устройств, входящих в криптографическую сеть ЦУС, не будет пропускать через свои внешние интерфейсы открытый трафик. По умолчанию режим изолированной сети выключен.

Внимание! Режим изолированной сети не может быть включен, если в сети зарегистрированы сетевые устройства версии ниже 3.7 и КШ с установленным СД, а также установлены связи со сторонними криптографическими сетями (см. стр. 154). При включенном режиме изолированной сети действуют следующие ограничения:

- На внешних интерфейсах сетевого устройства разрешены только управляющий трафик и трафик, передаваемый между связанными сетевыми устройствами (см. стр. 78).
- В режиме Multi-WAN функция тестирования каналов недоступна.
- Запрещена отправка во внешнюю сеть DNS- и NTP-запросов.
- В дополнительном меню локального управления сетевого устройства (см. [2]) команды "Выполнить ping" и "Выполнить traceroute" с адресами, принадлежащими внешним сетям, выполняться не будут.
- Динамическая адресация на внешних интерфейсах сетевого устройства не используется.
- Пакеты от DHCP-ретранслятора с внешнего интерфейса КШ не отправляются.

Для включения/выключения режима изолированной сети:

1. Активируйте в меню "ЦУС" команду "Свойства".
Появится диалоговое окно "Свойства ЦУС".



2. Установите или удалите отметку в поле "Режим изолированной сети" и нажмите кнопку "OK".

Диалоговое окно закроется. На всех сетевых устройствах будет установлен режим, соответствующий выполненному действию, и автоматически будут обновлены правила фильтрации.

Установка времени на ЦУС

Правильную текущую дату и время на ЦУС можно установить вручную или использовать режим синхронизации с NTP-серверами точного времени.

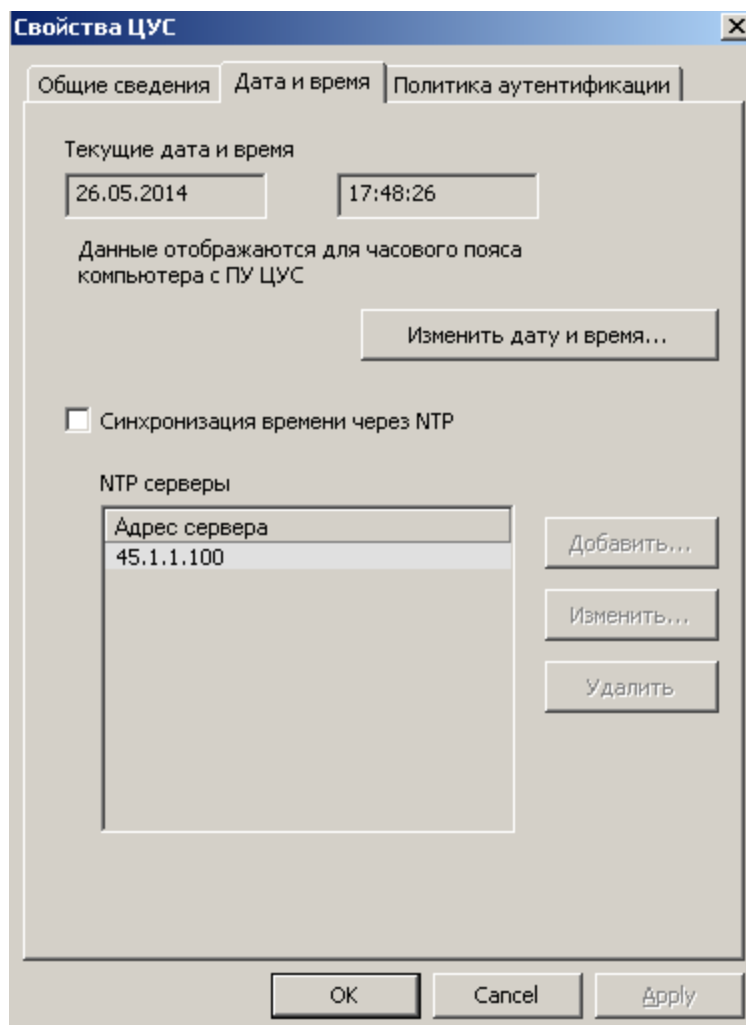
Для задания режима синхронизации с NTP-сервером необходимо указать его DNS или IP-адрес. Синхронизация с NTP-сервером осуществляется каждый час. Предусмотрена возможность задать список серверов точного времени. В этом случае для синхронизации автоматически выбирается наиболее точный из них.

Внимание! Для NTP-сервера, работающего под управлением ОС Windows, должны быть установлены следующие значения параметров реестра:

- `regedit SYSTEM\CurrentControlSet\Services\W32Time\Config\LocalClockDispersion = 0`
- `regedit SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags = 5`

Для установки времени на ЦУС:

1. Активируйте в меню "ЦУС" команду "Свойства".
Появится диалоговое окно "Свойства ЦУС".
2. Перейдите на вкладку "Дата и время".



На вкладке отображаются:

- текущая дата и время для часового пояса компьютера с ПУ ЦУС;
- признак включенного или выключенного режима синхронизации с NTP-серверами;
- список NTP-серверов (если задан).

3. Для установки даты и времени вручную удалите отметку в поле "Синхронизация времени через NTP" (если она установлена) и нажмите кнопку "Изменить дату и время".

Станут доступными поля "Текущие дата и время".

4. Введите дату и время и перейдите к п.8.
5. Для задания режима синхронизации установите отметку в поле "Синхронизация времени через NTP".
Станет доступной кнопка "Добавить".
6. Нажмите кнопку "Добавить".

На экране появится окно для ввода адреса NTP-сервера.

Введите адрес NTP-сервера и нажмите кнопку "OK".

Примечание. Допускается ввод как IP-адреса NTP-сервера, так и его сетевого имени. Если вводится сетевое имя, в свойствах КШ с ЦУС необходимо указать DNS-сервер (см. ниже).

Диалог ввода адреса закроется и NTP-сервер будет добавлен в список.

7. При необходимости добавьте в список другие серверы.
Для работы со списком используйте кнопки, расположенные справа.

Для изменения адреса уже имеющегося в списке сервера выделите его и нажмите кнопку "Изменить".

8. Для сохранения выполненных изменений нажмите кнопку "ОК" на вкладке "Дата и время".

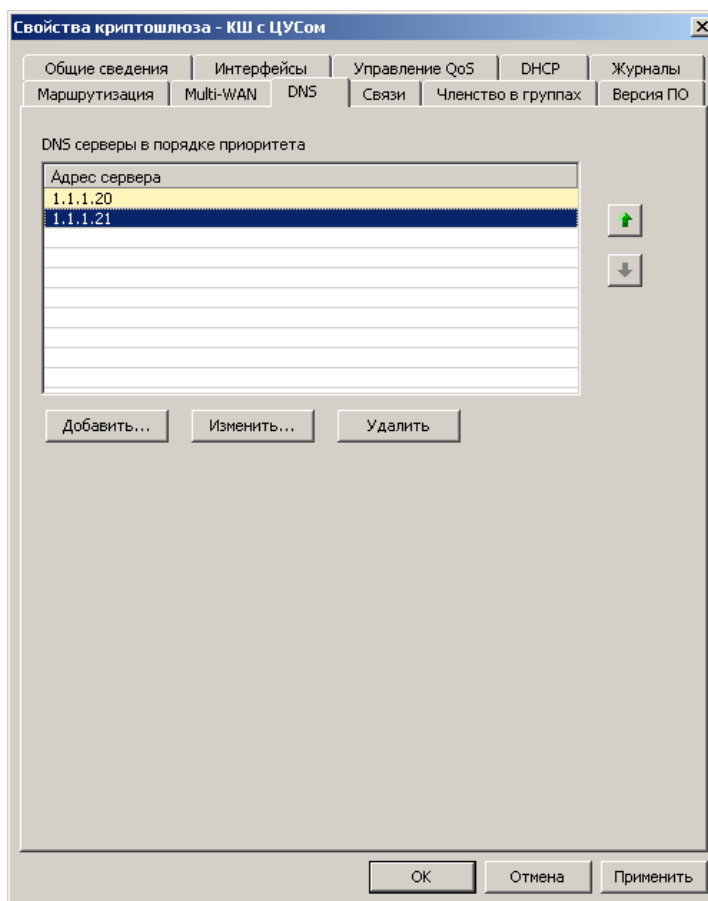
Диалоговое окно "Свойства ЦУС" закроется.

Для указания DNS-сервера:

1. Откройте список криптошлюзов, вызовите контекстное меню для КШ с ЦУС и активируйте команду "Свойства".

На экране появится окно "Свойства криптошлюза"

2. Перейдите к вкладке "DNS".



На вкладке отображается список DNS-серверов, упорядоченный по убыванию приоритета.

3. Для добавления нового сервера в список нажмите кнопку "Добавить".
На экране появится окно ввода IP-адреса.
4. Выберите протокол (IPv4 или IPv6), введите IP-адрес и нажмите кнопку "ОК".
Указанный адрес появится в списке DNS-серверов.
5. При необходимости добавьте другие DNS-серверы и упорядочьте список в соответствии с приоритетами серверов с помощью кнопок "Вверх" и "Вниз", расположенных справа.
Для удаления или изменения адреса выбранного в списке сервера используйте кнопки "Удалить" и "Изменить" соответственно.
6. Для сохранения выполненных изменений нажмите кнопку "ОК".

Управление криптографической коммутируемой сетью

Для создания криптографической коммутируемой сети необходимо добавить в список объектов ЦУС объект "виртуальный коммутатор" и включить в его состав

порты криптокоммутаторов с указанием для каждого из них внутренних интерфейсов коммутируемых хостов.

Для перехода к списку виртуальных коммутаторов:

- Выберите в дереве объектов узел "Центр управления сетью" и в нем – папку "Виртуальные коммутаторы".

В главном окне отобразится список зарегистрированных виртуальных коммутаторов.

Примечание. Если виртуальные коммутаторы не создавались, список будет пустым.

Для каждого виртуального коммутатора приводятся:

- краткое описание;
- общее количество коммутируемых портов;
- статус парных связей, указывающий на наличие всех необходимых парных связей или отсутствие каких-либо из них.

Для добавления в список нового виртуального коммутатора:

1. Нажмите на панели инструментов кнопку "Создать виртуальный коммутатор".

На экране появится диалог "Виртуальный коммутатор".

Виртуальный коммутатор

Название: test ipc25-1115

Описание:

Порты коммутации

Криптокоммутатор	Порт криптокоммутатора	Класс трафика
test8	em1	Нормальный
test8	em2	Нормальный
test9	em1	Нормальный

Добавить...
Изменить...
Удалить
MAC-адреса
OK
Отмена

☒ Автоматически создавать парные связи

2. Введите название и краткое описание нового виртуального коммутатора.
3. Сформируйте список портов криптокоммутаторов, входящих в состав данного виртуального коммутатора. Для этого нажмите кнопку "Добавить".

На экране появится диалог "Порт коммутации".

Порт коммутации

Криптокоммутатор: test8

Порт криптокоммутатора: em1

Класс трафика: Нормальный

Режим безопасности:

- ☒ **Выключен**
Динамические адреса хранятся не более 20 минут
Допустимы статические адреса, явно указанные в конфигурации
- ☐ **Мягкий**
Динамические адреса сохраняются до перезагрузки криптокоммутатора
Допустимы статические адреса, явно указанные в конфигурации
- ☐ **Жёсткий**
Динамическое обучение запрещено
Допустимы только статические адреса, указанные в конфигурации

Размер таблицы коммутации порта:

- ☐ Не более 0 адресов
- ☒ Автоматически определяется системой

☒ Фиксировать события НСД на пакеты от небезопасных MAC-адресов

OK Отмена

4. Заполните поля диалога.

Криптокоммутатор	Криптокоммутатор, входящий в состав создаваемого виртуального коммутатора
Порт коммутации	Внутренний интерфейс криптокоммутатора, к которому подключена защищаемая подсеть
Класс трафика	Класс трафика, назначаемый данному порту коммутации для приоритизации трафика

Примечание. Для всех портов коммутации, входящих в состав виртуального коммутатора, должно быть установлено одинаковое значение MTU (см. стр. 60).

- Укажите режим безопасности.
- Задайте размер таблицы коммутации. Предусмотрено ограничение количества адресов вручную или автоматическое определение размера таблицы.
Внимание! Данная настройка выполняется только для криптокоммутаторов версии 3.7.5. Для устройств предыдущих версий следует установить значение "Автоматически определяется системой".
- Установите отметку, если необходимо фиксировать события НСД на пакеты от небезопасных MAC-адресов.
Внимание! Данная настройка выполняется только для криптокоммутаторов версии 3.7.5. Для устройств предыдущих версий отметку следует удалить.
- После настройки параметров нажмите кнопку "OK".
Диалог "Порт коммутации" закроется и указанные сведения отобразятся в списке диалога "Виртуальный коммутатор".

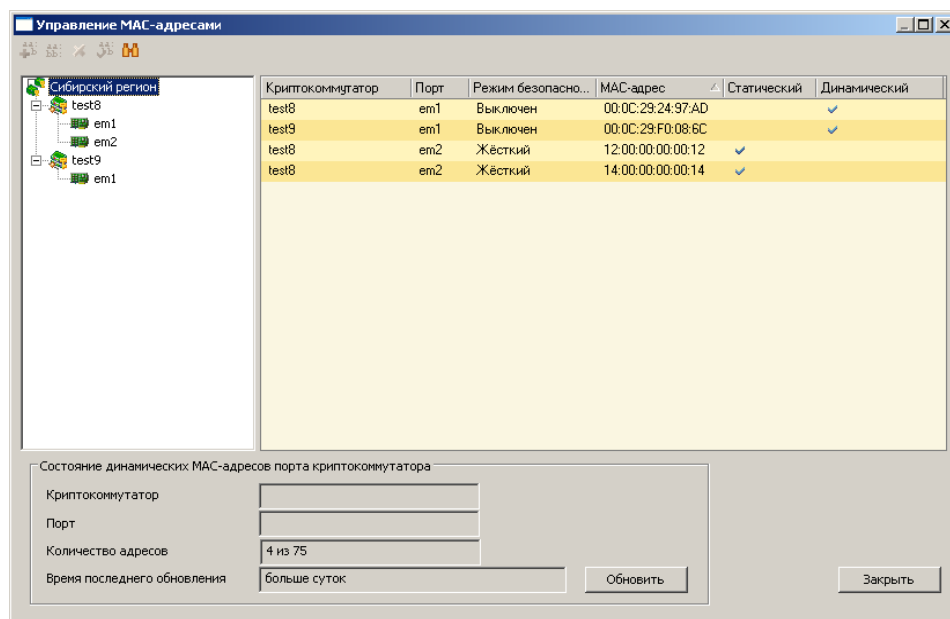
Примечание. Для редактирования списка портов коммутации в диалоге "Виртуальный коммутатор" используйте кнопки "Удалить" и "Изменить", расположенные справа от списка.

9. Если необходимо, чтобы между добавленными в список криптокоммутаторами не должны быть установлены парные связи, удалите отметку в поле "Автоматически создавать парные связи".

Примечание. Отметка в поле "Автоматически создавать парные связи" установлена по умолчанию.

10. Для формирования списка MAC-адресов виртуального коммутатора нажмите кнопку "MAC-адреса".

На экране появится окно "Управление MAC-адресами".



В окне отображается список статических и динамических MAC-адресов виртуального коммутатора.

Примечание. Если MAC-адреса не назначались, в зависимости от выбранного выше режима безопасности список будет пустым или содержать только динамические адреса.

11. Сформируйте список MAC-адресов. Для этого выделите в левой части окна порт, вызовите в правой части окна контекстное меню и выберите команду "Добавить статический адрес". Далее введите адрес.

При формировании списка MAC-адресов предусмотрены следующие операции:

- добавление, изменение и удаление статического адреса;
- преобразование динамического адреса в статический.

Для выполнения перечисленных выше операций используйте команды контекстного меню или кнопки на панели инструментов в верхней части окна.

Внимание! В некоторых случаях (например, по каким-либо причинам сведения о статическом адресе не были переданы из ЦУС в криптокоммутатор) на криптокоммутаторе может быть сформирован динамический адрес, совпадающий со статическим. В этом случае в окне "Управление MAC-адресами" будет отображаться только статический адрес. После удаления этого адреса он будет отображаться в списке как динамический.

При добавлении в список определенного количества статических адресов в сумме с динамическими они могут превысить максимально допустимое количество для данного порта и тем самым нарушить корректную работу криптокоммутатора. В этом случае рекомендуется перезагрузить криптокоммутатор.

12. Для завершения процедуры нажмите кнопку "ОК" в диалоге "Виртуальный коммутатор".

Диалог закроется и в списке виртуальных коммутаторов появится новый объект с указанными выше параметрами.

Для изменения параметров виртуального коммутатора:

1. Вызовите контекстное меню выбранного в списке виртуального коммутатора и выберите команду "Свойства".

На экране появится диалог "Виртуальный коммутатор".

2. Введите необходимые изменения в полях "Название" и "Описание" и при необходимости отредактируйте список "Порты коммутации".

Внимание! Если добавляется новый криптокоммутатор в список, установление парных связей с уже имеющимися в списке криптокоммутаторами зависит от наличия или отсутствия отметки в поле "Автоматически создавать парные связи".

При удалении портов коммутации парные связи не удаляются. Эти связи необходимо удалить вручную.

3. Для сохранения изменений нажмите кнопку "ОК".

Для удаления виртуального коммутатора из списка:

1. Выберите в списке нужный коммутатор и на панели инструментов нажмите кнопку "Удалить".

На экране появится предупреждение об удалении объекта.

2. Нажмите кнопку "ОК" в окне предупреждения.

Виртуальный коммутатор будет удален из списка.

Управление пользователями

Управление списком пользователей

Для вызова списка:

- В окне объектов в левой части окна программы управления выберите папку "Центр управления сетью> Пользователи".

В правой части окна отобразится список зарегистрированных пользователей. Список пользователей отображается в форме таблицы, каждая строка которой соответствует одной учетной записи. Перечень полей, отображаемых в списке, и их описание представлены в таблице ниже.


Табл.14 Перечень полей списка пользователей

Поле	Описание
Имя	Имя пользователя, зарегистрированное в комплексе
Описание	Произвольный текстовый комментарий
Логин	Имя пользователя для идентификации с помощью программы "Клиент аутентификации пользователя"
Заблокирован	При наличии отметки учетная запись пользователя заблокирована

Для регистрации пользователя:

- Выполните одно из следующих действий:
 - вызовите контекстное меню в любом месте списка пользователей и активируйте команду "Создать пользователя";
 - нажмите на панели инструментов кнопку "Создать пользователя...".
 На экране появится диалог "Пользователь".
- Настройте и сохраните параметры учетной записи. Порядок настройки параметров учетной записи см. стр. 95.

Для изменения параметров учетной записи:

- Выберите нужную учетную запись и выполните одно из следующих действий:
 - активируйте в контекстном меню команду "Свойства...";
 - нажмите на панели инструментов кнопку "Свойства пользователя" ().
 После выполнения любого из указанных действий на экране появится диалог "Пользователь".
- Настройте и сохраните параметры учетной записи. Порядок настройки параметров правила см. стр. 95.

Для удаления пользователя:

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

Для создания группы пользователей:

- Выполните одно из следующих действий:
 - вызовите контекстное меню в любом месте списка пользователей и активируйте команду "Создать группу пользователей...";
 - нажмите на панели инструментов кнопку "Создать группу пользователей".
 На экране появится диалог "Группа пользователей".

2. Настройте и сохраните параметры группы. Порядок настройки параметров группы см. стр. **95**.

В окне объектов в папке "Пользователи" появится папка с названием созданной группы. При выборе папки в информационном окне отобразится перечень пользователей, входящих в группу.

Для изменения параметров группы пользователей:

1. Выберите в окне объектов нужную группу пользователей и активируйте в контекстном меню команду "Свойства...".
На экране появится диалог "Группа пользователей".
2. Настройте и сохраните параметры группы. Порядок настройки параметров группы см. стр. **95**.

Для удаления группы пользователей:

- Выберите в окне объектов нужную группу пользователей и активируйте в контекстном меню команду "Удалить группу пользователей...".

Настройка параметров учетной записи

Для настройки параметров учетной записи:

1. Вызовите на экран диалог "Пользователь". Описание процедуры вызова диалога при регистрации пользователя или изменении параметров учетной записи см. стр. **94**.
2. Заполните поля диалога и нажмите кнопку "ОК".

Имя	Имя пользователя, отображаемое в списке пользователей
Описание	Дополнительные сведения (необязательный параметр)
Логин	Имя пользователя для идентификации с помощью программы "Клиент аутентификации пользователя"
Пароль	Пароль пользователя для аутентификации с помощью программы "Клиент аутентификации пользователя". Пароль должен удовлетворять требованиям политики аутентификации администраторов (см. стр. 51)
Подтверждение пароля	
Заблокирован	Установка отметки блокирует учетную запись без удаления ее из списка

Вкладка "Членство в группах" предназначена для ознакомления с перечнем групп, в которые входит пользователь.

Настройка параметров группы пользователей

Доступ предоставляют группам пользователей с помощью правил фильтрации IP-пакетов и правил трансляции сетевых адресов. Группа пользователей связана с определенным сетевым объектом. Доступ, предоставляемый этой группе, действует только на компьютерах, относящихся к этому сетевому объекту.

Для настройки параметров группы пользователей:

1. Вызовите на экран диалог "Группа пользователей". Описание процедуры вызова диалога при создании новой группы или изменении ее параметров см. стр. **94**.
2. Заполните поля диалога и нажмите кнопку "ОК".

Название	Наименование группы
Описание	Дополнительные сведения (необязательный параметр)
Размещение	Наименование зарегистрированного сетевого объекта, с которым будет связана группа

Пользователи	Перечень пользователей, входящих в данную группу. Для формирования списка используйте кнопки "Добавить..." и "Удалить"
--------------	--

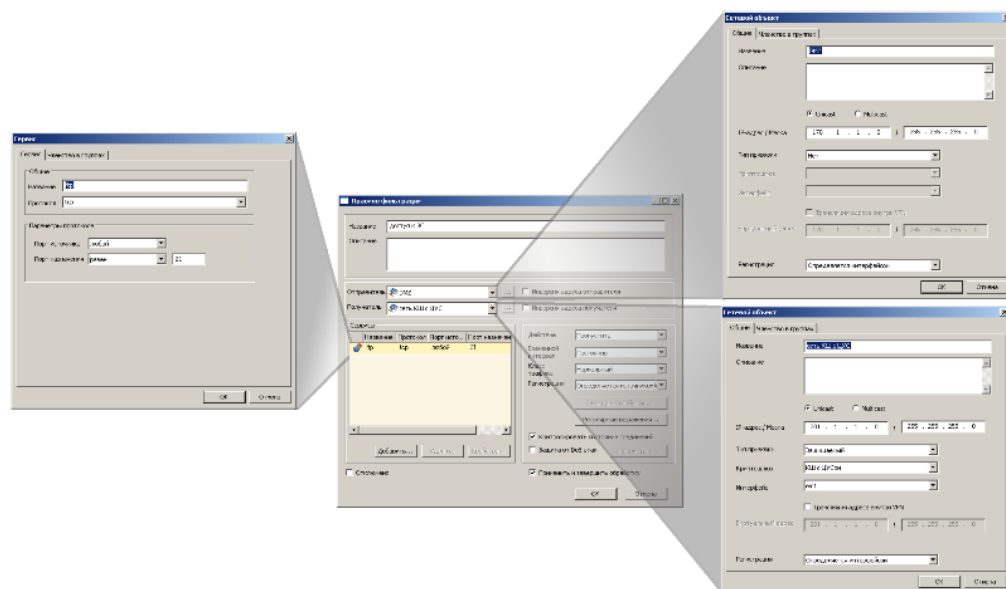
Правила фильтрации IP-пакетов и правила трансляции сетевых адресов

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. [45](#).

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.15 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: <ul style="list-style-type: none"> • 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): <ul style="list-style-type: none"> • 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. 78)
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 (см. стр. 135). Поле доступно только в том случае, если в поле "Тип привязки" установлено значение "Защищаемый"

Виртуальный адрес	Виртуальный IP-адрес, назначенный данному сетевому объекту (см. стр. 135). Поле доступно, если установлена отметка в поле "Трансляция адреса внутри VPN"
Регистрация	Задание правила регистрации событий в журналах. Значения: <ul style="list-style-type: none"> • 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".

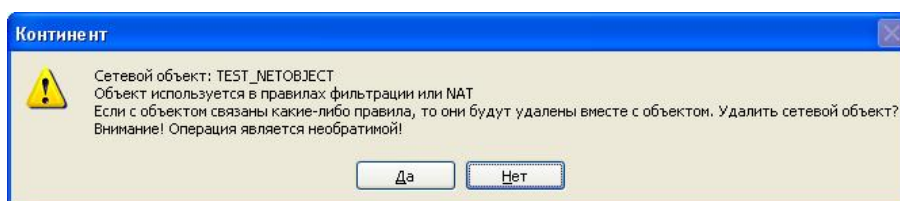
Для удаления сетевого объекта:

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".

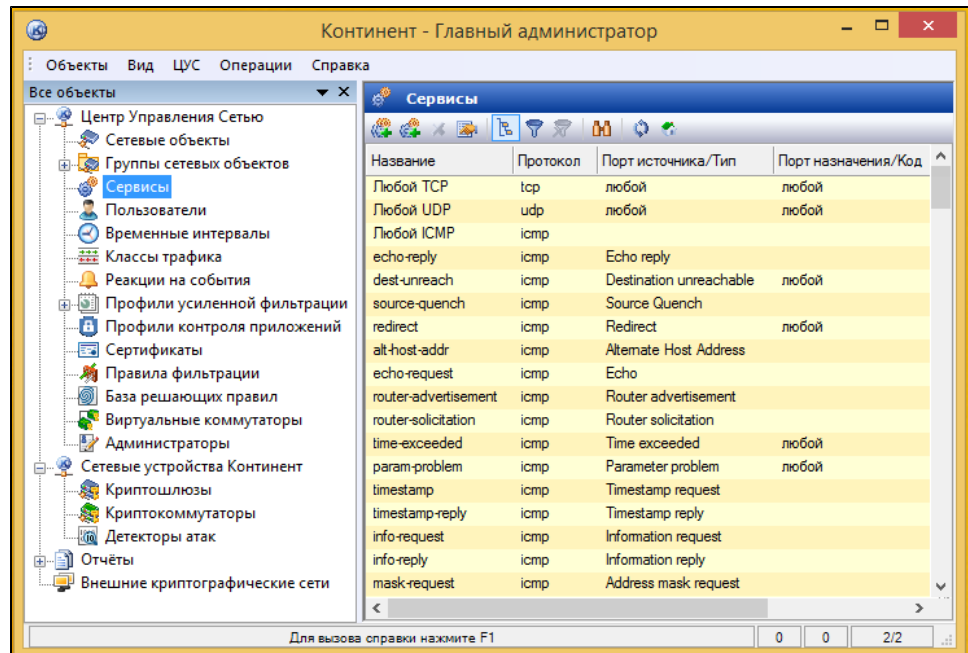
Объект будет удален из списка немедленно, а сведения о нем — из базы данных ЦУС без возможности восстановления.

Сервис

Для вызова списка сервисов:

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

В правой части окна отобразится список сервисов.



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

Управление группами сервисов см. стр.45.

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.

Параметр	Описание
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: <ul style="list-style-type: none"> • 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.

Временной интервал

Название: Рабочий 1

Описание: Дневная смена

☒ Графическое представление ☐ Текстовое представление

Временной интервал действия правила для каждого дня недели следует задавать в следующем формате: Время начала - Время завершения. Несколько интервалов задаются через разделитель (;). К примеру: 10:00 - 11:00; 14:00 - 19:00.

	0	6	12	18	24
Пн					
Вт					
Ср					
Чт					
Пт					
Сб					
Вс					

Время: 00:00

OK Отмена Справка

Временной интервал

Название: Рабочий 1

Описание: Дневная смена

☐ Графическое представление ☒ Текстовое представление

Временной интервал действия правила для каждого дня недели следует задавать в следующем формате: Время начала - Время завершения. Несколько интервалов задаются через разделитель (;). К примеру: 10:00 - 11:00; 14:00 - 19:00.

Понедельник	8:00 - 17:00
Вторник	8:00 - 17:00
Среда	8:00 - 17:00
Четверг	8:00 - 17:00
Пятница	8:00 - 17:00
Суббота	
Воскресенье	

OK Отмена Справка

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.

Внимание! Время, указанное в настройках интервалов, соответствует времени по Гринвичу (GMT). Поэтому при настройке временных интервалов необходимо вводить поправку, учитывающую часовой пояс, в котором должны действовать правила фильтрации.

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 "OK".

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.16 Перечень полей списка правил фильтрации

Поле	Описание
Действие	Пропустить или отбросить IP-пакет и пиктографическое обозначение типа правила фильтрации (см. Табл.17)
Контроль состояния	Пиктографическое обозначение значения параметра правила фильтрации "Контролировать состояние соединения" (см. Табл.17). 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


Поле	Описание
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.17 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. [112](#).

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. **112**.

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 (см. стр. **115**).

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

Регулярные выражения

В настройке параметров разрешающего правила фильтрации может быть использован механизм регулярных выражений. С помощью этого механизма задается дополнительный признак, на основании которого определяется необходимость применения данного правила к IP-пакетам. Таким признаком является наличие в поле данных IP-пакета определенного информационного объекта или атрибута.

В регулярном выражении кроме самого атрибута или информационного объекта задается также способ его обнаружения в поле данных передаваемого IP-пакета. При этом используются общие правила применения метасимволов в регулярных выражениях. Описание метасимволов, используемых в регулярных выражениях, см. стр. **201**.

Проверка на регулярные выражения выполняется в зависимости от трафика. Для UDP-трафика проверка выполняется по пакетно: пропускаются только те пакеты, которые содержат регулярные выражения, указанные в разрешающем правиле фильтрации. Для TCP-трафика проверка осуществляется потоком:

поток прекращается, если в установленном сегменте не обнаружено указанное в правиле фильтрации регулярное выражение.

При обнаружении в поле данных IP-пакета заданного объекта и совпадении значений остальных параметров правила выполняется действие, предусмотренное этим правилом. В журнале сетевого трафика или журнале НСД регистрируется (в зависимости от настроек) соответствующее событие. Анализ событий, зарегистрированных в журнале, осуществляется в рамках аудита с помощью программы просмотра журналов.

Таким образом, используя механизм регулярных выражений, можно контролировать трафик на уровне прикладных программ. Для удобства в программе управления ведется список регулярных выражений. При настройке правила фильтрации достаточно указать выражение, выбрав его в списке. Если подходящего выражения нет, его можно составить и добавить в список.

Предусмотрено одновременное использование нескольких регулярных выражений в одном правиле фильтрации. Действие правила будет выполнено при обнаружении одного из этих выражений.

Для работы со списком регулярных выражений:

1. Активируйте в главном меню программы управления команду "ЦУС > Регулярные выражения правил фильтрации".
На экране появится диалог со списком используемых регулярных выражений.
2. Сформируйте список регулярных выражений:
 - для добавления в список нового выражения введите в поля ввода в нижней части диалога название и само выражение и нажмите кнопку "Добавить";
 - для удаления из списка выберите выражение и нажмите кнопку "Удалить";

- для изменения выберите выражение в списке, внесите необходимые изменения в поля ввода в нижней части диалога и нажмите кнопку "Изменить".

3. После внесения изменения в список нажмите кнопку "Заккрыть".

Ниже приведены примеры применения регулярных выражений для некоторых протоколов.

Протокол TFTP

Атрибутами для протокола TFTP могут быть коды выполняемых операций (запрос на запись или на чтение). Чтобы предотвратить несанкционированную передачу данных по протоколу TFTP, необходимо составить правило фильтрации, запрещающее передачу пакетов (на порт #69), и задать дополнительный признак — наличие в передаваемых пакетах запросов на запись, чтение и др. Задание дополнительного признака осуществляется в виде регулярного выражения. Только пакеты с перечисленными регулярными выражениями будут пропущены фильтром.

