Аппаратно-программный комплекс шифрования "Континент"

Версия 3.9 (исполнение 3.М3)

Комментарии к релизу 3.9.3.3438

Документ содержит описание основных возможностей, особенностей работы и ограничений применения изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3)" (далее – комплекс), которые необходимо учитывать при его эксплуатации.

Список сокращений

БД	База данных
КК	Криптографический коммутатор – сетевое устройство
КШ	Криптографический шлюз – сетевое устройство
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ППЖ	Программа просмотра журналов
ПУ	Программа управления
ПУ ЦУС	Программа управления центром управления сетью
СУ	Сетевое устройство
СУБД	Система управления базами данных
ЦУС	Центр управления сетью
VPN	Virtual Private Network – виртуальная частная сеть

Оглавление

1.	Размещение файлов (ПО и документации) на компакт-диске	3
1.1.	Диск 1	3
1.2.	Диск 2	3
2.	Изменения и новые возможности	4
2.1.	Версия 3.9.3.3438 (3.М3).....	4
2.2.	Версия 3.8.0.347 (3.М2)	5
3.	Ограничения на поддержку аппаратных и программных средств	8
4.	Особенности работы и ограничения	9
4.1.	Общесистемные	9
4.2.	Обновление	10
4.3.	Резервирование	10
4.4.	Центр управления сетью	11
4.5.	Сетевые устройства.....	13
4.6.	Программа управления ЦУС	15
4.7.	Агент ЦУС	16
4.8.	Программа просмотра журналов.....	17

1. Размещение файлов (ПО и документации) на компакт-диске

1.1. Диск 1

Каталог	Содержимое
Дистрибутивы АПКШ "Континент"	
\boot	Модули для установки АПКШ "Континент", включая модули ОС FreeBSD
\Setup\Continent\RCP	Дистрибутив ПУ АПКШ "Континент"
\Setup\Continent\AC	Дистрибутив программы аутентификации хоста в защищенной сети
\Setup\Continent\UPDATE	Файл обновления ПО АПКШ "Континент"
\Setup\Continent\FLASH\IMAGES	Установочные образы модулей АПКШ "Континент", предназначенные для установки с USB-флеш-накопителя
\isolinux	Загрузчик FreeBSD
Служебные программы	
\Tools\Код безопасности\ServiceTool	Каталог установки служебных программ
\Tools\Код безопасности\DiagnosticTool	Каталог установки диагностических программ
Описание версии	
\Version.TXT	Файл с описанием версии ПО АПКШ "Континент"

1.2. Диск 2

Каталог	Содержимое
Документация АПКШ "Континент"	
Эксплуатационная документация\ Continent - AU - Admin Guide.pdf	АПКШ "Континент". Версия 3.9. Руководство администратора. Клиент аутентификации пользователя
Эксплуатационная документация\ Continent - Audit - Admin Guide.pdf	АПКШ "Континент". Версия 3.9. Руководство администратора. Аудит
Эксплуатационная документация\ Continent - Basics - Admin Guide.pdf	АПКШ "Континент". Версия 3.9. Руководство администратора. Принципы функционирования комплекса
Эксплуатационная документация\ Continent - Deployment - Admin Guide.pdf	АПКШ "Континент". Версия 3.9. Руководство администратора. Ввод в эксплуатацию
Эксплуатационная документация\ Continent - Firewall - Admin Guide.pdf	АПКШ "Континент". Версия 3.9. Руководство администратора. Межсетевое экранирование
Эксплуатационная документация\ Continent - Management - Admin Guide.pdf	АПКШ "Континент". Версия 3.9. Руководство администратора. Управление комплексом
Эксплуатационная документация\ Continent - Network - Admin Guide.pdf	АПКШ "Континент". Версия 3.9. Руководство администратора. Сетевые функции
Эксплуатационная документация\ Continent - VPN - Admin Guide.pdf	АПКШ "Континент". Версия 3.9. Руководство администратора. Настройка VPN
Эксплуатационная документация\ Continent - Release Notes.pdf	Release Notes - сведения об основных возможностях, особенностях и ограничениях применения АПКШ "Континент"
Техническая документация\ RU.88338853.501430.022 30 - Формуляр.pdf	АПКШ "Континент". Версия 3.9. Формуляр
Техническая документация\ RU.88338853.501430.022 30-1 Приложение к ФО.pdf	АПКШ "Континент". Версия 3.9. Приложение 1 к формуляру

Каталог	Содержимое
Техническая документация\ RU.88338853.501430.022 ТУ - Техни- ческие условия.pdf	АПКШ "Континент". Версия 3.9. Технические условия
Техническая документация\ RU.88338853.501430.022 99 - Правила пользования.pdf	АПКШ "Континент". Версия 3.9. Правила пользования

2. Изменения и новые возможности

Ниже приводятся сведения об изменениях и новых возможностях АПКШ "Континент" версии 3.9 (исполнение 3.М3) по сравнению с сертифицированным ФСБ России АПКШ "Континент" версии 3.М2.

2.1. Версия 3.9.3.3438 (3.М3)

1. Реализована возможность доступа к защищаемой сети, находящейся одновременно за несколькими АПКШ.
2. Реализована возможность выбора приоритетного маршрута трафика, поступающего в защищаемую сеть.
3. Добавлен функционал фильтрации трафика на основе меток ToS.
4. Добавлена возможность аутентификации при получении настроек даты и времени для ЦУС и КШ с NTP-сервера.
5. Установлен минимальный интервал доступности контрольных точке в Multi-WAN.
6. В локальном меню КШ отображается статус соединения с ЦУС.
7. Реализована возможность приоритизации трафика на основе меток ToS на КК.
8. Реализована возможность автоматического развертывания компонентов комплекса для оптимизации построения сетей.
9. Реализована возможность создания, подключения и управления сетевыми устройствами версий 3.9.3 (класс KB), 3.9.3, 3.М2, 3.9.2 с ЦУС версии 3.9.3 (класс KB).
10. Реализована возможность управления сетевыми устройствами версий 3.9.3 (класс KB), 3.9.3, 3.М2, 3.9.2 с ЦУС версии 3.9.3 (класс KB).
11. Реализована возможность построения VPN между внешними сетями АПКШ "Континент" версий 3.7.7, 3.9.0, 3.9.1, 3.9.2 и узлами класса КС версий 3.9.2, 3.9.3 под управлением ЦУС класса KB.
12. Реализована возможность изменения тайм-аута в локальном меню сетевого устройства.
13. Реализована регистрация подключений к узлам в системном журнале.
14. Реализован экспорт и импорт объектов конфигурации в xml-файл через ПУ ЦУС.
15. Реализована обязательная смена пароля от openconsole при первой успешной авторизации.
16. Добавлена локальная настройка режима работы DHCP-ретранслятора.
17. В локальном меню сетевого устройства добавлена возможность установить значение тайм-аута MTU.
18. Добавлена возможность резервирования полосы пропускания для управляющего трафика.
19. Реализована возможность добавления кастомных платформ.
20. Реализован механизм экспорта системных событий на внешний syslog-сервер.
21. Реализована возможность смены идентификатора engine_id в SNMP.
22. Реализована возможность задания пароля на ключевой контейнер в Агенте ЦУС и СД.
23. Реализована возможность получения информации по SNMP: значение версии ОС, значение предыдущей версии ОС, тип платформы, конфигурация устройства, ID устройства, мягкий режим, состояния устройства (введен в эксплуатацию или нет), часовой пояс, значения таблицы маршрутизации, agr-таблица, значения состояний таблицы соединений, значения счетчика расхода ключа ВПН, время подключения/недоступности ЦУС, срок годности ключа управления, срок годности межсетевого ключа, выработка ресурса межсетевого ключа.

