Аппаратно-программный комплекс шифрования "Континент" Версия 3.9 Комментарии к версии 3.9.3.3887

Документ содержит описание основных возможностей, особенностей и ограничений применения изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.9" (далее — комплекс, АПКШ "Континент"), которые необходимо учитывать при эксплуатации комплекса.

Список сокращений

АП	Абонентский пункт
АПМДЗ	Аппаратно-программный модуль доверенной загрузки
БД	База данных
ВКС	Внешние криптографические сети
ДА	Детектор атак
КК	Криптографический коммутатор
КС	Контрольная сумма
КШ	Криптографический шлюз
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ППЖ	Программа просмотра журналов
ПУ	Программа управления
ПУ СД	Программа управления сервером доступа
ПУ ЦУС	Программа управления ЦУС
РКН	Роскомнадзор
РМ	Рабочее место
СД	Сервер доступа
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
СУ	Сетевое устройство (КШ, КК)
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр
ЦУС	Центр управления сетью
CRL	Certificate Revocation List
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Оглавление

1. Размещение программного обеспечения и документации на компакт-дисках

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
\Packages	Компоненты ОС для работы комплекса
Служебные программы	
\Tools\Код безопасности\ServiceTool	Каталог установки служебных программ
\Tools\Код безопасности\DiagnosticTool	Каталог установки диагностических программ
\Tools\Код безопасности\csum2020	Утилита для расчета КС
integrity.xml	Файл с эталонными КС дистрибутива
integrity-check.bat	Скрипт для проверки КС дистрибутива под Windows
integrity-check.sh	Скрипт для проверки КС дистрибутива под Linux
Описание версии	
\Version.TXT	Файл с описанием версии ПО АПКШ "Континент"

1.2. Диск 2

ФСБ

Каталог	Содержимое
Документация АПКШ "Континент"	
Эксплуатационная документация\ Continent - Access Server – Admin Guide.pdf	АПКШ "Континент". Версия 3.9. Руководство администратора. Сервер доступа
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

Каталог	Содержимое
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
Техническая документация\ RU.88338853.501430.022 ТУ - Технические 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

ФСТЭК

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 - IDS – Admin Guide.pdf	АПКШ "Континент". Версия 3.9. Руководство администратора. Обнаружение вторжений
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 - ФО Приложение 1.pdf	АПКШ "Континент". Версия 3.9. Формуляр. Приложение 1
Техническая документация\ RU.88338853.501430.022 30-2 - ФО Приложение 2.pdf	АПКШ "Континент". Версия 3.9. Формуляр. Приложение 2
Техническая документация\ RU.88338853.501430.022 ТУ - Технические условия.pdf	АПКШ "Континент". Версия 3.9. Технические условия

1.3. Диск 3*

Каталог	Содержимое
Документация АПКШ "Континент"	
\БРП	База решающих правил
Continent – Import of IPS protections – Admin Guide.pdf	АПКШ "Континент". Версия 3.9. Руководство администратора. Загрузка базы решающих правил

* Диск поставляется только с системой обнаружения вторжений.

2. Изменения и новые возможности

2.1. Версия 3.9.3.3887

1. Реализована функция информирования об истечении срока действия ключей парной связи и сертификатов для ВКС по электронной почте (экспериментальный функционал).

2. Обновлен модуль доверенной загрузки.

3. Реализована функция контроля целостности установленного дистрибутива в меню инсталлятора.

4. Реализована функция контроля целостности ПУ ЦУС и ПУ СД без использования СЗИ Secret Net Studio.

5. Добавлена поддержка аппаратной платформы IPC-3000F40.

6. Реализована возможность изменения приоритета правил NAT в ПУ ЦУС методом Drag-and-drop.

7. Реализована функция сортировки и поиска в списке пользователей в ПУ СД.

8. Реализована возможность смены ключа хранения на КШ/КК и ЦУС без переинициализации.

9. Реализован инженерный режим в ПУ ЦУС для более тонких настроек сетевых устройств.

10. Добавлена возможность использования адреса интерфейса вместо адреса трансляции в правилах.

11. Добавлена поддержка работы высокопроизводительного криптографического коммутатора с использованием DAC-кабеля 40G->4x10G.

12. Для ЦУС версии 3.9.3 (класс КВ) реализована возможность управления сетевыми устройствами версии 3.9.3 (класс КС).

13. Для агента обновлений БРП добавлена возможность работы без использования "Континент-АП" 3.7.

14. Добавлена опция аутентификации на КШ/КК до старта СКЗИ.

15. Реализована возможность работы аппаратных платформ IPC-10/50, IPC-R10/R50, IPC-R300/R550 без АПМДЗ.

16. Добавлена возможность трансляции портов резервного провайдера с основного в режиме Multi-WAN.

17. Реализована поддержка внешней СУБД Postgres Pro.

18. Добавлена возможность экспорта журналов через syslog.

2.2. Версия 3.9.2.4443

1. Повышена стабильность работы СД.