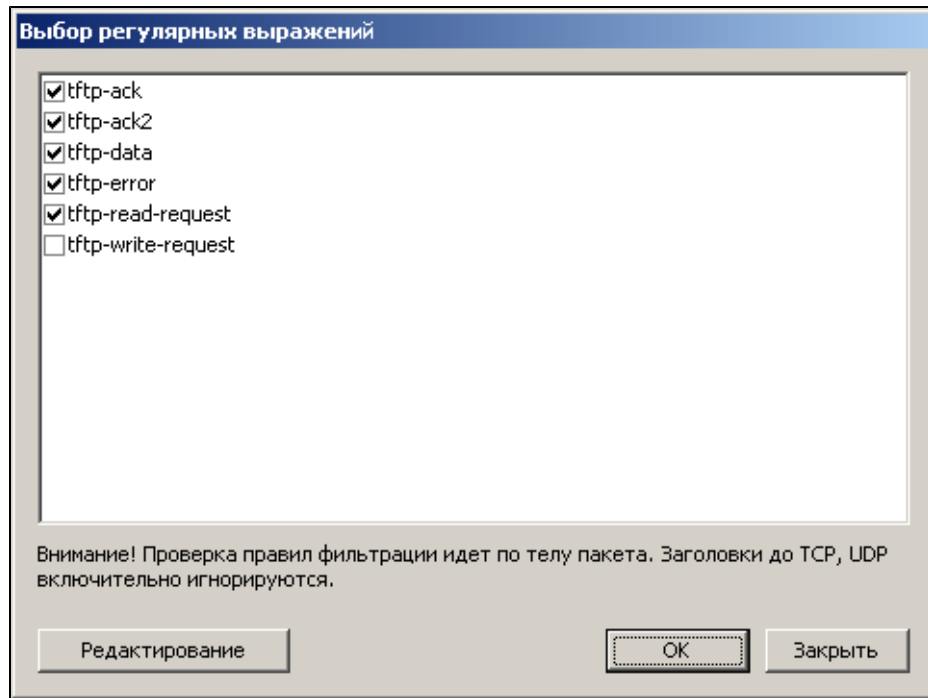
Используются следующие регулярные выражения:

Регулярные выражения правил фильтрации	
Название	Выражение
tftp-ack	^.{28}\x00\x04
tftp-data	^.{28}\x00\x03
tftp-ack2	^.{28}\x00\x06
tftp-read-request	^.{28}\x00\x01
tftp-error	^.{28}\x00\x05
tftp-write-request	^.{28}\x00\x02

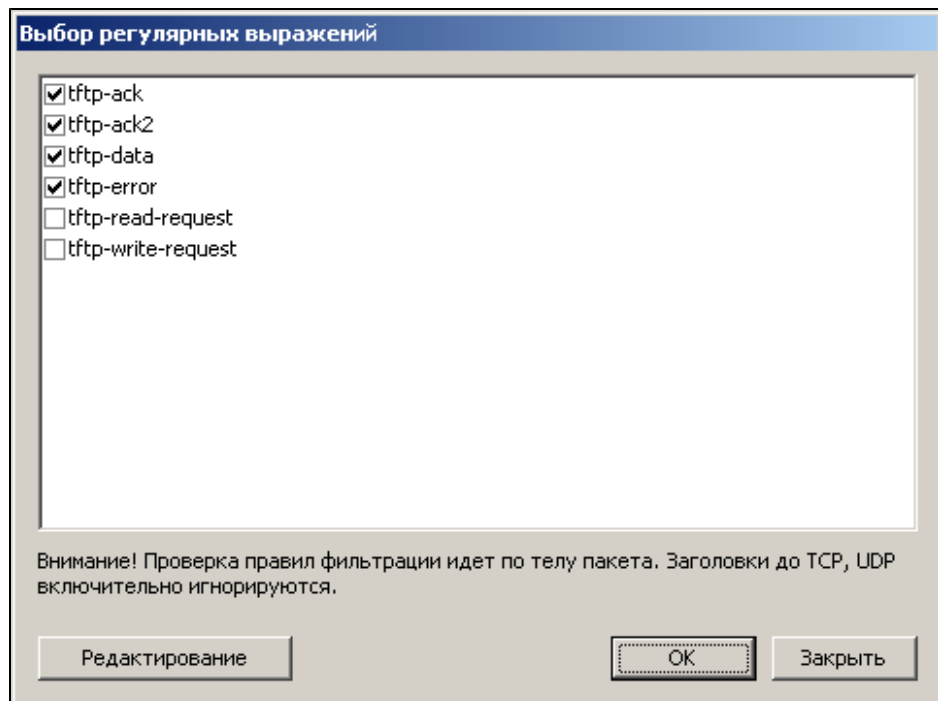
Для ограничения действий пользователя (например, только чтение) добавляются следующие правила фильтрации:

Правила фильтрации							
№	Название	Отправитель	Получатель	Сервисы	Д..	К..	Н.
1	inner-out tftp	TFTP-client	TFTP-server	tftp	✓	✗	✗
2	out-inner tftp	TFTP-server	TFTP-client	tftp	✓	✗	✗
3	client-srv UDP highport	TFTP-client	TFTP-server	udp-high-ports	✓	✗	✗
4	srv-client UDP highport	TFTP-server	TFTP-client	udp-high-ports	✓	✗	✗

В первом правиле фильтрации (от клиента к серверу) регулярными выражениями клиенту разрешаются только служебные пакеты и команда на чтение:



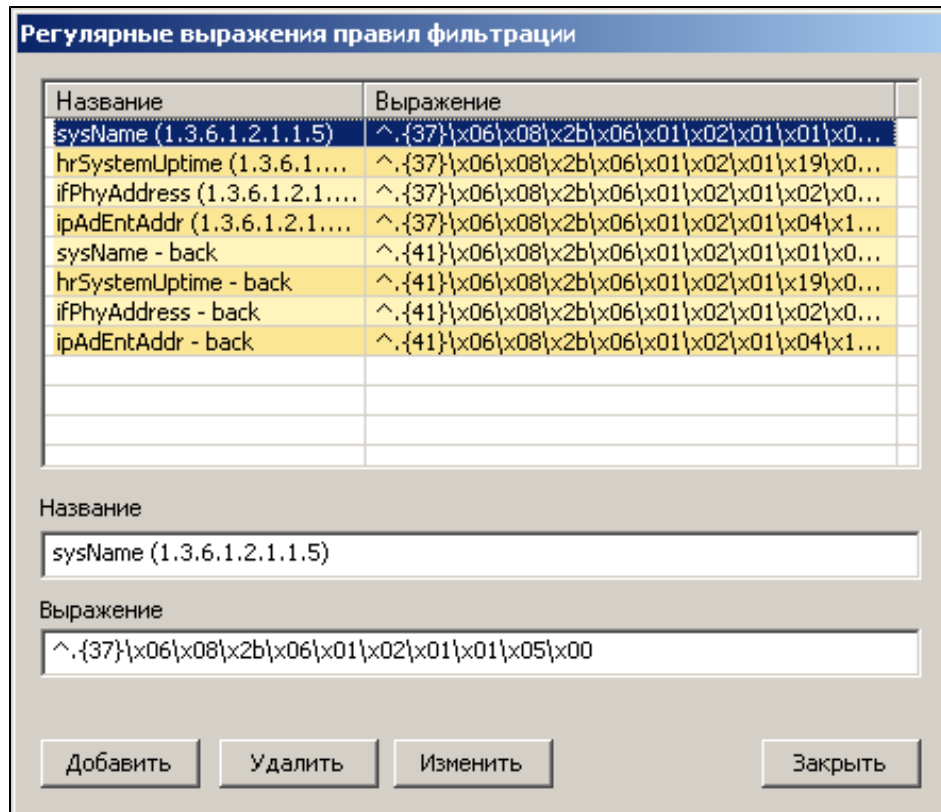
Во втором правиле фильтрации (от сервера к клиенту) разрешены только служебные пакеты:



В третьем и четвертом правилах фильтрации для сервисов UDP highport между клиентом и сервером также разрешена передача только служебных пакетов.

Протокол SNMP

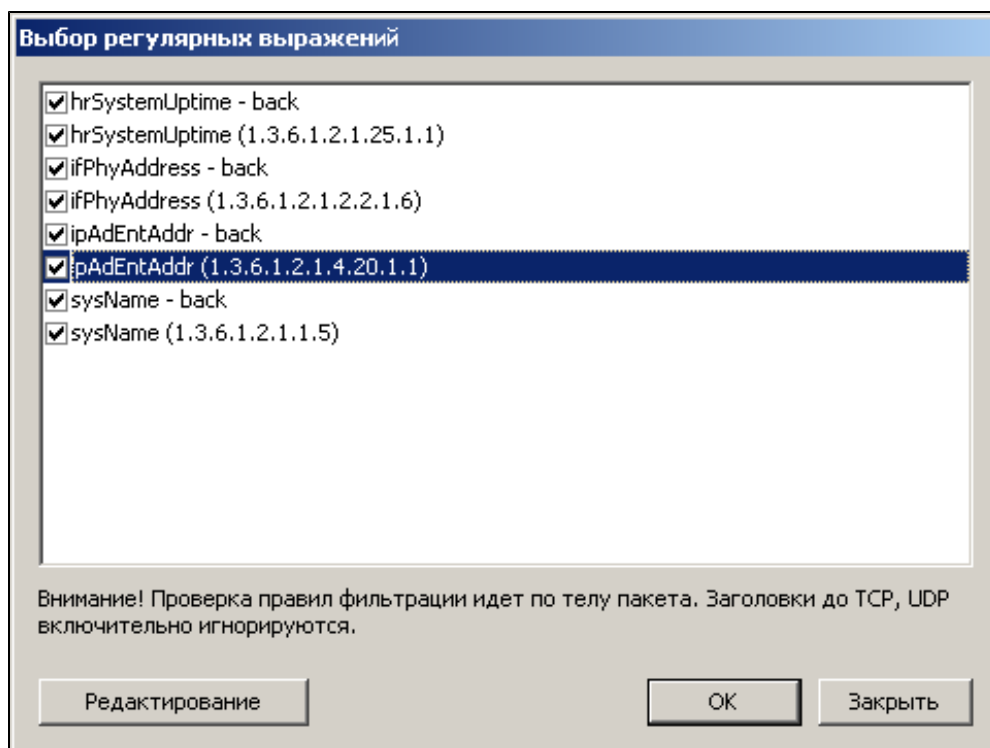
Если необходимо ограничить пакеты SNMP на основе их содержимого (например OID), можно использовать следующие регулярные выражения:



Правила фильтрации, регулирующие запросы SNMP-get:

Правила фильтрации					
Название	Отправитель	Получатель	Сервисы	Д..	Контроль соо
SNMP - get	SNMP-request	SNMP-responder	snmp		
SNMP-reply	SNMP-responder	SNMP-request	SNMP-reply		Контролир

Оба правила срабатывают на пропуск пакетов только тогда, когда в них встречается одно из регулярных выражений (request или replay):



Таким образом запросы будут фильтроваться по содержимому пакета на основе регулярных выражений. Пользователь сможет получить ответ только на snmp-запрос, удовлетворяющий любому из перечисленных регулярных выражений.

Протокол HTTP (фильтрация по командам)

Другим примером атрибута или информационного объекта является наличие команд в поле данных IP-пакета для протоколов HTTP (GET, POST и т. д.). В этом случае для запрета передачи или отправки данных к правилу фильтрации необходимо добавить регулярное выражение, содержащее в явном виде наименование разрешенной команды.

Так как данные протоколы относятся к семейству TCP, правила фильтрации должны быть с контролем состояния. Для работы контентной фильтрации по TCP необходимо задать размер проверяемого сегмента данных, в котором будет производиться поиск регулярного выражения, начиная с момента установки соединения (размер проверяемого сегмента данных устанавливают в настройках общих параметров сетевого устройства).

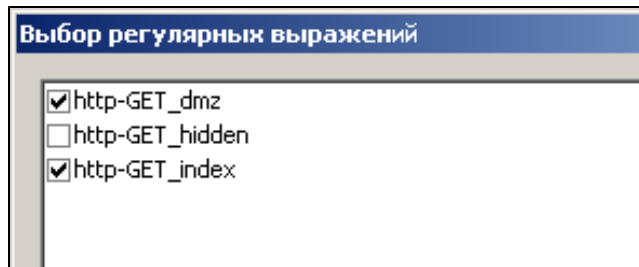
Если искомое регулярное выражение найдено, дальнейший трафик по данному соединению будет идти без ограничений. Если не найдено – пакеты по соединению начинают блокироваться.

К примеру, размер проверяемого сегмента установлен в 200 байт.

Примеры регулярных выражений для разграничения доступа по http:

Регулярные выражения правил фильтрации	
Название	Выражение
http-GET_index	GET /index.html
http-GET_hidden	GET /hidden/
http-GET_dmz	GET /dmz/

Создано правило фильтрации от http-client к http-srv, сервис http:



Выбор регулярных выражений

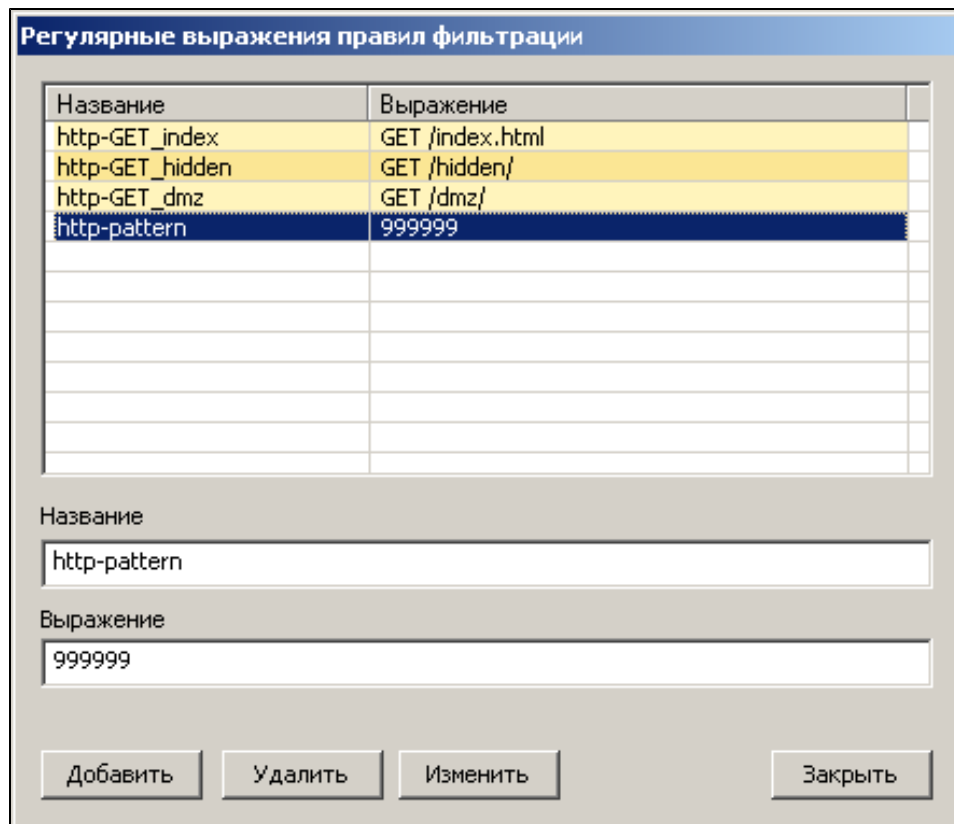
☒ http-GET_dmz
☐ http-GET_hidden
☒ http-GET_index

При попытке обратиться к файлу из папки \hidden\ будет передано только начало файла (в пределах проверяемого сегмента). При попытке обратиться к файлу из папки \dmz\ файл будет передан в полном объеме.

Протокол HTTP (фильтрация по содержимому)

В качестве информационного объекта может быть указан фрагмент текста, на основании которого можно сделать вывод о передаче той или иной информации.

Пример регулярного выражения:



Регулярные выражения правил фильтрации

Название	Выражение
http-GET_index	GET /index.html
http-GET_hidden	GET /hidden/
http-GET_dmz	GET /dmz/
http-pattern	999999

Название:

Выражение:

Добавить Удалить Изменить Заккрыть

Если при попытке получить html-страницу в начале файла встретится данное регулярное выражение, файл будет передан полностью. Если не встретится – файл будет передан частично (в пределах размера проверяемого сегмента).

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. [104](#).
2. Заполните поля диалога и нажмите кнопку "ОК".

Поле/Кнопка	Описание
Название	Наименование правила

Поле/Кнопка	Описание
Описание	Дополнительные сведения (необязательный параметр)
Отправитель	Имя одного из следующих объектов: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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
Действие	<ul style="list-style-type: none"> • 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**	<ul style="list-style-type: none"> • 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 приложений
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

Поле/Кнопка	Описание
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. 114)
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. [77](#)).

*** В таблице состояния соединений может быть зафиксировано ограниченное количество одновременно открытых соединений (см. стр. [11](#)). При превышении этой величины для всех вновь открываемых соединений фиксируется ошибка "Connection Refused". В этом случае используйте правила без контроля состояния соединений (см. стр. [195](#)).

При вводе криптографического шлюза в эксплуатацию список правил фильтрации пуст и прохождение любых IP-пакетов через данный КШ запрещено. Порядок формирования списка правил фильтрации при вводе КШ в эксплуатацию см. стр. [49](#).

Регистрация IP-пакетов

Вид регистрации IP-пакетов (заголовок пакета/ тело пакета) можно указать в свойствах следующих объектов комплекса:

- правило фильтрации;
- группа сетевых объектов;
- сетевой объект;
- сетевой интерфейс.

Регистрация IP-пакета выполняется в соответствии со значением, указанным в примененном к пакету правиле фильтрации. Чтобы регистрация IP-пакета выполнялась в соответствии с указанным значением для данного объекта, параметр "Регистрация" всех объектов более высокого уровня должен иметь значение "Определяется <название объекта более низкого уровня>". При указании в свойствах сетевого интерфейса значения "Определяется сетевым устройством" выполняется регистрация тела пакета.

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. [104](#).
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 "ОК".

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

Очистка таблицы состояния соединений

Отметку "Контролировать состояние соединения" в свойствах правила фильтрации 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 в списке правил фильтрации не отображаются. Таблица состояния соединений формируется на каждом КШ.

Принудительная очистка таблицы состояния соединений требуется в следующих случаях:

- редактирование правила фильтрации с контролем состояния соединения;
- изменение объектов, используемых в правиле фильтрации с контролем состояния:
 - изменение привязки сетевого объекта, используемого как индивидуально, так и в составе группы;
 - изменение состава группы сетевых объектов;
 - изменение свойств временного интервала;
- изменение списка правил фильтрации:
 - удаление правила фильтрации с контролем состояния соединения;
 - добавление или перемещение отменяющего правила ниже по списку;
 - добавление или перемещение отменяющего правила с признаком немедленного действия выше по списку;
 - перемещение правила с контролем состояния относительно отменяющего правила;
- изменение значения параметра "Автоматический исходящий NAT" в настройках Multi-WAN (режим "Обеспечение отказоустойчивости канала связи").

Для очистки таблицы:

- 1.** Вызовите контекстное меню нужного КШ и активируйте команду "Очистить таблицу состояний соединений".

Примечание. Возможен множественный выбор объектов.

На экране появится запрос на подтверждение очистки таблицы.

- 2.** Нажмите кнопку "Да".

Усиленная фильтрация

Средствами межсетевого экрана, входящего в состав комплекса, предусмотрена усиленная фильтрация, которая позволяет анализировать и обрабатывать сетевой трафик на уровне прикладных протоколов. Такими протоколами являются:

- HTTP;

- HTTPS;
- FTP.

В механизме усиленной фильтрации используются настраиваемые профили. Каждый профиль включает в себя один или несколько наборов фильтров (агентов) и описание действия, которое должно быть выполнено с пакетом, удовлетворяющим одновременно всем условиям, заданным в фильтрах.

В каждом наборе фильтров (агенте) задаются атрибуты, по которым должна выполняться фильтрация трафика:

Атрибут	Описание
Адрес	IP-адрес (IP-адреса) или DNS-имя получателя. Для указания всех IP-адресов используются символы ".*" (без кавычек). При указании DNS-имени допускается использование латинских символов и символов кириллицы
Команды/методы	Фильтрация сетевого трафика осуществляется по FTP-командам и HTTP-методам
Контент	Фильтрация осуществляется по MIME-типам передаваемых данных. Используется стандартный список MIME-заголовков и расширений файлов. Для варианта FTP не используется
Маршруты	Фильтрация сетевого трафика осуществляется по маршрутам, описанным с помощью регулярных выражений POSIX. В описаниях маршрутов допускается использование латинских символов и символов кириллицы

Действия, которые могут быть выполнены с пакетом при срабатывании фильтра:

- блокирование — уничтожение сетевых пакетов сессии данного соединения с регистрацией отброшенных пакетов в журнале сетевого трафика;
- разрешение — отсутствие каких-либо действий над сетевыми пакетами и отправка их адресату без изменений;
- перенаправление — перенаправление клиента на заранее заданный адрес.

Для усиленной фильтрации сетевого трафика необходимо создать подходящий профиль и включить его в состав правила фильтрации.

Таким образом, для запуска режима усиленной фильтрации необходимо:

1. Выполнить предварительные настройки.
2. Создать профиль для требуемого протокола.
3. Создать необходимые наборы фильтров (агенты) и включить их в профиль.
4. Создать правило фильтрации и включить в него профиль.

Предварительные настройки

Настройки включают в себя:

1. Указание адреса DNS-сервера для работы с URL. Данную настройку выполняют для всех зарегистрированных КШ комплекса.
2. Создание корневого сертификата Удостоверяющего центра для усиленной фильтрации по HTTPS. Сертификат издают средствами ЦУС.

Внимание! Для корректной работы https-соединений корневой сертификат Удостоверяющего центра должен быть установлен на всех компьютерах защищаемых сетей комплекса. Для этого после создания корневого сертификата необходимо выполнить процедуру экспорта сертификата в файл (см. ниже) и далее передать файл для установки сертификата на компьютеры.

Примечание. За 14 и 7 дней до истечения срока действия сертификата в ПУ ЦУС появляется соответствующее сообщение с указанием даты истечения срока действия.

Для указания адреса DNS-сервера:

1. В ПУ ЦУС выберите в списке КШ, вызовите контекстное меню и выберите пункт "Свойства".
На экране появится диалог "Свойства КШ".
2. Перейдите на вкладку "DNS", введите адрес DNS-сервера и нажмите кнопку "ОК".

Для создания корневого сертификата:

1. В главном окне ПУ ЦУС раскройте папку "Центр управления сетью" и выберите объект "Сертификаты".
В правой части главного окне отобразится список зарегистрированных в ЦУС сертификатов.
2. На панели инструментов нажмите кнопку "Добавить".
На экране появится диалог "Создание нового сертификата".

Создание нового сертификата
Заполните соответствующие поля для создания сертификата выбранного назначения.

Название:

Описание:

Организация:

Подразделение:

Регион:

Город: Страна: RU

Электронная почта:

Алгоритм подписи: sha256WithRSAEncryption

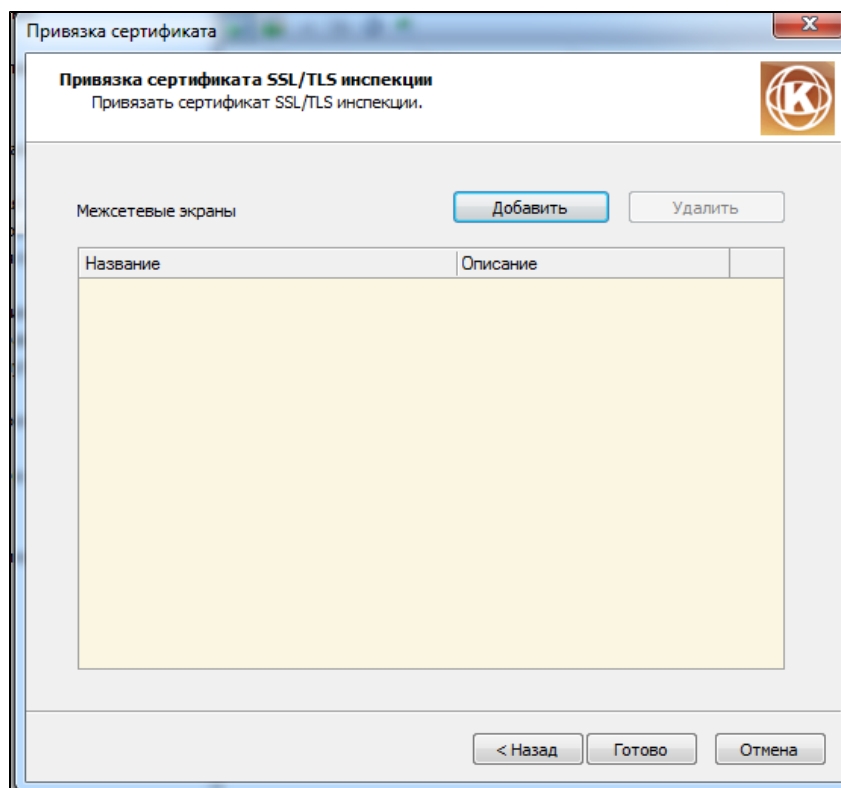
Алгоритм ключа: RSAEncryption

Начало действия: 29.09.2016 Окончание действия: 29.09.2019

Назначение: SSL/TLS инспекция

< Назад Далее > Отмена

3. Заполните поля диалога. В поле "Назначение" укажите "SSL/TLS инспекция", выбрав это значение из раскрывающегося списка.
Нажмите кнопку "Далее".
На экране появится диалог "Привязка сертификата".



4. Нажмите кнопку "Добавить".

На экране появится список зарегистрированных криптошлюзов.

5. Выберите КШ, на котором должна действовать усиленная фильтрация по HTTPS, и нажмите кнопку "ОК".

В диалоге "Привязка сертификата" появится строка, отображающая привязку создаваемого сертификата к криптошлюзу.

6. Выполните пп. 4-5 для всех КШ, на которых должна действовать усиленная фильтрация по HTTPS.

Для удаления привязки сертификата к КШ выберите соответствующую строку в диалоге "Привязка сертификата" и нажмите кнопку "Удалить".

7. После привязки сертификата ко всем необходимым КШ нажмите кнопку "Готово".

Диалог "Привязка сертификата" закроется и в списке сертификатов появится вновь созданный сертификат.

Для экспорта корневого сертификата в файл:

- Выполните процедуру экспорта сертификата в соответствии с описанием, приведенным в разделе "Инфраструктура открытых ключей" (см. стр. **154**).

Профили усиленной фильтрации

Список профилей

Для просмотра списка и работы с профилями:

1. В дереве объектов главного окна ПУ ЦУС выделите папку "Профили усиленной фильтрации".

В правой части главного окна отобразится список профилей усиленной фильтрации.

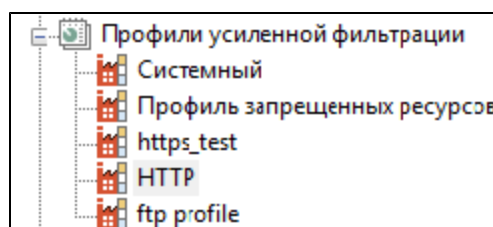
Профили усиленной фильтрации				
Название	Описание	Вариант усиленной фильтрации	Действие	
Системный	Системный	?	?	
Профиль запрещенных ре...	Профиль запрещенных ресурсов	?	?	
new_profile_2		HTTP	запретить	

Список содержит созданные администратором профили и два профиля, заданных по умолчанию: "Профиль запрещенных ресурсов" и "Системный".

"Профиль запрещенных ресурсов" не подлежит редактированию и удалению и используется в правилах фильтрации для запрета доступа к ресурсам единого реестра Роскомнадзора (см. стр. 134).

Профиль "Системный" является служебным и в правилах фильтрации не используется. Он предназначен для хранения наборов фильтров (агентов), входивших в удаленные профили. Предусмотрено удаление агентов из данного профиля. Сам профиль "Системный" удалению не подлежит.

- Для просмотра состава профиля раскройте папку "Профили усиленной фильтрации" и выберите его в списке объектов.



В правой части окна отобразится список наборов фильтров (агентов), включенных в состав профиля.

Агенты усиленной фильтрации						
Название	Описание	Адрес	Вариант усиленной ...	Фильтр методов	Фильтр контента	Фильтр маршрута
TEST_HTTPS1			HTTPS	GET;		
TEST_HTTP_POST		192.168.1.1	HTTP	POST;		

В верхней части списка расположены кнопки, с помощью которых выполняются следующие операции с профилями:

- создание нового профиля;
- удаление;
- редактирование;
- обновление списка профилей.

Создание нового профиля

Для создания нового профиля:

- Откройте список профилей усиленной фильтрации (см. п. 1 процедуры выше) и на панели инструментов нажмите кнопку "Создать профиль усиленной фильтрации"

На экране появится диалог "Профиль усиленной фильтрации".

2. Заполните поля диалога.

Поле	Описание
Название	Название создаваемого профиля
Описание	Краткое описание профиля
Агенты усиленной фильтрации	Список агентов, включаемых в создаваемый профиль. Для добавления агента в список нажмите кнопку "Добавить" и выберите его из раскрывающегося списка. Если агенты не создавались, данное поле можно заполнить позднее после создания требуемых агентов
Действие	Действие, которое должно быть выполнено при срабатывании фильтра. Доступные значения: <ul style="list-style-type: none"> • отбросить; • пропустить; • перенаправить
Вариант усиленной фильтрации	Варианты: <ul style="list-style-type: none"> • HTTP; • HTTPS; • FTP
Адрес для перенаправления	Заполняется, если в поле "Действие" указано "Перенаправить". Для http-соединения достаточно ввести доменное имя. Для https-соединения адрес необходимо ввести в формате https://<доменное имя>

3. Нажмите кнопку "ОК".

Диалог "Профиль усиленной фильтрации" закроется и в списке появится новый профиль.

Удаление профиля

Для удаления профиля

1. Выберите профиль в списке и на панели инструментов нажмите кнопку "Удалить".

На экране появится запрос на подтверждение удаления профиля.

2. Выберите "Да".

Профиль будет удален.

Внимание! Агенты, входящие в удаляемый профиль, будут помещены в профиль "Системный". Если удаляемый профиль включен в одно или несколько правил фильтрации, на экране появится предупреждение о необходимости предварительно исключить его из правила (правил).

Редактирование профиля

Для редактирования профиля:

1. Выберите профиль в списке, вызовите контекстное меню и выберите команду "Свойства".

На экране появится диалог "Профиль усиленной фильтрации".

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

Агенты усиленной фильтрации

Создание агента

Для создания агента:

1. В дереве объектов главного окна ПУ ЦУС раскройте папку "Профили усиленной фильтрации" и выберите в ней профиль, для которого должен быть создан агент.

В правой части главного окна отобразится список агентов усиленной фильтрации, входящих в данный профиль.

2. На панели инструментов нажмите кнопку "Создать агента усиленной фильтрации".

На экране появится диалог "Агент усиленной фильтрации".

Агент усиленной фильтрации

Агент усиленной фильтрации | Профили усиленной фильтрации

Название: GET

Описание: Фильтрация http по методу GET

Адрес:

Фильтры

Команды/методы: GET

Контент: application/zip

Маршруты:

OK Отмена

3. Заполните поля диалога на вкладке "Агент усиленной фильтрации".

Обязательным для заполнения является поле "Название". Остальные поля можно заполнить позже.

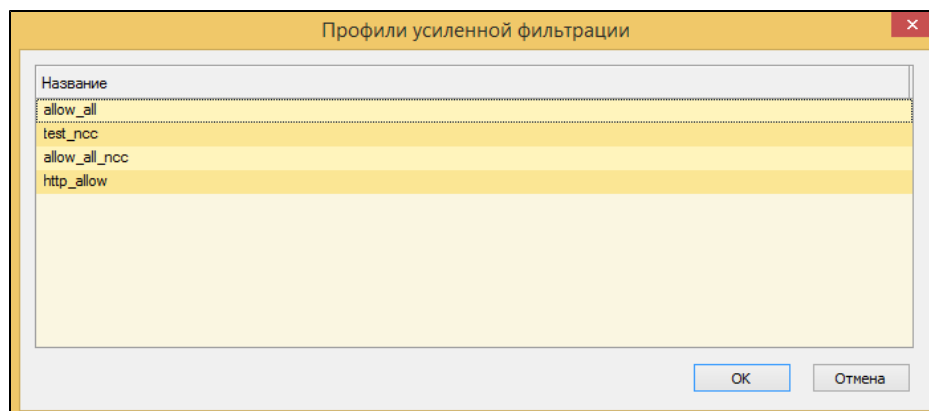
4. Если необходимо включить данный агент в другие профили, перейдите на вкладку "Профили усиленной фильтрации".

На вкладке отображается список профилей, в которые входит данный агент.

Внимание! Включить агента можно только в профиль соответствующего варианта усиленной фильтрации (HTTP, HTTPS, FTP).