- 24.** Добавлена звуковая сигнализация необходимости загрузки подготовленного ключа на сетевое устройство.
- 25.** Добавлена возможность записи конфигурации и ключей сетевых устройств на один носитель (добавление id устройства в название файлов).
- 26.** Добавлена панель с состоянием устройств, датами действия ключа управления, версиями устройств, с возможностью выгрузки таблицы в формате xml/csv.
- 27.** Реализована возможность указать диапазон портов во входящем правиле NAT.
- 28.** Реализована возможность настройки опций на DHCP-сервере, включая настройку пользовательских опций.
- 29.** Обновлен интерфейс Агента ЦУС и СД.
- 30.** В ПУ ЦУС появилась возможность проведения групповых операций с СУ.
- 31.** На криптокоммутаторе появилась возможность включения балансировки соединений по ядрам на основе заголовков L3-пакетов.
- 32.** Добавлена возможность менять MSS трафика, проходящего через КК.
- 33.** Реализовано резервирование ЦУС.
- 34.** Добавлена возможность агрегации интерфейсов по протоколу LACP (802.3ad).
- 35.** Реализован доступ к КШ/КК по протоколу SSH.
- 36.** Внедрено централизованное управление локальными администраторами.
- 37.** Добавлена возможность создания отладочного журнала КШ/КК средствами ПУ.
- 38.** Добавлена поддержка Jumbo frame (MTU 9000 байт) на КШ и КК.
- 39.** Добавлена локальная настройка прохождения специальных протоколов на КК (LACP, STP, 802.1x).
- 40.** Увеличена стабильность и производительность работы сетевых устройств за счет перехода на новую версию базовой ОС и архитектуру x86_64.
- 41.** В криптошлюзах реализована поддержка механизма расширения для DNS (EDNS).
- 42.** Реализована процедура ввода лицензий ЦУС с использованием файла лицензий.

2.2. Версия 3.8.0.347 (3.M2)

- 1.** В состав комплекса добавлено новое сетевое устройство – КК.
- 2.** Добавлена возможность одновременного подключения КШ к нескольким внешним сетям – режим Multi-WAN.
- 3.** Обеспечена совместная работа КШ с сетевыми устройствами, поддерживающими трансляцию сетевых адресов NAT.
Ограничение. Между двумя связанными КШ не должно быть более одного устройства с поддержкой динамической трансляции адресов.
- 4.** Увеличена производительность ЦУС. Например, максимальное количество КШ, управляемых одним ЦУС, может достигать 5000 единиц для платформы IPC-1000 (при достаточной пропускной способности канала).
- 5.** Увеличено максимальное количество записей в таблице состояния соединений:

Платформа	Максимальное количество записей
IPC-1000F	1000000
IPC-3000F	1500000
Неопределенная	50000

- 6.** Средствами локального или централизованного управления можно выполнить диагностику сетевого устройства (КШ, КК), выведенного из эксплуатации.
- 7.** На КШ реализован сервис DHCP. Сервис может функционировать в режиме сервера или ретранслятора.

- 8.** Изменен протокол взаимодействия между КШ. В версии 3.М использовался порт 250 IP-протокола. В текущей версии взаимодействие между КШ осуществляется по UDP-протоколу (порты 10000–10031), что значительно упрощает настройку межсетевых экранов, расположенных на пути трафика.
- 9.** Изменен принцип локального управления КШ – управление КШ осуществляют с локальной консоли с помощью главного и дополнительного меню.
- 10.** Изменен формат записи конфигурации, используемой для инициализации КШ, на отчуждаемый носитель. В текущей версии конфигурация КШ записывается отдельно от криптографических ключей. Такой формат позволяет пересылать конфигурацию без использования средств спецсвязи.
- 11.** Добавлена поддержка работы с каналами связи общих сетей передачи данных, использующих протоколы IPv6. Данная возможность предназначена для организации защищенного соединения через IPv6-сети провайдеров.
- 12.** Реализована возможность обмена информацией по защищенному каналу между подсетями, защищенными разными КШ и использующими одинаковое адресное пространство. Для этого реализован механизм виртуальной адресации.
- 13.** Добавлена возможность просмотра средствами локального управления сетевого устройства таблицы состояний (keep-state), отображающей количество установленных соединений.
- 14.** Увеличена предельная пропускная способность криптографического шлюза. С этой целью в ПО КШ добавлен программный криптоускоритель. Предельная пропускная способность зависит от аппаратной платформы. Для платформы IPC-3000F максимальная производительность в режиме VPN+МЭ достигает 2,5 Гбит/с.
- 15.** Добавлены следующие возможности:
- настройка обработки mtu path discovery на сетевых устройствах;
 - настройка STUN-сервера на ЦУС.
- 16.** Для повышения производительности сетевого устройства добавлена оптимизация правил. Оптимизация применяется к правилам фильтрации, в которых используются группы сетевых объектов.
- 17.** Добавлено централизованное управление MSS и MTU.
- 18.** В свойствах узла добавлено отображение значения параметра "Статус автозагрузки сетевого устройства". Значение (отключена/включена) задается в настройках ПАК "Соболь".
- 19.** При первом запуске (включении) КШ необходимо предъявить персональный идентификатор администратора ПАК "Соболь" и загрузить комплект ключей, хранящихся на ключевом носителе (USB-флеш-накопитель).
- 20.** Добавлена возможность управления очередностью IP-пакетов с учетом приоритета трафика.
- 21.** Для удобства просмотра и управления добавлена возможность объединения объектов (сетевые объекты, сервисы, пользователи, сетевые устройства) в ПУ ЦУС в группы. Появилась возможность создавать иерархию групп сетевых устройств. При удалении группы объекты, входящие в нее, не удаляются.
- 22.** В подсистему управления комплексом добавлен новый компонент "Конфигуратор БД журналов ЦУС". Конфигуратор предназначен для решения следующих задач:
- настройка параметров подключения агента к СУБД;
 - обеспечение доступа администраторов комплекса к БД журналов.
- 23.** Добавлена возможность смены внешнего адреса ЦУС средствами централизованного управления.
- 24.** Добавлена поддержка криптосхемы 2.0 в ПАК "Соболь".
- 25.** Изменены условия лицензирования комплекса. Добавлены лицензии на обновление ПО КШ. Действует ограничение на параметры ЦУС – максимальное количество криптографических шлюзов, имеющих статус "Введен в эксплуатацию".
- 26.** Добавлена возможность сохранения и восстановления конфигурации КШ с локальной консоли. Сохранение резервной копии осуществляют на USB-флеш-накопитель.
- 27.** Добавлена возможность выключения КШ средствами ПУ ЦУС.
- 28.** Изменен формат хранения журналов. Обеспечена работа пользователя с журналами, содержащими несколько миллионов записей.
- 29.** Некоторые среды (например, ОС МСВС) используют поле IP-опций в заголовке IP-пакета в обязательном порядке. Для функционирования комплекса "Континент" в таких средах теперь предусмотрен режим прохождения пакетов с IP-опциями. По умолчанию этот режим выключен. Включение режима выполняют средствами локального управления КШ.