2. Исправлены ошибки в работе.

2.3. Версия 3.9.2.3759

1. Добавлена возможность указать диапазон портов во входящем правиле NAT.

2. Добавлена возможность выбора версии ПО при создании нового устройства.

3. Реализована возможность доступа к защищаемой сети, находящейся одновременно за несколькими КШ.

4. Реализована возможность задать в локальном меню КШ время устаревания подобранного MTU на канале (PMTU aging).

5. Реализована возможность настройки опций на DHCP-сервере, включая настройку пользовательских опций.

6. Реализована возможность использовать аутентификацию при настройке NTP-сервера при задании времени на ЦУС.

7. Обновлен интерфейс агента ЦУС и СД.

8. В агенте ЦУС и СД реализована возможность автоматического создания резервных копий БД сервера доступа по расписанию.

9. Реализована возможность приоритизации трафика на основе меток ToS на КШ и КК.

10. Добавлены утилиты для упрощения развертывания сетей, обеспечивающие:

- экспорт конфигураций и ключей сетевых устройств;
- экспорт и импорт XML-файлов, содержащих параметры сетевых устройств и сетевых объектов.

11. Добавлена возможность создания исключений для профилей усиленной фильтрации.

12. Установлен минимальный интервал диагностики доступности контрольных точек в Multi-WAN.

13. Производительность МЭ на старшей платформе увеличена до 20 Гбит/с.

14. Добавлена возможность просмотра адреса и статуса соединения КШ с ЦУС в локальном меню КШ.

15. Добавлена новая версия аппаратной платформы IPC-3000FC с производительностью шифрования 40 Гбит/с.

2.4. Версия 3.9.1.2732

1. Реализованы контроль СУ комплекса по протоколу SNMP и централизованное управление параметрами SNMP.

2. Разработан коннектор "Континент-Skybox" для работы с сервером Skybox Security.

3. В ЦУС комплекса текущей версии появилась возможность создавать СУ АПКШ "Континент" предыдущих версий, начиная с версии 3.7.

4. Реализовано автоматическое переключение в кластере при использовании VLAN.

5. В комплексе реализован групповой экспорт пользовательских сертификатов из СД.

6. В ПУ ЦУС появилась возможность проведения групповых операций с СУ.

7. Восстановлена корректная работа с OID 1.3.6.1.2.1.2.2.1.16. "ifOutOctets".

8. На криптокоммутаторе появилась возможность включения балансировки соединений по ядрам на основе заголовков L3-пакетов.

9. Используемые в комплексе БРП оптимизированы в связи с обновлением SNORT.

10. В СД появилась поддержка работы с сертификатами, выпущенными внешним УЦ, а также поддержка возможности проверки отозванных сертификатов по CRL.

11. Оптимизирована работа ЦУС с большим количеством КШ/КК, повышена его стабильность и производительность.

12. Увеличена скорость подключения ПУ к ЦУС с большим количеством КШ/КК.

13. Улучшен диалог создания парных связей.

14. На КК добавлена возможность распределять трафик по шифраторам на основе L3-заголовков пакетов.

15. Добавлена возможность менять MSS трафика, проходящего через КК.

16. Оптимизирована отправка журналов от КШ на ЦУС.

17. Реализовано резервирование ЦУС.

18. Добавлена возможность агрегации интерфейсов по протоколу LACP (802.3ad).

19. Реализован доступ к КШ/КК по протоколу SSH.

20. Внедрено централизованное управление локальными администраторами.

21. Появилась возможность выполнения групповых операций над КШ/КК.

22. Добавлена возможность создания отладочного журнала КШ/КК средствами ПУ.

23. Альтернативные узлы КШ/КК не требуют доступности ЦУС.

24. Выполнена поддержка Jumbo frame (MTU 9000 байт) на КШ и КК.

25. Появилась возможность настройки параметров потоков шифрования.

26. Расширены опции DHCP-сервера.

27. Разработан новый интерфейс ПУ.

28. Уменьшено время переключения в кластере (до 2 секунд).

29. Добавлена возможность увеличения размера таблицы коммутации порта КК.

30. Добавлена локальная настройка прохождения специальных протоколов на КК (LACP, STP, 802.1x).

31. Увеличена стабильность и производительность работы сетевых устройств за счет перехода на новую версию базовой ОС и архитектуру x86_64.

32. В криптошлюзах реализована поддержка механизма расширения для DNS (EDNS).

33. Появилась возможность размещать защищаемую сеть за двумя и более КШ.