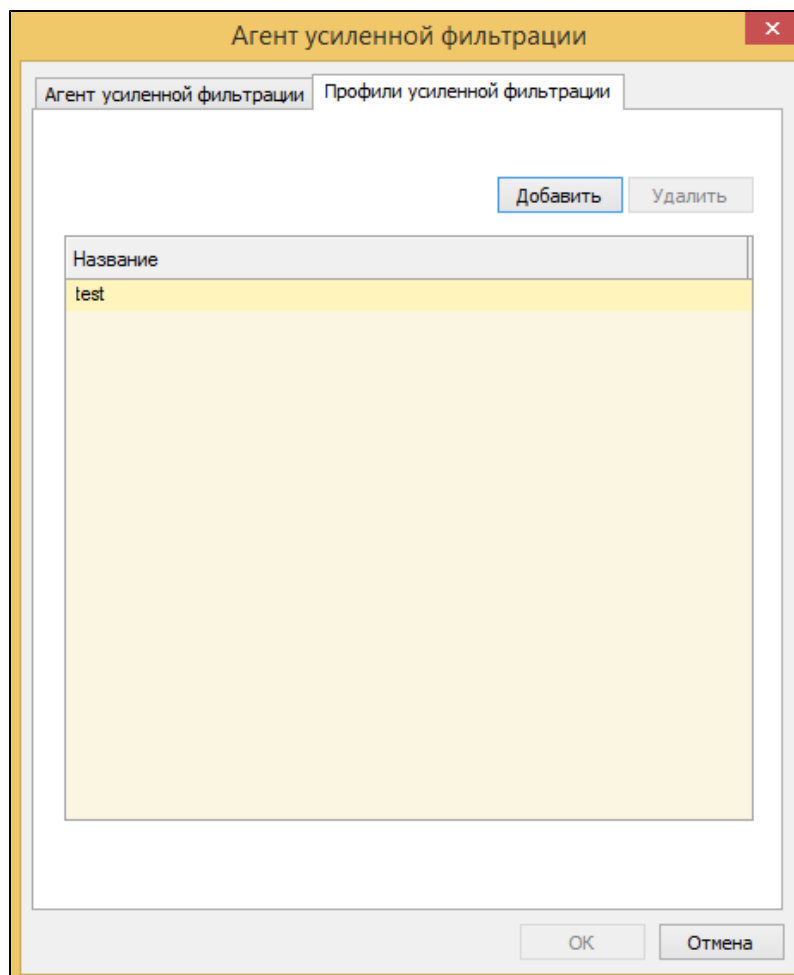
5. Для включения агента в другой профиль нажмите кнопку "Добавить".

На экране появится список профилей усиленной фильтрации соответствующего варианта (HTTP, HTTPS, FTP).



6. Выберите профиль и нажмите кнопку "OK".

Выбранный профиль появится в списке на вкладке "Профили усиленной фильтрации".



Примечание. Для удаления профиля выберите его в списке и нажмите кнопку "Удалить".

7. Для завершения процедуры создания агента нажмите кнопку "ОК" в нижней части диалога.

Диалог "Агент усиленной фильтрации" закроется и в списке агентов появится соответствующая строка.

Удаление агента

Предусмотрено два варианта удаление агента:

- из профиля усиленной фильтрации;
- из системы.

Для удаления агента из профиля:

1. В дереве объектов главного окна ПУ ЦУС выделите папку "Профили усиленной фильтрации".
В правой части главного окна отобразится список профилей усиленной фильтрации.
2. В списке профилей усиленной фильтрации выделите профиль, из которого необходимо удалить агента, вызовите контекстное меню и выберите пункт "Свойства".
На экране появится диалог "Профиль усиленной фильтрации".
3. В списке агентов, входящих в профиль усиленной фильтрации, выберите агента и нажмите кнопку "Удалить".
Агент будет удален из профиля.

Для удаления агента из системы:

1. В дереве объектов главного окна ПУ ЦУС раскройте папку "Профили усиленной фильтрации" и выберите в ней профиль, в который входит агент.
В правой части окна отобразится список агентов, входящих в выбранный профиль.
2. Выделите в списке агента и нажмите в панели инструментов кнопку "Удалить" или используйте соответствующую команду контекстного меню.
На экране появится запрос на подтверждение выполнения операции.
3. Нажмите кнопку "Да" в окне запроса.
Агент будет удален из системы.

Включение профиля в правило фильтрации

Для включения профиля в правило фильтрации:

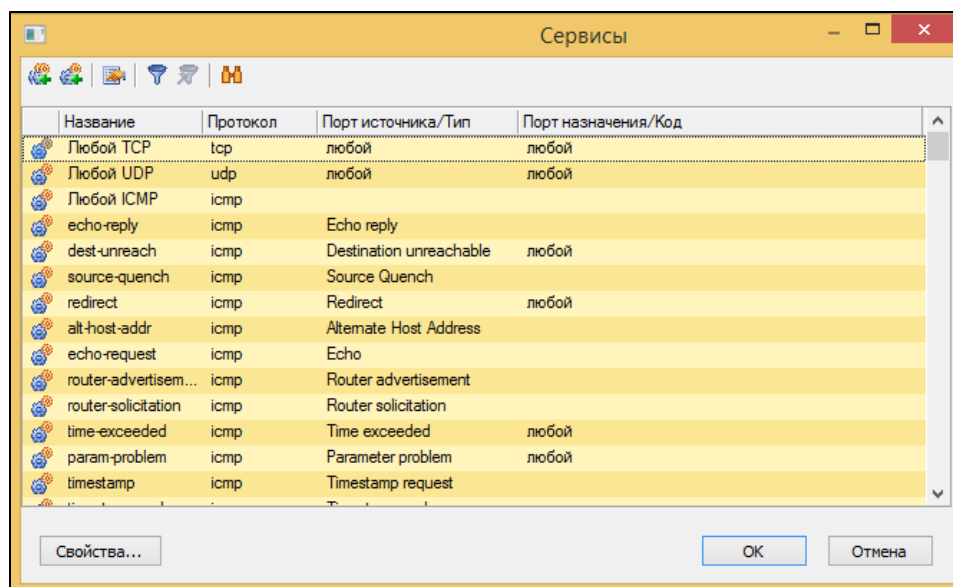
1. Выберите подходящее правило фильтрации или создайте новое (о работе с правилами фильтрации см. стр. [104](#)).
2. Вызовите диалог редактирования параметров правила фильтрации.

3. В поле "Действие" выберите значение "Усиленная фильтрация", а в поле "Профиль усиленной фильтрации" укажите нужный профиль, выбрав его из раскрывающегося списка.

4. Если поле "Сервисы" не заполнено, нажмите кнопку "Добавить".

Примечание. Если поле заполнено, проверьте в указанном сервисе значения параметров "Протокол" и "Порт назначения" в соответствии с приведенным ниже замечанием.

На экране появится список сервисов.



Внимание! Сетевой трафик, предназначенный для усиленной фильтрации, должен поступать в КШ по строго определенному TCP-порту. В зависимости от используемого протокола такими портами являются:

Протокол	Порт
HTTP	80
HTTPS	443
FTP	21

При указании сервиса должно соблюдаться соответствие между значениями параметров "Протокол" и "Порт назначения", как указано в приведенной выше таблице.

5. Выберите из списка сервис и нажмите кнопку "OK".

Выбранный сервис появится в поле "Сервисы".

6. Нажмите кнопку "OK" в нижней части диалога.

Диалог настройки параметров правила фильтрации закроется.

Контроль приложений

Для контроля приложений средствами межсетевого экрана применяют правила фильтрации, в которых используются профили, содержащие перечень контролируемых приложений и указание действия, которое должно быть выполнено над пакетом при срабатывании фильтра.

Для запуска режима контроля приложений необходимо выполнить следующее:

1. Создать профиль с перечнем контролируемых приложений.
2. Создать правило фильтрации и включить в него профиль.

Профили контроля приложений

Для просмотра списка профилей контроля приложений:

- В дереве объектов главного окна ПУ ЦУС выберите папку "Профили контроля приложений".

В правой части окна отобразится список созданных профилей.

Профили контроля приложений		
Название	Блокируемые приложения	Детектируемые приложения
22	Jabber;	IRC; MSN; ICQ; SIP; Skype; WHATSAPP;
ssh_block	WHATSAPP;	SSH (в том числе инкапсулированные в HTTP);

Для создания нового профиля:

1. В списке профилей нажмите на панели инструментов кнопку "Создать профиль контроля приложений" или используйте команду контекстного меню.
2. На экране появится окно "Профиль контроля приложений".

3. Введите название и краткое описание создаваемого профиля.
4. В списке приложений установите отметки у тех приложений, которые должны контролироваться. При этом вид отметки обозначает действие:

<input type="checkbox"/>	Не обрабатывать (трафик будет пропущен без регистрации в журнале)
	Детектирование (трафик будет пропущен с регистрацией в журнале НСД криптошлюза)
	Блокировка (трафик будет отброшен с регистрацией в журнале НСД криптошлюза)

Для установки требуемой отметки установите курсор в поле перед названием приложения и последовательно нажимайте левую кнопку мыши.

5. Нажмите кнопку "ОК".

Окно закрывается и в списке профилей контроля приложений появится новый профиль.

Для редактирования профиля:

1. Выберите профиль в списке, вызовите контекстное меню и выберите команду "Свойства".

На экране появится диалог "Профиль контроля приложений".

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

Для удаления профиля:

1. Выберите профиль в списке и нажмите на панели инструментов кнопку "Удалить профиль контроля приложений".

На экране появится запрос на подтверждение удаления профиля.

2. Выберите "Да".

Профиль будет удален.

Внимание! Если удаляемый профиль включен в одно или несколько правил фильтрации, на экране появится предупреждение о необходимости предварительно исключить его из правила (правил).

Включение профиля контроля приложений в правило фильтрации

Для включения профиля в правило фильтрации:

1. Выберите подходящее правило фильтрации или создайте новое (о работе с правилами фильтрации см. стр. [104](#)).
2. Вызовите диалог редактирования параметров правила фильтрации.
3. В поле "Действие" выберите значение "Контроль приложений", а в поле "Профиль контроля приложений" укажите нужный профиль, выбрав его из раскрывающегося списка.
4. Заполните поле "Сервисы" или оставьте его пустым.
Если оставить поле пустым, контролироваться будет весь проходящий трафик.
5. Нажмите кнопку "ОК" в нижней части диалога.

Диалог настройки параметров правила фильтрации закрывается.

Фильтрация пакетов по информации от системы обнаружения вторжений

Одной из защитных функций межсетевого экрана является возможность блокировки трафика при регистрации события НСД системой обнаружения вторжений (СОВ).

При обнаружении атаки ДА регистрирует событие НСД и отправляет в ЦУС его описание. На основании полученной информации ЦУС определяет — на какие сетевые узлы должна быть выдана команда на блокировку в соответствии с обнаруженной атакой.

Команда на блокировку представляет собой временное (динамическое) правило фильтрации, автоматически сформированное в ЦУС и распространяемое на соответствующие узлы. Динамическое правило фильтрации действует на сетевом узле в течение ограниченного времени и после его истечения удаляется.

Для реализации описанного выше механизма фильтрации необходимо выполнить настройку детекторов атак (см. далее).

Настройка параметров детектора атак

Настройку выполняют в ПУ ЦУС для каждого ДА, сведения от которого должны использоваться для блокировки трафика при обнаружении атаки.

Для настройки ДА:

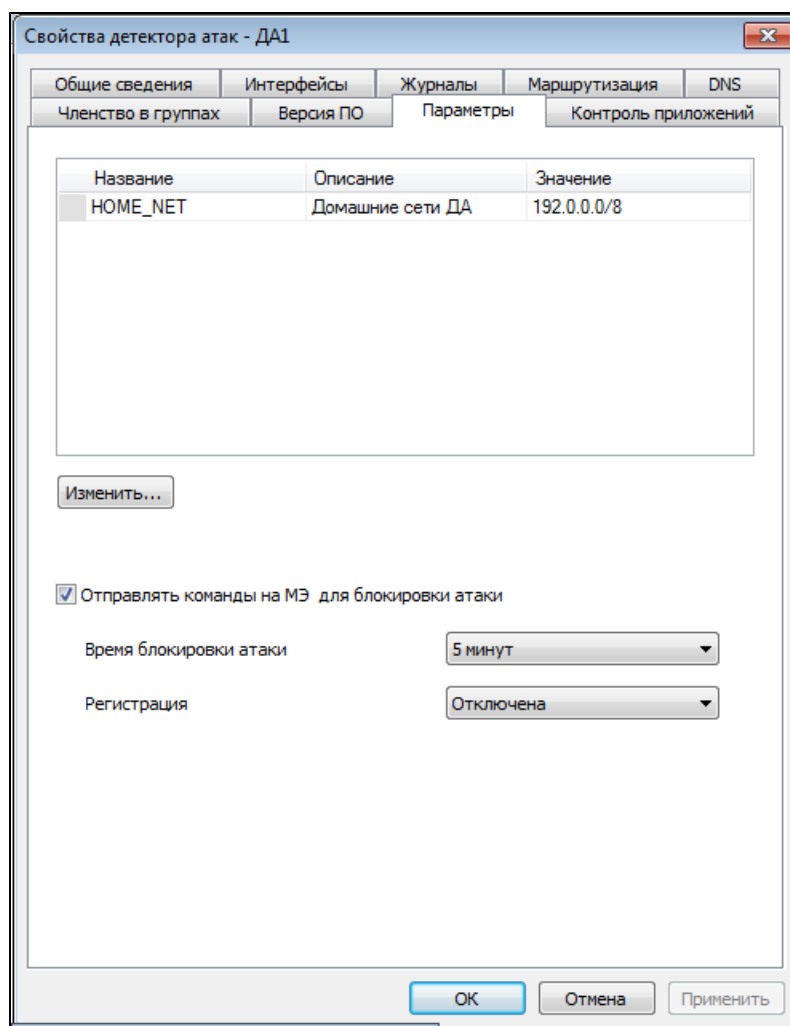
1. В дереве объектов главного окна ПУ ЦУС раскройте узел "Сетевые устройства Континент" и выберите папку "Детекторы атак".

В правой части главного окна отобразится список зарегистрированных ДА.

2. Выберите в списке ДА, вызовите контекстное меню и выберите команду "Свойства".

На экране появится диалог "Свойства детектора атак", открытый на вкладке "Общие сведения".

3. Установите отметку в поле "Сигнатурный анализатор включен" и перейдите на вкладку "Параметры".



4. Установите отметку в поле "Отправлять команды на МЭ для блокировки атаки" и укажите значения параметров:

Параметр	Описание
Время блокировки атаки	Время действия правила (блокировки) с момента его появления на сетевом узле. По истечении указанного времени, если от ЦУС не приходит новая команда (правило), трафик разблокируется

Параметр	Описание
Регистрация	<p>Информация о пакете, отображаемая в журнале сетевого трафика. Доступные значения:</p> <ul style="list-style-type: none"> информация из заголовка (информация о субъектах взаимодействия, дате/времени атаки, действии, совершенном над пакетом, времени действия правила, получателя команды на блокировку (ДА); тело пакета (отображение всего тела идентифицированного пакета/пакетов; отключена (регистрация для данного правила отключена)

5. Нажмите кнопку "ОК" в нижней части диалога.

Диалог закрывается.

Выполните описанную процедуру для других детекторов атак.

Динамические правила фильтрации

Динамические правила фильтрации – это правила, создаваемые автоматически в ЦУС и передаваемые на криптографические шлюзы для отражения сетевой атаки.

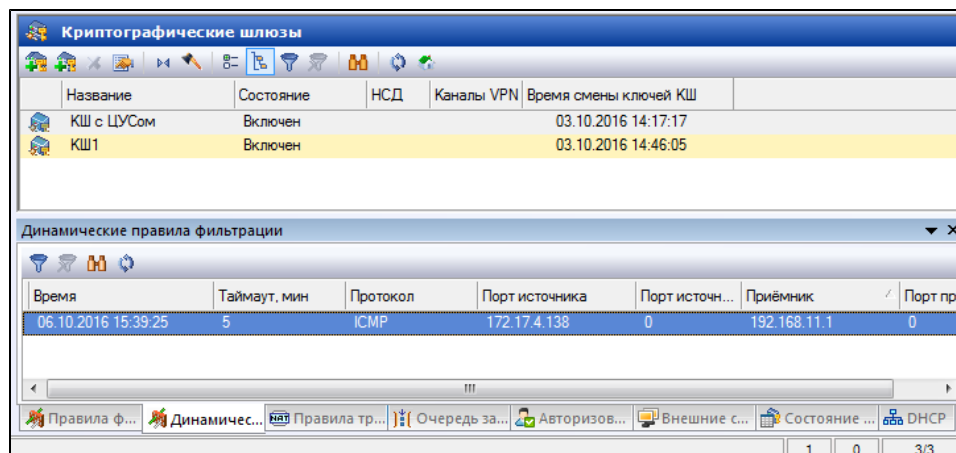
Для просмотра правил:

1. В главном окне ПУ ЦУС в дереве объектов раскройте узел "Сетевые устройства Континент" и выберите папку "Криптошлюзы".

В правой части окна отобразится список зарегистрированных КШ.

2. Выберите в списке КШ и в дополнительном окне перейдите на вкладку "Динамические правила фильтрации".

На вкладке отобразится список динамических правил фильтрации, действующих в данный момент на выбранном КШ.



3. Для просмотра динамических правил другого КШ выберите его в списке.

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. 97).

Внимание! До начала работы с правилами трансляции создайте нужные элементы правил (см. стр. 98).

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. 130.

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. 130.

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 "ОК".

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. 129).
2. Заполните поля диалога и нажмите кнопку "ОК":

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

Поле	Описание
Источник	Имя одного из следующих объектов: <ul style="list-style-type: none"> • группа пользователей; • сетевой объект. Определяет абонентов-отправителей, для которых будет действовать правило
Получатель	Имя одного из следующих объектов: <ul style="list-style-type: none"> • 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)
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 имеющегося 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: <ul style="list-style-type: none"> • 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 "ОК". 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:

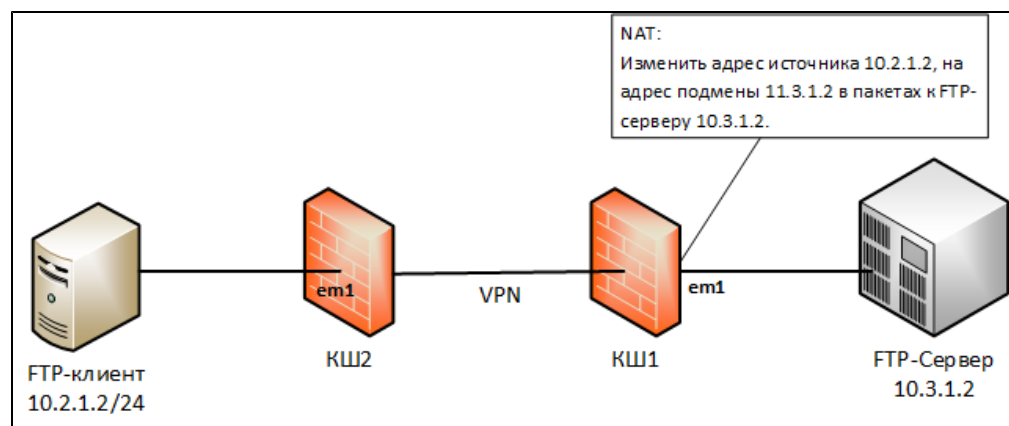
- протокол — TCP или UDP;
- порт источника — любой (определяется с помощью оператора "Любой");
- порт назначения — конкретное значение одного порта (определяется с помощью оператора "==").

Процедуру настройки параметров сервиса см. стр. [100](#).

Для регистрации пакетов в журнале сетевого трафика необходимо дополнительно установить отметки в соответствующих полях диалога "Журналы" свойств КШ (см. стр. [77](#)).

Пример использования правила трансляции

В данном разделе приведен пример использования правила трансляции для обеспечения доступа к FTP-серверу, расположенному в защищенной сети КШ1 (IP-адрес 10.3.1.2), с рабочих станций, расположенных в защищенной сети парного КШ2 (IP-адрес 10.2.1.2). При этом адрес источника (клиента) должен быть изменен с 10.2.1.2 на 11.3.1.2.



В данном примере предполагается, что изменение адреса источника будет осуществляться на внутреннем интерфейсе КШ1 (em1).

Для обеспечения вышеописанных требований необходимо выполнить следующие настройки:

1. Сформировать правила фильтрации, обеспечивающие передачу зашифрованного трафика между сетями, защищаемыми КШ1 и КШ2. Для этого перед началом формирования правил фильтрации необходимо создать и описать элементы этих правил — сетевые объекты 1 и 2. Далее в примере названия этих объектов — соответственно ЗС КШ1 и ЗС КШ2.

Сетевые объекты:

Параметр	Сетевой объект 1	Сетевой объект 2
Название	ЗС КШ1	ЗС КШ2
IP-адрес	10.3.1.0	10.2.1.0
Маска	255.255.255.0	255.255.255.0
Тип привязки	Защищаемый	Защищаемый
Криптошлюз	КШ1	КШ2
Интерфейс	em1	em1

Правила фильтрации:

Отправитель	Получатель	Сервисы	Действие
ЗС КШ1	ЗС КШ2	Любой TCP	Пропустить

Отправитель	Получатель	Сервисы	Действие
ЗС КШ2	ЗС КШ1	Любой TCP	Пропустить

Примечание. При необходимости настройте остальные параметры в правилах фильтрации или оставьте их значения как установленные по умолчанию.

- Создать правила фильтрации, разрешающие прохождение трафика между FTP-сервером (10.3.1.2) и сетевым объектом с адресом трансляции на внутреннем интерфейсе КШ1. Сетевой объект должен иметь адрес, совпадающий с адресом источника-клиента (в нашем случае 10.2.1.2), но быть привязанным к внутреннему интерфейсу em1 КШ1. Перед созданием правил фильтрации необходимо создать и описать два сетевых объекта — сетевой объект 3 и сетевой объект 4. Далее в примере названия этих объектов — соответственно ftp-сервер и ftp_client_fake.

Сетевые объекты:

Параметр	Сетевой объект 3	Сетевой объект 4
Название	ftp-сервер	ftp_client_fake
IP-адрес	10.3.1.2	11.3.1.2
Маска	255.255.255.255	255.255.255.255
Тип привязки	Внутренний	Внутренний
Криптошлюз	КШ1	КШ1
Интерфейс	em1	em1

Правила фильтрации:

Отправитель	Получатель	Сервисы	Действие	Контроль состояния
ftp-сервер	ftp_client_fake	Любой TCP	Пропустить	+
ftp_client_fake	ftp-сервер	Любой TCP	Пропустить	+

- Создать правило трансляции на внутреннем интерфейсе КШ1. Перед созданием правила трансляции необходимо создать новый сетевой объект со следующими значениями параметров:

Параметр	Сетевой объект 5
Название	ftp_client
IP-адрес	10.2.1.2
Маска	255.255.255.255
Тип привязки	Внутренний
Криптошлюз	КШ1
Интерфейс	em1

Правило трансляции:

Параметр	Значение
Направление	Исходящее
Источник	ftp-client
Получатель	ftp-server
Интерфейс	em1
Трансляция адреса источника	
IP-адрес/Маска	Заполняются автоматически

Параметр	Значение
Изменить на	IP-адрес: 11.3.1.2 Маска: 255.255.255.255
Сервисы и трансляция портов	
Название сервиса	ftp
Протокол	TCP
Порт назначения	21 Внимание! Трансляция ftp работает только по 21 порту.
Порт трансляции	Не используется
Трансляция FTP	Установите отметку. При установленной отметке поддерживается корректная работа FTP в активном режиме

Запрет доступа к ресурсам единого реестра Роскомнадзора

Используя правила фильтрации, можно организовать запрет на доступ к ресурсам, включенным в состав единого реестра Роскомнадзора. При этом предусмотрено два варианта фильтрации: по IP-адресам и по URL.

Для фильтрации по IP-адресам необходимо сформировать правило (или правила), в котором в качестве источника или получателя указана группа сетевых объектов с именем "Реестр запрещенных ресурсов". Группа содержит сведения обо всех ресурсах единого реестра Роскомнадзора, в том числе IP-адреса запрещенных ресурсов. Группа "Реестр запрещенных ресурсов" создается автоматически при инициализации ЦУС и изначально не содержит объектов. Заполнение группы объектами осуществляется загрузкой в БД ЦУС сведений о запрещенных ресурсах, полученных в Роскомнадзоре (см. далее).

Для фильтрации по URL необходимо сформировать правило усиленной фильтрации, в котором используется специальный профиль — профиль запрещенных ресурсов. Профиль формируется автоматически на основании загружаемых в БД ЦУС сведений о запрещенных ресурсах. Сведения загружаются в БД ЦУС в виде xml-файла. Профиль содержит список агентов, которые также формируются автоматически. Поле "Адрес" в свойствах агента заполняется из тега domain загружаемого xml-файла. При формировании правила в поле "Действие" следует указать значение "Усиленная фильтрация", а в поле "Профиль усиленной фильтрации" — "Профиль запрещенных ресурсов" (о работе с правилами фильтрации см. стр. 104).

Загрузка сведений о запрещенных ресурсах

Порядок получения сведений о запрещенных ресурсах единого реестра приведен на портале Роскомнадзора по адресу <http://vigruzki.rkn.gov.ru/>.

Сведения (выгрузка) представляют собой xml-файл, который должен быть загружен в БД ЦУС.

Загрузка файла в БД ЦУС может быть выполнена вручную средствами ПУ ЦУС или автоматически агентом Роскомнадзора (о настройке и работе агента см. стр. 160).

Для загрузки файла вручную:

1. В ПУ ЦУС выберите команду "ЦУС | Загрузить файл реестра запрещенных ресурсов".

На экране появится стандартный диалог выбора файла.

2. Укажите файл выгрузки и нажмите в диалоге кнопку "Открыть".

Сведения о запрещенных ресурсах будут загружены в БД ЦУС.

Для просмотра сведений о запрещенных ресурсах в БД ЦУС:

- В ПУ ЦУС в окне объектов раскройте папку "Центр Управления Сетью\ Группы сетевых объектов\ Реестр запрещенных ресурсов".

В главном окне отобразится список запрещенных ресурсов. В дополнительном окне отобразится список правил фильтрации, в которых используется группа сетевых объектов "Реестр запрещенных ресурсов".

Примечание. Если такие правила фильтрации не создавались, список в дополнительном окне будет пустым.

Внимание! Группа "Реестр запрещенных ресурсов" удалению и редактированию не подлежит.

Виртуальная адресация

Для обеспечения возможности обмена информацией по защищенному каналу между пересекающимися подсетями, защищенными разными КШ, используется механизм виртуальной адресации.

Отправителю и получателю, находящимся в пересекающихся подсетях за разными КШ, назначаются виртуальные адреса.

Отправитель шлет пакет со своего реального адреса на виртуальный адрес получателя. При этом КШ отправителя перед шифрованием заменяет реальный адрес отправителя на виртуальный.

В зашифрованном пакете адреса отправителя и получателя – виртуальные.

КШ получателя после расшифровки заменяет адрес получателя на реальный. В результате пакет приходит на реальный адрес получателя с виртуального адреса отправителя.

Для настройки схемы с применением виртуальной адресации необходимо для каждой пары отправитель – получатель назначить виртуальные адреса. Виртуальный адрес отправителя или получателя назначается хосту или подсети, которые являются зарегистрированными сетевыми объектами.

Для назначения виртуального адреса сетевому объекту:

1. Вызовите список сетевых объектов.
2. Выберите в списке сетевой объект, для которого необходимо назначить виртуальный адрес, вызовите контекстное меню и активируйте команду "Свойства".

На экране появится окно настройки параметров сетевого объекта.

Описание полей окна настройки см. стр. [99](#).

3. Установите отметку в поле "Трансляция адреса внутри VPN" и введите назначаемый виртуальный адрес.

Поле "Трансляция адреса внутри VPN" доступно только в том случае, если в поле "Тип привязки" установлено значение "Защищаемый".

4. Нажмите кнопку "OK".

Окно настройки параметров сетевого объекта закроется.

Управление криптографическими ключами

Управление осуществляется в одном из двух режимов (см. стр. [20](#)):

- по базовой схеме;
- по усиленной схеме.

По умолчанию при вводе комплекса в эксплуатацию задается режим управления ключами по базовой схеме. После запуска ПУ ЦУС и процессе эксплуатации комплекса режим можно изменить (см. следующий подраздел).

Внимание! При выполнении операций смены ключей, описанных в данном разделе, не рекомендуется производить каких-либо действий по управлению сетевым устройством до завершения синхронизации с БД ЦУС. О завершении синхронизации свидетельствует пустая очередь заданий (для базовой схемы) или признак "включен" в общем списке сетевых устройств (для усиленной схемы).

Примечание. Смена ключей на КШ с ЦУС средствами ПУ ЦУС невозможна. Главный ключ и ключ связи с ЦУС меняется на КШ с ЦУС средствами локального управления (см. [2]).

Изменение режима управления ключами

Для изменения режима управления ключами:

1. Активируйте в меню "ЦУС" команду "Свойства".
Появится диалоговое окно "Свойства ЦУС" (см. стр. [86](#)).
2. В разделе "Режим управления ключевой информацией" выберите нужный режим и нажмите кнопку "ОК".
Диалоговое окно "Свойства ЦУС" закроется.

Внимание! После каждого изменения режима управления ключами необходимо выполнить смену ключей для всех сетевых устройств, входящих в состав комплекса. При переходе с базовой на усиленную схему смену ключей выполняют в соответствии с описанием, приведенным на стр. [141](#).

При переходе с усиленной на базовую схему смену ключей выполняют в соответствии с общим порядком смены ключей (см. стр. [137](#)).

Базовая схема управления ключами

Режим управления ключами по базовой схеме устанавливается по умолчанию при вводе комплекса в эксплуатацию. При этом генерацию ключей и их распределение по узлам сети выполняют в соответствии с общим порядком ввода комплекса в эксплуатацию.

Срок действия ключей составляет один год. По истечении срока их действия выполняют смену ключей. Кроме того, смену ключей выполняют в случае их компрометации. Общий порядок смены ключей приведен в следующем подразделе.

Предусмотрена также возможность в случае необходимости дистанционно средствами ПУ ЦУС сменить ключи на отдельных сетевых устройствах или на всех устройствах комплекса (см. стр. [140](#)).

Общий порядок смены ключей

Смену ключей шифрования осуществляют периодически в соответствии с принятым планом смены ключей, а также в случае компрометации ключей.

Общий порядок смены ключей:

1. Обновление исходной ключевой информации. Выполняют до истечения срока действия ключа сетевого устройства исходя из оперативности процедуры рассылки. Исходную ключевую информацию загружают на ЦУС сред-

ствами локального управления (см. [2], "Обновление исходной ключевой информации").

2. Генерация резервного ключевого материала для сетевого устройства (см. стр. 138). Ключи нумеруют и учитывают в журнале выпуска ключей. Для каждого сетевого устройства выпускают несколько комплектов резервных ключей.
3. Рассылка резервного ключевого материала локальным администраторам средствами спецсвязи.
4. Смена ключей сетевых устройств средствами программы управления ЦУС и локального управления сетевыми устройствами (см. стр. 139).
5. Смена ключей парной связи сетевых устройств (см. стр. 139).

Порядок действий при смене ключей в зависимости от сменяемого ключа представлен в таблице ниже.

Табл.18 Порядок действий при смене ключей

Причина	Действия
Исходная ключевая информация	Выполните пп. 5 общего порядка смены ключей
Резервный ключевой материал для сетевого устройства	Выполните пп. 5 общего порядка смены ключей
Ключи сетевого устройства	Выполните пп. 4–5 общего порядка смены ключей

Назначение ключей и места их хранения см. Табл.3 на стр.22.

Генерация резервного ключевого материала

Резервный ключевой материал используют для смены следующих ключей сетевого устройства:

- главный ключ сетевого устройства;
- ключ связи с ЦУС.

Резервный ключевой материал создают средствами программы управления.

В зависимости от версии сетевого устройства ключевой материал создается в новом (для версии 3.7) или старом (для версии 3.6 и ниже) формате.

Если резервный ключевой материал создается для сетевого устройства версии 3.7, он будет сохранен в файле keyset. Для сетевого устройства версии 3.6 и ниже ключевой материал сохраняется в файлах, представленных в таблице ниже.

Табл.19 Файлы резервных ключей

Файл	Описание
main.key	Резервный ключевой материал для смены главного ключа сетевого устройства
backup.key	Резервный ключевой материал для смены ключей связи с ЦУС

Для генерации резервного ключевого материала:

1. Выберите в списке нужное сетевое устройство, вызовите контекстное меню и активируйте команду "Создать резервные ключи".

На экране появится стандартный диалог для ввода пароля. Этот пароль служит для защиты ключевого материала от несанкционированного доступа.

2. Введите пароль, подтвердите его и нажмите кнопку "ОК".

Внимание! Пароль должен удовлетворять требованиям политики аутентификации администраторов (см. стр. 51). В противном случае кнопка "ОК" в диалоге назначения пароля будет неактивной.

На экране появится окно выбора каталога, предназначенного для сохранения ключевого материала.

3. Выберите нужный каталог и нажмите кнопку "Сохранить".

На экране появится сообщение "Резервные ключи сохранены".

4. Закройте сообщение, нажав кнопку "ОК".

Смена ключей сетевого устройства с использованием резервного ключевого материала

В результате выполнения данной процедуры происходит смена главного ключа сетевого устройства и ключа связи с ЦУС.