- 30.** Обновлен механизм проверки качества паролей администраторов. Средствами ПУ ЦУС можно настроить следующие параметры:
- минимальная длина пароля;
 - количество неудачных попыток входа до блокировки;
 - время блокировки при превышении количества неудачных попыток входа;
 - контроль слабых паролей.
- 31.** Добавлена настройка времени ожидания ответа от активного сетевого устройства в кластере, после которого происходит переключение канала связи с резервного на основной и с основного на резервный.
- 32.** Добавлена возможность входа администратора в локальное меню по паролю (без предъявления идентификатора администратора ПАК "Соболь").
- 33.** Реализована автоматическая синхронизация парных связей при ошибках в канале VPN (расхождение ключей парной связи или расхождение номеров пакетов).
- 34.** Для повышения производительности сетевого устройства реализованы настройки оптимизатора шифратора по ядрам CPU (по MAC-адресам для КК и по сессиям для КШ) и настройки дефрагментации пакетов.
- 35.** Добавлена возможность принудительной очистки таблицы состояния соединений.
- 36.** Обеспечена возможность одновременной передачи одного и того же трафика группе клиентов (multicast). На криптографических шлюзах, которые участвуют в групповой рассылке, автоматически включается режим ip multicast-routing. Перечень таких КШ определяют с помощью сетевого объекта типа Multicast.
- 37.** Добавлена поддержка аппаратного резервирования (создания кластера высокого доступа) для криптографических шлюзов, подключенных к внешней сети по протоколу PPPoE.
- 38.** Появилась возможность использовать несколько интерфейсов КШ в качестве интерфейсов резервирования.
- 39.** Добавлена возможность отправки агентом ЦУС почтовых уведомлений о критических изменениях в состоянии КШ на указанный адрес электронной почты.
- 40.** В качестве источника исходной ключевой информации для инициализации ЦУС используется ключевой блокнот РДП-003.
- 41.** Добавлена возможность управления локальной сигнализацией о событии НСД. Сообщения могут выводиться на экран монитора, подключенного к КШ, и/или воспроизводиться в виде звукового сигнала. Включение и выключение сигнализации выполняют непосредственно с локальной консоли КШ.
- 42.** Добавлена возможность фильтрации IP-пакетов по указанному сочетанию символов (регулярному выражению). В качестве сочетания символов могут использоваться как команды прикладных протоколов, так и содержимое передаваемых в незашифрованном виде файлов (для протоколов ftp и http).
- 43.** В программе управления агентом добавлен параметр "Отключить уведомление об ошибках".
- 44.** Изменены параметры управления программой Flash.exe из командной строки. Теперь для записи образа диска на USB-флеш-накопитель необходимо указать полное имя файла программы Flash.exe с параметрами <имя диска> и <имя файла>, где <имя диска> – буквенное обозначение подключенного USB-флеш-накопителя, <имя файла> – полное имя файла образа диска.
- 45.** Реализована защита корпоративной сети от DoS-атак типа SYN-флуд.
- 46.** Добавлена возможность идентификации и аутентификации пользователей, работающих на компьютерах в защищаемой сети КШ, с помощью программы "Клиент аутентификации пользователя", установленной на компьютере пользователя.
- 47.** Добавлена настройка регистрации IP-пакетов.
- 48.** Добавлена настройка реакции агента на события.
- 49.** Расширены настройки функционирования кластера.

3. Ограничения на поддержку аппаратных и программных средств

1	Ключевые устройства	Сетевые устройства (КШ, КК)	USB-флеш-накопитель
		ПУ ЦУС Агент ЦУС и СД	<ul style="list-style-type: none"> • USB-флеш-накопитель; • USB-ключ eToken PRO (Java); • смарт-карта eToken Pro (Java) с USB-считывателем Athena ASEDrive IIIe USB V2; • Рутокен S/ЭЦП; • ПАК "Соболь" 3.0/3.1/3.2; • iButton DS1994/DS1995/DS1996; • Монитор с разрешением экрана не менее 1024x768
2	Операционная система	PM администратора	<ul style="list-style-type: none"> • Windows Server 2008 R2 SP1 x64 (при наличии купленных расширенных обновлений безопасности (ESU)); • Windows Server 2012 x64; • Windows Server 2012 R2 x64; • Windows Server 2016 x64; • Windows Server 2019 x64; • Windows 8.1 x64 (кроме всех выпусков Starter и Home Edition); • Windows 10 x64 (кроме всех выпусков Starter и Home Edition) • Windows 10 x86/x64 (кроме всех выпусков Starter и Home Edition)
3	Предыдущие версии АПКШ "Континент"	Совместная работа с предыдущими версиями комплекса	3.9.2, 3.M2
		Обновление предыдущих версий сетевых устройств и ЦУС	3.M2
4	СКЗИ "КриптоПро CSP" СКЗИ "Код Безопасности CSP"		4.0, 5.0 Не ниже 4.0.573.0
5	Аппаратные платформы (КШ, КК, ЦУС)	IPC-25	S115
		IPC-100	MS-92E3
		IPC-100	S102
		IPC-1000F	S021
		IPC-3000F	S021
		IPC-R300	SC R300
		IPC-R550	SC R300
		IPC-R10	SC R15
		IPC-R50	SC R15
		IPC-R1000NF2	SC R1000
6	Поддерживаемые версии БД		<ul style="list-style-type: none"> • MS SQL Server 2012 Express x64; • MS SQL Server 2012 x64; • MS SQL Server 2014 Express x64; • MS SQL Server 2017 Express x64; • MS SQL Server 2019 x64
7	Поддерживаемые версии ключевых документов		РДП-003, РДП-006 Собственные ключи для КС1/КС2/КС3