3. Ограничения поддержки аппаратных и программных средств

1	Ключевые устройства	Сетевые устройства (КШ, КК)	USB-флеш-накопитель
		ПУ ЦУС Агент ЦУС и СД ПУ СД	• USB-флеш-накопитель; • USB-ключ eToken PRO (Java); • смарт-карта eToken Pro (Java) с USB-считывателем Athena ASEDrive IIIe USB V2; • Рутокен S; • ПАК "Соболь" 3.0/3.1/3.2; • iButton DS1994/DS1995/DS1996; • JaCarta (только на РМ администратора сервера доступа для соединения ПУ СД с СД)
2	Операционная система	РМ администратора	• Windows Server 2012 R2 Rollup Update; • Windows Server 2016; • Windows Server 2019; • Windows 8.1 x86/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	3.9.1.2732, 3.9.1.6495, 3.9.2.3759, 3.9.2.4443
		Обновление предыдущих версий сетевых устройств и ЦУС	3.9.1.2732, 3.9.1.6495, 3.9.2.3759, 3.9.2.4443
4	СКЗИ "КриптоПро CSP" СКЗИ "Код Безопасности CSP"		4.0, 5.0 Не ниже 4.0.970.0
5	Аппаратные платформы (КШ, КК, ЦУС, СД)	IPC-10	S088 (жесткий диск не менее 4 Гбайт)
			LN-010A
		IPC-25	S115
			92D9 (жесткий диск не менее 4 Гбайт)
		IPC-50	LN-010C
		IPC-100	S102
			92E3 (жесткий диск не менее 4 Гбайт)
		IPC-400	S021
		IPC-500	LN-015B
		IPC-500F	LN-015C
		IPC-600	DV-030A
		IPC-800F	DV-030B
		IPC-1000	S021
		IPC-1000F	S021
			DV-031B
		IPC-1000F2	S021
		IPC-1000NF2	DV-031F
		IPC-3000F	S021
			LN-021
		IPC-3000F LE	LN-021
		IPC-3000FC	LN-021A (только КК)
		IPC-3000FC-40G	LN-021A (только КК)
		IPC-3000FC-H	LN-021A (только КК)
		IPC-3000F40	LN-021E

		IPC-3000NF2	LN-021E
		IPC-3000NF2 LE	LN-021E
		IPC-3020F	S021
		IPC-3034	S021
		IPC-3034F	S021
		IPC-R10	SC R15
		IPC-R50	SC R15
		IPC-R300	SC R300
		IPC-R550	SC R300
		IPC-R800	SC R1000
		IPC-R1000	SC R1000
		IPC-R1000NF2	SC R1000
		IPC-R3000	SC R1000
6	Аппаратные платформы (ДА)	IPC-25	S115 (ОЗУ 8 Гбайт)
		IPC-50	LN-010C
		IPC-100	S102 (ОЗУ 8 Гбайт)
		IPC-400	S021 (ОЗУ 16 Гбайт)
		IPC-500	LN-015B
		IPC-500F	LN-015C
		IPC-600	DV-030A
		IPC-800F	DV-030B
		IPC-1000	S021
		IPC-1000F	S021 (ОЗУ 32 Гбайт)
			DV-031B
		IPC-1000F2	S021 (ОЗУ 32 Гбайт)
		IPC-3000F	S021 (ОЗУ 32 Гбайт)
			LN-021
		IPC-3000F LE	LN-021
		IPC-R3000	SC R1000
		IPC-R1000	SC R1000
		IPC-R800	SC R1000
		IPC-R300	SC R300
		IPC-R550	SC R300
		IPC-R50	SC R15
7	Поддерживаемые версии БД		• MS SQL Server 2012 Express x32/x64; • MS SQL Server 2012 x32/x64; • MS SQL Server Express 2014 x32/x64; • MS SQL Server Express 2017 x32/x64; • Postgres Pro 12.15.1; • Postgres Pro 13.11.2; • Postgres Pro 14.8.2; • Postgres Pro 15.3.2 и выше
8	Поддерживаемые версии ключевых документов		РДП-006 Собственные ключи для КС1/КС2/КС3

4. Особенности работы и ограничения

4.1. Общесистемные

1. 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".

2. Особенности исправления ПО компонентов комплекса средствами программы установки. После выполнения процедуры исправления необходимо проверить правильность настроек подключения компонентов программы управления.

3. Для одинаковых IP-адресов невозможна совместная работа правил NAT и правил фильтрации с профилем усиленной фильтрации.

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".

4. 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.

5. Работа с БД ЦУС, созданной конфигуратором версии 3.7, 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.

6. Сведения о цифровой подписи отображаются некорректно в Windows Server 2019, если подпись привязана к истекшему сертификату УЦ.

7. В некоторых версиях ОС Windows сведения о цифровой подписи могут отображаться некорректно, если она привязана к истекшему сертификату УЦ.

8. 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.

9. При инсталляции ПО комплекса на аппаратную платформу IPC-100 (S021) USB-флеш-накопитель необходимо устанавливать только с тыловой стороны платформы.

10. Агент БРП не принимает ключи ЦУС с паролем более 8 символов.

11. Не происходит подключение к ПУ ЦУС/ПУ СД с ключами на токенах.

12. Для корректной работы аппаратных платформ с cdce-модемом Huawei (E3372) без установленного Соболя, необходимо после загрузки конфигурации, при инициализации КШ дважды выполнить загрузку AUTOLOAD.

