Аппаратно-программный комплекс шифрования "Континент"
Версия 3.7 (исполнение 1)
Комментарии к версии 3.7.7.671

Документ содержит описание новых возможностей исполнения 1 изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.7" (далее – комплекс, АПКШ "Континент") версии 3.7.7.671 по сравнению с версиями 3.7.6.602 и 3.7.5.493, а также особенностей и ограничений, которые необходимо учитывать при эксплуатации комплекса.

Список сокращений

АП	Абонентский пункт
БРП	База решающих правил
ДА	Детектор атак
КК	Криптографический коммутатор
КШ	Криптографический шлюз
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
РМ	Рабочее место
СД	Сервер доступа
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
ЦУС	Центр управления сетью криптографических шлюзов
VLAN	Virtual Local Area Network – виртуальная локальная сеть
VPN	Virtual Private Network – виртуальная частная сеть

Оглавление

1. Размещение файлов (ПО, документация) на компакт-диске

1.1. Диск 1

Каталог	Содержимое
Дистрибутивы АПКШ "Континент"	
\Boot	Модули для установки АПКШ "Континент", включая модули ОС FreeBSD. База решающих правил и сертификат для обновления БРП
\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\csum-2012.exe	Программа расчета контрольных сумм
\Tools\ServiceTools	Каталог установки служебных 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 3.7. Руководство администратора. Аутентификация пользователя
Эксплуатационная документация\ Continent - Audit - Admin Guide.pdf	АПКШ "Континент". Версия 3.7. Руководство администратора. Аудит
Эксплуатационная документация\ Continent - Central - Admin Guide.pdf	АПКШ "Континент". Версия 3.7. Руководство администратора. Централизованное управление комплексом
Эксплуатационная документация\ Continent - Local - Admin Guide.pdf	АПКШ "Континент". Версия 3.7. Руководство администратора. Локальное управление сетевыми устройствами
Эксплуатационная документация\ IDS – Admin Guide.pdf	АПКШ "Континент". Версия 3.7. Руководство администратора. Система обнаружения вторжений
Эксплуатационная документация\ KG - Admin Guide.pdf	АПКШ "Континент". Версия 3.7. Руководство администратора. Автоматизированное рабочее место генерации ключей
Эксплуатационная документация\ Access Server - Admin Guide.pdf	АПКШ "Континент". Версия 3.7. Руководство администратора. Сервер доступа
Эксплуатационная документация\ Tools\Continent - Update Guide.pdf	АПКШ "Континент". Версия 3.7. Руководство администратора. Обновление программного обеспечения
Техническая документация\ RU.88338853.501430.006 ТУ - Технические условия.pdf	АПКШ "Континент". Версия 3.7. Технические условия. RU.88338853.501430.006 ТУ
Техническая документация\ RU.88338853.501430.006 30 - Формуляр.pdf	АПКШ "Континент". Версия 3.7. Формуляр. RU.88338853.501430.006 30
Техническая документация\ RU.88338853.501430.006 ATE_FUN – Функциональное тестирование.doc	Описание методик проверки работоспособности комплекса

Каталог	Содержимое
Техническая документация\Состав ПО АПКШ Континент 3.7 (исполнение 1).xlsx	Состав ПО комплекса с контрольными суммами

1.3. Диск 3*

Каталог	Содержимое
База решающих правил системы обнаружения вторжений	
\БРП	База решающих правил и сертификат для обновления БРП
Инструкция по загрузке БРП.pdf	Инструкция по загрузке базы решающих правил

* Диск поставляется только с системой обнаружения вторжений.

2. Изменения и новые возможности

2.1. Версия 3.7.7.671

1. Усовершенствована процедура ввода лицензий ЦУС.

2. Исправлены ошибки, появлявшиеся в ходе резервирования БД СД в кластере.

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

4. Изменена логика работы кластера при падении интерфейса.

2.2. Версия 3.7.6.602

1. При изменении настроек VLAN отменена необходимость последующей перезагрузки КШ.

2. Реализована поддержка идентификатора JaCarta в качестве ключевого носителя для подключения ПУ СД к серверу доступа.

3. Согласована с ФСБ России трехлетняя схема хранения ключей с использованием АРМ ГК, позволяющая обеспечить более долгий срок хранения ключевого материала в АПКШ "Континент".

4. Реализована поддержка USB-модема, выполняющего функции виртуального Ethernet-адаптера.

5. Добавлена возможность работы сервера FTP за шлюзом с NAT, в том числе в канале VPN.

6. Реализованы требования ФСТЭК России к МЭ по 3-му классу типа "А".

7. Добавлена локальная настройка прохождения специальных протоколов на КК.

8. Добавлена усиленная фильтрация (фильтрация HTTP(S)- и FTP-трафика по критериям, заданным пользователем).

9. Реализована обработка команд от ДА на МЭ.

10. Добавлен контроль трафика различных приложений с возможностью их блокировки.

11. Улучшено управление сертификатами безопасности.