4. Особенности работы и ограничения

4.1. Общесистемные

- 1.** Особенности исправления ПО компонентов комплекса средствами программы установки. После выполнения процедуры исправления проверьте правильность настроек подключения компонентов программ управления.
- 2.** Версия ПО, установленного на сетевом устройстве, должна соответствовать версии ПО, установленного на ЦУС, или быть более ранней. Если на сетевом устройстве установлено ПО новой версии по отношению к версии ПО ЦУС, это приводит к невозможности загрузки конфигурации сетевого устройства или появлению ошибки вида "Завершился/etc/rc.running/3agent".
- 3.** Для одинаковых IP-адресов невозможна совместная работа правил NAT и правил фильтрации с профилем усиленной фильтрации.
- 4.** Для перечисленных выше платформ рекомендуется обновить более ранние версии ПО BIOS на указанные в таблице. По вопросам, связанным с обновлением ПО BIOS, следует обращаться в авторизованные сервис-центры компании – разработчика ПО АПКШ "Континент".
- 5.** При включенной усиленной фильтрации поддерживается работа со следующими FTP-серверами и FTP-клиентами:

Серверы	Microsoft Internet Information Services (7.5.7600.16385)
	ProFTPD 1.3.5a
	Vstpd 3.0.3
Клиенты	wget 1.17.1, curl 7.47.0, fetch, ftp (Unix)
	Filezilla 3.22.1
	Windows FTP Client (Explorer 11.0.9600.17031)
	WinSCP 5.9.3 (сборка 7136)

Работа со всеми клиентами поддерживается только в активном режиме.

- 6.** Работа с БД ЦУС, созданной конфигуратором версии 3.M2, не поддерживается. Для работы с базами данных версий 3.7 и 3.9 необходимо использовать две отдельные программы просмотра журналов (версий 3.7 и 3.9), установленные на разных компьютерах.
- 7.** Сведения о цифровой подписи отображаются некорректно в Windows Server 2019, если подпись привязана к истекшему сертификату УЦ.
- 8.** Для корректной работы программы просмотра отчетов необходимо удалить и заново установить SAP Crystal Reports при помощи файла ..\Setup\Continent\RCP\setup.exe, расположенного на дистрибутивном диске.
- 9.** Для корректной работы ПУ ЦУС на ОС Windows 7 и Windows Server 2008 R2 необходимо установить обновления KB4490628 и KB4474419.
- 10.** При необходимости блокировки по IP-адресу из списка РКН нужно использовать правило фильтрации со списком реестра запрещенных ресурсов РКН с любыми сервисами. Внимание! Обработка такого правила значительно снижает производительность МЭ.
- 11.** Агент БРП не принимает ключи ЦУС с паролем больше 8 символов.
- 12.** Не происходит подключение к ПУ ЦУС с ключами на токенах.

4.2. Обновление

1. Особенности обновления. После обновления ПО ЦУС с версии 3.М2 на версию 3.М3 в журнале НСД ЦУС может возрасти количество зарегистрированных событий НСД "Неверный номер входящего пакета". В этом случае рекомендуется в ПУ ЦУС удалить и повторно создать парные связи.

2. Особенности обновления ПО КШ:

- Если при дистанционном обновлении автоматически не определяется тип платформы, в конфигурации КШ данный параметр принимает значение "Неизвестная платформа". При этом устанавливаются усредненные значения параметров, определяющих производительность КШ. Для задания параметров, обеспечивающих максимальную производительность КШ на установленной платформе, рекомендуется выполнить локальное обновление ПО, указав тип платформы вручную.
- При неудачном обновлении ПО и возврате к предыдущей версии необходимо выполнить инициализацию ПАК "Соболь". В противном случае повторное дистанционное обновление ПО невозможно.
- Свободное пространство на диске КШ должно быть не менее 75 Мбайт.
- Перед обновлением ПО наименования всех имеющихся VLAN-интерфейсов должны иметь формат `vlan<числовой номер>` (латиница, нижний регистр, без спецсимволов). Если наименования имеющихся VLAN-интерфейсов не соответствуют указанному формату, такие интерфейсы необходимо переименовать без применения операции удаления интерфейса.

3. При дистанционном обновлении ПО перезагрузка сетевого устройства выполняется дважды.

4. Особенность обновления BIOS сетевого устройства на платформе 92Е3. После обновления BIOS сетевое устройство постоянно перезагружается. В этом случае следует:

- Выключить сетевое устройство и отсоединить сторожевой кабель ПАК "Соболь".
- Включить сетевое устройство и дождаться завершения его запуска и готовности устройства к работе.
- Выключить сетевое устройство и подсоединить сторожевой кабель ПАК "Соболь".
- Включить сетевое устройство и дождаться завершения его запуска и готовности устройства к работе.

Внимание! Для выполнения данной процедуры необходимо вскрытие корпуса сетевого устройства. Разрешение на вскрытие корпуса получают в службе вендорской поддержки ООО "Код Безопасности".

5. При обновлении конфигурации КШ, не связанном с настройками BGP, возможны обрыв и последующее восстановление bgr-сессии.

6. Для обновления БРП необходимо использовать "Континент АП" версии 3.7.7.

7. При обновлении комплекса с версии 3.М2 до версии 3.9.3 (исполнение 3.М) после актуализации ключа управления 3.М2 необходимо создать новый ключ агента ЦУС и СД.

8. При обновлении комплекса с версии 3.М3 до 3.9.3 необходимо удалить с РМ администратора ПУ ЦУС со всеми дополнительными компонентами, выполнить перезагрузку РМ администратора и установить ПУ ЦУС версии 3.9.3.

9. После обновления КШ с версии 3.М2 до версии 3.9.3 (исполнение 3.М) необходимо заново создать его парные связи.

10. Обновление ПО сетевых устройств версии 3.9.3 (класс КС) под управлением ЦУС версии 3.9.3 (исполнение 3.М3) выполняется только при локальном управлении.