13. Нельзя добавлять IP-адрес компьютера с ПУ ЦУС и ПУ СД в защищаемые сетевые объекты других КШ, с которыми ЦУС или СД строит парные связи.

4.2. Обновление

1. Поддерживается обновление ПО комплекса со следующих версий: 3.9.1.2732, 3.9.1.4695, 3.9.1.5205, 3.9.1.6495, 3.9.2.3759, 3.9.2.4443.

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. Особенности обновления ПО сетевых устройств. Если количество лицензий на обновление меньше общего количества сетевых устройств, процедуру обновления не рекомендуется выполнять с помощью групповых операций. В этом случае следует поочередно выполнить обновление на каждом сетевом устройстве. Для этого выберите требуемое сетевое устройство в списке, откройте окно "Свойства" и в разделе "Версия ПО" выполните обновление.

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

5. Особенность обновления BIOS сетевого устройства на платформе 92E3. 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".

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

7. После обновления комплекса до версии 3.9.3.3887 настройки профилей контроля приложений не сохраняются. Профили необходимо настроить заново в разделе "Центр управления сетью" ПУ ЦУС. Новые категории приложений могут не регистрироваться при работе с КШ и ДА предыдущих версий.

8. Если ранее был организован запрет на доступ к ресурсам, включенным в состав единого реестра РКН, после обновления до версии 3.9.3.3887 необходимо заново загрузить файл реестра запрещенных ресурсов в ПУ ЦУС.

9. Для обновления БРП необходимо использовать "Континент-АП" версии 4.1.725.0.

10. При удаленной загрузке файлов обновлений необходимо предварительно отключать правила трансляции, использующие диапазон портов.

11. Перед обновлением ПО ЦУС необходимо на сетевых устройствах , использующих правила трансляции с включенной опцией "Трансляция FTP", указать только TCP-сервисы.

12. Для корректной работы комплекса необходимо обновить прошивки для плат с 10G интерфейсами для платформ IPC-1000NF (DV-031F), IPC-1000F (DV-031), IPC-3000F (LN-021), IPC-3000FC (LN-021A), IPC-3000FC-40G (LN-021A), IPC-3000FC-H (LN-021A), IPC-30000F40 (LN-021E), IPC-3000NF2 (LN-021E), IPC-3000NF2 LE (LN-021E), IPC-R800 (SC R1000), IPC-R1000 (SC R1000), IPC-R1000NF2 (SC R1000), IPC-R3000 (SC R1000) с версии 4.26 до версии 7.20.

13. Для обновления КШ версий 3.9.1.2732, 3.9.2.3759, 3.9.2.4443 необходимо использовать update_legacy_release.tar.signed из состава дистрибутива версии 3.9.3.3887 (исполнение КС). Для обновления КШ версии 3.9.1.6495 UEFI перед обновлением необходимо загрузить на ЦУС файл

preupdate-3.9.1.6495.tar.signed (файл необходимо запросить в службе технической поддержки), далее загрузить его на сетевое устройство версии 3.9.1.6495 UEFI и обновить дистанционно. После этого следует выполнить обновление при помощи файла обновления update_all_release.tar.signed из состава дистрибутива версии 3.9.3 (исполнение КС).
Внимание! Если сетевое устройство было ранее обновлено с помощью файла preupdate-9.1.6495.tar.signed, повторно обновлять его с помощью этого файла нельзя.

14. При дистанционном обновлении ПО СУ с СД, работающего в режиме 3.x, версии 3.9.1 до 3.9.3 автоматически установится режим 4.x. Необходимо на обновленном СУ с СД переключить режим на 3.x в ПУ СД. При локальном обновлении СУ с СД режим 3.x не меняется.

15. Для корректной работы контроля приложений после обновления ЦУС с версии 3.9.1 до версии 3.9.3 необходимо обновить узлы до версии 3.9.3, заново создать профиль контроля приложений и привязать его к правилам фильтрации.

16. После обновления комплекса в конфигураторе БД отсутствует база данных MSSQL от предыдущей версии, для просмотра старых журналов необходимо установить на другом компьютере ППЖ той версии, в которой была создана БД, и подключиться к БД.

17. Если БД ЦУС формировалась с версии 3.7, то при обновлении комплекса необходимо восстановить БД из ПУ ЦУС.

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. 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.

5. При создании кластера сетевых устройств MAC-адреса сетевых интерфейсов аппаратных платформ IPC-10 (S088) не меняются, остаются разными для основного и резервного устройства.

6. 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.

7. 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.

8. 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.

9. При изменении параметра "Время ожидания ответа от активного сетевого устройства" на кластере необходимо локально загрузить конфигурацию на обе ноды кластера.

10. Смена значения MTU в шифраторе на кластере КШ произойдет только после перезагрузки устройства.