Процедура смены ключей выполняется индивидуально для каждого сетевого устройства и состоит из следующих этапов:

- установка ключей сетевого устройства на ЦУС;
- установка ключей на сетевое устройство.

Установку ключей сетевого устройства на ЦУС выполняют с помощью программы управления. Установку ключей на сетевое устройство — с помощью локальной консоли. Для установки ключей используют сгенерированный ранее средствами программы управления резервный ключевой материал.

Для установки ключей сетевого устройства на ЦУС:

1. Выберите в иерархическом списке устройство, на котором необходимо сменить ключи, вызовите на экран контекстное меню и активируйте команду "Загрузить ключи <сетевого устройства> с носителя на ЦУС".

На экране появится стандартный диалог выбора каталога.

2. Выберите каталог, в котором хранятся резервные ключи.

На экране появится стандартный диалог для ввода пароля.

3. Укажите пароль, назначенный при генерации резервного ключевого материала, и нажмите кнопку "ОК".

На экране появится сообщение "Резервные ключи загружены на ЦУС".

4. Закройте сообщение, нажав кнопку "ОК".

Об установке ключей на сетевое устройство с помощью локальной консоли см. [2], "Смена ключей на сетевом устройстве".

Примечание. При использовании базовой схемы управления резервный ключ на сетевое устройство, используя средства локальной консоли, следует устанавливать как активный.

Смена ключей парной связи

При смене ключей парной связи КШ и КК защищенные соединения, установленные на старых ключах, автоматически разрываются и затем создаются уже на новых ключах. В результате кратковременного разрыва соединения возможны потери трафика.

Для смены ключей парной связи:

1. Выберите в иерархическом списке КШ или КК, на котором необходимо сменить ключи парной связи, вызовите на экран контекстное меню и активируйте команду "Сменить все ключи парных связей".

Примечание. Команда "Сменить все ключи парных связей" недоступна при пустом списке связанных КШ или КК (см. стр. 78).

На экране появится запрос на подтверждение смены ключей.

2. Нажмите кнопку "Да".

На экране появится сообщение "Ключи парной связи изменены".

3. Закройте сообщение, нажав кнопку "ОК".

Внеплановая смена ключей сетевого устройства

При использовании базовой схемы предусмотрена внеплановая смена ключей сетевых устройств. В результате выполнения данной операции на сетевом устройстве происходит смена главного ключа и ключа связи с ЦУС.

Смена ключей может быть выполнена как одновременно для всех сетевых устройств комплекса, так и выборочно для одного устройства или для группы.

Предусмотрена также одновременная смена ключей всех сетевых устройств по настраиваемому расписанию.

Для смены ключей сетевого устройства:

1. Выберите в списке нужное сетевое устройство и активируйте в контекстном меню команду "Сменить ключи <сетевого устройства>...".

Примечание. Возможен множественный выбор объектов.

На экране появится диалог "Смена ключей <сетевого устройства>".

2. Укажите время, отводимое на смену ключей, и нажмите кнопку "Да".

Для смены ключей группы сетевых устройств:

1. Выберите в окне объектов нужную группу сетевых устройств и активируйте в контекстном меню команду "Сменить ключи всех устройств в группе...".

Примечание. Возможен множественный выбор объектов.

На экране появится диалог "Смена ключей".

2. Укажите время, отводимое на смену ключей, и нажмите кнопку "Да".

Для смены ключей всех сетевых устройств:

1. Выберите в окне объектов папку ЦУС и активируйте в контекстном меню команду "Сменить ключи всех сетевых устройств...".

На экране появится диалог "Смена ключей".

2. Укажите время, отводимое на смену ключей, и нажмите кнопку "Да".

Для настройки расписания смены ключей всех сетевых устройств:

1. Выберите в окне объектов папку ЦУС и активируйте в контекстном меню команду "Настройка смены ключей сетевых устройств по расписанию...".

На экране появится диалог "Настройка смены ключей сетевых устройств по расписанию".

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

Автоматически менять ключи на всех сетевых устройствах	Установка отметки включает режим автоматической смены ключей
Начиная с	Начало действия расписания
Повторять смену через	Период времени, через который выполняется автоматическая смена ключей
Время, отводимое на смену ключей	Период времени, отведенный на смену ключей
Блокировать трафик через сетевое устройство с истекшим сроком действия ключей	При наличии отметки зашифрованный трафик через сетевое устройство, у которого истек срок действия ключей, блокируется. Блокировка распространяется как на управляющий трафик, так и на трафик VPN

Примечание. Не рекомендуется устанавливать длительный период времени, отводимый на смену ключей. Во время смены ключей управление сетевым устройством средствами централизованного управления невозможно.

Усиленная схема управления ключами

Порядок и схема распространения ключей

Работа, связанная с генерацией ключей и распространением их между узлами в АПКШ "Континент", рассчитана на три года. Далее весь описанный ниже трехлетний цикл повторяется.

Первый год эксплуатации

Работы выполняют последовательно в три этапа.

1. Подготовка к использованию усиленной схемы управления ключами.

На этом этапе необходимо выполнить следующее:

- Проинициализировать КШ с ЦУС (если не был проинициализирован ранее).
- Установить ПО на узлы сети (если не было установлено ранее).
- Включить режим управления ключами по усиленной схеме (см. стр. **137**).
- Приготовить N+1 USB-ключей Rutoken ЭЦП, где N — количество узлов сети (не считая КШ с ЦУС), и один USB-флеш-накопитель.

2. Выпуск серии ключевых документов на АРМ ГК.

Процедура выпуска серии описана в [9] (см. раздел "Изготовление серии ключевых документов").

В результате выполнения процедуры будет получен комплект ключевых носителей. В комплект входят:

- N ключевых документов (ключевых носителей узлов). Каждый ключевой документ содержит ключ хранения со сроком действия 3 года и ключ связи со сроком действия один год и три месяца.
- ключевой носитель АРМ ГК с записанными в его памяти ключами хранения данной серии.
- USB- флеш- накопитель с записанными всеми ключами связи и соответствующими им комплектами ключей, зашифрованными на ключе хранения.

Каждый ключевой носитель узла должен быть промаркирован, например, с помощью бирки, содержащей следующие сведения:

- номер серии;
- порядковый номер ключевого носителя в серии (от 1 до N);
- дата выпуска;
- имя узла сети, в котором должен использоваться данный ключевой носитель.

Ключевой носитель АРМ ГК также должен быть промаркирован, например, биркой другого цвета, чтобы визуально отличаться от ключевых носителей узлов. В бирке должен отображаться номер серии ключевых документов, для которой он был выпущен.

Перечисленные выше сведения о каждом ключевом носителе, а также его серийный номер должны быть внесены в журнал.

3. Распределение ключей.

На этом этапе необходимо выполнить следующее:

- Доставить ключевые носители на соответствующие узлы.
- Загрузить ключи на узлы (см. [2], подраздел "Загрузка ключей").
- В ПУ ЦУС назначить каждому узлу соответствующий комплект ключей, хранящийся на USB-флеш-накопителе (см. стр. **144**).
- В ПУ ЦУС активировать ключи узлов (см. стр. **146**).

После выполнения описанных выше работ начнется эксплуатация АПКШ "Континент" по усиленной схеме управления ключами.

Второй год эксплуатации

По истечении года с даты выпуска ключевых документов необходимо выполнить перевыпуск комплектов ключей. Работы по перевыпуску выполняют в три этапа.

1. Перевыпуск комплектов ключей на АРМ ГК.

Для перевыпуска требуются чистый USB-флеш-накопитель и ключевой носитель АРМ ГК, выпущенный в составе комплекта ключевых носителей.

В результате перевыпуска на USB-флеш-накопитель будет записана серия новых комплектов ключей, зашифрованных на соответствующих ключах хранения ключевого носителя АРМ ГК. При этом номер серии остается прежним.

Процедура перевыпуска комплектов ключей приведена в [9] (см. раздел "Выпуск новых ключевых комплектов").

2. Смена комплектов ключей на узлах.

Для смены комплектов ключей на узлах необходимо выполнить следующее:

- В ПУ ЦУС назначить каждому узлу соответствующий перевыпущенный комплект ключей, хранящийся на USB-флеш-накопителе (см. стр. 144).
- В ПУ ЦУС выполнить отправку назначенных комплектов новых ключей с USB-флеш-накопителя на узлы.

Процедура отправки описана на стр. 148.

- Средствами локального управления на каждом из узлов загрузить ключи, присланные с ЦУС. При выполнении данной процедуры необходимо предъявить ключевой носитель узла и ввести его ПИН-код.

Процедура загрузки описана в [2] (см. подраздел "Загрузка ключей").

Внимание! Смену комплектов ключей на узлах и переход к следующему этапу необходимо провести в минимально возможные сроки, так как после смены комплектов ключей на узлах управление сетевыми узлами со стороны ЦУС будет ограничено.

3. Загрузка и смена комплектов ключей на ЦУС.

Для завершения перевыпуска ключей необходимо загрузить новые ключи с USB-флеш-накопителя в БД ЦУС и выполнить их активацию (см. стр. 146).

После завершения данного этапа эксплуатация АПКШ "Континент" по схеме трехлетнего хранения ключей будет продолжена.

Третий год эксплуатации

По истечении двух лет с даты выпуска ключевых документов необходимо провести повторный перевыпуск комплектов ключей, т.е. выполнить все работы, описанные для второго года эксплуатации.

По истечении трех лет с даты выпуска ключевых документов цикл эксплуатации АПКШ "Континент" завершается. Для продолжения работы необходимо подготовить новые ключевые носители и начать цикл с выпуска серии ключевых документов на АРМ ГК.

Вызов мастера управления ключами

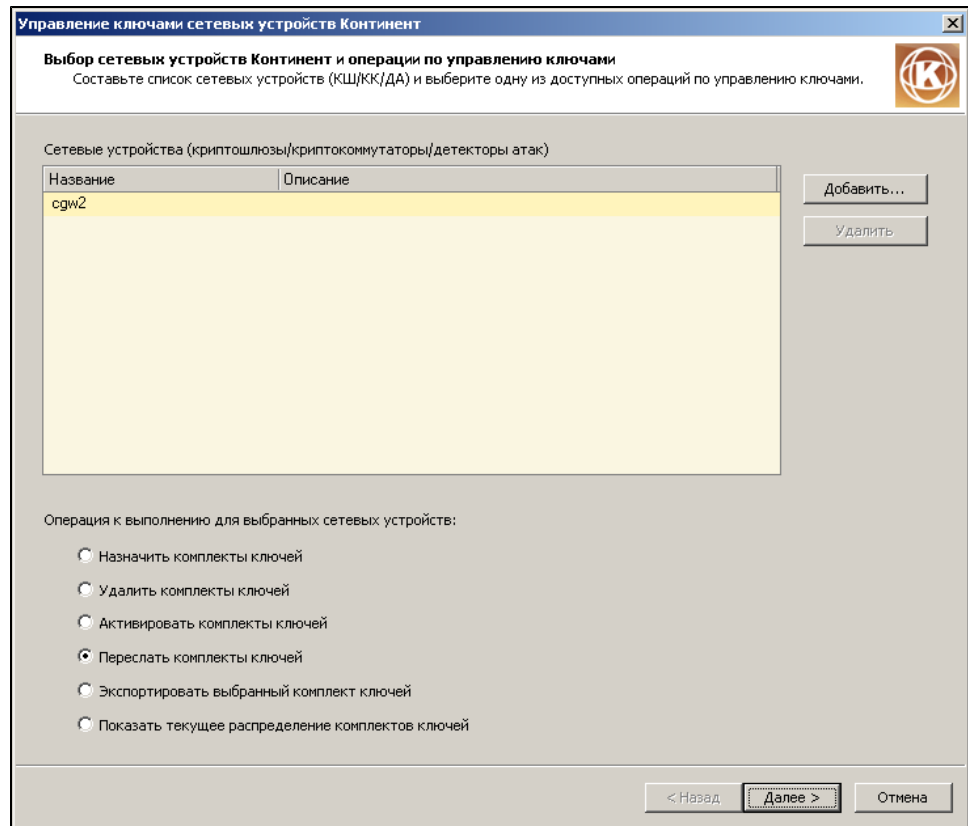
Для запуска мастера управления ключами:

1. Выберите в окне объектов главного окна папку с наименованием сетевого устройства.

В главном окне отобразится список зарегистрированных сетевых устройств.

2. Выделите одно или несколько сетевых устройств, для которых должна быть выполнена операция с ключами, вызовите контекстное меню и выберите в нем команду "Управление ключами <сетевых устройств>".

Появится стартовый диалог мастера управления ключами.



В верхней части диалога представлен список сетевых устройств, выбранных в предыдущем пункте процедуры. Список устройств может быть откорректирован с помощью кнопок "Добавить" и "Удалить", расположенных справа от списка.

В нижней части диалога находится перечень операций с ключами, которые могут быть выполнены одновременно для всего списка сетевых устройств.

Операция	Описание
Назначить комплекты ключей	Назначение комплектов ключей сетевым устройствам/группам сетевых устройств (без загрузки ключей в ЦУС)
Удалить комплекты ключей	Удаление комплекта ключей из БД ЦУС с одновременным удалением его с ключевого носителя и занесением в список использованных комплектов
Активировать комплекты ключей	Загрузка в БД ЦУС назначенного сетевому узлу комплекта. Загруженный комплект ЦУС начинает использовать для связи с сетевым узлом
Переслать комплекты ключей	Отправка комплектов ключей с ЦУС на сетевые узлы для последующей их смены средствами локального управления
Экспортировать выбранный комплект ключей	Извлечение комплекта ключей сетевого устройства из USB-флеш-накопителя (ЦУС) для загрузки в сетевое устройство с использованием USB-флеш-накопителя вместо ключевого носителя Rutoken
Показать текущее распределение комплектов ключей	Просмотр текущего распределения комплектов и наборов ключей

3. Для выполнения той или иной операции выберите ее в перечне и нажмите кнопку "Далее".

Описание операций приведено в последующих подразделах.

Назначение комплектов ключей сетевым устройствам

Выполняется назначение из числа комплектов ключей, сгенерированных на АРМ ГК и хранящихся на USB-ключе ТОКЕН_ЦУС (подробнее см. [9]).

Одному сетевому устройству можно назначить несколько комплектов ключей. Один комплект ключей может быть назначен только одному сетевому устройству.

Один ключ может быть назначен только одному сетевому устройству.

Назначение комплектов может быть выполнено как вручную, так и автоматически.

При назначении комплектов ключей сами комплекты в БД ЦУС не загружаются.

Для назначения комплектов ключей:

1. Запустите мастер управления ключами и выберите одно или несколько сетевых устройств для назначения им комплектов ключей (см. стр. 142).
2. Вставьте ключевой носитель ТОКЕН_ЦУС с записанными на нем комплектами ключей.
3. В окне мастера в перечне операций с ключами выберите "Назначить комплекты ключей" и нажмите кнопку "Далее".

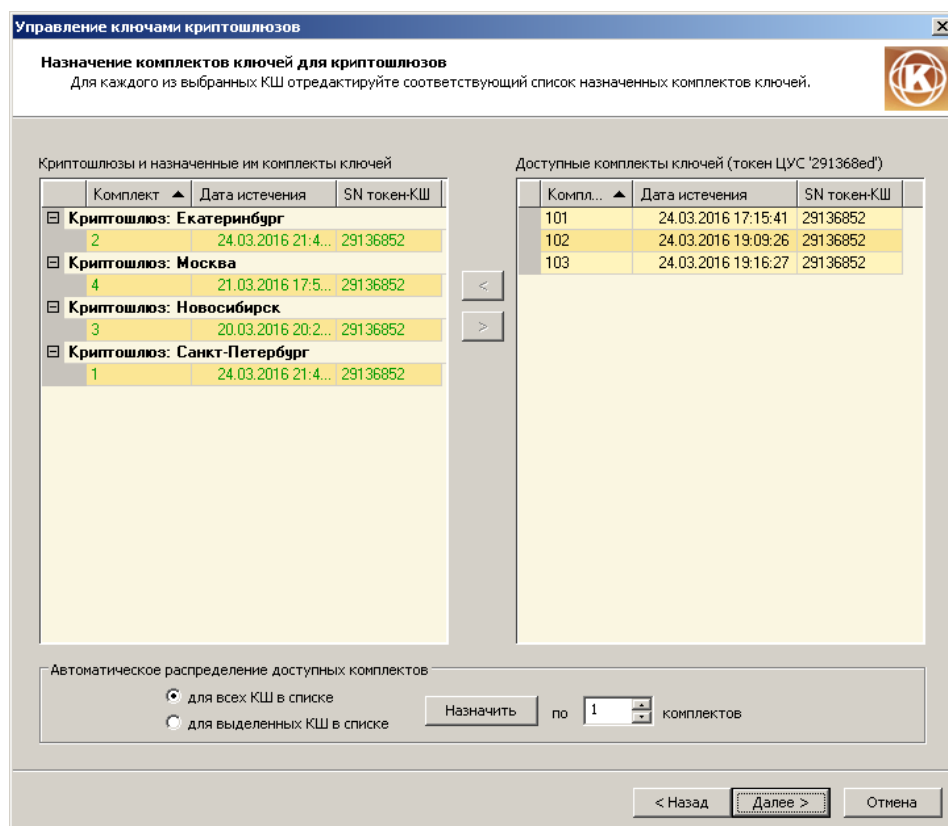
Появится диалоговое окно назначения комплектов ключей.

В левой части окна представлен список выбранных сетевых устройств и назначенные им комплекты ключей.

В правой части окна отображается список комплектов ключей, хранящихся на предъявленном ключевом носителе. Комплекты, у которых истекает срок хранения, отмечены восклицательным знаком красного цвета.

- Для ручного назначения комплектов ключей перейдите к п. 4.
 - Для автоматического распределения комплектов по устройствам перейдите к п. 8.
4. Выберите в левом списке сетевое устройство, которому необходимо назначить комплект. Для этого выделите его название или строку любого уже назначенного ему комплекта.
 5. Выделите в правом списке комплект или несколько комплектов, которые должны быть назначены выбранному сетевому устройству.
Станет доступна кнопка переноса влево.
 6. Нажмите кнопку переноса.

У выбранного сетевого устройства появится вновь назначенный комплект (или список комплектов), выделенный зеленым цветом. При этом назначенные комплекты из списка, расположенного справа, будут удалены.



Примечание. Перенос комплектов в список сетевых устройств и обратно можно выполнить способом Drag and Drop.

7. Для назначения комплектов следующему сетевому устройству повторите выполнение пп.4–6.

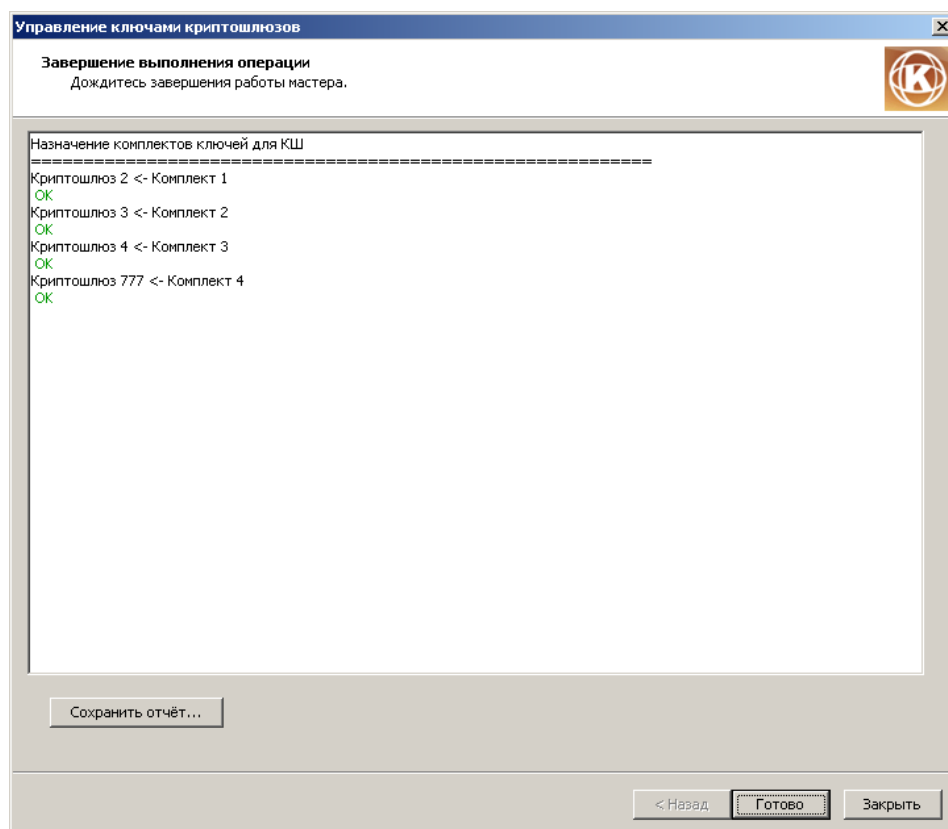
- Для отмены назначения комплекта выделите его в списке устройств и нажмите кнопку переноса вправо.

Из списка сетевых устройств комплект будет удален и перемещен в список комплектов.

После назначения комплектов всем сетевым устройствам при необходимости откорректируйте список сетевых устройств и назначенных им комплектов ключей и затем перейдите к п. 12.

8. Для автоматического распределения комплектов выберите вариант: для всех устройств в списке или для выделенных.
9. Если выбран вариант только для выделенных устройств, выделите их в списке.
10. Укажите количество комплектов, которое должно быть назначено для каждого из выделенных сетевых устройств, и нажмите кнопку "Назначить".
Будет выполнено автоматическое распределение комплектов. Вновь назначенные комплекты будут отображены в списке сетевых устройств и удалены из списка доступных комплектов.
11. При необходимости откорректируйте ручную распределение комплектов, отображаемое в списке сетевых устройств. Для этого используйте описание ручного назначения (см. пп. 4–7).
12. После окончательной проверки распределения комплектов по сетевым устройствам нажмите кнопку "Далее".

Будет выполнено распределение комплектов и затем появится окно, отображающее результаты выполнения операции.



13. Для сохранения результатов в файл нажмите кнопку "Сохранить отчет" и выберите формат файла: *.txt или *.xml.

14. Для завершения работы мастера нажмите кнопку "Готово".

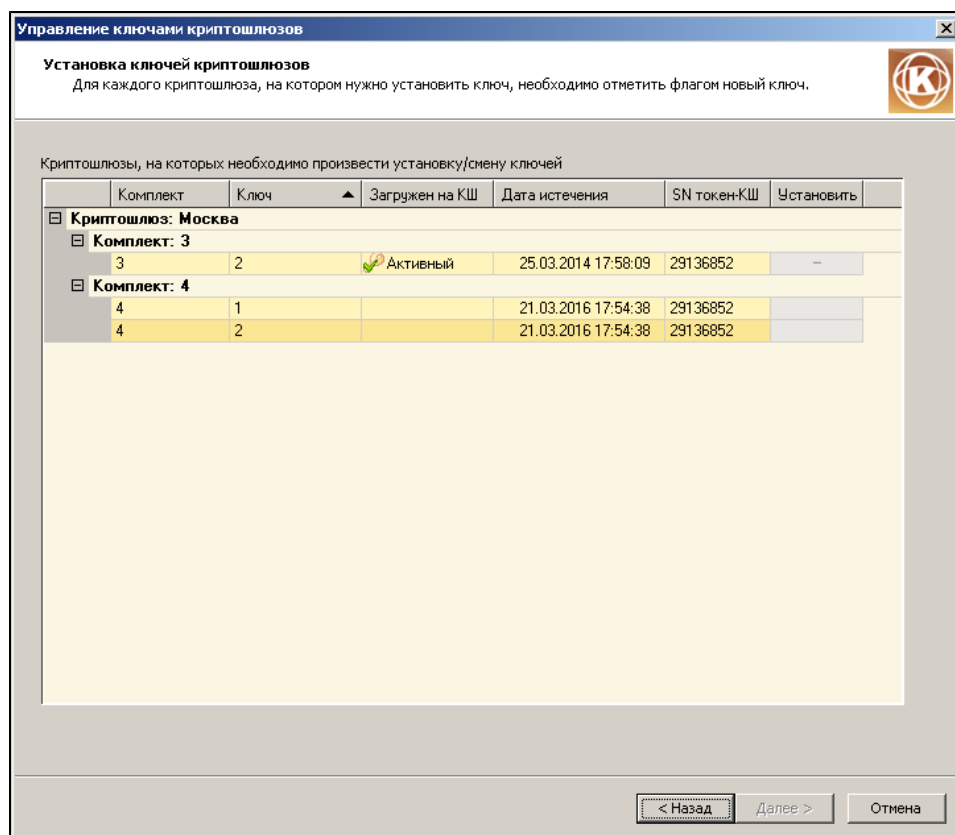
Загрузка и активация ключей в ЦУС

Загрузка выполняется при необходимости сменить ключи сетевого устройства или установить их при инициализации устройства.

Для загрузки ключей:

1. Запустите мастер управления ключами и выберите одно или несколько сетевых устройств, для которых необходимо выполнить загрузку и активацию ключей (см. стр. **142**).
2. Вставьте ключевой носитель ТОКЕН_ЦУС с записанными на нем комплектами ключей.
3. В окне мастера в перечне операций с ключами выберите "Активировать комплекты ключей" и нажмите кнопку "Далее".

На экране появится окно "Установка ключей <сетевых устройств>".



В окне представлен список выбранных <сетевых устройств> и назначенные им комплекты ключей. Для каждого комплекта приводится список ключей. Для каждого ключа приводится следующая информация:

- номер комплекта;
- номер ключа;
- статус (загружен на устройство/не загружен); если загружен – активный или резервный;
- дата окончания срока хранения;
- серийный номер ключевого носителя (ТОКЕН_КШ), на котором хранится ключ.

- Последовательно для каждого сетевого устройства в списке выделите ключ, подлежащий активации, и левой кнопкой мыши установите отметку.

У выделенного ключа в поле "Установить" появится отметка в виде флага, означающая, что данный ключ будет загружен и активирован.

Если необходимо отменить выбор ключа, удалите отметку.

- После назначения ключей для всех сетевых устройств списка нажмите кнопку "Далее".

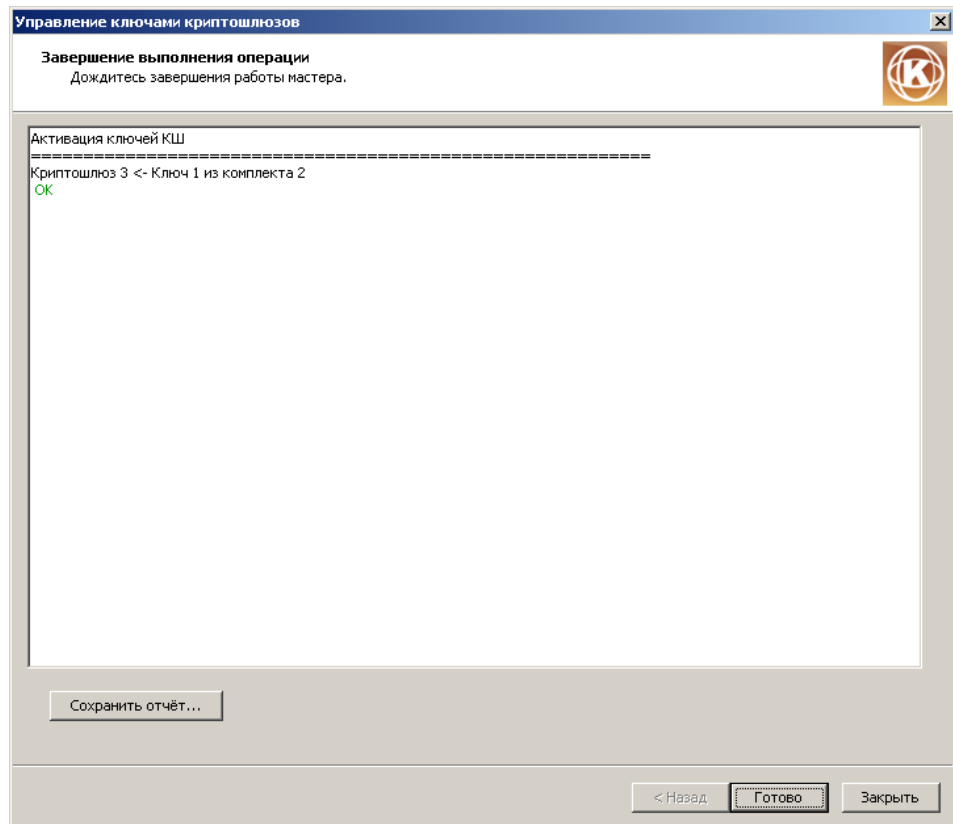
На экране появится сообщение о необходимости ввести PIN-код пользователя.

- Введите PIN-код пользователя.

Начнется операция загрузки ключей в БД ЦУС и удаление ключей, которые до начала процедуры были активными.

Если загружается ключ из комплекта, не содержащего загруженный ключ, весь комплект, включающий в себя активный ключ, будет удален. Удаление осуществляется как из БД ЦУС, так и с ключевого носителя.

После завершения операции на экране появится отчет с результатами выполненных действий.



7. Ознакомьтесь с отчетом и при необходимости сохранить его в одном из двух форматов (*.txt или *.xml) нажмите кнопку "Сохранить отчет".
8. Для завершения работы мастера нажмите в окне отчета кнопку "Готово".

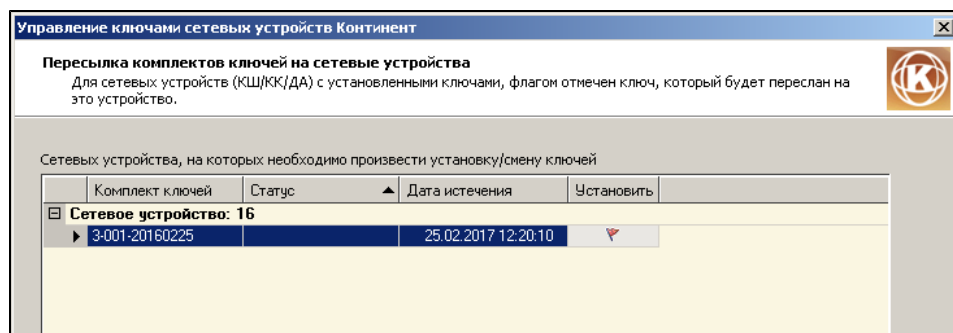
Отправка комплектов новых ключей на узлы

Данную процедуру выполняют после перевыпуска комплектов ключей на АРМ ГК и назначения их сетевым узлам для последующей загрузки отправленных ключей на сетевые узлы средствами локального управления.

Для отправки комплектов ключей:

1. Выберите в списке сетевой узел, на который должен быть отправлен комплект ключей, и запустите мастер управления ключами.
Откроется стартовый диалог мастера.
2. Выделите в списке диалога сетевое устройство, выберите в списке операцию "Переслать комплекты ключей" и нажмите кнопку "Далее".

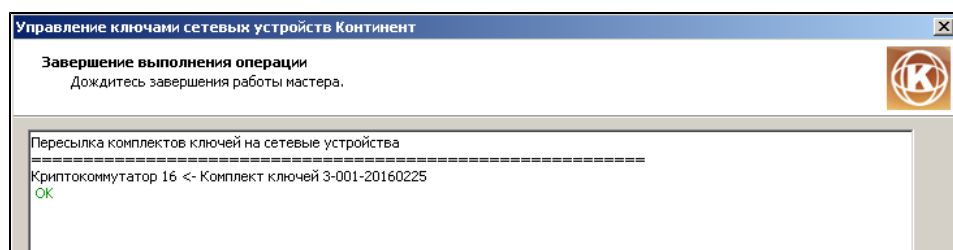
На экране появится следующий диалог мастера, отображающий список назначенных выбранному сетевому устройству комплектов ключей.



3. Выделите комплект ключей, который должен быть отправлен на сетевое устройство, и установите отметку в поле "Установить" (см. рисунок выше).

4. Нажмите кнопку "Далее", расположенную в нижнем правом углу диалога мастера.

На экране появится завершающий диалог мастера.



5. Нажмите кнопку "Готово", расположенную в нижнем правом углу диалога. Мастер завершит работу и в очереди заданий появится новое задание по отправке комплекта ключей на сетевой узел.

Экспорт комплектов ключей

Данная операция предусмотрена для тех случаев, когда по каким-либо причинам необходимо выполнить локальную загрузку ключей на сетевое устройство с USB-флеш-накопителя.

Для записи комплекта ключей сетевого устройства на USB-флеш-накопитель необходимо предварительно извлечь комплект из USB-флеш-накопителя ЦУС и далее сохранить в указанный каталог в виде файла, защищенного паролем.

Для извлечения и сохранения комплекта ключей:

1. Запустите мастер управления ключами.
2. Вставьте USB- флеш- накопитель (ЦУС), выберите в списке операций "Экспортировать выбранный комплект ключей" и нажмите кнопку "Далее".
В окне мастера появится список назначенных данному устройству комплектов ключей.
3. Выберите в списке нужный комплект ключей, установите отметку и нажмите кнопку "Далее".

