Аппаратно-программный комплекс шифрования "Континент"
Версия 3.M2
Комментарии к релизу 3.8.0.347

Документ содержит описание основных возможностей, особенностей работы и ограничений применения изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.M2" (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

1.1. Диск 1

Каталог	Содержимое
Дистрибутивы АПКШ "Континент"	
\boot	Модули для установки АПКШ "Континент" (ЦУС, КШ, КК), включая модули ОС FreeBSD
\Setup\Continent\RCP	Дистрибутив ПУ АПКШ "Континент"
\Setup\Continent\AC	Дистрибутив программы аутентификации хоста в защищенной сети
\Setup\Continent\FLASH\IMAGES	Установочные образы модулей АПКШ "Континент", предназначенные для установки с USB-флеш-накопителя
\isolinux	Загрузчик FreeBSD
Описание версии	
\Version.txt	Файл с описанием версии ПО АПКШ "Континент"
Служебные программы	
\Setup\csum-2012.exe	Программа расчета контрольных сумм
\Setup\ServiceTools	Каталог установки служебных программ

1.2. Диск 2

Каталог	Содержимое
Документация АПКШ "Континент"	
Эксплуатационная документация\ Continent 3M2 - Release Notes.pdf	Release Notes – сведения о новых возможностях и ограничениях в АПКШ "Континент"
Эксплуатационная документация\ Continent - Central - Admin Guide.pdf	АПКШ "Континент". Версия 3.М2. Руководство администратора. Централизованное управление комплексом
Эксплуатационная документация\ Continent - Local - Admin Guide.pdf	АПКШ "Континент". Версия 3.М2. Руководство администратора. Локальное управление сетевыми устройствами
Эксплуатационная документация\ Continent - Audit - Admin Guide.pdf	АПКШ "Континент". Версия 3.М2. Руководство администратора. Аудит
Эксплуатационная документация\ Continent - AU – Admin Guide.pdf	АПКШ "Континент". Версия 3.М2. Руководство администратора Аутентификация пользователя
Эксплуатационная документация\ Дополнительная\Continent – Monitoring CG – Admin Guide.pdf	АПКШ "Континент". Версия 3.М2. Руководство администратора. Программа мониторинга КШ
Эксплуатационная документация\ Дополнительная\Continent – PortChecker – Admin Guide.pdf	АПКШ "Континент". Версия 3.М2. Руководство администратора. Тестирование каналов связи
Эксплуатационная документация\ Дополнительная\Continent - Update Guide.pdf	АПКШ "Континент". Версия 3.М2. Руководство администратора. Обновление программного обеспечения
Техническая документация\ RU.88338853.501430.003 30 - Формуляр.pdf	АПКШ "Континент". Версия 3.М2. Формуляр. RU.88338853.501430.003 30
Техническая документация\ RU.88338853.501430.003 ТУ - Технические условия.pdf	АПКШ "Континент". Версия 3.М2. Технические условия. RU.88338853.501430.003 ТУ
Техническая документация\ RU.88338853.501430.003 99 - Правила пользования.pdf	АПКШ "Континент". Версия 3.М2. Правила пользования. RU.88338853.501430.003 99

2. Изменения и новые возможности

Ниже приводятся сведения об изменениях и новых возможностях АПКШ "Континент" версии 3.М2 по сравнению с сертифицированным ФСБ России АПКШ "Континент" версии 3.М.

2.1. Версия 3.М2

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 документы	Носители	• Компакт-диск РДП-003; • USB-флеш-накопитель
2	Операционная система	ПУ ЦУС	• Windows 2012 Server R2; • Windows 2008 Server R2 SP1; • Windows 8.1; • Windows 7 SP1 (кроме всех выпусков Starter и Home Edition)
		КШ, КК	Сокращенная версия ОС FreeBSD
3	Предыдущие версии АПКШ "Континент"	Обновление предыду-щих версий КШ и ЦУС	3.М
		Совместная работа с предыдущими версиями КШ	3.М
4	Аппаратные платформы	IPC-3000F	S021
		IPC-1000F	9297, S021
		IPC-100	S102, 92E3
		IPC-25	S115
5	Поддерживаемые версии БД		MS SQL 2015 Express, MS SQL 2012 Express, MS SQL 2012

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. Особенности обновления. После обновления ПО ЦУС с версии 3.М на версию 3.М2 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.

4.2. ЦУС

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.

4.3. 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 9297 (IPC-1000F) – 37;
- платформа S021 (IPC-1000F, IPC-3000F) – 38.

5. Особенности работы КШ. Если модем используется в режиме выделенной линии, то перед обновлением ПО необходимо на модеме включить режим "Disable AT command set".

6. Особенности работы кластера КШ. Отсутствует возможность подключения резервного устройства к основному через промежуточный маршрутизатор.

7. Особенности работы КШ. При переключении с основного устройства на резервное возможна потеря трафика, передаваемого по сети через данный кластер.

8. 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.

9. 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.

10. 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.

11. Включение полной регистрации сетевого трафика снижает производительность КШ.

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

13. Ограничения на работу с Dial-UP:

- На КШ может быть настроен только один внешний Dial-UP-интерфейс (один модем).
- Подключение кластера через Dial-UP-интерфейс (модем) не поддерживается.

14. Нельзя настроить более одного PPPoE-интерфейса на кластере КШ.

15. Режим Multi-WAN Routing Table не может работать на КШ с двумя и более PPP-интерфейсами.

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

17. На 10-гигабитных интерфейсах поддержка QoS отсутствует.

18. Особенность работы криптокоммутатора. В зашифрованный пакет подставляется ToS из исходного пакета. При этом настройка ToS, заданная в свойствах класса трафика, игнорируется.

19. Если в процессе работы СУ произошло искажение файлов на жестком диске, что проявилось как отказ VPN-каналов, необходимо вновь создать парную связь.

4.4. 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. 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.

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 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. Чтобы изменения настроек VLAN (VLAN ID и номер родительского интерфейса) вступили в силу, необходимо перезагрузить КШ.

15. Особенности настройки Multi-WAN. Настройка Multi-WAN выполняется только на КШ версии 3.М2.

4.5. 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 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" работает. При остановленной службе "Агент ЦУС" настройка агента из ПУ невозможна.

4. 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.

5. 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).

6. 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.

4.6. 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