11. Удаление отключенного агрегированного интерфейса в кластере КШ не выполняется на КШ, активном в момент удаления интерфейса.

12. Удаление нескоммутированного интерфейса на кластере невозможно. Для удаления необходимо скоммутировать интерфейс перед удалением. Для восстановления работы проблемного кластера необходимо перезагрузить основное устройство кластера.

13. Не рекомендуется использовать в кластере LACP с коммутатором с включенной функцией блокировки портов, в связи с особенностью реализации кластера.

14. Нельзя использовать маску /31 для интерфейсов резервирования кластера.

15. 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).

16. 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.

17. При удалении приоритетного интерфейса из lagg, кластер КШ теряет связь с ЦУС.

18. При отключении основного PPPoE-интерфейса не создается маршрут на резервном кластере.

19. В режиме MW Balancer, при наличии PPPoE-интерфейса, маршрут, по умолчанию заданный в ПУ ЦУС, переписывается на маршрут через PPPoE-интерфейс.

20. На PPPoE-интерфейсе не срабатывает метод "Автоматический исходящий NAT". Для каждого PPPoE-интерфейса необходимо вручную создать правило исходящего NAT.

4.4. Центр управления сетью

1. Для ЦУС список связанных КШ должен быть пуст, если ЦУС установлен в защищенной сети другого КШ. Список связанных КШ определяют в диалоговом окне "Свойства КШ" ПУ ЦУС.

2. Размер журнала на ЦУС должен быть не менее суммы значений, определяющих размеры журналов на каждом КШ.

3. 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.

4. 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.

5. Работа ЦУС за КШ в режиме Multi-WAN Failover не поддерживается.

6. Работа ЦУС за КШ в режиме Multi-WAN "Балансировка трафика" не поддерживается.

7. При удалении одного из внешних интерфейсов ЦУС автоматическое оповещение КШ не осуществляется. Необходимо выполнить принудительное обновление конфигурации всех КШ сети средствами централизованного управления.

8. Перед импортом БД ЦУС необходимо убедиться, что интерфейсы на каждом из КК, входящие в один и тот же виртуальный коммутатор, имеют одинаковый размер MTU.

9. 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.

10. 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.

11. 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.

12. Для прохождения трафика между ЦУС, расположенным за NAT и имеющим непубличный адрес, и КШ, подключенным с помощью 3G-модема (CDCE), на КШ с ЦУС необходимо выполнить настройку STUN. Настройку выполняют средствами локального администрирования в меню "Управление". При этом если 3G-модем используется в качестве резервного канала, работа такого канала в режиме Multi-WAN не поддерживается.

13. Резервирование базы данных ЦУС возможно только для ЦУС с одинаковой версией ПО.

14. 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.

15. Особенность обновления ЦУС в сети, связанной со сторонними криптографическими сетями. В каждой из связанных сетей после обновления ЦУС необходимо пересоздать его парные связи.

16. Поддерживается построение шифрованного соединения со сторонними криптографическими сетями под управлением АПКШ "Континент" версий 3.9.2.3759, 3.9.2.4443, 3.9.1.2732, 3.9.0.3338, 3.9.0.2808, 3.7.7.671.

17. Если ранее был организован запрет на доступ к ресурсам, включенным в состав единого реестра РКН, после восстановления конфигурации ЦУС из резервной копии необходимо заново загрузить файл реестра запрещенных ресурсов в ПУ ЦУС.

4.5. Сетевые устройства

1. 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.

2. Особенности работы КШ и КК. Если на интерфейс сетевого устройства поступает IP-пакет или Ethernet-кадр, размер которого превосходит установленное значение MTU для данного интерфейса, то такой пакет или кадр будет отброшен.

3. Включение полной регистрации сетевого трафика снижает производительность сетевых устройств.

4. Одновременная работа динамической маршрутизации и режима Multi-WAN Failover не поддерживается.

5. Протокол PPP поддерживается только в режиме PPPoE.

6. 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.

7. Режим Multi-WAN Routing Table не может работать на сетевом устройстве с двумя и более PPP-интерфейсами.

8. Возможна самопроизвольная перезагрузка КШ с PPP-интерфейсом при недоступном RAS-сервере.

9. На 10-гигабитных интерфейсах поддержка QoS отсутствует.

10. Особенности работы КК. Просмотр средствами локального управления таблицы состояния невозможен, так как фильтрация Ethernet-кадров на устройстве не поддерживается.

11. Особенности настройки режима Multi-WAN "Обеспечение отказоустойчивости канала связи (Failover)". После отключения опции "Автоматический исходящий NAT" необходимо перезагрузить сетевое устройство.

12. 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.

13. 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".

14. 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.

15. 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".

16. 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.

17. Особенность настройки Multi-WAN в режиме обеспечения отказоустойчивости канала связи. Если контрольные точки находятся за маршрутизатором, на канале с наименьшим приоритетом (резервном канале) необходимо выключить режим диагностики работоспособности канала.

18. 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.