На экране появится запрос на задание пароля для доступа к комплекту ключей. Этот пароль потребуется ввести при загрузке ключей в сетевое устройство.

4. Задайте и подтвердите пароль.

Внимание! Пароль должен удовлетворять требованиям политики аутентификации администраторов (см. стр. 51). В противном случае кнопка "OK" в диалоге назначения пароля будет неактивной.

На экране появится стандартный диалог выбора каталога для хранения комплекта ключей.

5. Укажите каталог и сохраните файл.

Примечание. В качестве каталога можно указать USB-флеш-накопитель. Если файл комплекта ключей был сохранен в каталог, скопируйте его на USB-флеш-накопитель для передачи локальному администратору сетевого устройства.

6. Передайте USB- флеш- накопитель локальному администратору сетевого устройства и сообщите ему пароль.

Удаление комплектов ключей

Администратор ПУ ЦУС имеет возможность удалять комплекты ключей из БД ЦУС (например, в случае компрометации ключей, комплектов или носителей ТОКЕН_КШ).

Комплект, имеющий в своем составе активный ключ, удалению не подлежит.

Удаление комплектов может быть выполнено как с предъявлением ключевого носителя ТОКЕН_ЦУС, на котором хранятся подлежащие удалению комплекты, так и без него.

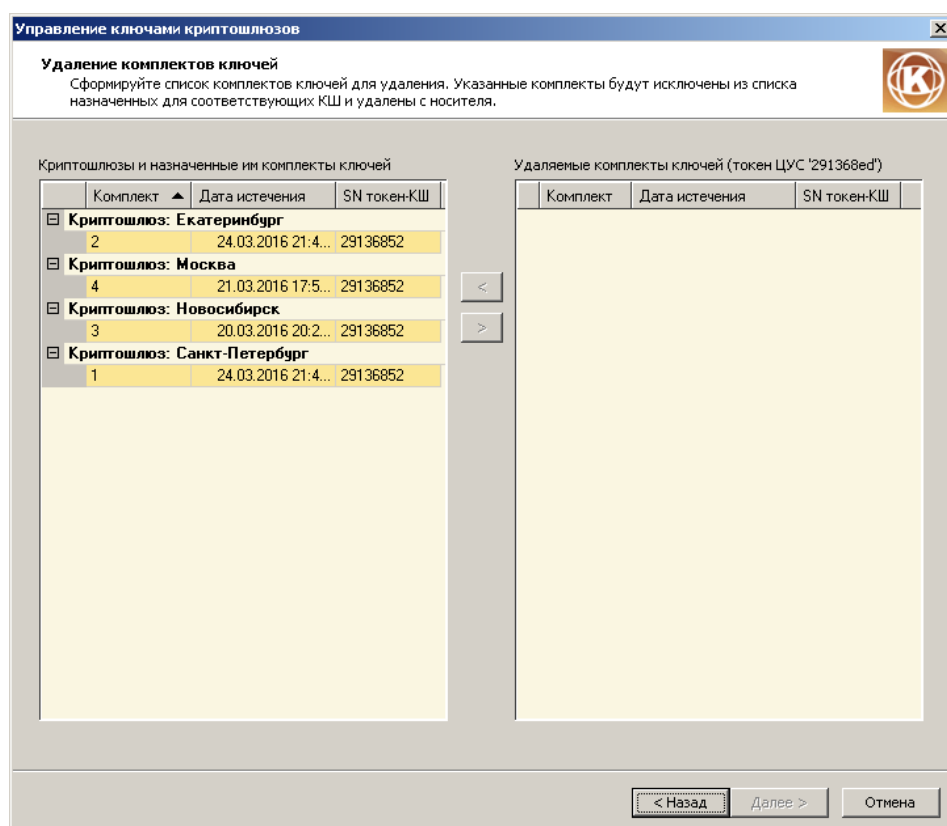
Если удаление выполняется с предъявлением ключевого носителя, удаляемые из БД ЦУС комплекты будут удалены и с него.

Если удаление комплекта выполняется без предъявления ключевого носителя, после успешного выполнения операции попытка загрузки ключей из данного комплекта будет невозможна.

Для удаления комплектов ключей:

1. Запустите мастер управления ключами и выберите сетевые устройства, для которых должно быть выполнено удаление комплекта (комплектов) ключей (см. стр. 142).
2. Вставьте ключевой носитель ТОКЕН_ЦУС с записанными на нем комплектами ключей.
3. В перечне операций в окне мастера выберите "Удалить комплекты ключей" и нажмите кнопку "Далее".

На экране появится окно "Удаление комплектов ключей".



В левой части окна расположен список выбранных сетевых устройств и назначенных им комплектов ключей. Для каждого комплекта приведена следующая информация:

- номер комплекта;
- дата истечения срока действия;
- серийный номер ключевого носителя, на котором хранится данный комплект.

В правой части расположен список удаляемых комплектов ключей.

4. Выберите в списке сетевых устройств комплект или группу комплектов, подлежащих удалению, и нажмите кнопку переноса вправо.

Удаляемые комплекты будут перенесены в список удаляемых и выделены красным цветом.

Управление ключами криптошлюзов

Удаление комплектов ключей
Сформируйте список комплектов ключей для удаления. Указанные комплекты будут исключены из списка назначенных для соответствующих КШ и удалены с носителя.

Криптошлюзы и назначенные им комплекты ключей

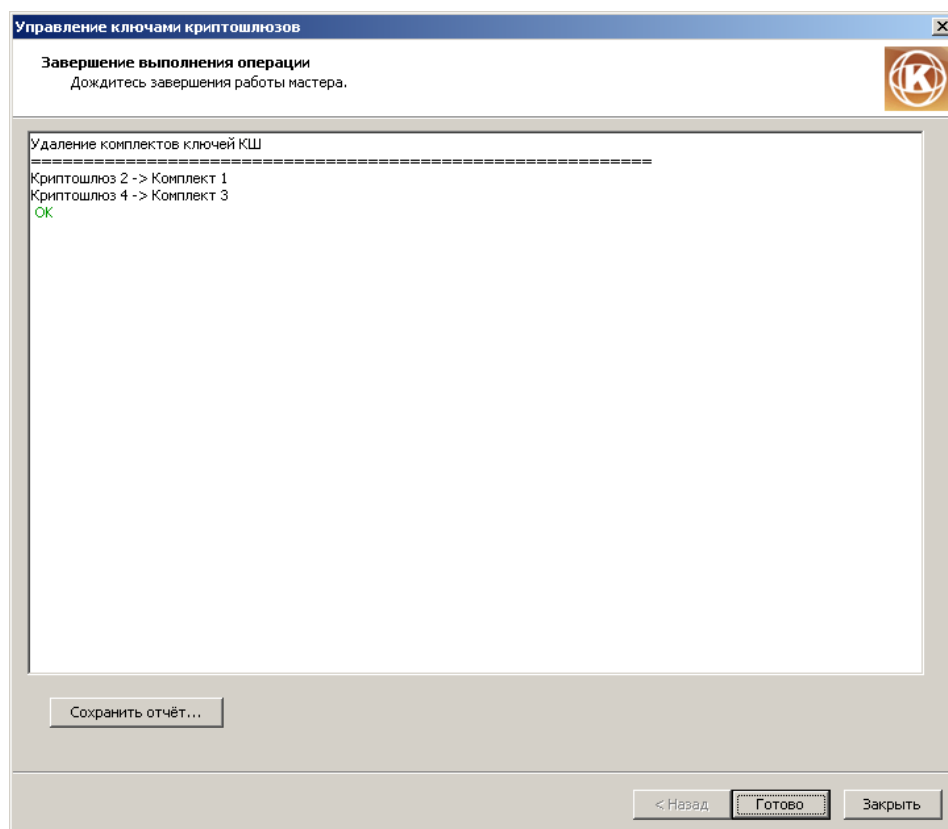
Комплект	Дата истечения	SN токен-КШ
<input type="checkbox"/> Криптошлюз: Екатеринбург		
2	24.03.2016 21:4...	29136852
<input type="checkbox"/> Криптошлюз: Москва		
4	21.03.2016 17:5...	29136852
<input type="checkbox"/> Криптошлюз: Новосибирск		
(не назначен)		
<input type="checkbox"/> Криптошлюз: Санкт-Петербург		
(не назначен)		

Удаляемые комплекты ключей (токен ЦУС '291368ed')

Комплект	Дата истечения	SN токен-КШ
1	24.03.2016 21:43:01	29136852
3	20.03.2016 20:22:27	29136852

< Назад **Далее >** Отмена

- При необходимости отменить удаление комплекта выделите его в списке удаляемых и нажмите кнопку переноса влево.
Удаляемый комплект будет восстановлен в списке сетевых устройств.
- После окончательного формирования списка удаляемых комплектов нажмите кнопку "Далее".
Начнется удаление указанных комплектов из БД ЦУС и с ключевого носителя ТОКЕН_ЦУС (если он был предъявлен) и после завершения на экране появится окно отчета о выполненных операциях.



Если в составе удаляемого комплекта был активный ключ, операция завершится с ошибкой и ни один из удаляемых комплектов из БД ЦУС удален не будет.

7. Ознакомьтесь с отчетом и при необходимости сохранить его в одном из двух форматов (*.txt или *.xml) нажмите кнопку "Сохранить отчет".
8. Для завершения процедуры нажмите в окне отчета кнопку "Готово".

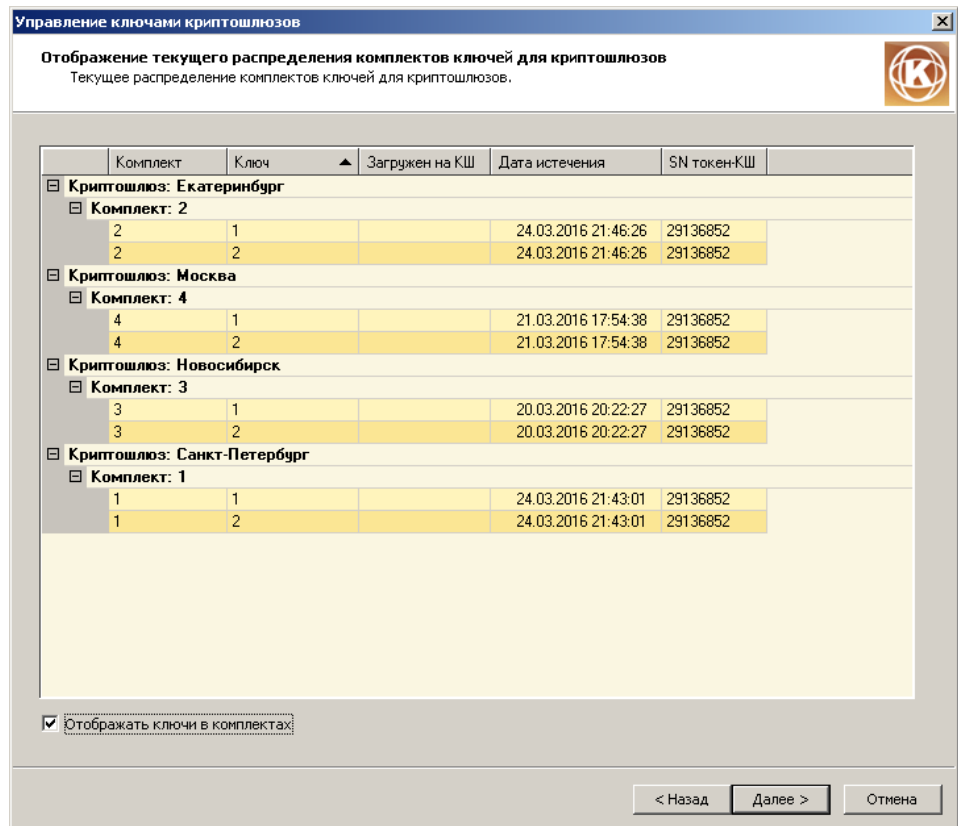
Просмотр текущего распределения ключей

Администратор ПУ ЦУС имеет возможность просмотреть текущее распределение по сетевым устройствам комплектов и входящих в них ключей и сохранить полученную информацию в виде текстового файла или файла формата xml.

Для просмотра:

1. Запустите мастер управления ключами и выберите сетевые устройства, для которых требуется просмотреть назначенные им комплекты ключей (см. стр. 142).
2. В перечне операций в окне мастера выберите "Показать текущее распределение комплектов и ключей" и нажмите кнопку "Далее".

На экране появится окно "Отображение текущего распределения комплектов ключей для <сетевых устройств>".



В окне отображается список выбранных сетевых устройств и назначенных им комплектов ключей. Каждый комплект представлен списком входящих в него ключей.

- Для просмотра комплектов без отображения входящих в них ключей удалите отметку в поле "Отображать ключи в комплектах".

Для каждого ключа приводится следующая информация:

- номер комплекта;
- номер ключа;
- статус (загружен на сетевое устройство/не загружен); если загружен – активный или резервный;
- дата окончания срока хранения;
- серийный номер ключевого носителя (ТОКЕН_КШ), на котором хранится ключ.

Ключи с истекающим сроком хранения отмечены восклицательным знаком красного цвета.

3. После просмотра представленной информации нажмите кнопку "Далее".

На экране появится окно, в котором просмотренные сведения отображаются в виде отчета и могут быть сохранены в виде файла формата *.txt или *.xml.

4. При необходимости сохранить отчет нажмите кнопку "Сохранить отчет" и выберите формат файла.
5. Для завершения просмотра сведений нажмите кнопку "Готово" в окне отчета.

Организация связи со сторонними криптографическими сетями

Общий порядок организации связи

Для организации связи со сторонней криптографической сетью, управляемой другим ЦУС, необходимо выполнить следующие действия:

1. Регистрация внешней сети средствами программы управления (см.стр.157).
2. Обмен сертификатами открытых ключей.
 - Создание и экспорт сертификата собственной сети (см.стр.154).
 - Импорт сертификата сторонней сети (см.стр.157).
3. Обмен файлами конфигурации разрешенных к доступу ресурсов.
 - Создание и экспорт файла конфигурации разрешенных к доступу ресурсов собственной сети (см.стр.157).
 - Импорт файла конфигурации разрешенных к доступу ресурсов сторонней сети (см.стр.157).
4. Создание межсетевого ключа (см.стр.158).
5. Настройка соединений между КШ (см.стр.78).
6. Создание правил фильтрации для информационного обмена между сетями (см.стр.104).

Внимание!

- При организации взаимодействия со сторонней криптографической сетью связи устанавливаются только между криптошлюзами.
- Связь со сторонней криптографической сетью не может быть установлена, если хотя бы на одном из связываемых ЦУС включен режим изолированной сети (см. стр.86).
- Для установки соединения между КШ, принадлежащими разным криптографическим сетям, хотя бы один из этих КШ должен обладать однозначно идентифицируемым статическим IP-адресом.
- Загрузка конфигурации внешней сети при совпадении идентификаторов КШ в домашней и внешней сети невозможна.

Инфраструктура открытых ключей

Собственная инфраструктура открытых ключей предназначена для установки защищенного соединения с внешней криптографической сетью.

Удостоверяющим центром является ЦУС. Здесь выполняются генерация ключевой пары и издание сертификата открытого ключа, а также их хранение.

Для вызова списка сертификатов:

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

В правой части окна отобразится список сертификатов.

Табл.20 Перечень полей списка сертификатов

Поле	Описание
Имя сертификата	Наименование сертификата открытого ключа
Серийный номер	Уникальный номер сертификата открытого ключа
Действителен с	Дата и время начала срока действия сертификата
Действителен по	Дата и время окончания срока действия сертификата

Для создания сертификата:

1. Вызовите контекстное меню в любом месте списка сертификатов и активируйте команду "Создать сертификат" или нажмите одноименную кнопку на панели инструментов.

На экране появится диалог "Создание сертификата".

2. Заполните поля диалога.

Поле	Описание
Название	Наименование сертификата открытого ключа
Описание	Дополнительная текстовая информация
Организация	Наименование организации, издавшей сертификат
Подразделение	Наименование подразделения, издавшего сертификат
Регион	Почтовые атрибуты организации, издавшей сертификат
Город	
Страна	
Электронная почта	

В поле "Назначение" выберите значение "Подключение к внешним сетям" и нажмите кнопку "Далее".


На экране появится следующий диалог "Привязка сертификата".

В диалоге отображается привязка создаваемого сертификата к домашней сети.

3. Нажмите кнопку "Готово".


Диалог мастера закроется и в списке сертификатов появится вновь созданный сертификат.

Для просмотра сертификата:

- Выберите нужную запись в списке и нажмите кнопку  на панели инструментов.

На экране появится стандартный диалог Windows для просмотра свойств сертификата.

Для удаления сертификата:

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

Для экспорта сертификата в файл:

1. Выберите сертификат в списке, вызовите контекстное меню и выберите пункт "Свойства".

На экране появится стандартный диалог Windows для просмотра свойств сертификата.

2. Перейдите на вкладку "Состав" и нажмите кнопку "Копировать в файл".

На экране появится диалог мастера экспорта сертификата.

3. Выберите формат, в котором должен быть экспортирован сертификат, и нажмите кнопку "Далее".

На экране появится стандартный диалог сохранения файла.

4. Укажите имя сохраняемого файла и путь и нажмите кнопку "Далее".

На экране появится завершающий диалог мастера экспорта.

5. Нажмите кнопку "Готово".

Диалог мастера закроется и сертификат будет сохранен в файл.

Управление внешними сетями

Перечень сторонних криптографических сетей отображается в окне "Внешние криптографические сети". Управление внешними сетями выполняют в этом окне.

Для вызова списка внешних сетей:

1. В левой части окна программы управления выберите папку "Внешние криптографические сети".

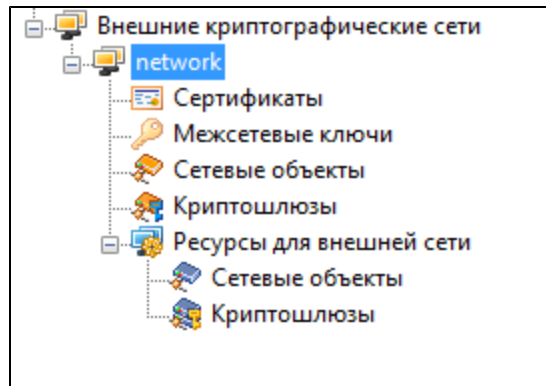
В правой части окна отобразится список зарегистрированных внешних сетей.

Табл.21 Перечень полей списка внешних сетей

Поле	Описание
Название	Наименование внешней криптографической сети
Описание	Дополнительная текстовая информация

2. Для просмотра подробных сведений о внешней сети раскройте в левой части окна папку "Внешние криптографические сети" и далее раскройте вложенную папку с нужным названием.

Появится список папок, содержащих всю необходимую информацию для работы с данной сетью.



3. Для просмотра содержимого папки выберите ее в списке.

В правой части окна отобразится содержимое папки.

Для регистрации внешней сети:

1. Вызовите контекстное меню в любом месте списка внешних сетей в правой части окна и активируйте команду "Создать внешнюю криптографическую сеть" или нажмите одноименную кнопку на панели инструментов.


На экране появится диалог "Внешняя криптографическая сеть".

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

Название	Наименование внешней криптографической сети
Описание	Дополнительная текстовая информация

В списке внешних сетей появится новая сеть.

Для редактирования внешней сети:

1. Выберите нужную запись в списке и активируйте команду контекстного меню "Свойства" или нажмите одноименную кнопку () на панели инструментов.

На экране появится диалог "Внешняя криптографическая сеть".

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

Название	Наименование внешней криптографической сети
Описание	Дополнительная текстовая информация

Для импорта сертификата внешней сети:

1. Выберите нужную запись в списке и активируйте команду контекстного меню "Импортировать сертификат внешней сети...".

На экране появится стандартный диалог Windows для открытия файла.

2. Выберите нужный файл сертификата (*.cer) и нажмите кнопку "ОК".

Сертификат будет добавлен в папку "Сертификаты".

Для импорта конфигурации разрешенных к доступу ресурсов:

1. Выберите нужную запись в списке и активируйте команду контекстного меню "Импортировать конфигурацию внешней сети...".

На экране появится стандартный диалог Windows для открытия файла.

2. Выберите нужный файл конфигурации (*.nc) и нажмите кнопку "ОК".

Для экспорта конфигурации разрешенных к доступу ресурсов:


1. Выберите нужную запись в списке и активируйте команду контекстного меню "Экспортировать конфигурацию для внешней сети...".

На экране появится диалог "Экспорт конфигурации для внешней сети".

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

Поле	Описание
Сертификат своей сети	Наименование сертификата собственной сети, предназначенного для создания электронной подписи файла конфигурации
Сертификат внешней сети	Наименование сертификата внешней сети для зашифровывания файла конфигурации
Сетевые объекты и криптошлюзы, доступные для внешней сети	Перечень сетевых объектов собственной сети, к которым разрешен доступ из данной внешней сети. Для формирования списка используйте кнопки "Добавить..." и "Удалить"
Имя файла для сохранения экспортируемой конфигурации	Полное имя файла конфигурации ресурсов собственной сети, разрешенных для доступа из сторонней сети

Для удаления внешней сети:

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

Управление межсетевыми ключами

Межсетевой ключ используется для генерации ключей парной связи КШ. Для создания межсетевого ключа необходимо заранее издать сертификат собственной сети и импортировать сертификат сторонней сети, с которой устанавливается связь.

Для вызова списка межсетевых ключей:




- В левой части окна программы управления выберите папку "Внешние криптографические сети > <Наименование нужной сети> > Межсетевые ключи".

В правой части окна отобразится список межсетевых ключей для данной внешней сети.


Табл.22 Перечень полей списка межсетевых ключей

Поле	Описание
Пиктограмма ключа	Пиктографическое обозначение состояния межсетевого ключа (см. Табл.23)
Действителен с	Дата и время начала срока действия межсетевого ключа
Действителен по	Дата и время окончания срока действия межсетевого ключа. Дополнительные отметки: ! — до окончания срока действия осталось меньше месяца; !! — до окончания срока действия осталось меньше недели
Сертификат своей сети	Наименование сертификата домашней сети, использованного для создания данного межсетевого ключа
Сертификат внешней сети	Наименование сертификата внешней сети, использованного для создания данного межсетевого ключа
Хэш ключа	Результат хэширования ключа
Ресурс ключа	Оставшееся время жизни ключа в процентах в зависимости от интенсивности использования его производных – ключей парной связи

Табл.23 Пиктографические обозначения состояния межсетевого ключа



Пиктограмма	Описание
	Активный межсетевой ключ. Этот ключ используется для генерации ключей парной связи КШ. Только один ключ из списка может быть активен
	Неактивный действительный межсетевой ключ
	Недействительный межсетевой ключ

Для создания межсетевого ключа:


1. Вызовите контекстное меню в любом месте списка межсетевых ключей и активируйте команду "Создать межсетевой ключ" или нажмите одноименную кнопку на панели инструментов ().
На экране появится диалог "Межсетевой ключ".
2. Заполните поля диалога и нажмите кнопку "ОК".

Сертификат своей сети	Наименование сертификата собственной сети, использованного для создания данного межсетевого ключа
Сертификат внешней сети	Наименование сертификата внешней сети, использованного для создания данного межсетевого ключа

Для активирования межсетевого ключа:

- Вызовите контекстное меню нужной записи и выберите команду "Активировать" или нажмите кнопку на панели инструментов ().
Пиктограмма выбранного ключа примет вид .

Для удаления межсетевого ключа:

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

Внимание! Для поддержания корректной работы комплекса со сторонней криптографической сетью не рекомендуется удалять активный межсетевой ключ. Если по каким-либо причинам произошло его ошибочное удаление, необходимо повторно выполнить все действия в соответствии с общим порядком организации связи (см. стр.154), используя новые сертификаты.

Агент Роскомнадзора

Агент предназначен для автоматической загрузки в БД ЦУС сведений о запрещенных ресурсах единого реестра Роскомнадзора. Для получения агентом сведений о запрещенных ресурсах используется веб-сервис портала Роскомнадзора.

Примечание. Сведения о запрещенных ресурсах могут быть загружены в ручном режиме без использования агента (см. стр. 134).

Установка агента

Агент Роскомнадзора устанавливаются как компонент, входящий в состав подсистемы управления.

Компьютер, на который устанавливают агент, должен удовлетворять следующим требованиям:

- На компьютере установлены компоненты операционной системы, обеспечивающие доступ к portalу Роскомнадзора по сетевым протоколам TCP/IP.
- Поддерживается связь агента с ЦУС по зашифрованному каналу для передачи сведений о запрещенных ресурсах в БД ЦУС.
- На компьютере установлено программное обеспечение криптопровайдера КриптоПро CSP.
- В хранилище локального компьютера установлены сертификат пользователя (устанавливается в раздел "Личное"), корневой сертификат и сертификат Роскомнадзора (устанавливаются в раздел "Доверенные корневые центры сертификации").



Примечание. При создании запроса на получение сертификата средствами КриптоПро CSP формируется закрытый ключ. Для хранения ключевой информации используется внешний носитель.

Для установки агента:

1. Выполните процедуру установки (см. стр. 34).
Вид установки – "Выборочная". Устанавливаемый компонент – "Агент Роскомнадзор".
2. После завершения процедуры установки перезагрузите компьютер.
На экране появится сообщение с инструкцией по накоплению энтропии для биологического датчика случайных чисел.
3. Нажмите кнопку "ОК" в окне сообщения и, следуя инструкции, нажимайте на мишень, перемещающуюся по экрану, до завершения процесса накопления энтропии.
Внимание! Непопадание в мишень может привести к понижению уровня накопленной энтропии и необходимости повторного выполнения данной операции.
После завершения операции накопления энтропии на экране появится окно настройки параметров агента.
4. Укажите значения параметров или откажитесь от настройки нажатием кнопки "Отмена".
Настройку параметров можно выполнить позже (см. стр. 161).
5. После настройки параметров нажмите кнопку "ОК".
Окно настройки параметров агента закроется.

После завершения процедуры установки на компьютере будут установлены агент и программа управления агентом, а на панели задач Windows появится пиктограмма программы управления.

Цвет пиктограммы программы управления указывает на состояние агента:

	Зеленый	Агент запущен
	Красный	Агент остановлен

Внимание! После установки, а также после настройки параметров агент находится в состоянии "остановлен".

Программа управления агентом Роскомнадзора

Программа используется для настройки и локального управления агентом Роскомнадзора.

После завершения процедуры установки агента программа изначально находится во включенном состоянии. При этом агент находится в состоянии "остановлен".

Во включенном состоянии программы управления доступны команды контекстного меню пиктограммы в панели задач.

При выходе из программы управления пиктограмма из панели задач удаляется и вызов контекстного меню становится невозможным. При этом агент, если он был запущен, продолжает свою работу в соответствии с заданными настройками.

Команды управления агентом Роскомнадзора

Ниже в таблице приведены все команды программы управления агентом Роскомнадзора.

Название команды	Описание
Запустить агент	Осуществляет запуск агента
Остановить агент	Осуществляет остановку агента
Параметры агента...	Открывает окно настройки параметров агента
Удалить сохраненный пароль к ЦУС	Удаляет сохраненный пароль доступа к ключам ЦУС. При выполнении команды "Запустить агент" потребуются ввести пароль
Отключить уведомления об ошибках	Отключает/включает вывод всплывающих сообщений об ошибках в работе агента
Журнал приложений системы	Вызывает на экран журнал событий 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 параметров агента

Для настройки параметров агента:

1. Вызовите контекстное меню пиктограммы программы управления агентом и выберите команду "Параметры агента".
На экране появится окно настройки параметров.
2. Укажите требуемые значения параметров.

Параметр	Описание
Общие настройки	

Параметр	Описание
URL службы загрузки	Адрес страницы на портале Роскомнадзора для получения загрузки. Значение вводится автоматически
Сертификат	Сертификат, предъявляемый агентом при обращении в Роскомнадзор. Хранится в хранилище локального компьютера
Путь хранения последнего отчета	Папка локального компьютера, в которую агент сохраняет загрузку Роскомнадзора для последующей передачи в ЦУС
Подключения к ЦУС	
Адрес	IP-адрес для подключения агента к ЦУС
Тип ключевого носителя	Тип съемного носителя, на котором хранятся ключи связи с ЦУС. Возможные значения: дисковод и USB-флеш-накопитель
Прокси HTTP	
Адрес	Адрес прокси-сервера для подключения агента к portalу Роскомнадзора
Порт	Используемый порт при подключении к portalу Роскомнадзора через прокси-сервер
Оператор связи	
Наименование	Полное наименование оператора связи
ИНН	ИНН оператора связи (10 цифр для юридических лиц)
ОГРН	ОГРН оператора связи (13 цифр для юридических лиц)
E-mail	Электронный адрес технического специалиста, ответственного за использование механизма получения загрузки; может использоваться для оперативной обратной связи в случае возникновения технических вопросов или проблем (необязательное поле)

3. Нажмите кнопку "ОК".

Окно настройки параметров закроется.

Примечание. После изменения параметров, если агент был запущен, он переходит в состояние "остановлен". Для продолжения работы агент необходимо запустить (см. далее).

Запуск агента

Перед запуском агента подготовьте носитель с дубликатом административного ключа (создание дубликата административного ключа см. стр. 52).

Для запуска агента:

1. Вставьте носитель с дубликатом административного ключа.
2. Вызовите контекстное меню пиктограммы программы управления агентом и выберите команду "Запустить".

На экране появится запрос на ввод административного пароля.

Примечание. Запрос не появится, если при предыдущем запуске агента в запросе на ввод пароля была установлена отметка в поле "Сохранить пароль".

3. Введите пароль администратора.

Если необходимо сохранить пароль, установите отметку в поле "Сохранить пароль".

4. Нажмите кнопку "ОК".

Агент будет запущен и пиктограмма программы управления агентом изменит цвет с красного на зеленый.

Сообщения об ошибках

Ошибки подключения агента к веб-сервису портала Роскомнадзора регистрируются в журнале событий Windows в разделе Windows Logs/Application.

Для просмотра событий:

1. Вызовите контекстное меню программы управления агентом и выберите команду "Журнал приложений системы".

Откроется журнал.

2. Перейдите в раздел Windows Logs/Application.

Ниже приведено описание событий, связанных с ошибками подключения агента к веб-сервису портала Роскомнадзора.

Событие	Описание
Event ID: 4. Network connection fail to RKN-service. Error: HTTP error: 408 HTTP/1.1 408 Request Time-out, <html>Your request timed out. Please retry the request	Данная ошибка вызвана невозможностью подключения к сервису Роскомнадзора. Это может быть связано как с нарушением сетевого соединения на стороне пользователя, так и недоступностью сервиса со стороны Роскомнадзора. В зависимости от установленного в параметрах агента периода опроса службы выгрузки попытка подключения будет выполнена позже
Event ID: 7. Verify sign fail. Error: Невозможно построить цепочку доверенных сертификатов	Причиной ошибки является недействительный сертификат. Недействительным может быть как один из сертификатов, загружаемых пользователем, так и сертификат, присылаемый со стороны Роскомнадзора при подключении
Event ID: 9. Service wait result, a112a3375b80b156726829cd69ef95002	Событие, описывающее подключение к сервису. С шестнадцатеричным номером, указанным в описании события, можно обратиться в Роскомнадзор и получить список, если он не был загружен по каким-либо причинам из сервиса

Мониторинг и оперативное управление

Контроль работы комплекса (мониторинг) и оперативное вмешательство по результатам контроля является основной деятельностью администратора при эксплуатации комплекса. Действия администратора при этом следующие:

1. Получение оповещения о событии.
2. Ознакомление с ситуацией по журналу регистрации (при необходимости).
3. Изменение настроек объектов или их связей (при необходимости).

Мониторинг состояния комплекса

Общая таблица состояния компонентов комплекса

Общая таблица состояния отображается при выборе в окне объектов папки:

- Криптокоммутаторы;
- Детекторы атак;
- Криптошлюзы.

Таблица содержит сведения о состоянии всех устройств данной папки (см. [Табл.24](#)). Часть сведений о выбранном в таблице устройстве отображается на вкладках дополнительного окна (см. [Табл.25](#)). Разделы вкладки "Состояние" отображаются при нажатии соответствующей кнопки в верхней части дополнительного окна (см. [Табл.26](#)).