11. После обновления комплекса с версии 3.М2, для обеспечения максимальных показателей производительности L3VPN на платформе IPC-3000F (S021) с ОЗУ 4 Гбайт следует использовать 12 потоков шифрования, для платформ с ОЗУ 16 Гбайт — 14 потоков шифрования.

4.3. Резервирование

1. При переключении с основного устройства на резервное возможна потеря трафика, передаваемого по сети через данный кластер.

2. Нельзя настроить более одного PPPoE-интерфейса на кластере сетевого устройства.

3. Особенности работы кластера КШ или КК. Отсутствует возможность подключения резервного устройства к основному через промежуточный маршрутизатор.

- 4.** Особенности работы кластера КШ или КК в режиме прохождения пакетов с IP-опциями. Для корректной работы данный режим должен быть включен средствами локального управления по отдельности на обоих сетевых устройствах кластера.
- 5.** При определении состояния кластера кроме физических учитываются и его дочерние VLAN-интерфейсы. При отказе физического интерфейса основного КШ все его дочерние VLAN-интерфейсы также будут считаться отказавшими.
- 6.** Особенность восстановления работы основного КШ в кластере после изменения IP-адреса у связанного КШ. Если после включения основного КШ отсутствует трафик в другие защищаемые сети, перезагрузите кластер с помощью программы управления.
- 7.** При изменении параметра "Время ожидания ответа от активного сетевого устройства" на кластере необходимо локально загрузить конфигурацию на обе ноды кластера.
- 8.** Смена значения MTU в шифраторе на кластере КШ произойдет только после перезагрузки устройства.
- 9.** Удаление отключенного агрегированного интерфейса в кластере КШ не выполняется на КШ, активном в момент удаления интерфейса.
- 10.** Удаление нескоммутированного интерфейса на кластере невозможно. Для удаления необходимо сккоммутировать интерфейс перед удалением. Для восстановления работы проблемного кластера необходимо перезагрузить основное устройство кластера.
- 11.** Не рекомендуется использовать в кластере LACP с коммутатором с включенной функцией блокировки портов, в связи с особенностью реализации кластера.
- 12.** Нельзя использовать маску /31 для интерфейсов резервирования кластера.
- 13.** Особенности работы кластера КШ или КК. Синхронизация логических MAC-адресов сетевых интерфейсов основной и резервной нод кластера с физическим MAC-адресом сетевого интерфейса основной ноды происходит только в случае "холодной" перезагрузки кластера (обе ноды выключены, сначала включается основная, затем резервная).
- 14.** Резервный узел должен быть отключен в случае изменения следующих настроек при локальном управлении СУ:
 - изменение адреса активного ЦУС;
 - настройка PPP-соединений;
 - настройка отладочного журнала;
 - настройка доступа удаленного терминала;
 - настройки коммутации (отключение автоматического поиска PMTU для канала управления, отключение автоматического поиска PMTU для канала VPN, настройка MSS);
 - изменение внешнего адреса СУ.

При первом обращении СУ к ЦУС вышеуказанные настройки будут заменены на заданные в БД ЦУС.

- 15.** Для синхронизации БД ЦУС необходимо обеспечить доступность между ЦУС через внутренние интерфейсы. IP-адреса этих интерфейсов должны быть в списках альтернативных адресов соответствующих ЦУС.
- 16.** Удаление из агрегации одного интерфейса в кластере приводит к тому, что на резервном узле не обновляется конфигурация MAC-адресов с основного узла. При удалении интерфейсов из агрегации необходимо перезагрузить узлы кластера. Резервный узел необходимо отключить и включить после успешной перезагрузки основного узла.

4.4. Центр управления сетью

- 1.** Работа ЦУС за КШ не поддерживается.
- 2.** Размер журнала на ЦУС должен быть не менее суммы значений, определяющих размеры журналов на каждом КШ.
- 3.** 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 ЦУС с восстановленной базой данных ЦУС невозможна.
- 4.** При удалении одного из внешних адресов ЦУС автоматическое оповещение КШ не осуществляется. Необходимо выполнить принудительное обновление конфигурации всех КШ сети средствами централизованного управления.

- 5.** Размер журнала на ЦУС должен быть не менее суммы значений, определяющих размеры журналов на каждом КШ.
- 6.** Особенность работы ЦУС при включенном PPPoE. При отсутствии адреса на внешнем интерфейсе КШ с ЦУС отображается в программе управления как отключенный. Причиной отсутствия адреса может быть, например, сбой в работе сервиса PPPoE во время подключения КШ с ЦУС к RAS-серверу. В этом случае убедитесь в корректной работе сервера. ЦУС должен иметь статический IP-адрес, получаемый с RAS-сервера.
- 7.** Работа ЦУС за КШ в режиме Multi-WAN Failover не поддерживается.
- 8.** Работа ЦУС за КШ в режиме Multi-WAN "Балансировка трафика" не поддерживается.
- 9.** При удалении одного из внешних интерфейсов ЦУС автоматическое оповещение КШ не осуществляется. Необходимо выполнить принудительное обновление конфигурации всех КШ сети средствами централизованного управления.
- 10.** После обновления ПО необходимо выполнить дополнительную настройку правил трансляции типа "Входящий" в соответствии с документацией на комплекс.
- 11.** До обновления ПО КШ возможна некорректная работа исходящих правил трансляции.
- 12.** После изменения IP-адреса на внутреннем интерфейсе КШ предыдущей версии необходима перезагрузка КШ новой версии.
- 13.** После обновления ПО ЦУС конфигурация сетевого устройства сохраняется только в формате новой версии.
- 14.** Перед обновлением ПО требуется в обязательном порядке удалить правила трансляции 1:1, в которых источником является сетевой объект с маской 32 (хост), а трансляция выполняется на адрес внешнего интерфейса КШ. В противном случае при обновлении ПО возникает неисправимая ошибка.
- 15.** Перед импортом БД ЦУС необходимо убедиться, что интерфейсы на каждом из КК, входящие в один и тот же виртуальный коммутатор, имеют одинаковый размер MTU.
- 16.** Особенность восстановления конфигурации ЦУС из резервной копии. При выполнении процедуры восстановления на экране появляется сообщение "Для корректной работы КШ с ЦУС требуется наличие лицензии обновления". Так как в данной версии восстановление из резервной копии не считается обновлением, наличие упомянутой лицензии не требуется. Закройте окно сообщения и продолжите процедуру восстановления.
- 17.** При работе в режиме Multi-WAN Failover или "Балансировка трафика" рекомендуется создать правило фильтрации для прохождения трафика от АРМ администратора комплекса к внутреннему интерфейсу ЦУС. Это правило должно находиться в начале списка правил фильтрации. В противном случае при добавлении новых правил фильтрации возможна потеря управления комплексом.
- 18.** При установленных парных связях КШ с ЦУС и других КШ (к примеру, при использовании для VPN) после обновления ПО и восстановления БД ЦУС из резервной копии в журнале НСД КШ с ЦУС в течение нескольких минут могут регистрироваться события о неверной имитовставке в трафике с адресов КШ, с которыми у этого КШ с ЦУС есть парная связь.
- 19.** Резервирование базы данных ЦУС возможно только для ЦУС с одинаковой версией ПО.
- 20.** После загрузки в БД ЦУС конфигурационного файла, содержащего достаточно большое количество криптошлюзов, подключение ПУ ЦУС к ЦУС и обмен данными между ними могут происходить с задержкой.
- 21.** Особенность обновления ЦУС в сети, связанной со сторонними криптографическими сетями. В каждой из связанных сетей после обновления ЦУС необходимо пересоздать его парные связи.
- 22.** Поддерживается построение шифрованного соединения со сторонними криптографическими сетями под управлением АПКШ "Континент" версий 3.9.2.4443, 3.9.2.3759, 3.9.1.2732, 3.9.0.3338, 3.9.0.2808, 3.7.7.671.
- 23.** Особенность сохранения резервной копии конфигурации ЦУС и ее восстановления. Для успешного сохранения конфигурации все задания должны быть выполнены и очередь заданий должна быть пустой. В противном случае сетевые устройства, у которых это требование не соблюдено, при восстановлении конфигурации будут автоматически выведены из эксплуатации. Невыполненные и стоявшие в очереди задания будут удалены. Для восстановления работы сети такие сетевые устройства необходимо ввести в эксплуатацию вручную.
- 24.** Не рекомендуется использовать ix-интерфейсы для управления ЦУС на аппаратных платформах R300/R550. Подключение работает нестабильно.