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

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

21. На аппаратной платформе IPC-10 (S088) невозможно установить MTU более 6000 байт.

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

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

24. 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.

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

26. При дистанционной смене ключа СУ версии 3.9.0 в журнале отображаются ошибки выполнения операции. В реальности ключ успешно сменится.

27. При использовании платформы IPC-3000F (LN-021) в качестве межсетевого экрана рекомендуется отключить в BIOS функцию Hyper threading.

28. Нельзя использовать один интерфейс одновременно в качестве интерфейса интеграции и в качестве родительского интерфейса для PPPoE-соединения.

29. Приоритизация трафика не работает на физических интерфейсах, входящих в lagg с настроенным QoS.

30. КК с криптоускорителем не поддерживает дефрагментацию пакетов на внешнем интерфейсе.

31. Невозможно установить QoS на ixl-интерфейсы.

32. На КК с криптоускорителем не работает функционал Port Security.

33. На КШ не срабатывает QoS при исходящем методе NAT.

34. На tun-интерфейсах неверно распределяются адреса при включении потоков обработки СД, если они заняты статическими адресами пользователей.

35. Механизм контроля приложений не блокирует подключение TeamViewer.

36. Перед настройкой в качестве SPAN-порта сетевой интерфейс должен быть предварительно скоммутирован и должен пройти автоматическое согласование интерфейса на активном оборудовании.

37. 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.

38. Блокировка атак не работает с настроенным NAT.

39. Если в настройках криптокоммутатора установлен запрет на прохождение STP-пакетов, это не влияет на прохождение в L2VPN кадров протокола RPVST (cisco-based rstp).

40. В текущей версии нельзя назначать SPAN-порт на агрегированный интерфейс в режиме LACP.

41. При изменении пароля в openconsole можно задать пароль длиной только в 40 символов.

42. 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.

43. Не приоритизируется трафик для агрегированного интерфейса.

44. КШ со значением приоритета "Нет" считается КШ с наивысшим приоритетом.

45. АП постоянно получает адрес с маской /24 при назначении адреса из динамического диапазона в режиме СД 3.x.

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. Особенность настройки коммутатора при работе с ДА. Для интерфейса мониторинга ДА необходимо на коммутаторе (например, Cisco Nexus) настроить мониторинг VLAN-интерфейса.

49. В терминальных приложениях, подключенных через SSH, при вызове некоторых пунктов меню (использующих text-based user interface) некорректно отображаются кириллические символы.

50. Весь служебный трафик в комплексе направляется в очередь по умолчанию. При заполнении очереди возможны задержки в обработке служебного трафика.

51. Не допускается использование для хранения конфигурации и ключей КШ USB-флеш-накопителя, на котором ранее был записан UEFI-образ для установки комплекса.

52. Сетевые устройства версии 3.9.3 (класс КС) могут устанавливать парные связи с сетевыми устройствами версий 3.9.1, 3.9.2 и 3.9.3 (исполнение 3.М3). Сетевые устройства версий 3.М2 и 3.9.3 (класс КС) парные связи между собой устанавливать не могут.

53. Для избежания возникновения асиметричной маршрутизации в настройках bgp.conf КШ, анонсирующих ЗС, надо настроить редистрибуцию с метрикой, равной приоритету канала через этот КШ.

54. После загрузки конфигурации и ключей на сетевое устройство происходит автоматическая перезагрузка устройства.

55. Pause-пакеты не проходят через ixl-интерфейсы платформы.

56. На аппаратной платформе IPC-3000FC-40G в режиме КК допускается использование только одного кабеля SC-QSFP+/4SFP+CabA-10. В такой схеме скорость ограничена 34 Гбит/с.

57. Звуковые сообщения о работе сетевого устройства при функционировании без монитора отсутствуют на аппаратных платформах: IPC-R10 (SC R15), IPC-R50 (SC R15), IPC-R300 (SC R300), IPC-R550 (SC R300), IPC-500 (LN-015B), IPC-500F (LN-015C).

4.6. Программа управления ЦУС

1. Установку и удаление ПУ ЦУС может выполнить только пользователь с правами локального администратора компьютера.

2. Перед установкой ПУ новой версии необходимо удалить имеющуюся на компьютере ПУ предыдущей версии и перезагрузить компьютер.

3. 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.

4. 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 состояний соединений, с которым можно либо согласиться, либо нет.

5. Управление ЦУС текущей версии возможно только с помощью ПУ той же версии.

6. В ПУ ЦУС не отображается признак "КШ за NAT", если на КШ настроен внешний интерфейс PPPoE и между КШ и ЦУС на промежуточном роутере работает NAT.

7. 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.

8. При создании правил NAT на КШ с Multi-WAN-балансировкой следует выбирать интерфейс и класс трафика, которые указаны в настройках балансировки.

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 ПУ время отказа канала VPN отсчитывается от следующих событий:

- прохождение последнего пакета по парной связи в сторону докладывающего СУ;
- 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. Реализована процедура ввода лицензий ЦУС с использованием файла лицензий.