Табл.24 Параметры устройства

Параметр	Описание
Пиктограмма	Индикатор состояния устройства (см. Табл.27 на стр. 166)
Название	Имя, под которым устройство зарегистрировано в базе данных ЦУС
Описание	Дополнительные сведения об устройстве
Состояние	Состояние устройства (включено, отключено)
НСД	Наличие НСД на данном устройстве
Связь с КШ из других сетей	Наличие защищенного соединения между криптографическими шлюзами из разных сетей (сетей, управляемых различными ЦУС)
Кластер	Индикатор режима аппаратного резервирования. При наличии сбоя отображается "!" и состояние кластера
Multi-WAN	Включенный режим Multi-WAN (Failover, Balance). При наличии сбоя отображается "!"
Каналы VPN	Индикатор состояния каналов VPN. При наличии сбоя отображается "!"
СД	Наличие сервера доступа в конфигурации КШ
Время смены ключей	Дата и время последней смены ключа связи с ЦУС и главного ключа устройства
Идентификатор	Индивидуальный идентификационный номер устройства
NAT	Индикатор совместной работы КШ с сетевыми устройствами, поддерживающими трансляцию сетевых адресов (NAT): <ul style="list-style-type: none"> • синий значок — динамический NAT; • зеленый значок — статический NAT
Версия ПО	Номер версии программного обеспечения, установленного на устройстве
DHCP	Включен сервис DHCP

Табл.25 Вкладки дополнительного окна

Вкладка	Описание
Правила фильтрации	Перечень правил фильтрации IP-пакетов, установленных для данного КШ администратором
Правила трансляции	Перечень правил трансляции сетевых адресов, установленных для данного КШ
Очередь заданий	Содержит информацию о заданиях, выполняемых устройством
Авторизованные пользователи	Перечень авторизованных пользователей, подключенных к данному устройству
Внешние сети	Список внешних криптографических сетей, в которых задействовано устройство
Состояние сетевого устройства	Перечень параметров, характеризующих состояние сетевого устройства . Отображение секций осуществляется с помощью кнопок (см. Табл.26)
DHCP (только для КШ)	Настройки DHCP данного КШ
Привязка правил к детектору атак	Список правил, привязанных к данному ДА
Виртуальные коммутаторы	Список виртуальных коммутаторов, в которые входит данный КК

Табл.26 Кнопки вкладки "Состояние сетевого устройства"

Кнопка	Описание
Общие сведения	Отображает перечень основных параметров, характеризующих состояние сетевого устройства
Состояние кластера	Отображает перечень параметров, характеризующих состояние кластера КШ/криптокоммутаторов
Каналы WAN	Отображает адрес контрольной точки и состояние канала. Доступна при включенном режиме Multi-WAN
Каналы VPN	Отображает количество неработоспособных каналов VPN и время выхода канала из строя*. Доступна при наличии списка связанных устройств
Статистика по интерфейсам	Отображает характеристики трафика, детализированные по интерфейсам
Статистика по классам трафика	Дополнительно детализирует характеристики трафика по классам трафика. Доступна при нажатой кнопке "Статистика по интерфейсам"

* Время выхода канала из строя отсчитывается от одного из следующих событий:

- прохождение последнего пакета по парной связи в сторону докладывающего сетевого устройства;
- создание парной связи, если пакеты не проходили;
- включение сетевого устройства, если связь создана ранее и пакеты не проходили.

Отчеты о состоянии проблемных компонентов

Отчеты о состоянии проблемных сетевых устройств находятся в папке "Отчеты". Отчеты содержат перечень сетевых устройств , отфильтрованных по определенному параметру:

Сетевые устройства с НСД	Перечень сетевых устройств, на которых зафиксированы события несанкционированного доступа (НСД)
Проблемные кластеры	Перечень кластеров КШ и криптокоммутаторов, на которых зафиксированы сбои
Неактивные сетевые устройства	Перечень отключенных сетевых устройств
Сетевые устройства с заданиями	Перечень сетевых устройств, сформированные задания на которых еще не выполнены
Не введенные в эксплуатацию сетевые устройства	Перечень сетевых устройств, имеющих статус "Не введен в эксплуатацию"
Просроченные ключи сетевых устройств	Перечень сетевых устройств, имеющих просроченные ключи
Обновляемые сетевые устройства	Перечень сетевых устройств, находящихся в процессе загрузки и обновления ПО

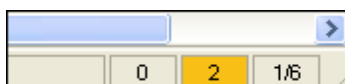
Все отчеты имеют те же поля, что и общая таблица состояния сетевого устройства (см. Табл.24 на стр.164).

Средства оповещения о событиях

Индикаторы состояния сетевых устройств

Индикаторы состояния сетевых устройств отображаются в правой части строки состояния программы управления.

Примечание. Условия отображения строки состояния см. стр.43.



Имеются следующие индикаторы (слева направо):

Индикатор наличия НСД	Отображает количество сетевых устройств, на которых зафиксировано событие НСД. Двойное нажатие левой кнопки мыши открывает отчет "Сетевые устройства с НСД"
Индикатор наличия проблемных кластеров	Отображает количество кластеров, в которых одно из сетевых устройств неработоспособно, или отключенные кластеры, в которых оба сетевых устройства неработоспособны. Двойное нажатие левой кнопки мыши открывает отчет "Проблемные кластеры"
Указатель количества активных сетевых устройств	Отображает количество активных и общее число зарегистрированных сетевых устройств. Двойное нажатие левой кнопки мыши открывает отчет "Неактивные сетевые устройства"

Индикатор состояния сетевого устройства

Для отображения текущего состояния сетевых устройств в программе управления используются пиктографические изображения, представленные в таблице ниже.

Табл.27 Индикатор состояния сетевого устройства

Пиктограмма	Описание
	Сетевое устройство выключено (пиктограмма серого цвета)
	Сетевое устройство включено (цветная пиктограмма)
	Сбой в работе сетевого устройства/кластера

Пиктограмма	Описание
	Состояние сетевого устройства неизвестно (отсутствует информация о состоянии)
	Данное сетевое устройство включено и для него в ЦУС готова обновленная конфигурация, которая будет применена при очередном обращении устройства к ЦУС
	Детектор атак включен
	Детектор атак выключен
	Криптокоммутатор включен

Чтобы сбросить отображение признака НСД, откройте контекстное меню данного сетевого устройства и активируйте в нем команду "Сбросить признак НСД".

Признак "Состояние сетевого устройства неизвестно" устраняется автоматически после обновления информации о состоянии сетевого устройства.

Индикатор наличия НСД

Индикатор наличия НСД (✖) отображается в поле "НСД" общей таблицы состояния сетевого устройства.

Настройка реакции на события

Агент ЦУС и СД может отслеживать определенные события и реагировать на них указанным образом. Предусмотрены следующие реакции на события:

- уведомление по электронной почте;
- запуск внешней программы;
- звуковое оповещение.

Настройка реакции на события состоит из следующих этапов:

- настройка реакции на события (см. ниже);
- назначение определенной реакции правилу фильтрации IP-пакетов или правилу трансляции сетевых адресов (см. стр. [112](#) и стр. [130](#)).

Вызов списка реакций на события

Для вызова списка реакций на события:

- В левой части окна программы управления выберите папку "Центр управления сетью> Реакции на события".

В правой части окна отобразится перечень реакций. Для формирования списка используйте кнопки панели инструментов (см. таблицу ниже).

Табл.28 Инструменты списка реакций на события

Инструмент	Команда	Описание
	Создать реакцию на событие...	Вызывает диалог "Реакция на события" для регистрации нового объекта
	Удалить реакцию на событие	Удаляет из списка выбранный объект. Объект, используемый в правиле фильтрации или правиле трансляции, удалить невозможно
	Свойства реакции на событие	Вызывает диалог "Реакция на события" для редактирования выбранного объекта
	Обновить содержимое	Обновляет содержимое окна

Настройка уведомления по электронной почте

Для рассылки уведомлений по электронной почте в настройках агента ЦУС и СД должен быть указан почтовый сервер, через который будут рассылаться уведомления. Описание настройки агента средствами локального управления см. [3].

Для настройки уведомления по электронной почте:

1. Вызовите диалог "Реакция на события" (см. Табл.28).
2. Установите отметку в поле "Уведомлять по электронной почте".
3. Заполните поля данного диалога и нажмите кнопку "ОК":

Название	Наименование объекта, уникальное для списка реакций на события
Описание	Произвольный текстовый комментарий
Список адресатов	Список адресов электронной почты получателей уведомлений (через ";")
Адрес отправителя	Произвольный адрес электронной почты для отображения в поле "Отправитель" сообщения с уведомлением
Тема	Тема сообщения с уведомлением
Содержимое письма	Текст уведомления. Для вставки в текст изменяемых характеристик событий используйте кнопку "Добавить шаблонный параметр..."

Настройка запуска внешней программы

Для настройки запуска внешней программы:

1. Вызовите диалог "Реакция на события" (см. Табл.28).
2. Установите отметку в поле "Запуск внешней программы".
3. Заполните поля данного диалога и нажмите кнопку "ОК":

Название	Наименование объекта, уникальное для списка реакций на события
Описание	Произвольный текстовый комментарий
Исполняемый файл	Полное имя исполняемого файла. Для выбора файла в стандартном диалоге Windows используйте кнопку "..."
Параметры	Перечень параметров запуска программы. Для вставки изменяемых характеристик событий используйте кнопку "Добавить шаблонный параметр..."

Настройка звукового оповещения

Звуковое оповещение осуществляется на компьютере, на котором установлен агент ЦУС и СД.

Для настройки звукового оповещения:

1. Вызовите диалог "Реакция на события" (см. Табл.28).
2. Установите отметку в поле "Воспроизведение звука".
3. Заполните поля данного диалога и нажмите кнопку "ОК":

Название	Наименование объекта, уникальное для списка реакций на события
Описание	Произвольный текстовый комментарий
Имя wav-файла	Имя звукового файла в формате WAV. Для выбора файла в стандартном диалоге Windows используйте кнопку "..."

Оперативное управление комплексом

Оперативное управление комплексом осуществляют из контекстных меню общей таблицы состояния сетевых устройств или отчетов о состоянии проблемных устройств. Списки команд контекстных меню представлены в таблицах ниже.

Табл.29 Команды контекстного меню ЦУС

Команда	Описание
Загрузить файл конфигурации...	Запускает процедуру загрузки файла конфигурации для восстановления конфигурации ЦУС из резервной копии (см. стр. 172).
Изменить внешний адрес ЦУС...	Вызывает на экран диалог "Изменение адреса ЦУС" (см. стр. 62)
Копирование ключей ЦУС и сервера доступа...	Запускает программу копирования ключей (при наличии программы)
Лицензии...	Запускает процедуру управления лицензиями (см. стр. 47)
Настройка агента ЦУС и СД...	Вызывает на экран диалог настройки агента. См. [3]
Настройка смены ключей сетевых устройств по расписанию...	Запускает процедуру настройки расписания для автоматической смены ключей сетевого устройства (см. стр. 140)
Параметры соединения с агентом ЦУС и СД...	Вызывает на экран диалог с параметрами соединения программы управления с агентом ЦУС и СД (см. стр. 46)
Параметры соединения с ЦУС...	Вызывает на экран диалог с параметрами соединения программы управления с ЦУС (см. стр. 46)
Разорвать соединение	Запускает процедуру разрыва защищенного соединения программы управления с ЦУС
Регулярные выражения правил фильтрации...	Вызывает на экран список используемых регулярных выражений (см. стр. 107)
Свойства...	Вызывает на экран диалог настройки свойств ЦУС
Сменить ключи всех сетевых устройств...	Запускает процедуру смены ключей всех сетевых устройств (см. стр. 140)
Создание ключевого носителя агента...	Запускает программу создания ключевого носителя для агента ЦУС и СД. См. [3]
Сохранить файл конфигурации...	Открывает стандартный диалог для сохранения файла резервной копии конфигурации ЦУС (см. стр. 172)
Управление ключами сетевых устройств...	Вызывает на экран мастер управления ключами (см. стр. 142)
Установить соединение	Запускает процедуру установки защищенного соединения программы управления с ЦУС

Табл.30 Команды контекстного меню сетевого устройства

Команда	Описание
Выключить сетевое устройство	Выключает сетевое устройство
Загрузить ключи сетевого устройства с носителя на ЦУС	Запускает процедуру смены ключей сетевого устройства с использованием резервного ключевого материала (см. стр. 139)
Обновить	Выполняет обновление отображаемой информации
Обновить конфигурацию	Запускает процедуру обновления конфигурации (см. стр. 56)
Очистить очередь заданий	Запускает процедуру удаления очереди заданий (см. стр. 85)
Очистить таблицу состояний соединений	Запускает процедуру очистки таблицы состояний соединений сетевого устройства (см. стр. 115)

Команда	Описание
Перезагрузить сетевое устройство	Запускает процедуру перезагрузки сетевого устройства (см. стр. 55)
Просмотр журналов	Вызывает программу просмотра журналов регистрации. См. [3]
Сбор журналов	Запускает процедуру сбора журналов регистрации. Если агент ЦУС и СД недоступен, то процедура сбора журналов запущена не будет. См. [3]
Сбросить признак НСД	Удаляет признак НСД для выбранного сетевого устройства
Свойства	Вызывает на экран диалог настройки свойств выбранного сетевого устройства
Сменить все ключи парных связей КШ/криптокоммутаторов	Запускает процедуру смены ключей парной связи КШ/криптокоммутаторов (см. стр. 139)
Сменить ключи сетевых устройств	Запускает процедуру смены ключей сетевых устройств (см. стр. 140)
Создать сетевое устройство	Запускает процедуру регистрации нового сетевого устройства (см. стр. 54)
Сохранить конфигурацию	Вызывает на экран диалог сохранения конфигурации сетевого устройства (см. стр. 39)
Сохранить текущие ключи на носитель	Запускает процедуру сохранения ключей на отчуждаемый носитель (см. стр. 39)
Удалить сетевое устройство	Удаляет из списка выбранное сетевое устройство (см. стр. 55)
Создать резервные ключи сетевого устройства	Создание резервных ключей для сетевого устройства
Управление ключами сетевых устройств	Вызов окна управления ключами по усиленной схеме (см. стр. 142)
Диагностика сетевого устройства	Вызывает окно формирования отчетов о работе устройства (см. стр. 212). Команда доступна только после вывода устройства из эксплуатации

Обеспечение отказоустойчивости комплекса

Резервное копирование и восстановление конфигурации ЦУС

Резервное копирование конфигурации ЦУС

В комплексе предусмотрена возможность резервного копирования конфигурации ЦУС. Резервная копия позволяет быстро восстановить работу сети при выходе из строя штатного ЦУС.

Существуют два способа создания резервной копии:

- автоматически агентом ЦУС и СД в соответствии с заданным расписанием;
- вручную администратором.

Автоматическое копирование

Агент сохраняет резервную копию конфигурации ЦУС в папку, которую можно указать средствами локального управления агента. См. [3]. По умолчанию это папка %PUBLIC% \Documents\Continent3\<имя_базы_данных>. Имя файла резервной копии Save_at_yy_mm_dd-hh_mm.dat. Всего в данной папке одновременно может храниться от 2 до 365 последних файлов резервных копий (в зависимости от настроек ЦУС; по умолчанию — 30).

Имеются два типа расписания работы агента:

- периодическое;
- еженедельное.

Периодическое расписание определяет интервал времени, через который агент выполняет свои функции. Еженедельное расписание определяет точное время действия агента по дням недели. Можно определить расписание работы агента любым из этих методов.

Для настройки расписания:

1. Вызовите окно настройки агента. Для этого в меню "ЦУС" активируйте команду "Настройки агента ЦУС и СД".
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 способом, 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.

Ручное копирование

Ручное копирование конфигурации ЦУС рекомендуется выполнять всякий раз после внесения очередного изменения в настройки комплекса. При ручном копировании резервную копию можно сохранить в любом каталоге под любым именем.

Примечание. Используйте для хранения резервной копии специально выделенный и защищенный жесткий диск.

Для создания резервной копии базы данных ЦУС вручную:

1. В окне объектов выберите папку "Центр управления сетью".
2. Вызовите меню "Операции" и активируйте команду "Сохранить файл конфигурации ЦУС".
На экране появится диалог задания пароля для зашифрования файла конфигурации ЦУС.
3. Введите и подтвердите пароль.
Внимание! При задании пароля должны выполняться требования, предъявляемые к паролям в соответствии с политикой аутентификации администраторов (см. стр. 51).
Нажмите кнопку "ОК".
На экране появится стандартный диалог сохранения файла.
4. Выберите нужную папку и укажите имя файла для создания резервной копии. Нажмите кнопку "Сохранить". Файл будет создан и зашифрован, а на экране появится сообщение об успешном завершении записи. Закройте окно этого сообщения.

Восстановление конфигурации ЦУС из резервной копии

В случае выхода из строя штатного ЦУС существует возможность быстрого восстановления работы сети с помощью резервной копии конфигурации. Описание процедуры создания резервной копии см. выше.

Сохраняйте резервную копию конфигурации ЦУС всякий раз после внесения очередного изменения в настройки комплекса.

Особенности замены вышедшего из строя ЦУС на новый. При установке ПО на новый КШ необходимо указать идентификатор вышедшего из строя КШ. При инициализации нового ЦУС сетевые настройки должны полностью совпадать с использовавшимися ранее. В противном случае корректная работа нового КШ с восстановленной базой данных ЦУС невозможна.

Для восстановления конфигурации ЦУС из резервной копии:

1. Выполните первичную инициализацию ЦУС средствами локального управления. См. [2].
В процессе проведения инициализации ЦУС на отчуждаемый носитель записывается административный ключ. Этот ключ необходим только для первого после инициализации ЦУС запуска программы управления.
2. Запустите программу управления (см. стр. 37). При этом запуске программы управления используйте носитель со вновь созданным административным ключом.
3. Откройте в окне объектов контекстное меню объекта "Центр управления сетью" и активируйте команду "Загрузить файл конфигурации ЦУС".
На экране появится стандартный диалог выбора файла.
4. Выберите нужную папку и укажите имя файла резервной копии. Нажмите кнопку "Открыть".
На экране появится диалог ввода пароля.

5. Введите пароль, заданный при создании резервной копии базы данных ЦУС (см. стр. 171), и нажмите кнопку "ОК".

Начнется процедура расшифрования и восстановления конфигурации ЦУС, при успешном завершении которой на экране появится соответствующее сообщение. Закройте окно этого сообщения.

Примечание. Если файл резервной копии испорчен, на экране появится сообщение об ошибке.

ЦУС приступит к загрузке сохраненной конфигурации и затем автоматически перезагрузится. После окончания перезагрузки на экране монитора ЦУС появится сообщение:

Успешный запуск <Дата> <Время>

При перезагрузке ЦУС соединение с программой управления будет разорвано.

6. Извлеките из считывателя ключевой носитель администратора, созданный при последней инициализации ЦУС. Данный ключевой носитель больше не понадобится.
7. Установите соединение программы управления с ЦУС. Для этого активируйте в меню "ЦУС" команду "Установить соединение".
На экране появится запрос идентификатора.

8. Предъявите старый ключевой носитель администратора, относящийся к загруженной конфигурации ЦУС.

Защищенное соединение программы управления с ЦУС будет установлено и в основном окне программы управления отобразится восстановленная конфигурация комплекса.

Примечание. 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.

9. Для всех устройств, на которых могли быть изменения, средствами программы управления выполните следующие действия:
 - обновите конфигурацию устройства (см. стр. 56);
 - перезагрузите устройство (см. стр. 55).

Управление кластером

Условия функционирования кластера

Кластер обеспечивает аппаратное резервирование КШ (криптокоммутатора) и автоматическое переключение канала связи с основного КШ (криптокоммутатора) на резервный при выходе основного из строя.

Примечание. Возможность аппаратного резервирования отсутствует у следующих криптографических шлюзов:

- ЦУС;
- КШ, подключенные к телефонным линиям с помощью модема.

Для корректной работы кластера необходимо соблюдать следующие условия:

- Оба устройства, образующих кластер, должны иметь одинаковые аппаратные платформы, а также одинаковое ПО одной и той же версии.
- Среда передачи пакетов, к которой подключены интерфейсы обоих устройств кластера, должна допускать наличие одинаковых MAC-адресов. Это требование относится как к внешним, так и к внутренним сетям комплекса.
- Интерфейсы резервирования обоих устройств кластера запрещено подключать к тем сетям, к которым подключены внешние и внутренние интерфейсы этих устройств. Для подключения интерфейсов резервирования необходимо использовать отдельную сеть.

Создание кластера

Имеются два варианта создания кластера:

- подключение резервного устройства к уже действующему;
- оба устройства кластера вводят в эксплуатацию впервые.

Создание кластера выполняют в следующей последовательности:

- Регистрация КШ (криптокоммутатора).
- Настройка интерфейсов резервирования.
- Включение режима резервирования.
- Запись конфигурации и ключей КШ (криптокоммутатора) на отчуждаемый носитель.
- Установка ПО и инициализация КШ (криптокоммутатора).
- Ввод кластера в эксплуатацию.

Программное обеспечение криптографического шлюза (криптокоммутатора) может поставляться на носителях следующих типов:

- CD-ROM;
- USB-флеш-накопитель.

Конфигурация и ключи КШ (криптокоммутатора) могут считываться с носителей типа USB-флеш-накопитель.

Необходимо заранее подготовить два носителя: один — для записи конфигурации основного устройства, другой — для записи конфигурации резервного устройства.

При использовании USB-флеш-накопителя и программное обеспечение, и конфигурацию можно записать на одном носителе.

Ключи КШ (криптокоммутатора) можно записать либо на те же носители, на которых записана конфигурация, либо на отдельный носитель.

Программное обеспечение криптографического шлюза (криптокоммутатора) может быть скопировано с CD-ROM на USB-флеш-накопитель с помощью программы Flash.exe (см. [2]).

Для корректной работы кластера необходимо в настройках ПАК "Соболь" указать следующие значения параметра "Автоматический вход в систему":

- для основного устройства — 5 сек.;
- для резервного устройства — 20 сек.

Шаг 1. Регистрация КШ (криптокоммутатора)

Регистрацию КШ (криптокоммутатора) выполняют только в том случае, если оба устройства кластера вводят в эксплуатацию впервые. Описание процедуры регистрации КШ (криптокоммутатора) см. стр. 54.

При подключении резервного КШ (криптокоммутатора) к действующему регистрацию КШ (криптокоммутатора) не выполняют. Достаточно вывести этот КШ (криптокоммутатор) из эксплуатации (см. стр. 54).

Шаг 2. Настройка интерфейсов резервирования

Настройку интерфейсов выполняют с помощью программы управления ЦУС. Имеется возможность использовать несколько интерфейсов резервирования.

Описание настройки интерфейсов см. стр. 60. При выборе типа интерфейса укажите значение "Резервирование КШ (криптокоммутатора)".

Шаг 3. Включение режима резервирования

Включение режима резервирования выполняют с помощью программы управления ЦУС.

Для включения режима резервирования:

1. Вызовите на экран окно настройки параметров КШ (криптокоммутатора). Для этого в окне объектов откройте контекстное меню того КШ (криптокоммутатора), к которому требуется подключить резервный КШ (криптокоммутатор), и активируйте команду "Свойства".
2. Перейдите к вкладке "Резервирование".
3. Нажмите кнопку "Включить". Поля диалога будут активированы.
4. Заполните поля данного диалога (см. стр. [176](#)) и нажмите кнопку "ОК".

Шаг 4. Запись конфигурации и ключей КШ (криптокоммутатора) на отчуждаемый носитель

Запись конфигурации КШ (криптокоммутатора) на носитель выполняют с помощью программы управления. Данную процедуру выполняют дважды: для основного устройства и для резервного. Каждую конфигурацию необходимо записывать на отдельный носитель.

При записи конфигурации для основного устройства в поле "Режим" выберите значение "Основной". При записи конфигурации для резервного устройства — "Резервный".

Запись ключей КШ (криптокоммутатора) на носитель выполняют также с помощью программы управления. Ключи и для основного, и для резервного устройства одинаковы. Ключи можно записать либо на те же носители, на которых записана конфигурация, либо на отдельный носитель.

Описание процедур см. стр. [39](#) и стр. [39](#).

Шаг 5. Установка ПО и инициализация КШ (криптокоммутатора)

Данную процедуру выполняют средствами локального управления дважды: сначала на основном устройстве, затем на резервном. Подробное описание процедур см. в [2].

При подключении резервного устройства к действующему установка ПО на действующем устройстве не требуется.

Внимание! Идентификационные номера основного и резервного устройства должны быть идентичны. Поэтому при установке программного обеспечения на резервный КШ (криптокоммутатор) необходимо указать идентификационный номер основного устройства кластера. Идентификационный номер указан в п. 2.2 документа "АПКШ "Континент". Криптографический шлюз. Паспорт" и на задней панели системного блока устройства.

При инициализации основного и резервного устройства используйте носители с соответствующей конфигурацией. После инициализации каждого устройства кластера дождитесь появления на консолях обоих устройств сообщения "Успешный старт".

Шаг 6. Ввод кластера в эксплуатацию

Ввод кластера в эксплуатацию выполняют с помощью программы управления ЦУС.

Для ввода кластера в эксплуатацию:

1. Введите КШ (криптокоммутатор) в эксплуатацию (см. стр. [54](#)).
2. Перезагрузите кластер (см. стр. [55](#)).

Дождитесь отображения рабочего состояния кластера в общей таблице состояния устройства:



КШ (криптокоммутатор) включен (цветная пиктограмма), см. [Табл. 27](#) на стр. [166](#)



Нормальная работа кластера (цвет синий)

После этого основной и резервный КШ (криптокоммутатор) начнут функционировать в режиме резервирования. При выходе из строя основного

криптографического шлюза (криптокоммутатора) канал связи будет автоматически переключен на резервный, а в окне объектов программы управления пиктограмма, отображающая вышедший из строя КШ (криптокоммутатор), изменит свой вид (🔴).

Настройка параметров резервирования

Для настройки резервирования:

1. Вызовите на экран окно настройки параметров КШ (криптокоммутатора). Для этого в окне объектов откройте контекстное меню КШ (криптокоммутатора) и активируйте команду "Свойства".
2. Перейдите к вкладке "Резервирование".

Примечание. При необходимости нажмите кнопку "Включить". Поля диалога будут активированы. При этом кнопка "Включить" будет переименована в кнопку "Выключить". Нажатие этой кнопки отключает режим резервирования данного устройства.

3. Заполните поля данного диалога и нажмите кнопку "ОК".

Интерфейсы	Перечень интерфейсов, у которых параметр "Тип" имеет значение "Резервирование" (процедуру настройки интерфейсов см. стр. 60).
Режим обратного переключения устройства	Порядок обратного переключения канала связи с резервного устройства на основной (возврат в состояние "как было"): <ul style="list-style-type: none"> • Автоматический — переключение осуществляется автоматически; • Ручной — переключение осуществляет администратор нажатием кнопки "Переключиться на парный"
Адреса	IP-адрес интерфейса резервирования и маска подсети, к которой он подключен, для основного и резервного устройства. Адреса этих интерфейсов должны быть уникальными для данной корпоративной сети и принадлежать одной подсети
Время ожидания ответа от активного сетевого устройства, сек.	Переключение канала связи (с резервного на основной и с основного на резервный) происходит при превышении времени, указанного в данном поле. Допустимые значения: 3-60 (секунд)

Добавление и удаление дополнительных интерфейсов резервирования

Внимание! При добавлении и удалении дополнительных интерфейсов резервное устройство должно быть включено.

Для добавления интерфейса резервирования:

1. Настройте интерфейс (см. стр. **60**). При выборе типа интерфейса укажите значение "Резервирование".
2. Нажмите кнопку "Применить" в окне "Свойства <устройства>".

Будет выполнено обновление конфигурации кластера.

Если резервное устройство выключено, для добавления интерфейса резервирования выполните **пп. 1-2** приведенной выше процедуры и после включения резервного устройства выполните следующее:

1. Запишите конфигурацию устройства на носитель (см. стр. **39**), указав в поле "Режим" значение "Резервный".
2. Выполните средствами локального управления инициализацию резервного устройства (см. [2]).

Для удаления интерфейса резервирования:

1. Откройте окно "Свойства <сетевого устройства>" (см. стр. **60**) и перейдите на вкладку "Интерфейсы".

2. Выберите удаляемый интерфейс резервирования и в поле "Тип" измените значение "Резервирование" на "Не определен".
3. Нажмите кнопку "Применить".
Будет выполнено обновление конфигурации кластера.

Изменение адреса на интерфейсах резервирования

При выполнении процедуры изменения адреса на интерфейсе резервирования кластер должен быть введен в эксплуатацию. При этом оба устройства (основное и резервное) должны функционировать в режиме резервирования.

Для изменения адреса на интерфейсе резервирования:

1. Выберите кластер в списке, вызовите контекстное меню и активируйте команду "Свойства".
На экране появится окно "Свойства <сетевого устройства>".
2. Перейдите к вкладке "Резервирование" и в группе полей "Адреса" внесите необходимые изменения.
3. Нажмите кнопку "Применить".
Будет выполнено обновление конфигурации кластера.
4. Выполните перезагрузку кластера (см. стр. 55).

Внимание! Если по каким-либо причинам при изменении адреса на интерфейсе резервирования резервное устройство кластера было выключено (или находилось в ремонте), после изменения адреса (см. процедуру выше) необходимо выполнить следующее:

1. Запишите конфигурацию устройства на носитель (см. стр. 39). При записи конфигурации в поле "Режим" выберите значение "Резервный".
2. Выполните средствами локального управления загрузку конфигурации на резервном устройстве (см. [2]).

Определение состояния кластера

Сведения о работоспособности кластера отображаются в общей таблице состояния устройства (см. стр. 164). Сведения о состоянии каждого устройства кластера представлены в главном окне на странице характеристик кластера.

Для просмотра сведений о состоянии устройства в кластере:

- Выберите в окне объектов название нужного кластера.
В главном окне отобразится страница с характеристиками кластера. Текущее состояние устройств, составляющих кластер, отображается в группе полей "Состояние кластера". Состояние устройства может принимать следующие значения:

Включен (Трафик)	Кластер функционирует в нормальном режиме. Данное устройство выполняет роль основного и обрабатывает трафик
Включен	Кластер функционирует в нормальном режиме. Данное устройство выполняет роль резервного и готово к обработке трафика
Активен	В кластере функционирует только данное устройство
Неактивен	Данное устройство в кластере не функционирует
Отключен	У обоих устройств питание отключено

Переключение канала связи в кластере

Существуют два режима переключения канала связи в кластере между основным и резервным устройством:

- автоматический;
- ручной.

Выбор режима осуществляется в диалоге "Резервирование". В автоматическом режиме переключение канала связи осуществляется системой самостоятельно. Описание алгоритма автоматического переключения см. стр. 23. При выборе ручного режима переключение канала связи выполняет администратор.

Совет. Если при включенном автоматическом режиме переключение канала связи с резервного устройства на основное не происходит, перезагрузите устройство (см. стр. 55).

Для переключения канала связи:

1. Вызовите на экран окно настройки параметров устройства. Для этого в окне объектов откройте контекстное меню нужного устройства и активируйте команду "Свойства".
2. Перейдите к вкладке "Резервирование".
3. Нажмите кнопку "Переключиться на парный".
4. Закройте окно настройки, нажав кнопку "ОК".

После этого основное устройство начнет функционировать в активном режиме, а в окне объектов программы управления пиктограмма данного устройства будет отображать состояние "включено".

Совет. Если переключение канала связи с резервного устройства на основное не происходит, перезагрузите устройство (см. стр. 55).

Выключение режима резервирования

Внимание! Выключение режима резервирования у работающего кластера запрещено.

Для выключения режима:

1. Выключите электропитание у резервного устройства.
2. Вызовите на экран окно настройки параметров устройства. Для этого в окне объектов откройте контекстное меню нужного устройства и активируйте команду "Свойства".
3. Перейдите к вкладке "Резервирование".
4. Нажмите кнопку "Выключить".
5. Закройте окно настройки, нажав кнопку "ОК".

После этого основное устройство будет автоматически перезагружено, а режим резервирования выключен.

Нештатные ситуации при работе кластера

В таблице представлены описание нештатных ситуаций при работе кластера резервирования, причины возникновения таких ситуаций и способы устранения их последствий.

Кластер*	Трафик	Сообщение в журнале НСД	Причина	Действие
✓ (нет резервного)	Есть	—	Отключено электропитание резервного устройства	Подключить электропитание
			Отсутствует соединение резервного устройства с основным через интерфейс резервирования	Восстановить работоспособность интерфейса резервирования

Кластер*	Трафик	Сообщение в журнале НСД	Причина	Действие
✓ (резервный)	Есть	Неправильный номер пакета**	Отключено электропитание основного устройства	Подключить электропитание
			У основного устройства нарушено подсоединение и внешнего интерфейса, и интерфейса резервирования	1. Восстановить подсоединение интерфейсов. 2. Разорвать и заново установить парную связь
✓	Нет	Неправильный номер пакета	У одного или обоих устройств было нарушено и затем восстановлено подсоединение внешнего интерфейса и интерфейса резервирования	Разорвать и заново установить парную связь

* Этот параметр отображается в общей таблице состояния устройства и отчетах о состоянии проблемных кластеров (см. стр. 164 и стр. 165).

** Сообщения в журнале НСД появляются после подсоединения интерфейсов.

Во всех случаях, когда разрешить нештатные ситуации не удалось, следует обращаться в службу технической поддержки поставщика комплекса.