4.5. Сетевые устройства

1. При каждом запуске сетевого устройства необходимо локально загрузить комплект ключей и ввести пароль, заданный при сохранении ключей на носителе.
2. Нельзя использовать протоколы динамической маршрутизации на сетевом устройстве с IPv6-адресами.
3. Настройка "Автоматический поиск MTU в канале управления", выполняемая при настройке общих параметров сетевого устройства, распространяется только на управляющий трафик от данного устройства к ЦУС.
4. Режим DHCP-ретранслятора на КШ. Максимальное допустимое количество логических интерфейсов, на которых настроен DHCP-ретранслятор, составляет:
 - платформа S115 (IPC-25) – 5;
 - платформы 92E3, S102 (IPC-100) – 4;
 - платформа S021 (IPC-1000F, IPC-3000F) – 38.
5. Особенности работы кластера КШ. Отсутствует возможность подключения резервного устройства к основному через промежуточный маршрутизатор.
6. Особенности работы КШ. При переключении с основного устройства на резервное возможна потеря трафика, передаваемого по сети через данный кластер.
7. Особенности рассылки правил фильтрации на КШ. Если в группе сетевых объектов, включающей защищенные сети различных КШ, добавлен или удален один объект, то правила фильтрации загружаются на все КШ, защищенные сети которых перечислены в этой группе.
8. Особенности работы кластера КШ в режиме прохождения пакетов с IP-опциями. Для корректной работы данный режим должен быть включен средствами локального управления по отдельности на обоих устройствах кластера.
9. Особенности работы КШ. Если на интерфейс КШ поступает IP-пакет или Ethernet-кадр, размер которого превосходит установленное значение MTU для данного интерфейса, то такой пакет или кадр будет отброшен.
10. Включение полной регистрации сетевого трафика снижает производительность КШ.
11. Одновременная работа динамической маршрутизации и режима Multi-WAN Failover не поддерживается.
12. Нельзя настроить более одного PPPoE-интерфейса на кластере КШ.
13. Режим Multi-WAN Routing Table не может работать на КШ с двумя и более PPP-интерфейсами.
14. Возможна самопроизвольная перезагрузка КШ с PPP-интерфейсом при недоступном RAS-сервере.
15. На 10-гигабитных интерфейсах поддержка QoS отсутствует.
16. Особенность работы криптокоммутатора. В зашифрованный пакет подставляется ToS из исходного пакета. При этом настройка ToS, заданная в свойствах класса трафика, игнорируется.
17. Если в процессе работы СУ произошло искажение файлов на жестком диске, что проявилось как отказ VPN-каналов, необходимо вновь создать парную связь.
18. Особенности рассылки правил фильтрации на КШ. Если в группе сетевых объектов, включающей защищенные сети различных КШ, добавлен или удален один объект, то правила фильтрации загружаются на все КШ, защищенные сети которых перечислены в этой группе.
19. Включение полной регистрации сетевого трафика снижает производительность сетевых устройств.
20. Протокол PPP поддерживается только в режиме PPPoE.
21. Использование режима Multi-WAN при подключении сетевого устройства через модем может приводить к самопроизвольному переключению каналов связи. Причиной является ложный отрицательный результат тестирования канала при высокой загрузке.
22. Режим Multi-WAN Routing Table не может работать на сетевом устройстве с двумя и более PPP-интерфейсами.
23. Просмотр средствами локального управления таблицы состояния невозможен, так как фильтрация Ethernet-кадров на устройстве не поддерживается.

24. Если в сетевое устройство загружена некорректная конфигурация, при включении такого устройства появляется ошибка вида "Завершился/etc/rc.running/Agentserver". В этом случае необходимо заново в ПУ ЦУС сохранить конфигурацию устройства на внешний носитель и далее локально загрузить ее в устройство.

25. В сетевых устройствах на платформе S021 возможно раннее срабатывание сторожевого таймера в ПАК "Соболь", вследствие чего инициализация устройства останавливается на значении "36" и переходит в цикл от "15" до "36". В этом случае необходимо увеличить время срабатывания сторожевого таймера в настройках ПАК "Соболь".

26. Срабатывание датчика вскрытия корпуса, вызванное нарушением условий транспортировки или попыткой вскрытия корпуса сетевого устройства, приводит к отображению ошибки "Warning! Chassis has been opened. Press F1 to Resume" (вид ошибки может отличаться в зависимости от платформы). Для сброса ошибки или отключения сигнализации о вскрытии корпуса выполните следующее:

- Перезагрузите сетевое устройство и войдите в BIOS. При входе в BIOS укажите пароль администратора (если пароль администратора не назначался, пароль по умолчанию — 123456).
- В BIOS Setup перейдите на вкладку "Security".
- У параметра "Chassis intrusion" выберите значение "Reset" (для сброса ошибки) или "Disabled" (для отключения сигнализации).
- Сохраните настройки и выйдите из BIOS Setup, используя клавишу <F10>.
- Нажмите клавишу <Enter> и перезагрузите сетевое устройство.