12. Реализована возможность подключения к консольному порту для следующих платформ:

- IPC-10 (S088)
- IPC-25 (92D9)
- IPC-25 (S115)
- IPC-100 (S102)
- IPC-400 (S021)
- IPC-500 (LN-015B)
- IPC-1000 (S021)
- IPC-1000F (S021)
- IPC-1000F2 (S021)
- IPC-2000F (S021)
- IPC-3034 (S021)
- IPC-3034F (S021)
- IPC-3020F (S021)
- IPC-3000F (S021)

13. Для обновления всех типов сетевых устройств (КК, КШ, ДА) используется единый файл обновления update_all_release.tar.

14. Изменен порядок регистрации пользователей на сервере доступа. Теперь можно зарегистрировать нового пользователя в случае отсутствия свободных лицензий. Проверка превышения количества действующих лицензий на сервере доступа выполняется при подключении пользователя.

2.3. Версия 3.7.5.493

1. В программу установки ПУ ЦУС и ПУ СД добавлена установка ПО СЗИ Secret Net 7.4.

2. В ПУ СД доработан мастер создания пользователя – при создании пользователя имеется возможность сформировать шаблон настроек для подключения абонентского пункта к СД.

3. В ПУ СД добавлена возможность задавать корневой сертификат и срок действия сертификата пользователя, которые будут подставляться по умолчанию при создании пользователя или выпуске сертификата.

4. Доработан криптопровайдер "Код Безопасности CSP" – на одном наборе энтропии можно создавать нескольких пользователей. Набор энтропии действителен в течение суток или до перезагрузки системы.

5. Добавлена возможность в ПУ СД при создании нового пользователя по запросу от абонентского пункта определять порядок действий – создать нового пользователя или добавить новый сертификат уже имеющемуся пользователю.

6. Для повышения производительности сетевого устройства добавлена оптимизация правил. Оптимизация применяется к правилам фильтрации, в которых используются группы сетевых объектов.

7. В состав программного обеспечения обновления добавлен файл preupdate.tar. При обновлении ПО сетевого узла с версий 3.5 и 3.6 предварительно необходимо выполнить загрузку файла обновления preupdate.tar.

8. В настройках безопасности КК добавлено управление MAC-адресами.

9. Добавлен модуль агента Роскомнадзора для синхронизации с сервером выгрузки реестра запрещенных ресурсов и использования его в правилах фильтрации.

10. 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.

11. Обеспечена возможность использования в кластере сетевых устройств на аппаратной платформе IPC-10.

12. Добавлена возможность входа администратора в локальное меню по паролю (без предъявления идентификатора администратора ПАК "Соболь").

13. Добавлено централизованное управление MSS и MTU.

14. Реализована автоматическая синхронизация парных связей при ошибках в канале VPN (расхождение ключей парной связи или расхождение номеров пакетов).

15. В свойствах узла добавлено отображение значения параметра "Статус автозагрузки сетевого устройства". Значение (отключена/включена) задается в настройках ПАК "Соболь".

16. 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.

17. Добавлены новые аппаратные платформы IPC-2000F и IPC-3034F.

3. Ограничения на поддержку аппаратных и программных средств

1	Ключевые устройства	Накопители	• Компакт-диск; • USB-флеш-накопитель; • Рутокен ЭЦП
		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/ЭЦП; • ПАК "Соболь" 3.0; • iButton DS1994/DS1995/DS1996; • JaCarta (только на АРМ администратора сервера доступа для соединения ПУ СД с СД)
2	Операционная система	РМ администратора	• Windows 7 SP1 x86/x64 (кроме всех выпусков Starter и Home Edition); • Windows 8.1 x86/x64; • Windows 10; • Windows 2012 Server R2 x64
3	Предыдущие версии АПКШ "Континент"	Совместная работа с предыдущими версиями комплекса	3.7.6.602, 3.7.5.493
		Обновление предыдущих версий сетевых устройств и ЦУС	3.7.6.602, 3.7.5.493
4	СКЗИ "КриптоПро CSP" СКЗИ "Код Безопасности CSP"		4.0 Не ниже 3.7.7.568
5	Аппаратные платформы	IPC-10	S088, LN-010A
		IPC-25	92D9, S115
		IPC-100	92E3, S102
		IPC-400	S021, 9297
		IPC-500	LN-015B
		IPC-1000	S021, 9297
		IPC-1000F	S021, 9297
		IPC-1000F2	S021, 9297
		IPC-1010	9297
		IPC-3000F	S021
		IPC-3020F	S021
		IPC-3034	S021
		IPC-3034F	S021
		IP-64	S088
6	Поддерживаемые версии БД		• MS SQL 2012 x32/x64; • MS SQL 2012 Express x32/x64
7	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 программ управления.

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

4. Список рекомендуемых версий ПО BIOS для аппаратных платформ приведен в таблице ниже.