Восстановление работы кластера после ремонта основного устройства

Если основное устройство кластера было отправлено в ремонт, после возвращения устройства из ремонта подключите его к сетевым коммуникациям, включите питание и дождитесь загрузки. При необходимости средствами локального управления выполните процедуру повторной инициализации устройства для загрузки последней сохраненной конфигурации (см. [2]).

Чтобы убедиться в возобновлении работы кластера, проверьте прохождение IP-пакетов в другие защищаемые сети. Для проверки можно использовать команду ping (см. [2]).

Если работоспособность кластера не восстановлена (IP-пакеты не проходят в другие защищаемые сети), проверьте наличие соединения резервного устройства с основным через интерфейс резервирования. При исправном соединении выполните действия в следующей последовательности:

1. Выключите резервное устройство (см. [2]).
2. Выполните процедуру обновления конфигурации основного устройства (см. стр. 56).
3. Выполните процедуру смены ключей для основного устройства (см. стр. 140).
4. Средствами локального управления выполните загрузку ключей для данного сетевого устройства. При загрузке используйте ключевой носитель с хранящимися на нем комплектами ключей для данного сетевого устройства. Загрузка ключей описана в [2]. В ходе процедуры загрузки укажите вариант "Загрузить активный ключ".
5. Средствами ПУ ЦУС выполните загрузку ключей в ЦУС (см. стр. 146).
6. Дождитесь выполнения заданий на основном устройстве. Для контроля очереди текущих заданий используйте папку "Очередь заданий" (см. стр. 85). После выполнения заданий проверьте прохождение IP-пакетов в защищенную сеть (например, с помощью команды ping). IP-пакеты должны проходить в защищенную сеть.
7. Включите резервное устройство (см. [2]).

Приложение

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.

Протокол/порт	Описание	Источник/получатель	Примечание
TCP/443	Обмен сообщениями между СД и АП. При включенном на АП режиме защищенного соединения "Потоковое подключение (ТСР)" 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 обновлений БРП / ЦУС	
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

Протокол/ порт	Описание	Источник/получатель	Примечание
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 ЦУС 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
TCP/5103	Передача файлов от ЦУС к СУ. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 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 ЦУС 5101. ЦУС отвечает с порта 5101 на порт 5100	СУ (исходящий порт 5100) / ЦУС	АПКШ "Континент" 3.0 и более поздние версии
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

Протокол/ порт	Описание	Источник/получатель	Примечание
UDP/5557	Передача сообщений об активности между СУ в кластере. Узлы кластера обмениваются пакетами с порта 5557 на порт 5557	Основное СУ / 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

Инициализация ПАК "Соболь" перед установкой ПУ ЦУС

Ниже приведена инструкция по настройке параметров безопасности при инициализации ПАК "Соболь" на АРМ администратора. Данную настройку выполняют до начала установки на АРМ администратора программы управления ЦУС.

1. При выключенном питании вскройте корпус устройства и в ПАК "Соболь" установите переключатель в положение, соответствующее режиму "Инициализация" (см. документацию на ПАК "Соболь").
2. Включите питание устройства.
На экране появится меню ПАК "Соболь".
3. Выберите в меню пункт "Инициализация платы" и нажмите клавишу <Enter>.
На экране появится диалог настройки общих параметров.
4. Проверьте и при необходимости установите значения параметров в соответствии с приведенной ниже таблицей с учетом версии ПАК "Соболь".

Параметр	Версия 3.0 (ПО версии 1.0.99)	Версия 3.0 (ПО версии 1.0.180)
Версия криптографической схемы	2.0	2.0
Число попыток тестирования ДСЧ	1	1

Параметр	Версия 3.0 (ПО версии 1.0.99)	Версия 3.0 (ПО версии 1.0.180)
Тестирование ДСЧ для пользователей	ДА	ДА
Показ статистики пользователям	НЕТ	НЕТ
Минимальная длина пароля пользователя	-	-*
Минимальная длина пароля	6	6
Предельное число неудачных входов пользователя	10	10
Время ожидания сторожевого таймера	Устанавливается значение, определенное автоматически на этапе инициализации комплекса, или может быть выбрано таким образом, чтобы оно превышало время появления приглашения на предъявление идентификатора не более чем на 10 секунд	
Период тестирования сторожевого таймера	1	1
Поддержка USB-идентификаторов	НЕТ	НЕТ
Контроль файлов и секторов	ДА	-
Контроль целостности журнала транзакций	ДА	-
Контроль целостности \ каталог с шаблонами КЦ	-	C:0
Контроль целостности \ контроль файлов и секторов	-	ДА
Контроль целостности \ контроль журнала транзакций	-	ДА
Контроль целостности \ контроль АСРІ	-	НЕТ
Контроль целостности \ контроль элементов реестра	-	ДА
Контроль целостности \ контроль PCI-устройств	-	НЕТ (функция недоступна)
Контроль целостности \ контроль SMBIOS	-	ДА
Контроль целостности \ контроль оперативной памяти	-	НЕТ

* Пункт отсутствует в данном меню или для данной версии ПАК "Соболь".

5. Осуществите создание учетной записи администратора (см. документацию на ПАК "Соболь").
6. Сохраните установленные значения параметров (см. документацию на ПАК "Соболь").
7. Дождитесь завершения инициализации платы и сообщения о готовности к перезагрузке или выключения устройства.
8. При выключенном питании вскройте корпус компьютера и в ПАК "Соболь" установите переключатель в положение, соответствующее режиму "Рабочий" (см. документацию на ПАК "Соболь").
9. При загрузке устройства предъявите персональный идентификатор.
На экране появится меню администратора ПАК "Соболь".
10. Проверьте и при необходимости установите значения параметров в соответствии с приведенной ниже таблицей с учетом версии ПАК "Соболь".

Параметр	Версия 3.0 (ПО версии 1.0.99)	Версия 3.0 (ПО версии 1.0.180)
Общие параметры системы		
Автономный режим работы	ДА	ДА
Контроль файлов и секторов	ДА	-
Число попыток тестирования ДСЧ	1	1
Тестирование ДСЧ для пользователей	ДА	ДА
Показ статистики пользователю	НЕТ	НЕТ
Минимальная длина пароля пользователя	-	-
Минимальная длина пароля	6	6
Использование случайных паролей	ДА	ДА
Максимальный срок действия пароля	42	42
Предельное число неудачных входов пользователя	10	10
Ограничение времени на вход в систему	5	5
Время ожидания автоматического входа в систему	НЕТ (функция недоступна)	НЕТ (функция недоступна)
Время ожидания сторожевого таймера	Устанавливается значение, определенное автоматически на этапе инициализации комплекса, или может быть выбрано таким образом, чтобы оно превышало время появления приглашения на предъявление идентификатора не более чем на 10 секунд	
Период тестирования сторожевого таймера	1	1
Поддержка USB-идентификаторов	НЕТ	НЕТ
Контроль файлов и секторов	ДА	-
Контроль целостности журнала транзакций	ДА	-
Контроль целостности		
Контроль SMBIOS	-	ДА
Контроль оперативной памяти	-	НЕТ (функция недоступна)
Контроль файлов и секторов -	-	ДА
Контроль журнала транзакций	-	ДА
Контроль ACPI	-	НЕТ
Контроль целостности элементов реестра	-	ДА
Контроль PCI-устройств	-	НЕТ (функция недоступна)
Список пользователей		
Режим контроля целостности	Жесткий (устанавливается для каждого зарегистрированного пользователя, за исключением привилегированных)	

Параметр	Версия 3.0 (ПО версии 1.0.99)	Версия 3.0 (ПО версии 1.0.180)
Замена аутентификатора при смене пароля	ДА	ДА
Запрет загрузки с внешних носителей	ДА (устанавливается для каждого зарегистрированного пользователя, за исключением привилегированных)	

11. Сохраните установленные значения параметров (см. документацию на ПАК "Соболь").

Права администраторов на управление комплексом

("+" — элемент управления доступен, "-" — элемент управления недоступен)

Элемент управления программы управления ЦУС	Роль администратора			
	Главный администратор	Администратор сети	Администратор ключей	Аудитор
Управление правилами фильтрации				
Просмотр правил фильтрации	+	+	-	+
Изменение правил фильтрации	+	+	-	-
Просмотр регулярных выражений правил фильтрации	+	+	+	+
Изменение регулярных выражений правил фильтрации	+	-	-	-
Управление настройками сетевого устройства				
Сбросить признак НСД	+	+	-	+
Обновить конфигурацию	+	+	-	-
Сохранение конфигурации...	+	+	-	-
Сохранить текущие ключи на носитель	+	-	+	-
Удалить сетевое устройство	+	+	-	-
Перезагрузить сетевое устройство	+	+	-	-
Загрузить ключи сетевого устройства с носителя на ЦУС	+	-	+	-
Сменить все ключи парной связи сетевого устройства	+	-	+	-
Очистить таблицу состояний соединений	+	+	+	+
Свойства сетевого устройства — Общие				
Название	+	+	-	-
Описание	+	+	+	+
Введен в эксплуатацию	+	+	-	-
Мягкий режим	+	+	-	-
Минимальный размер сжимаемого пакета	+	+	-	-
Период контроля целостности файлов	+	+	-	+
Часовой пояс	+	+	-	-

Элемент управления программы управления ЦУС	Роль администратора			
	Главный администратор	Администратор сети	Администратор ключей	Аудитор
Аутентификация пользователей	+	–	–	–
Свойства сетевого устройства — Журналы				
Максимальные размеры журналов	+	–	–	+
Регистрировать в журнале сетевого трафика пакеты	+	–	–	+
Свойства сетевого устройства — Интерфейсы	+	+	–	–
Свойства сетевого устройства — Маршрутизация	+	+	–	–
Свойства сетевого устройства — Резервирование	+	+	–	–
Настройки ЦУС				
Сохранить файл конфигурации	+	+	–	–
Загрузить файл конфигурации	+	+	–	–
Создать резервные ключи сетевого устройства	+	–	+	–
Свойства ЦУС — Журналы				
Максимальные размеры журналов	+	–	–	+
Настройки программы управления				
Параметры соединения с ЦУС	+	+	+	+
Параметры соединения с агентом	+	+	+	+
Режим входа	+	–	+	–
Настройка агента	+	–	–	+
Очередь заданий сетевого устройства				
Просмотр очереди заданий	+	+	–	–
Очистить очередь заданий	+	+	–	–
Управление администраторами				
Просмотр учетных записей	+	–	–	–
Изменение учетной записи	+	–	–	–

Модуль поддержки SNMP

Описание модуля

Модуль поддержки SNMP реализует обслуживание запросов "на чтение", а также отправку trap-сообщений при наступлении ряда событий.

В состав модуля входят два файла: snmp-сервер — исполняемый файл и файл конфигурации.

При запуске сервер считывает файл конфигурации. В случае его отсутствия сервер останавливает свою работу.

Модуль SNMP, реализованный в комплексе, протестирован с версией протокола SNMP 2.01.

Данные, предоставляемые модулем поддержки SNMP

Вся совокупность возможных выдаваемых модулем поддержки SNMP данных приведена ниже.

Общесистемные данные:

Идентификатор объекта	Объект
1.3.6.1.2.1.1.1.0	"sysDescr"
1.3.6.1.2.1.1.2.0	"sysObjectId"
1.3.6.1.2.1.1.3.0	"sysUpTime"
1.3.6.1.2.1.1.4.0	"sysContact"
1.3.6.1.2.1.1.5.0	"sysName"
1.3.6.1.2.1.1.6.0	"sysLocation"
1.3.6.1.2.1.1.7.0	"sysServices"
1.3.6.1.2.1.1.8.0	"sysORLastChange"

Информация о сетевых интерфейсах:

Идентификатор объекта	Объект
1.3.6.1.2.1.2.1.0	"ifNumber"
1.3.6.1.2.1.2.2.1.1.	"ifIndex"
1.3.6.1.2.1.2.2.1.2.	"ifDescr"
1.3.6.1.2.1.2.2.1.3.	"ifType"
1.3.6.1.2.1.2.2.1.4.	"ifMtu"
1.3.6.1.2.1.2.2.1.5.	"ifSpeed"
1.3.6.1.2.1.2.2.1.6.	"ifPhysAddress"
1.3.6.1.2.1.2.2.1.7.	"ifAdminStatus"
1.3.6.1.2.1.2.2.1.8.	"ifOperStatus"
1.3.6.1.2.1.2.2.1.9.	"ifLastChange"
1.3.6.1.2.1.2.2.1.10.	"ifInOctets"
1.3.6.1.2.1.2.2.1.11.	"ifInUcastPkts"
1.3.6.1.2.1.2.2.1.12.	"ifInNUcastPkts"
1.3.6.1.2.1.2.2.1.13.	"ifInDiscards"
1.3.6.1.2.1.2.2.1.14.	"ifInErrors"
1.3.6.1.2.1.2.2.1.15.	"ifInUnknownProtos"
1.3.6.1.2.1.2.2.1.16.	"ifOutOctets"
1.3.6.1.2.1.2.2.1.17.	"ifOutUcastPkts"
1.3.6.1.2.1.2.2.1.18.	"ifOutNUcastPkts"
1.3.6.1.2.1.2.2.1.19.	"ifOutDiscards"
1.3.6.1.2.1.2.2.1.20.	"ifOutErrors"
1.3.6.1.2.1.2.2.1.21.	"ifOutQLen"
1.3.6.1.2.1.2.2.1.22.	"ifSpecific"
1.3.6.1.2.1.31.1.1.1.1.	"ifName"
1.3.6.1.2.1.31.1.1.1.2.	"ifInMulticastPkts"
1.3.6.1.2.1.31.1.1.1.3.	"ifInBroadcastPkts"
1.3.6.1.2.1.31.1.1.1.4.	"ifOutMulticastPkts"

Идентификатор объекта	Объект
1.3.6.1.2.1.31.1.1.1.5.	"ifOutBroadcastPkts"
1.3.6.1.2.1.31.1.1.1.6.	"ifHCInOctets"
1.3.6.1.2.1.31.1.1.1.7.	"ifHCInUcastPkts",
1.3.6.1.2.1.31.1.1.1.8.	"ifHCInMulticastPkts"
1.3.6.1.2.1.31.1.1.1.9.	"ifHCInBroadcastPkts"
1.3.6.1.2.1.31.1.1.1.10.	"ifHCOctets"
1.3.6.1.2.1.31.1.1.1.11.	"ifHCOctetsUcastPkts"
1.3.6.1.2.1.31.1.1.1.12.	"ifHCOctetsMulticastPkts"
1.3.6.1.2.1.31.1.1.1.13.	"ifHCOctetsBroadcastPkts"
1.3.6.1.2.1.31.1.1.1.14.	"ifLinkUpDownTrapEnable"
1.3.6.1.2.1.31.1.1.1.15.	"ifHighSpeed"SNMP_NODE_COLUMN.
1.3.6.1.2.1.31.1.1.1.16.	"ifPromiscuousMode"
1.3.6.1.2.1.31.1.1.1.17.	"ifConnectorPresent"
1.3.6.1.2.1.31.1.1.1.18.	"ifAlias"SNMP_NODE_COLUMN.
1.3.6.1.2.1.31.1.1.1.19.	"ifCounterDiscontinuityTime"
1.3.6.1.2.1.4.1.	"ipForwarding"
1.3.6.1.2.1.4.20.1.1.	"ipAdEntAddr"
1.3.6.1.2.1.4.20.1.2.	"ipAdEntIfIndex"
1.3.6.1.2.1.4.20.1.3.	"ipAdEntNetMask"
1.3.6.1.2.1.4.20.1.4.	"ipAdEntBcastAddr"
1.3.6.1.2.1.4.20.1.5.	"ipAdEntReasmMaxSize"
1.3.6.1.4.1.34849.10.1.1	"wan channel failed"

Необходимая статистика:

Идентификатор объекта	Объект
1.3.6.1.4.1.9.9.109.1.1.1.5.0	"cpmCPUTotal5min"
1.3.6.1.4.1.9.9.171.1.2.1.25.0	"cikeGlobalHashValidFails"
1.3.6.1.4.1.9.9.171.1.3.1.9.0	"cipSecGlobalInPkts"
1.3.6.1.4.1.9.9.171.1.3.1.23.0	"cipSecGlobalOutDrops"

Файл /etc/snmp.conf

Обязательные параметры

Объявление имени community на чтение:

```
snmpdCommunityString.0.1="имя_community"
```

Значение этого параметра выступает в качестве "пароля" при обработке входящего запроса. Необъявление этого параметра, а также использование другого его значения при обращении к серверу приведет к "молчанию" сервера.

Адрес привязки сервера:

```
snmpdPortStatus.[адрес].порт=1/2
```

Указываются IP-адрес интерфейса и порт, к которому будет привязан сервер. В качестве значения используется разрешение/запрещение данной привязки. 1 — разрешить, 2 — запретить. Возможно объявление нескольких адресов или одного общего 0.0.0.0. Обычно используемый порт 161.

Необязательные параметры

Адрес отправки trap-сообщений:

```
TrapSinkComm.[адрес_trap_сервера].порт = "имя_trap_community"
```

Указываются IP-адрес и порт trap-сервера, на который snmp-сервер будет отсылать trap-сообщения. В качестве значения используется trap-community. Возможно объявление нескольких адресов. Обычно используемый порт 162.

Размер буфера передачи и приема:

```
snmpdTransmitBuffer="размер буфера передачи"
snmpdReceiveBuffer="размер приемного буфера"
```

По умолчанию определены равными 2048 байт. В случае необходимости через эти параметры данные размеры можно изменить.

В качестве символа комментария используется #. Комментируется вся строка.

Файл должен заканчиваться символом перевода каретки.

Пример файла /etc/snmp.conf

```
snmpdCommunityString.0.1 = "public"
# open standard SNMP ports
snmpdPortStatus.[10.4.0.98].161=1
snmpdPortStatus.[10.4.0.205].161=1
# send traps to the traphosts
trapSinkComm.[10.4.0.98].162 = "mytrap"
trapSinkComm.[10.4.0.205].162 = "mytrap"
sysContact      = "m.astapov@SecurityCode.ru"
sysLocation     = "room 201"
```

Особенности

Для того чтобы с комплексом можно было работать из пакета Cisco Works, в реализации модуля поддержки SNMP объекту sysObjectID установлено значение, соответствующее Cisco PIX Firewall. По этой причине комплекс опознается как Cisco PIX Firewall.

Индикация состояния модемного соединения выполнена следующим образом. Объект ifOperStatus для соответствующего интерфейса (типа tun) будет принимать следующие значения:

- up, если интерфейс подключен к линии;
- down, если интерфейс отключен от линии;
- testing, если интерфейс (модем) находится в процессе подключения к линии.

Формат и примеры конфигурационных файлов

Для создания конфигурационных файлов можно использовать любой текстовый редактор, например Блокнот.

В конфигурационных файлах должны быть определены:

- маршруты по умолчанию;
- статические маршруты, которые должны быть загружены в таблицу маршрутизации.

В конце конфигурационных файлов должна быть пустая строка.

Формат конфигурационного файла

В таблицах ниже представлены основные параметры конфигурационных файлов, используемые для настройки динамической маршрутизации.

Табл.31 Формат файла zebra.conf

Параметр	Описание
hostname <имя хоста>	Установка имени хоста
log stdout	Установка режима протоколирования на консоль
log file/var/zebra.log	Экспорт журналов событий динамической маршрутизации из КШ на USB-флеш-накопитель (локально)
ip route <адрес/маска> <шлюз>	Определение статического маршрута и маршрута по умолчанию

Табл.32 Формат файла ospfd.conf

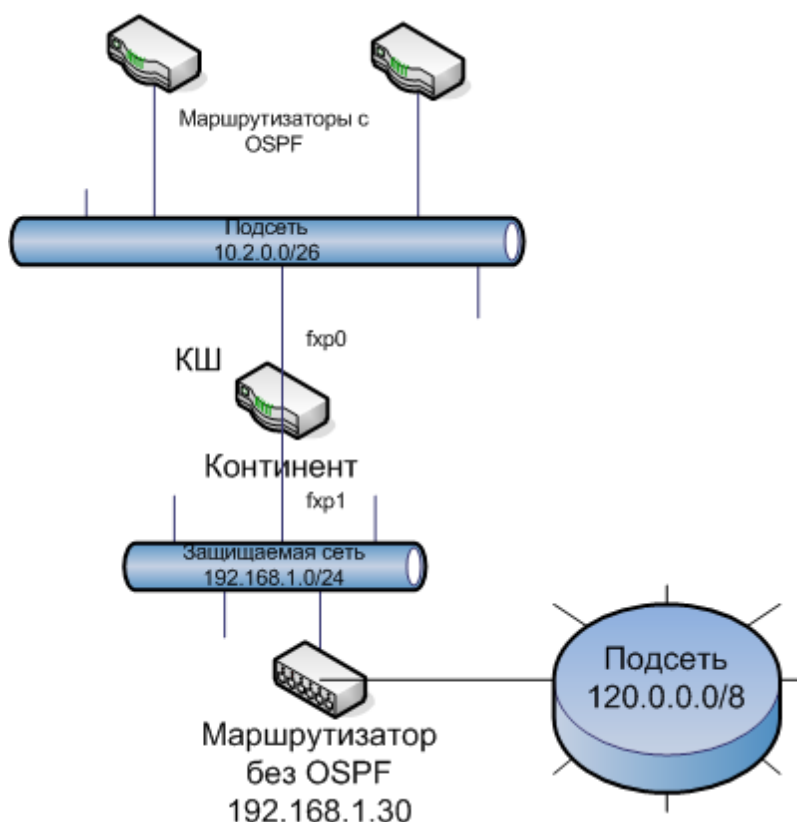
Параметр	Описание
router ospf	Включение OSPF-процесса
network <адрес/маска> area <номер>	Определение диапазона адресов интерфейсов, которые используются для обмена служебной информацией в процессе OSPF-маршрутизации
interface <имя>	Определение имени интерфейса, используемого для обмена служебной информацией в процессе OSPF-маршрутизации
ip ospf authentication message-digest	Установка режима аутентификации OSPF-маршрутизатора
ip ospf message- digest-key 1 <алгоритм> <ключ>	Установка аутентификационного ключа OSPF-маршрутизатора. Использовать указанный алгоритм и ключ (ключ может достигать длины 16 символов)

Примеры конфигурационных файлов

Данный пример иллюстрирует создание конфигурационных файлов для КШ в типовой схеме включения, показанной на рисунке ниже.

Защищаемая сеть 192.168.1.0/24 (например, территориальный филиал какой-либо организации) для связи с другим удаленным филиалом (на рисунке не показан) использует подсеть 10.2.0.0/26 с маршрутизаторами, поддерживающими OSPF.

В состав защищаемой сети входит подсеть 120.0.0.0/8. Для связи с подсетью используется маршрутизатор без OSPF (192.168.1.30).



Для того чтобы обеспечить динамическую маршрутизацию при прохождении трафика между подсетью 120.0.0.0/8 и другим удаленным филиалом, на КШ должна быть выполнена настройка динамической маршрутизации.

Для приведенной выше схемы конфигурационные файлы имеют следующий вид:

zebra.conf

```
hostname continent
log stdout
# статический маршрут в подсеть
ip route 120.0.0.0/8 192.168.1.30
```

ospfd.conf

```
log stdout
router ospf
network 10.2.0.0/26 area 0.0.0.1
area 0.0.0.1 authentication message-digest
# разрешается анонсирование статических маршрутов
redistribute static
interface fxp0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 1234567890
```

Примеры правил фильтрации

По умолчанию любой IP-пакет, поступивший на КШ, отбрасывается, если его прохождение не разрешено явно соответствующим правилом фильтрации.

Общий порядок настройки правил фильтрации:

1. Создайте необходимые элементы правил (см. стр. [98](#)):

- сетевые объекты;
- группы сетевых объектов;
- сервисы;

- временные интервалы.

Автоматически при инициализации ЦУС создаются следующие элементы правила фильтрации:

- сетевой объект "Любой", имеющий адрес "0.0.0.0" и определяющий сеть в диапазоне всех известных IP-адресов;
- набор наиболее часто используемых сервисов (pop-3, smtp, imap4, http, ftp, ftp-data и пр.);
- временной интервал "Постоянно", определяющий ежедневное круглосуточное действие правила.

2. Создайте правила фильтрации (см. стр.105).

Внимание! Если объект "Любой" участвует в правиле фильтрации, то разрешена связь с любыми внешними ресурсами и любыми ресурсами, находящимися за внутренними интерфейсами КШ, к которому привязан другой участник правила фильтрации.

Ввод КШ в эксплуатацию

При вводе криптографического шлюза в эксплуатацию список правил фильтрации пуст и прохождение любых IP-пакетов через данный КШ запрещено. Для определения используемых сетевых сервисов и необходимых для работы правил фильтрации создайте исходное правило с параметрами, представленными ниже. Это правило разрешает прохождение через данный КШ любых IP-пакетов. После дня опытной эксплуатации КШ проанализируйте журнал сетевого трафика и в соответствии с политикой безопасности, принятой в вашей организации, сформируйте список правил фильтрации для дальнейшей эксплуатации КШ.

Табл.33 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	Тест	Любой*
Описание	Тест	Любой
IP-адрес	0.0.0.0	0.0.0.0
Маска	0.0.0.0	0.0.0.0
Тип привязки	Внутренний	Нет
Криптошлюз	<Имя КШ>	—
Интерфейс	Любой	—

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

Табл.34 Параметры сервисов

Параметр	Значение		
	Сервис 1	Сервис 2	Сервис 3
Имя	Любой TCP*	Любой UDP*	Любой ICMP*
Протокол	tcp	udp	icmp
Порт источника	Любой	Любой	—
Порт назначения	Любой	Любой	—
ICMP-тип	—	—	Любой

* Сервисы "Любой TCP", "Любой UDP" и "Любой ICMP" создаются автоматически при инициализации ЦУС.

Табл.35 Параметры правила фильтрации

Параметр	Значение
Отправитель	Тест

Параметр	Значение
Инверсия адреса	—
Получатель	Любой
Инверсия адреса	—
Сервисы	Любой TCP, Любой UDP, Любой ICMP
Действие	Пропустить
Регистрировать	Заголовок пакета
Временной интервал	Постоянно
Контролировать состояние соединения	—
Отключено	—

Доступ рабочей станции из защищенной подсети КШ 1 к серверу из защищенной подсети КШ 2

Необходимо обеспечить доступ рабочей станции WS 1-1-1 (IP-адрес 10.1.1.1, КШ 1) к серверу Srv 2-1-1 (IP-адрес 10.2.1.1, КШ 2) (см. стр. 13). Инициатор соединения — только рабочая станция WS 1-1-1.

Примечание. Для прохождения трафика КШ 1 и КШ 2 должны быть связаны (см. стр. 78).

Табл.36 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	WS 1-1-1	Srv 2-1-1
Описание	Рабочая станция	Сервер
IP-адрес	10.1.1.1	10.2.1.1
Маска	255.255.255.255	255.255.255.255
Тип привязки	Защищаемый	Защищаемый
Криптошлюз	КШ 1	КШ 2
Интерфейс	Любой	Любой

Табл.37 Параметры правила фильтрации

Параметр	Значение
Отправитель	WS 1-1-1
Инверсия адреса	—
Получатель	Srv 2-1-1
Инверсия адреса	—
Сервисы	Любой TCP, Любой UDP, Любой ICMP
Действие	Пропустить
Регистрация	Нет
Временной интервал	Постоянно
Контролировать состояние соединения	Установить отметку
Отключено	—

Доступ рабочей станции из защищенной подсети КШ 1 к внешнему ресурсу

Необходимо обеспечить доступ рабочей станции WS 1-1-1 (IP-адрес 10.1.1.1 КШ 1) к внешнему ресурсу ExtRes (IP-адрес 198.23.75.1). Инициатор соединения — только рабочая станция.

Табл.38 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	WS 1-1-1	ExtRes
Описание	Рабочая станция	Внешний ресурс
IP-адрес	10.1.1.1	198.23.75.1
Маска	255.255.255.255	255.255.255.255
Тип привязки	Внутренний	Нет
Криптошлюз	КШ 1	—
Интерфейс	Любой	—

Табл.39 Параметры правила фильтрации

Параметр	Значение
Отправитель	WS 1-1-1
Инверсия адреса	—
Получатель	ExtRes
Инверсия адреса	—
Сервисы	Любой TCP, Любой UDP, Любой ICMP
Действие	Пропустить
Регистрировать	Нет
Временной интервал	Постоянно
Контролировать состояние соединения	Установить отметку
Отключено	—

Доступ к почтовому серверу из открытой сети

Необходимо обеспечить доступ к почтовому серверу Post, находящемуся в защищенной сети КШ1, от любого сетевого объекта "Любой" в открытой сети.

Предусмотрены два варианта использования правил фильтрации:

- с контролем состояния;
- без контроля состояния.

Второй вариант рекомендуется применять в тех случаях, когда использование правил фильтрации с контролем состояния затрудняет работу КШ ввиду большого количества открываемых соединений.

Использование правил с контролем состояния

В этом случае создается одно правило фильтрации со следующими параметрами:

Табл.40 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	10.1.1.25	0.0.0.0
Маска	255.255.255.255	0.0.0.0
Тип привязки	Внутренний	Нет
Криптошлюз	КШ 1	—
Интерфейс	fxp1*	—

* Имя внутреннего интерфейса КШ1, за которым находится почтовый сервер.

Табл.41 Параметры сервиса

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

Табл.42 Параметры правила фильтрации

Параметр	Значение
Отправитель	Любой
Инверсия адреса	—
Получатель	Post
Инверсия адреса	—
Сервисы	smtp
Действие	Пропустить
Регистрировать	Нет
Временной интервал	Постоянно
Контролировать состояние соединения	Установить отметку
Отключено	—

Использование правил без контроля состояния

В данном варианте требуется создание правил для прохождения tcp-трафика в обе стороны, а также создание правил для служебных icmp-сообщений, которые могут потребоваться для корректной отправки (получения) больших сообщений (Fragmentation Needed and Don't Fragment was Set).

Правила фильтрации для обмена сообщениями Fragmentation Needed and Don't Fragment was Set между любым интерфейсом КШ и сетевыми объектами "Любой" создаются автоматически.

Если требуется отправка сообщения Fragmentation Needed and Don't Fragment was Set между КШ и почтовым сервером в защищенной сети (почтовый сервер в защищенной сети не попадает под определение объекта "Любой" в силу нахождения не за внешним интерфейсом), следует создать дополнительные правила фильтрации (они описаны ниже в таблицах). Необходимость создания этих

правил определяется опытным путем в мягком режиме работы КШ при настройке сети. В таком случае дополнительно создаются "Сетевой объект 3", сервис "icmp need frag", правила фильтрации 3 и 4.

Также опытным путем можно обнаружить, что требуется добавление правил для других служебных сообщений icmp и других сетевых объектов — в зависимости от структуры сети в каждом конкретном случае. Настройка выполняется по результатам анализа журнала сетевого трафика.

Табл.43 Параметры сетевых объектов

Параметр	Значение		
	Сетевой объект 1	Сетевой объект 2	Сетевой объект 3
Название	Post	Любой	cgw
Описание	Почтовый сервер	Любой объект в открытой сети	Внутренний интерфейс КШ1
IP-адрес	10.1.1.25	0.0.0.0	10.1.1.1
Маска	255.255.255.255	0.0.0.0	255.255.255.255
Тип привязки	Внутренний	Нет	Внутренний
Криптошлюз	КШ 1	—	КШ1
Интерфейс	fxp1	--	fxp1

Табл.44 Параметры сервиса (стандартный)

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

Табл.45 Параметры сервиса (создается вручную)

Параметр	Значение
Название	smtp-back
Протокол	tcp
Порт источника	25
Порт назначения	Любой

Табл.46 Параметры сервиса (создается вручную)

Параметр	Значение
Название	icmp need frag
Протокол	icmp
Тип	dest unreachable (3)
Код	IP_DF caused drop (4)

Табл.47 Параметры правил фильтрации

Параметр	Значение			
	Правило 1	Правило 2	Правило 3	Правило 4
Отправитель	Любой	Post	Post	cgw
Инверсия адреса	—	—	—	—
Получатель	Post	Любой	cgw	Post
Инверсия адреса	—	—	—	—
Сервисы	smtp	smtp-back	icmp need frag	icmp need frag
Действие	Пропустить	Пропустить	Пропустить	Пропустить
Регистрировать	Нет	Нет	Нет	Нет
Временной интервал	Постоянно	Постоянно	Постоянно	Постоянно
Контролировать состояние соединения	—	—	—	—
Отключено	—	—	—	—

Информационный обмен между двумя рабочими станциями из подсетей, защищенных разными КШ

Необходимо обеспечить взаимный обмен информацией между рабочей станцией WS 1-1-1 (IP-адрес 10.1.1.1, КШ 1) и рабочей станцией WS 2-1-2 (IP-адрес 10.2.1.2, КШ 2) (см. стр.13). Инициатор соединения — любая рабочая станция.