15. 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.

16. В сетевой инфраструктуре, где к ЦУС подключены преимущественно кластеры и где количество подключенных устройств (с учетом того, что кластер — это 2 устройства) составляет 30% от максимального возможного количества устройств, управляемых ЦУС (зависит от используемой аппаратной платформы), необходимо использовать инженерную версию ПУ ЦУС с облегченным мониторингом состояний кластеров. Инженерная версия ПУ предоставляется по запросу в службу технической поддержки.

17. В текущей версии процедура резервного копирования для больших сетей может привести к временной визуальной недоступности сетевых устройств.

18. В ПУ ЦУС отсутствует сигнализация о выходе из строя одного из интерфейсов, входящих в агрегированный интерфейс типа LACP.

19. В правилах трансляции для интерфейса с двумя адресами необходимо явно указывать IP-адрес источника преобразованного пакета. В этом случае запрещено использовать параметр "Адрес интерфейса".

20. При перемещении нескольких правил трансляции через drag-n-drop правила переносятся с сохранением порядка, в котором они были выбраны.

21. Для смены ключа администратора необходимо заблокировать старого администратора и создать вместо него нового администратора с новым ключом.

4.7. Агент ЦУС и СД

1. Установку агента (вместе с ПУ ЦУС или отдельно) должен осуществлять пользователь, наделенный правами:

- локального администратора компьютера;

- администратора используемой базы данных.

2. Операционная система компьютера, на который устанавливают 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 и СД" работает. При остановленной службе "Агент ЦУС и СД" 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 ОС Windows для подключения агента к СУБД должна иметь права на изменение реестра (как минимум входить в группу "Опытные пользователи"). В противном случае сохранение настроек расписания невозможно.

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

4.8. Сервер доступа

1. Для корректной работы СД не рекомендуется в пул адресов для динамической раздачи добавлять следующие адреса:

- мультикастовые адреса;
- зарезервированные адреса;
- адреса, пересекающиеся с защищаемой подсетью;
- адреса, пересекающиеся с адресами внешнего интерфейса КШ;
- адреса, пересекающиеся с адресами интерфейсов резервирования.

2. Особенности работы СД в кластере. После восстановления базы данных СД в кластере требуется перезагрузка кластера.

3. Особенность работы кластера. Если при выключенном основном устройстве на резервном были выполнены какие-либо изменения, для сохранения этих изменений необходимо на резервном устройстве сохранить файл конфигурации и после включения основного устройства выполнить его синхронизацию с резервным устройством, используя сохраненный файл конфигурации.

4. Проверка CRL доступна только для внешнего УЦ.

5. Если на сервере доступа не используются сертификаты внешних удостоверяющих центров и все сертификаты были созданы в ПУ СД с применением СКЗИ "КриптоПро CSP", необходимо в ПУ СД в настройках сервера отключить использование списков отозванных сертификатов.

6. USB-флеш-накопители объемом 16 Мбайт и выше, определяемые системой как жесткий диск (HDD), непригодны для использования в качестве ключевого устройства.

7. Для абонентских пунктов, подключенных к сети через модем, режим запрета сторонних соединений не поддерживается.

8. В кластере КШ с СД допускается использовать не более одного интерфейса резервирования.

9. Не рекомендуется использовать СД на КШ, на котором планируется высокая нагрузка на МЭ и/или VPN, , а также если на нем часто осуществляется перенастройка правил МЭ.

10. Работа с сертификатами на основе ГОСТ Р 34.10-2001 не поддерживается. Для подключения пользователей к СД необходимо перевыпустить сертификаты с использованием ГОСТ Р 34.10-2012.

11. СД не поддерживает работу с ключами длиной 512 бит по алгоритму ГОСТ Р 34.10-2012.

12. Если КШ с СД или ЦУС с СД устанавливается впервые (т.е. ранее не проводилось обновление с версии 3.7), далее инициализируется СД, в локальном меню создается ключ администратора СД, подключается из ПУ СД и загружается БД СД от версии 3.7.7, то после этого необходимо локально создать новый ключ администратора. Старый ключ не подойдет.

13. Для восстановления конфигурации основного узла кластера СД, работающего в режиме 4.x, необходимо архивировать конфигурацию резервного узла и восстанавливать основной с использованием этой резервной копии.

14. Смена режима СД с 3.x на 4.x произойдет после перезагрузки СД через ЛМ узла или ПУ ЦУС.

15. При загрузке БД СД от СД ранних версий, в SNMP-запросах для старых сертификатов могут отображаться некорректные серийные номера. Также некорректные серийные номера старых сертификатов могут отображаться в журнале СД при создании подписанных ими сертификатов. Актуальный номер сертификата отображается в разделе "Свойства".

16. Для 3.x протокола СД соединение с СКЗИ "Континент-АП" (для мобильных устройств) возможно только по протоколу UDP.