27. Указание в настройках ПАК "Соболь" некорректной версии криптографической схемы приводит к ошибкам и следующим сообщениям:

- После загрузки конфигурации сетевого устройства появляется сообщение "Ошибка чтения идентификатора...".
- После перезагрузки сетевого устройства появляется сообщение ПАК "Соболь" "Нарушена целостность внутренних структур. Необходима переинициализация платы".

Для исправления ошибки необходимо переинициализировать ПАК "Соболь" и указать корректную версию криптографической схемы — 2.0.

Внимание! Для выполнения данной процедуры необходимо вскрытие корпуса сетевого устройства. Разрешение на вскрытие корпуса получают в службе вендорской поддержки ООО "Код Безопасности".

28. Если по каким-либо причинам в сетевое устройство не была загружена конфигурация, а в настройках ПАК "Соболь" задан автоматический вход в систему, после запуска устройства и появления сообщения "Успешный запуск" появляется сообщение "Перезагрузка через 15 сек.". В этом случае необходимо перезагрузить сетевое устройство, предъявив идентификатор администратора, и выполнить инициализацию сетевого устройства с загрузкой конфигурации.

29. Если на КШ выполнить следующие настройки Multi-WAN:

- установить режим балансировки трафика между внешними интерфейсами;
- в политике балансировки трафика для заданного класса трафика установить значение "Маршрут по умолчанию" для параметра "Канал шифрованного трафика";

то в случае отказа внешнего интерфейса, через который должен проходить зашифрованный трафик, он будет направлен по доступному WAN-каналу. Парный КШ будет обнаружен вне зависимости от канала шифрованного трафика, указанного в политике балансировки трафика.

30. Особенность настройки QoS. Для очереди по умолчанию с типами приоритизации CBQ и HFSC недопустимо значение "0%" в параметрах "Полоса пропускания" и "uprperlimit" соответственно.

31. После включения/перезагрузки СУ с подсоединенным через последовательный порт компьютером интерфейс ПАК "Соболь" на русском языке отображается некорректно.

32. На сетевых устройствах (КШ, КК) работа более чем одного PPPoE-интерфейса не гарантируется.

33. После перезагрузки КШ не осуществляется отправка SNMP trap получателю, маршрут к которому получен по протоколу динамической маршрутизации.

34. При использовании в качестве получателя SNMP trap хоста, доступного по маршрутам динамической маршрутизации, доставка trap не гарантируется. Рекомендуется использовать хост, доступный напрямую или по статическим маршрутам.

35. Резервный ЦУС не синхронизируется с основным при включенном методе NAT.

36. Нельзя использовать один интерфейс одновременно в качестве интерфейса агрегации и в качестве родительского интерфейса для PPPoE-соединения.

- 37.** На КШ не срабатывает QoS при исходящем методе NAT.
- 38.** Механизм контроля приложений не блокирует подключение TeamViewer.
- 39.** Перед настройкой в качестве SPAN-порта сетевой интерфейс должен быть предварительно скоммутирован и должен пройти автоматическое согласование интерфейса на активном оборудовании.
- 40.** Для успешной установки конфигурации на КШ с несколькими интерфейсами агрегации после перестановки интерфейсов между ними необходимо сохранить конфигурацию сразу после извлечения интерфейса из первой агрегации.
- 41.** Если в настройках криптокоммутатора установлен запрет на прохождение STP-пакетов, это не влияет на прохождение в L2VPN кадров протокола RPVST (cisco-based rstp).
- 42.** В текущей версии нельзя назначать SPAN-порт на агрегированный интерфейс в режиме LACP.
- 43.** При изменении пароля в openconsole можно задать пароль длиной только в 40 символов.
- 44.** Если в конфигурации внешней криптографической сети, экспортируемой из версии 3.9.x, содержится КШ, доступный по нескольким IP-адресам, то при импорте такой конфигурации в сеть версии 3.7.7.671, данный КШ добавляется с первым адресом из списка первого внешнего интерфейса.
- 45.** КШ со значением приоритета "Нет" считается КШ с наивысшим приоритетом.
- 46.** На порте агрегации запрещено использовать тип интерфейса SPAN.
- 47.** При построении туннеля с использованием криптоускорителей, между которыми расположен маршрутизатор, первые октеты IP-адресов внешних интерфейсов криптоускорителей на концах туннеля должны различаться.
- 48.** Кириллические символы в tui при доступе через SSH отображаются некорректно.
- 49.** Не допускается использование для хранения конфигурации и ключей КШ USB-флеш-накопителя, на котором ранее был записан UEFI-образ для установки комплекса.
- 50.** Сетевые устройства версии 3.9.3 (исполнение 3.M3) могут устанавливать парные связи с сетевыми устройствами версий 3.M2 и 3.9.3 (класс КС). Сетевые устройства версий 3.M2 и 3.9.3 (класс КС) парные связи между собой устанавливать не могут.
- 51.** При использовании КШ версии 3.9.1 под управлением ЦУС класса КВ необходимо отключить усиленную фильтрацию до обновления КШ до версии 3.9.3 класса КС.
- 52.** Невозможно включить изолированный режим на КШ версии 3.9.1 под управлением ЦУС класса КВ. Необходимо обновить КШ до версии 3.9.3 класса КС.
- 53.** Для избежания возникновения асимметричной маршрутизации в настройках bgr.conf КШ, анонсирующих ЗС, необходимо настроить редистрибуцию с метрикой, равной приоритету канала через этот КШ.
- 54.** Запрещается использовать в именах сетевых устройств следующие спецсимволы: < > & " ' '.
- 55.** На сетевых устройствах версии 3.M2 под управлением ЦУС версии 3.9.3 (исполнение 3.M3) нельзя прерывать дистанционную смену ключей из контекстного меню. Для отмены задания на дистанционную смену ключей, необходимо дождаться тайм-аута, который был выставлен при инициации смены ключей из ПУ ЦУС.
- 56.** При нескольких неудачных попыток входа, согласно политике аутентификации, локальное меню узла блокируется для всех пользователей, включая ПАК "Соболь".