Примечание. Для прохождения трафика КШ 1 и КШ 2 должны быть связаны (см. стр.78).

Табл.48 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	WS 1-1-1	WS 2-1-2
Описание	Рабочая станция	Рабочая станция
IP-адрес	10.1.1.1	10.2.1.2
Маска	255.255.255.255	255.255.255.255
Тип привязки	Защищаемый	Защищаемый
Криптошлюз	КШ 1	КШ 2
Интерфейс	Любой	Любой

Табл.49 Параметры правил фильтрации

Параметр	Значение	
	Правило 1	Правило 2
Отправитель	WS 1-1-1	WS 2-1-2
Инверсия адреса	—	—
Получатель	WS 2-1-2	WS 1-1-1
Инверсия адреса	—	—
Сервисы	Любой TCP, Любой UDP, Любой ICMP	Любой TCP, Любой UDP, Любой ICMP
Действие	Пропустить	Пропустить
Регистрировать	Нет	Нет

Параметр	Значение	
	Правило 1	Правило 2
Временной интервал	Постоянно	Постоянно
Контролировать состояние соединения	Установить отметку	Установить отметку
Отключено	—	—

Доступ из одной защищенной подсети к ресурсам другой

Необходимо обеспечить взаимный обмен информацией между рабочими станциями локальной сети LAN 1-1-0 (IP-адрес 10.1.1.0) и рабочими станциями LAN 1-2-0 (IP-адрес 10.1.2.0) (см. стр. 13). Обе локальные сети подключены к КШ 1: LAN 1-1-0 к интерфейсу Fxp2, LAN 1-2-0 к интерфейсу Fxp3. Инициатор соединения — любая рабочая станция любой локальной сети.

Табл.50 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	LAN 1-1-0	LAN 1-2-0
Описание	Локальная сеть	Локальная сеть
IP-адрес	10.1.1.0	10.1.2.0
Маска	255.255.255.0	255.255.255.0
Тип привязки	Защищаемый	Защищаемый
Криптошлюз	КШ 1	КШ 1
Интерфейс	Fxp2	Fxp3

Табл.51 Параметры правил фильтрации

Параметр	Значение	
	Правило 1	Правило 2
Отправитель	LAN 1-1-0	LAN 1-2-0
Инверсия адреса	—	—
Получатель	LAN 1-2-0	LAN 1-1-0
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	—	—

Защищенное управление маршрутизатором

Необходимо обеспечить прохождение управляющего трафика с рабочей станции WS 1-1-1 (IP-адрес 10.1.1.1, КШ 1) к маршрутизатору Router 2 (IP-адрес 198.200.23.1), зарегистрированному на КШ 2 как защищенная сеть (см. стр. 15). Управление маршрутизатором осуществляется по протоколу Telnet, для которого стандартным является порт 23.

Табл.52 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	WS 1-1-1	Router 2
Описание	Рабочая станция	Маршрутизатор
IP-адрес	10.1.1.1	198.200.23.1
Маска	255.255.255.255	255.255.255.255
Тип привязки	Защищаемый	Защищаемый
Криптошлюз	КШ 1	КШ 2
Интерфейс	Любой	Любой

Табл.53 Параметры сервиса

Параметр	Значение
Название	TELNET
Протокол	tcp
Порт источника	Любой
Порт назначения	23

Табл.54 Параметры правила фильтрации

Параметр	Значение
Отправитель	WS 1-1-1
Инверсия адреса	—
Получатель	Router 2
Инверсия адреса	—
Сервисы	TELNET
Действие	Пропустить
Регистрировать	Нет
Временной интервал	Постоянно
Контролировать состояние соединения	Установить отметку
Отключено	—

Доступ сторонних абонентов к FTP- серверу, находящемуся в защищенной подсети

Необходимо обеспечить доступ сторонних абонентов к FTP- серверу, расположенному на компьютере WS 3-1-2 (IP-адрес 10.3.1.2, КШ 3, см.стр.[13](#)). Режим работы FTP-сервера — пассивный, активный.

Необходимо, чтобы FTP- клиент имел маршрут к FTP-серверу через один из внешних интерфейсов КШ.

Табл.55 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	ftp_serv	Любой

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Описание	FTP-сервер	Любой объект в открытой сети за внешним интерфейсом КШЗ
IP-адрес	10.3.1.2	0.0.0.0
Маска	255.255.255.255	0.0.0.0
Тип привязки	Внутренний	Нет
Криптошлюз	КШ 3	—
Интерфейс	em1	—

Табл.56 Параметры правила фильтрации

Параметр	Значение
Отправитель	Любой
Инверсия адреса	—
Получатель	ftp_serv
Инверсия адреса	—
Сервисы	ftp
Действие	Пропустить
Регистрировать	Нет
Временной интервал	Постоянно
Контролировать состояние соединения	Установить отметку
Отключено	—

Доступ рабочих станций из защищенной подсети к FTP-серверу, расположенному в общей сети

Необходимо обеспечить доступ к FTP-серверу, расположенному в общей сети (IP-адрес 198.23.75.1), с рабочих станций, входящих в состав подсети 10.3.1.0, защищаемой КШ 3 (см. стр. 13). Режим работы FTP-сервера — пассивный, активный.

Необходимо, чтобы FTP-сервер имел маршрут в защищенную сеть через один из внешних интерфейсов КШ.

Табл.57 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	LAN 3-1-0	ftp_serv_ext
Описание	Локальная сеть	Внешний FTP-сервер
IP-адрес	10.3.1.0	198.23.75.1
Маска	255.255.255.0	255.255.255.255
Тип привязки	Защищаемый	Нет
Криптошлюз	КШ 3	—
Интерфейс	em1	—

Табл.58 Параметры правила фильтрации

Параметр	Значение
Отправитель	LAN 3-1-0
Инверсия адреса	—
Получатель	ftp_serv_ext
Инверсия адреса	—
Сервисы	ftp
Действие	Пропустить
Регистрировать	Нет
Временной интервал	Постоянно
Контролировать состояние соединения	Установить отметку
Отключено	—

Метасимволы в регулярных выражениях

В системе регулярные выражения используются для осуществления расширенного поиска. Регулярное выражение представляет собой поисковый шаблон в виде строки, состоящей из обычных символов и метасимволов. Например, для поиска имен пользователей Ivanov или Ivanof можно использовать следующее регулярное выражение: `Ivano(v|f)`, где `|` является метасимволом логического ИЛИ.

Ниже в таблице представлены метасимволы, наиболее применяемые в процессе расширенного поиска.

Метасимвол	Назначение	Пример
<code>.</code> (точка)	Любой символ	По шаблону <code>a.c</code> могут быть найдены последовательности символов <code>abc</code> , <code>apc</code> , <code>a4c</code> и т. п.
<code>+</code>	Совпадение 1 или более раз	По шаблону <code>a+</code> могут быть найдены последовательности <code>a</code> , <code>aa</code> , <code>aaa</code> , <code>aaaa</code> и т. д.
<code>?</code>	Совпадение 1 или 0 раз	По шаблону <code>ab?c</code> могут быть найдены две последовательности <code>abc</code> и <code>ac</code>
<code>*</code>	Совпадение 0 или более раз	По шаблону <code>ab*c</code> могут быть найдены последовательности <code>ac</code> , <code>abc</code> , <code>abbc</code> , <code>abbbc</code> , <code>abbbbc</code> и т. п.
<code>{n}</code>	Совпадение ровно <code>n</code> раз	По шаблону <code>a{5}</code> может быть найдена последовательность <code>aaaaa</code>
<code>{n,}</code>	Совпадение не менее <code>n</code> раз	По шаблону <code>a{3,}</code> могут быть найдены последовательности <code>aaa</code> , <code>aaaa</code> , <code>aaaaa</code> и т. д.
<code>{n,m}</code>	Совпадение от <code>n</code> до <code>m</code> раз	По шаблону <code>a{3,5}</code> могут быть найдены последовательности <code>aaa</code> , <code>aaaa</code> , <code>aaaaa</code>
<code>[...]</code>	Множество символов	По шаблону <code>[abc]</code> могут быть найдены последовательности, включающие любой из указанных в шаблоне символов: <code>at</code> , <code>bnm</code> , <code>cvbn</code> и др.
<code>[^...]</code>	Множество символов, кроме перечисленных в списке	По шаблону <code>[^abc]</code> могут быть найдены любые последовательности, за исключением <code>abc</code>
<code> </code>	Логическое ИЛИ	По шаблону <code>a b</code> будут найдены символы <code>a</code> или <code>b</code>
<code>^</code>	Начало строки	По шаблону <code>^Int</code> будет найдена строка, начинающаяся символами <code>Int</code> . Например: <code>Internet</code>

Метасимвол	Назначение	Пример
\$	Конец строки	По шаблону net\$ будет найдена строка, заканчивающаяся символами net. Например: Internet

Примеры правил трансляции

Общий порядок настройки правил трансляции:

1. Создайте элементы правил (см. стр. **98**), которые будут использоваться в правилах трансляции:

- сетевые объекты;
- сервисы;
- временные интервалы.

Примечание. Автоматически при инициализации ЦУС создаются следующие элементы правила фильтрации:

- сетевой объект "Любой", имеющий адрес "0.0.0.0" и определяющий сеть в диапазоне всех известных IP-адресов;
- набор наиболее часто используемых сервисов (pop-3, smtp, imap4, http, ftp, ftp-data и пр.);
- временной интервал "Постоянно", определяющий ежедневное круглосуточное действие правила.

2. Создайте правила трансляции (см. стр. **130**).

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 (см. стр. **13**). Публичный IP-адрес отправителя — 198.23.75.100. В этом случае на КШ 1 нужно создать исходящее правило трансляции.

Табл.59 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	em1	—

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

Табл.60 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, tcp-high-ports

Доступ сторонних абонентов к почтовому серверу, находящемуся в защищенной подсети

Необходимо обеспечить доступ сторонних абонентов к почтовому серверу, расположенному на компьютере WS 1-1-1 (IP-адрес 10.1.1.1, КШ 1, см. стр. 13). Сторонним абонентам известен публичный IP-адрес сервера — 198.23.75.100. В этом случае на КШ 1 нужно создать входящее правило трансляции для IP-пакетов, поступающих получателю WS 1-1-1.

Табл.61 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	WS 1-1-1	Любой
Описание	Почтовый сервер	Любой
IP-адрес	10.1.1.1	0.0.0.0
Маска	255.255.255.255	0.0.0.0
Тип привязки	Внутренний	Нет
Криптошлюз	КШ 1	–
Интерфейс	em1	–

Табл.62 Параметры входящего правила трансляции для КШ 1

Параметр	Значение
Направление	Входящие
Получатель	WS 1-1-1
Источник	Любой
IP-адрес	198.23.75.100
Интерфейс	em0
Сервисы	pop-3, smtp, imap4

Доступ сторонних абонентов к веб-серверу, находящемуся в защищенной подсети (с изменением порта)

Необходимо обеспечить доступ сторонних абонентов к веб-серверу, расположенному на компьютере Srv 1-2-2 (IP-адрес 10.1.2.2, КШ 1, см. стр. 13). Сторонним абонентам известен публичный IP-адрес сервера — 198.23.75.200. В этом случае на КШ 1 нужно создать два правила:

- входящее правило трансляции для IP-пакетов, поступающих на адрес 198.23.75.200; правило переопределяет порт назначения с 80 на 8080;
- исходящее правило.

Табл.63 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	Srv 1-2-2	Любой
Описание	Веб-сервер	Любой
IP-адрес	10.1.2.2	0.0.0.0
Маска	255.255.255.255	0.0.0.0
Тип привязки	Внутренний	Нет

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Криптошлюз	КШ 1	–
Интерфейс	em1	–

Табл.64 Параметры входящего правила трансляции для КШ 1

Параметр	Значение
Направление	Входящие
Источник	Любой
Получатель	Srv.1-2-2
IP-адрес	198.23.75.200
Интерфейс	em0
Название сервиса	http
Порт назначения	80
Порт трансляции	8080

Табл.65 Параметры исходящего правила трансляции для КШ 1

Параметр	Значение
Направление	Исходящие
Источник	Srv.1-2-2
Получатель	Любой
Интерфейс	em0
Изменить на	198.23.75.200
	255.255.255.255
Название сервиса	http, tcp-high-ports

Доступ сторонних абонентов к веб-серверу, находящемуся в защищенной подсети (с помощью NAT 1:1)

Необходимо обеспечить доступ сторонних абонентов к веб-серверу, расположенному на компьютере Srv 1-2-2 (IP-адрес 10.1.2.2, КШ 1, см. стр. 13). Сторонним абонентам известен публичный IP-адрес сервера — 198.23.75.200. В этом случае на КШ 1 нужно создать правило трансляции NAT 1:1, которое однозначно сопоставляет внутрисетевой и публичный адреса веб-сервера независимо от направления трафика.

Табл.66 Параметры сетевых объектов

Параметр	Значение
Название	Srv 1-2-2
Описание	Веб-сервер
IP-адрес	10.1.2.2
Маска	255.255.255.255
Тип привязки	Внутренний
Криптошлюз	КШ 1
Интерфейс	em1

Табл.67 Параметры правила трансляции NAT 1:1 для КШ 1

Параметр	Значение
Направление	1:1
Источник	Srv 1-2-2
Получатель	Любой
Интерфейс	em0
Изменить на	198.23.75.200
	255.255.255.255

Доступ сторонних абонентов к FTP- серверу, находящемуся в защищенной подсети

Необходимо обеспечить доступ сторонних абонентов к FTP- серверу, расположенному на компьютере WS 3-1-2 (IP-адрес 10.3.1.2, КШ 3, см.стр.13). Сторонним абонентам известен публичный IP-адрес сервера — 198.23.75.100. В этом случае на КШ 3 нужно создать входящее правило трансляции для IP-пакетов, поступающих на адрес 198.23.75.100. Режим работы FTP- сервера — пассивный. Для поддержки активного режима необходимо дополнительно добавить исходящее правило трансляции для IP-пакетов от отправителя ftp_serv.

Необходимо в настройках FTP- сервера указать внешний адрес КШ, а также оставить используемые порты 1024 и 1025.

Табл.68 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	ftp_serv	Любой
Описание	FTP-сервер	Любой
IP-адрес	10.3.1.2	0.0.0.0
Маска	255.255.255.255	0.0.0.0
Тип привязки	Внутренний	Нет
Криптошлюз	КШ 3	–
Интерфейс	em1	–

Табл.69 Параметры сервисов

Параметр	Значение	
	Сервис 1	Сервис 2
Имя	ftp-1024	ftp-1025
Протокол	tcp	tcp
Порт источника	Любой	Любой
Порт назначения	1024	1025

Табл.70 Параметры входящего правила трансляции для КШ 3

Параметр	Значение
Направление	Входящие
Источник	Любой
Получатель	ftp_serv

Параметр	Значение
IP-адрес	198.23.75.100
Интерфейс	em0
Сервисы	ftp, ftp-1024, ftp-1025

Табл.71 Параметры исходящего правила трансляции для КШ 3 (только для активного режима FTP-сервера)

Параметр	Значение
Направление	Исходящие
Источник	ftp_serv
Получатель	Любой
Интерфейс	em0
Изменить на	198.23.75.100
	255.255.255.255
Сервисы	tcp-high-ports

Доступ рабочих станций из защищенной подсети к FTP-серверу, расположенному в общей сети

Необходимо обеспечить доступ к FTP-серверу, расположенному в общей сети (IP-адрес 198.23.75.1), с рабочих станций, входящих в состав подсети 10.3.1.0, защищаемой КШ 3 (см. стр. 13). Публичный IP-адрес клиента — 198.23.75.100. В этом случае на КШ 3 нужно создать исходящее правило трансляции. Режим работы FTP-сервера — пассивный.

Табл.72 Параметры сетевых объектов

Параметр	Значение	
	Сетевой объект 1	Сетевой объект 2
Название	LAN 3-1-0	ftp_serv_ext
Описание	Локальная сеть	Внешний FTP-сервер
IP-адрес	10.3.1.0	198.23.75.1
Маска	255.255.255.0	255.255.255.255
Тип привязки	Защищаемый	Нет
Криптошлюз	КШ 3	—
Интерфейс	em1	—

Табл.73 Параметры исходящего правила трансляции для КШ 3

Параметр	Значение
Направление	Исходящие
Источник	LAN 3-1-0
Получатель	ftp_serv_ext
Интерфейс	em0
Изменить на	198.23.75.100
	255.255.255.255
Сервисы	ftp, tcp-high-ports

Примеры использования VLAN в защищенных сетях

Представлены примеры организации защищенного соединения между подсетями с пересекающимися адресными пространствами. Различаются два варианта:

- подсети защищены криптографическими шлюзами;
- подсети защищены криптографическими коммутаторами.

Информационный обмен между двумя подсетями, защищенными разными криптографическими шлюзами

Необходимо обеспечить взаимный обмен информацией между подсетью ЗС 1, защищаемой КШ 1, и подсетью ЗС 2, защищаемой КШ 2. Адресные пространства защищенных подсетей пересекаются.

Для настройки защищенного канала:

1. Зарегистрируйте на каждом КШ VLAN-интерфейс (см. стр.66).

Укажите следующие значения:

Параметр	КШ 1	КШ 2
Тип	Внутренний	Внутренний
VLAN-идентификатор	1	1
Родительский интерфейс	em1	em1
Регистрация	Определяется сетевым устройством	Определяется сетевым устройством
IP-адрес	20.1.1.1	20.1.1.1
Маска	255.255.255.0	255.255.255.0

2. Создайте следующие сетевые объекты (см. стр.98).

Укажите следующие значения:

Параметр	Сетевой объект 1	Сетевой объект 2
Название	KS1_PN	KS2_PN
Описание	Подсеть ЗС 1	Подсеть ЗС 2
IP-адрес	20.1.1.0	20.1.1.0
Маска	255.255.255.0	255.255.255.0
Тип привязки	Защищаемый	Защищаемый
Криптошлюз	КШ 1	КШ 2
Интерфейс	vlan0(ID=1)	vlan0(ID=1)
Трансляция адреса внутри VPN	Флаг	Флаг
Виртуальный адрес	22.1.1.0/ 255.255.255.0	33.1.1.0/ 255.255.255.0

3. Создайте правила фильтрации, разрешающие прохождение трафика между подсетями ЗС 1 и ЗС 2 (см. стр.104).

Укажите следующие значения:

Параметр	Правило фильтрации 1	Правило фильтрации 2
Название	KS1_PN_to_KS2_PN	KS2_PN_to_KS1_PN
Отправитель	KS1_PN	KS2_PN
Инверсия адреса отправителя	–	–
Получатель	KS2_PN	KS1_PN

Параметр	Правило фильтрации 1	Правило фильтрации 2
Инверсия адреса получателя	–	–
Сервисы	Любой TCP, Любой UDP, Любой ICMP	Любой TCP, Любой UDP, Любой ICMP
Действие	Пропустить	Пропустить
Временной интервал	Постоянно	Постоянно
Регистрация	Нет	Нет
Контролировать состояние соединения	Флаг	Флаг
Отключено	–	–

4. Установите парную связь между КШ 1 и КШ 2 (см. стр.78).

Информационный обмен между двумя подсетями, защищенными разными криптографическими коммутаторами

Необходимо обеспечить взаимный обмен информацией между подсетью ЗС 1, защищаемой КК 1, и подсетью ЗС 2, защищаемой КК 2. Адресные пространства защищенных подсетей пересекаются.

Для настройки защищенного канала:

1. Зарегистрируйте на каждом КК VLAN-интерфейс (см. стр.66).

Укажите следующие значения:

Параметр	КК 1	КК 2
Тип	Порт криптокоммутатора	Порт криптокоммутатора
VLAN-идентификатор	100	100
Родительский интерфейс	em1	em1

2. Создайте виртуальный коммутатор и сформируйте список КК (см. стр.89):

Укажите следующие значения:

Диалог "Виртуальный коммутатор"

Параметр	Значение
Название	VLAN100
Описание	Криптографическая коммутируемая сеть КК1-КК2

Диалог "Порт коммутации"

Параметр	КК 1	КК 2
Криптокоммутатор	КК 1	КК 2
Порт коммутации	em1	em1
Класс трафика	Нормальный	Нормальный

Пример использования групповой адресации в защищенных сетях

В данном разделе приводится пример реализации мультимедиа-трансляции из одной защищенной сети в другую. Задача – организовать передачу видеопотока от источника, расположенного в защищенной сети, нескольким адресатам другой защищенной сети. Источником видеопотока является IP-камера с IP-адресом 10.2.1.3, установленная в сети, защищенной КШ 2 (см. рисунок в разделе "Пример организации защищенной корпоративной сети" на стр. 13).

Получатели потока – 3 рабочие станции с IP-адресами 10.3.1.3, 10.3.1.4 и 10.3.1.5 сети, защищенной КШ 3.

Примечание. Мультикастовый трафик между КШ-источником и КШ-получателем возможен только при наличии между ними парных связей.

Для настройки видеотрансляции с использованием групповой адресации:

1. Создайте в ПУ ЦУС сетевой объект типа unicast, описывающий защищенную КШ 2 сеть с источником видеотрансляции (см. стр.98).

При настройке параметров сетевого объекта на вкладке "Общие" укажите следующие значения:

Параметр	Значение
Название	ЗС КШ2
Описание	Защищенная сеть источника видеотрансляции
IP-адрес	10.2.1.0
Маска	255.255.255.0
Тип привязки	Защищаемый
Криптошлюз	КШ2
Интерфейс	Любой

2. Создайте в ПУ ЦУС сетевой объект типа multicast, указав следующие значения параметров (см. стр.98):

Параметр	Значение
IP-адрес	224.0.0.0
Маска	255.0.0.0
Получатель	КШ3

3. Создайте в ПУ ЦУС правило фильтрации, разрешающее прохождение трафика между сетями, защищенными КШ 2 и КШ 3 (см. стр.104).

При настройке параметров правила фильтрации укажите следующие значения:

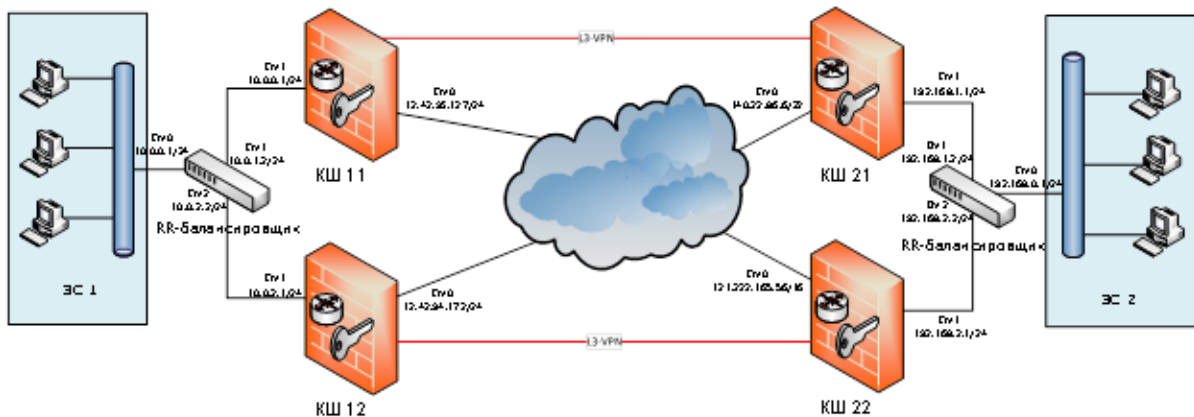
Параметр	Значение
Отправитель	ЗС КШ2
Инверсия адреса отправителя	–
Получатель	Сетевой объект, созданный в п.2
Инверсия адреса получателя	–
Сервисы	Любой TCP, Любой UDP, Любой ICMP
Действие	Пропустить
Временной интервал	Постоянно
Регистрация	Нет
Контролировать состояние соединения	Установить отметку
Отключено	–

В результате на КШ 3 будет автоматически включен режим ip multicast-routing.

Для начала видеотрансляции получатели должны отправить запрос (например, средствами приложения VLC media player) на UDP-адрес IP-камеры. Перенаправление трафика от IP-камеры получателям, отправившим запрос, будет осуществляться на КШ 3.

Пример использования фермы КШ для увеличения пропускной способности VPN-канала

Пример использования фермы КШ для увеличения пропускной способности VPN-канала по схеме "точка-точка".



В каждой сети устанавливают по одинаковой ферме. Нагрузка распределяется между КШ в ферме. Ферма состоит из нескольких КШ и балансировщика, распределяющего пакеты из защищенной сети между данными КШ по алгоритму Round Robin. Количество КШ определяется требуемой пропускной способностью VPN-канала. В качестве балансировщика может быть использован дополнительный КШ в режиме Multi-WAN "Балансировка трафика" (см. стр. 73). Также возможно использование балансировщиков типа RR-DNS, L3/L4.

КШ из разных сетей поддерживают связь попарно по непересекающимся каналам.

Для настройки фермы шлюзов:

1. Создайте следующие сетевые объекты:

Сетевые объекты с виртуальными адресами

Параметр	Сет. объект 1	Сет. объект 2	Сет. объект 3	Сет. объект 4
Название	ЗС КШ11	ЗС КШ12	ЗС КШ21	ЗС КШ22
Тип передачи данных	Unicast			
Описание	Защищаемая сеть КШ11	Защищаемая сеть КШ12	Защищаемая сеть КШ21	Защищаемая сеть КШ22
IP-адрес	10.0.0.0		192.168.0.0	
Маска	255.255.255.0			
Тип привязки	Защищаемый			
Криптошлюз	КШ11	КШ12	КШ21	КШ22
Интерфейс	Em1			
Трансляция адреса внутри VPN	Да			
Виртуальный адрес	173.17.2.0	173.17.3.0	173.17.0.0	173.17.1.0
Маска	255.255.255.0			
Регистрация	Определяется интерфейсом			

Сетевые объекты с реальными адресами

Параметр	Сет. объект 5	Сет. объект 6	Сет. объект 7	Сет. объект 8
Название	ВС КШ11	ВС КШ21	ВС КШ12	ВС КШ22
Тип передачи данных	Unicast			
Описание	Внутренняя сеть КШ11	Внутренняя сеть КШ21	Внутренняя сеть КШ12	Внутренняя сеть КШ22
IP-адрес	173.17.2.0	173.17.0.0	173.17.3.0	173.17.1.0
Маска	255.255.255.0			
Тип привязки	Внутренний			
Криптошлюз	КШ11	КШ21	КШ12	КШ21
Интерфейс	Em1			
Трансляция адреса внутри VPN	Нет			
Регистрация	Определяется интерфейсом			

2. Создайте следующие правила фильтрации:

Параметр	Прав. филт. 1	Прав. филт. 2	Прав. филт. 3	Прав. филт. 4
Название	ПФ11>21	ПФ21>11	ПФ12>22	ПФ22>12
Описание	Правило фильтрации 11>21	Правило фильтрации 21>11	Правило фильтрации 12>22	Правило фильтрации 22>12
Отправитель	ЗС КШ11	ЗС КШ21	ЗС КШ12	ЗС КШ22
Инверсия адреса отправителя	Нет			
Получатель	ЗС КШ21	ЗС КШ11	ЗС КШ22	ЗС КШ12
Инверсия адреса получателя	Нет			
Сервисы	Любой TCP, Любой UDP, Любой ICMP			
Действие	Пропустить			
Временной интервал	Постоянно			
Класс трафика	Нормальный			
Регистрация	Определяется источником/получателем			
Контролировать состояние соединения	Да			
Защита от DoS-атак	Нет			
Применить и завершить обработку	Да			
Отключено	Нет			

3. Создайте следующие правила трансляции:

Параметр	Прав. транс. 1	Прав. транс. 2	Прав. транс. 3	Прав. транс. 4
Устройство	КШ11	КШ21	КШ12	КШ22

Параметр	Прав. транс. 1	Прав. транс. 2	Прав. транс. 3	Прав. транс. 4
Название	ПТ11	ПТ21	ПТ12	ПТ22
Описание	Правило трансляции 1:1			
Направление	1:1			
Источник	ВС КШ11	ВС КШ21	ВС КШ12	ВС КШ22
Получатель	ЗС КШ11	ЗС КШ21	ЗС КШ12	ЗС КШ22
Интерфейс	Em1			
Временной интервал	Постоянно			
Класс трафика	Нормальный			
Регистрация	Определяется источником/получателем			
Трансляция адреса источника... изменить на	192.168.0.0 255.255.255.0	10.0.0.0 255.255.255.0	192.168.0.0 255.255.255.0	10.0.0.0 255.255.255.0
Отключено	Нет			

4. Установите парные связи КШ11 -- КШ21 и КШ12 -- КШ22.

Диагностика сетевого устройства

Средствами ПУ ЦУС можно выполнить диагностику работы сетевого устройства. Результаты диагностики представляются в виде следующих отчетов:

Отчет	Описание
Ресурсы <устройство>	Информация о загрузенности каждого процессора. Общий и свободный объем оперативной памяти. Общий объем жесткого диска, а также объем используемого и свободного пространства. Максимальные и текущие объемы журналов
arp/ndp	Содержимое ARP- и NDP-кеша
ping*	Результаты выполнения команды ping
tracert*	Результаты выполнения команды tracert
tcpdump	Информация о сетевом трафике выбранного интерфейса с возможностью применения фильтра в формате tcpdump. Отчет выводится в окне в виде текстового файла. Для сетевого устройства, выведенного из эксплуатации, предусмотрено сохранение отчета в двоичном коде для последующего просмотра специализированным приложением
Таблица состояний (только для КШ)	Количество установленных соединений с возможностью отдельного просмотра сессий IPv4 и IPv6. При просмотре сессий могут быть использованы фильтр и функция поиска
Сетевые соединения	Сведения об открытых сетевых соединениях
Шифратор (только для КШ и КК)	Статистическая информация о работе шифратора/криптокоммутатора
Технологический отчет	Технологический отчет, выгружаемый на отчуждаемый носитель для отправки в службу поддержки
Пропущенные пакеты (только для ДА)	Сведения о количестве пропущенных пакетов

- *Для выполнения команд ping и tracert на устройстве автоматически создаются временные правила фильтрации, разрешающие прохождение соответствующих пакетов.

Для формирования отчета:

1. Выберите в списке сетевое устройство, вызовите контекстное меню и выберите пункт "Диагностика".

На экране появится окно "Диагностика".

2. Перейдите на вкладку нужного отчета, настройте при необходимости его параметры и нажмите кнопку "Выполнить".

В зависимости от выбранного отчета результат будет выведен в окне "Диагностика сетевого устройства" или сохранен в соответствии с заданными настройками.

Внимание! При формировании нескольких отчетов задания по их подготовке и отображению ставятся в очередь с выводом на экран соответствующего предупреждения. Формирование каждого следующего отчета начинается только после завершения предыдущего. Поэтому не рекомендуется закрывать окно диагностики до вывода на экран очередного отчета, так как при закрытии окна формируемый отчет не сохраняется.

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.74 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
RCPTTray.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.75 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.76 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.77 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.78 Вспомогательные модули программы управления

Имя	Папка
ASKeyDuplicator.exe	\Program Files\Код Безопасности\Континент\KeyDuplicator

Имя	Папка
etsdk.dll	\Program Files\Код Безопасности\Континент\Hardware
key.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
SnTokenEx.dll	\Program Files\Код Безопасности\Континент\Hardware
SnSable.dll	\Program Files\Код Безопасности\Континент\Hardware
SnTokenSC.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
etsdk.dll - на Windows x86 etsdkx64.dll - на Windows x64	\Program Files\Код Безопасности\Континент\CSP
key.dll	\Program Files\Код Безопасности\Континент\CSP
SneToken.dll	\Program Files\Код Безопасности\Континент\CSP
SnTokenEx.dll	\Program Files\Код Безопасности\Континент\CSP
SnTokenSC.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.79 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

Имя	Папка
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
bootmgr	%Boot Drive% или %System Drive%\windows\boot\PCAT

Табл.80 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 RequireSecuritySignatureAutoShareWks 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

Сохранение базы данных ЦУС

В случае возникновения проблем, связанных с функционированием комплекса, может потребоваться передача копии БД ЦУС в службу технической поддержки.

В этом случае необходимо создать копию БД ЦУС. Файл копии не содержит конфиденциальной информации и предназначен исключительно для анализа в службе технической поддержки.

Внимание! Запрещается загрузка файла копии базы данных в БД ЦУС.

Для сохранения копии БД ЦУС:

1. Активируйте в меню "ЦУС" команду "Сохранить диагностический файл БД ЦУС".
На экране появится диалог задания пароля.
2. Введите и подтвердите пароль.
На экране появится стандартный диалог сохранения файла.
3. Укажите путь сохранения файла копии БД ЦУС, при необходимости измените имя и нажмите кнопку "ОК".

Примечание. Копия БД ЦУС сохраняется в виде файла с расширением *.support_cfg.

Файл копии БД ЦУС будет сохранен.

4. Передайте файл и пароль в службу технической поддержки.

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.