17. АП, подключенные к СД, будут отключены в момент переключения на резервный узел кластера или отказа активного узла.

18. При смене протокола СД необходимо вручную перезагрузить устройство. Если смена протокола выполняется для кластера СД, необходимо вручную перезагрузить основное и резервное устройство.

19. При использовании протокола 4.x СД рекомендуется отключить поддержку протокола UDP в свойствах клиента или сервера удаленного рабочего стола.

20. На СД протокола 4.x в качестве транспортного используется протокол TCP, из-за чего возможно снижение производительности протокола RDP при передаче UDP-трафика. При возникновении данной ситуации рекомендуется либо отключить использование UDP-трафика в RDP-подключениях, либо использовать протокол UDP 3.x.

4.9. Программа управления сервером доступа

1. Для корректной работы ПУ СД необходимо включить и настроить датчик случайных чисел, требуемый для выбранного уровня безопасности (биологический ДСЧ, ДСЧ ПАК "Соболь").

2. Особенности совместной работы ПУ СД и СЗИ Secret Net 7. Ключевой материал для идентификации администратора ПУ СД и ключевой материал для идентификации пользователя СЗИ Secret Net 7 должны быть записаны на разные носители. Корректное использование ключей-идентификаторов на одном носителе невозможно.

3. При возникновении ошибки 0x6BA (The RPC server is unavailable) создания сертификата в ПУ СД необходимо проверить, запущена ли системная служба "CryptoPro CSP key storage".

4. Внимание! Количество подключенных учетных записей, отображаемых в ПУ СД, может не совпадать с количеством реальных пользователей АП. Причина – одновременная работа нескольких реальных пользователей под одной учетной записью. Такой вариант возможен при установке АП на нескольких компьютерах и включенном режиме "Разрешить множественные подключения".

5. Управление СД текущей версии возможно только с помощью ПУ этой же версии.

6. Изменения, внесенные в учетные записи с отозванным сертификатом, не сохраняются.

7. Не рекомендуется в правилах фильтрации, назначаемых удаленным пользователям, использовать сервисы IPv6. В противном случае корректная работа пакетного фильтра не гарантируется.

8. Особенности копирования закрытого ключа для корневого сертификата СД из реестра на другой компьютер средствами СКЗИ "КриптоПро CSP". Средствами СКЗИ "КриптоПро CSP" можно переместить закрытый ключ только из реестра на отчуждаемый носитель. Копировать или перемещать закрытый ключ с отчуждаемого носителя в реестр средствами СКЗИ "КриптоПро CSP" невозможно. Поэтому использовать закрытый ключ на новом компьютере можно только с отчуждаемого носителя.

Запись закрытого ключа на носитель выполняют средствами СКЗИ "КриптоПро CSP" в следующем порядке:

- Предъявите отчуждаемый носитель для записи закрытого ключа.
- Вызовите мастер копирования контейнеров (закладка "Сервис", кнопка "Скопировать контейнер").
- В поле "Введенное имя задает ключевой контейнер:" укажите значение "Компьютера".
- Нажмите кнопку "Обзор" и выберите контейнер для корневого сертификата.
- Выделите и скопируйте (Ctrl+C) имя ключевого контейнера и нажмите "Далее".
- В поле "Имя ключевого контейнера" вставьте (Ctrl+V) имя копируемого контейнера.
- В поле "Введенное имя задает ключевой контейнер:" укажите значение "Пользователя" и нажмите кнопку "Готово".
- В открывшемся окне выберите отчуждаемый ключевой носитель и нажмите "ОК".
- Введите пароль.

- Завершите копирование и извлеките отчуждаемый носитель с записанным ключом из устройства чтения.

9. Не рекомендуется совместная установка ПУ СД и АП на один компьютер.

10. При установке ПУ СД на ноутбук набор энтропии с помощью сенсорной панели (тачпада) затруднителен. Поэтому набор энтропии следует выполнять с помощью манипулятора "мышь".

11. Набор энтропии при использовании средств удаленного доступа (RDP) невозможен.

12. В ПУ СД при создании пользователя по запросу в списке выбора корневого сертификата отображаются сертификаты, соответствующие алгоритму, используемому при создании запроса.

13. Предусмотрена возможность создавать пользователя с именем, уже имеющимся в базе данных СД. Для визуального различия таких пользователей в ПУ СД рекомендуется при создании учетной записи пользователя заполнять поле "Описание".

14. При использовании токенов совместно с АП версии 3.7 для Windows необходимо установить значение параметра "Разрывать связь с неактивным АП через..." более 90 секунд.

15. Невозможно получить доступ к токену из ПУ СД без ввода PIN-кода этого носителя в CSP.

16. В ПУ СД не рекомендуется использовать символ "<" в имени сертификата при его создании.

4.10. 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.

7. При построении диаграмм отчета "Статистика атак" отображается статистика для последних 500000 событий.

Компания "Код Безопасности"	
Почтовый адрес:	115127, 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