4.6. Программа управления ЦУС

- 1.** Установку и удаление ПУ ЦУС может выполнить только пользователь, наделенный правами локального администратора данного компьютера.
- 2.** После удаления ПУ ЦУС или других компонентов, входящих в состав подсистемы управления, необходимо выполнить перезагрузку компьютера. Для этого в процедуре удаления следует выбрать вариант завершения с немедленной перезагрузкой.
- 3.** Перед установкой программы управления новой версии необходимо удалить имеющуюся на компьютере программу управления предыдущей версии и перезагрузить компьютер.
- 4.** При удалении сетевого объекта появляется сообщение об одновременном удалении правил фильтрации, использующих этот сетевой объект. При подтверждении удаления будут удалены только те правила фильтрации, которые используют этот объект непосредственно. Правила фильтрации для групп, содержащих удаляемый объект, удалены не будут.

- 5.** При удалении или изменении правила фильтрации с контролем состояния соединения, ранее установленные в соответствии с удаленным правилом соединения, не закрываются. Для их принудительного закрытия следует выполнить команду "Очистка таблицы состояний соединений". При изменении таких правил фильтрации теперь в ПУ ЦУС выдается запрос на принудительную очистку таблицы состояния соединений, с которым можно либо согласиться, либо нет.
- 6.** Управление ЦУС текущей версии возможно только с помощью ПУ той же версии.
- 7.** В ПУ ЦУС не отображается признак "КШ за NAT", если на криптошлюзе настроен внешний интерфейс PPPoE и между криптошлюзом и ЦУС на промежуточном роутере работает NAT.
- 8.** Особенность совместной работы механизмов multicast и VLAN. Для корректной передачи multicast-трафика получателям в виртуальной локальной сети необходимо сначала настроить VLAN-интерфейс, а только затем параметры групповой передачи данных.
- 9.** При использовании одного порта для нескольких классов трафика, статистика входящих пакетов и объема входящего трафика для этих классов будет суммироваться и отображаться в первом из этих классов трафика.
- 10.** Особенности работы режима ip multicast-routing (групповая передача данных):
 - При использовании данного режима трафик всегда зашифровывается.
 - Трафик после расшифрования передается только в те защищенные сети, из которых был послан запрос на видеопередачу.
- 11.** Отображаемое в программе управления время отказа канала VPN отсчитывается от следующих событий:
 - прохождение последнего пакета по парной связи в сторону докладывающего сетевого устройства;
 - создание парной связи, если пакеты не проходили;
 - включение КШ, если связь создана ранее и пакеты не проходили.
- 12.** Если в правиле фильтрации используются группы с большим количеством объектов или значительное количество сервисов, рекомендуется использовать режим quick. В противном случае возможно снижение производительности межсетевого экрана.
- 13.** Изменена интерпретация диапазона портов «><» в сервисе. Теперь граничные условия входят в диапазон (включающий диапазон). При обновлении ПО с предыдущих версий необходимо скорректировать границы диапазона.
- 14.** В текущей версии комплекса в правиле трансляции адресов NAT рекомендуется указывать каждый сервис отдельной строкой. Если задать групповой сервис, то трансляция будет выполнена только для первого сервиса группы.
- 15.** В текущей версии процедура резервного копирования для больших сетей может привести к временной визуальной недоступности сетевых устройств.
- 16.** В ПУ ЦУС отсутствует сигнализация о выходе из строя одного из интерфейсов, входящих в агрегированный интерфейс типа LACP.

4.7. Агент ЦУС

- 1.** Установку агента (вместе с ПУ ЦУС или отдельно) должен осуществлять пользователь, наделенный правами:
 - локального администратора данного компьютера;
 - администратора используемой базы данных.
- 2.** Операционная система компьютера, на который устанавливается агент или ПУ с агентом, должна поддерживать русский язык. В региональных настройках этого компьютера должны быть указаны язык и региональные настройки России.
- 3.** Перед настройкой расписания агента из ПУ ЦУС убедитесь, что служба "Агент ЦУС" работает. При остановленной службе "Агент ЦУС" настройка агента из ПУ невозможна.
- 4.** Особенности работы агента и КШ с ЦУС при их совместном размещении в защищенной сети другого КШ. В этом случае необходимо создать правила фильтрации, разрешающие обмен пакетами между агентом и СД. Правила создают для КШ, в защищенной сети которого размещены агент и КШ с ЦУС, а также для всех КШ с СД. В этих правилах необходимо использовать сервис со следующими параметрами:
 - протокол – tcp;
 - порт источника – any;
 - порт назначения – 4431.

Эти правила позволяют агенту получать журналы с серверов доступа, расположенных на других КШ. При отсутствии в сети серверов доступа правила создавать не требуется.

5. Локальная учетная запись пользователя Windows для подключения агента к СУБД должна иметь права на изменение реестра (как минимум входить в группу "Опытные пользователи"). В противном случае невозможно сохранение настроек расписания.

6. Особенности работы агента совместно с СУБД MS SQL 2005. При наличии проблем с автоматическим запуском агента необходимо в свойствах службы агента указать зависимость от SQL Server (MSSQLSERVER).

7. Убедитесь, что каталог, задаваемый для сохранения резервной копии конфигурации ЦУС, действительно доступен учетной записи сервиса "агент ЦУС". Для этого после автоматического сохранения по расписанию проверьте наличие сохраненной копии в указанном каталоге.

4.8. Программа просмотра журналов

- 1.** Для доступа к ППЖ необходимо предъявить ключевой носитель с ключами администратора ЦУС.
- 2.** Функция очистки журнала доступна только ролям "Главный администратор" и "Аудитор".
- 3.** Если при просмотре журналов отображается сообщение об ошибке, рекомендуется повторить запрос к базе данных. Для этого используйте кнопку "Обновить" на панели инструментов ППЖ.
- 4.** Если при настройке параметров соединения с базой данных появляется сообщение об отсутствии SQLDMO.DLL, то необходимо установить клиентские утилиты MS SQL.
- 5.** После переинициализации ЦУС необходимо очистить базу данных для хранения регистрационных журналов или создать ее заново. Это требуется для корректного отображения регистрационной информации.
- 6.** Особенности отображения пакетов в ППЖ при изменении разрешающего правила фильтрации после обновления конфигурации КШ. Пакеты с такого КШ некоторое время отображаются как обработанные по исходному неизмененному правилу. Это продолжается до тех пор, пока агент в очередной раз не заберет журналы с КШ. После этого пакеты отображаются верно, как обработанные по измененному правилу.

Компания "Код Безопасности"

Почтовый адрес:	115127, Россия, Москва, а/я 66
Телефон:	8 495 982-30-20
Факс:	8 495 744-29-31
E-mail:	info@securitycode.ru
Сайт:	https://www.securitycode.ru