Аппаратная платформа	**Версия ПО BIOS**
S088 (IPC-10)	ES088ISC.105
92D9 (IPC-25)	A92D9ISC.222
S115 (IPC-25)	ES115ISC.171
92E3 (IPC-100)	A92E3ISC.133
S102 (IPC-100)	ES096ISC.131
S021 (IPC-400, IPC-1000*, IPC-3000*)	ES021ISC.141
LN-010A (IPC-10)	LN010AISC.003
LN-015B (IPC-500)	LN015BISC.001

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 сервисы компании – разработчика ПО АПКШ "Континент".

Внимание! Запрещается использовать для обновления версию BIOS, предназначенную для другой модели аппаратной платформы. Нарушение этого условия ведет к потере работоспособности аппаратной платформы и служит основанием для отказа в предоставлении гарантийного ремонта.

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. Особенность работы агента обновлений БРП. При работе агента в режиме с подключением к ЦУС возможны отказы в загрузке в ЦУС базы решающих правил.

7. Для получения по SNMP счетчика октетов с интерфейса следует использовать OID1.3.6.1.2.1.31.1.1.1.10. "ifHCOutOctets", так как OID1.3.6.1.2.1.2.2.1.16. "ifOutOctets" работает некорректно.

4.2. Центр управления сетью криптографических шлюзов

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 на ПО ЦУС версии 3.7.7.671 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.

4.3. Сетевые устройства

1. Для работы VPN с пакетами, размер которых превышает 1420 Б, необходимо на сетевых устройствах локально в пункте главного меню "Управление | Настроить параметры шифратора" установить значение "Разрешить дефрагментацию пакетов до пакетного фильтра".

2. Особенность работы КШ при использовании правил NAT. При преобразовании в локальные адреса КШ или при трансляции NAT 1:1 (для обратного трафика) возможна некорректная регистрация событий подсистемы контроля приложений.

3. Особенности работы сетевых устройств КШ и КК:

- Если модем используется в режиме выделенной линии, то перед обновлением ПО необходимо на модеме включить режим "Disable AT command set".
- При переключении с основного устройства на резервное возможна потеря трафика, передаваемого по сети через данный кластер.

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

5. При использовании VLAN-интерфейсов в кластере КШ или КК у родительского интерфейса необходимо указывать тип, соответствующий привязанного к нему VLAN-интерфейса — "внешний" или "внутренний".

6. 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.

7. 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.

8. 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 МБ.
- 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.

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

10. 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.

11. Особенность обновления кластера КШ. После обновления ПО кластера в настройках параметров резервирования для параметра "Время ожидания ответа от активного сетевого устройства" по умолчанию устанавливается значение "0". Для обеспечения бесперебойной работы кластера у данного параметра необходимо установить значение от 3 до 60 (секунд).

12. 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.

13. 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.

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

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

16. Ограничения на работу с DialUP:

- На сетевом устройстве может быть настроен только один внешний DialUP-интерфейс (один модем).
- Подключение кластера через DialUP-интерфейс (модем) не поддерживается.

17. 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.

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

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

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

21. На 10-гигабитных интерфейсах поддержка QoS отсутствует.

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

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

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

25. 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.

26. 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".

27. 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 следующие действия:

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

28. 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".

29. 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".

30. 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.

31. 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.

32. После изменения значения MTU на сетевом интерфейсе в сторону увеличения сетевое устройство необходимо перезагрузить.

33. При включенной SSL-инспекции возможно нарушение работоспособности ряда приложений, использующих технологию Certificate Pinning (Skype, ICQ, Windows Update, Google Drive, Яндекс.Диск, WhatsApp).

34. Для регистрации пропущенных пакетов в режиме изолированной сети рекомендуется настройку регистрации выполнять в свойствах правил фильтрации.

35. Для корректного переключения кластера КШ с СД рекомендуется в свойствах кластера открыть вкладку "Multi-WAN" и задать хотя бы один WAN-канал.

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

4.4. 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 состояния 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 те 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. Особенности работы ПУ с средствами аппаратной поддержки СЗИ Secret Net 7 (Secret Net Card, ПАК "Соболь"). Если носители ключей недоступны, необходимо выполнить одно из следующих действий:

- запустить ПУ от имени администратора;
- установить драйверы СЗИ Secret Net 7.

12. Отображаемое в ПУ 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.

13. 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.

14. Изменена интерпретация диапазона портов «><» в сервисе. Теперь граничные условия входят в диапазон (включающий диапазон). При обновлении ПО с предыдущих версий необходимо скорректировать границы диапазона.

15. Особенность установки ПУ ЦУС. СЗИ Secret Net 7, входящее в состав инсталлятора ПУ ЦУС, запрещается устанавливать на компьютер с ОС Windows 10.

16. Реализована процедура ввода лицензий ЦУС с использованием файла лицензий.

4.5. 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 забирать 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.

4.6. 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. Правила фильтрации, для которых установлен режим "Контролировать состояние соединений", после отключения их от учетной записи (флажок активности) и последующего обновления параметров подключенного пользователя, будут действовать до завершения сеанса работы АП.

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

4. Особенности использования сертификатов внешнего центра сертификации. Для проверки отозванных сертификатов информация о точках распространения списков отзыва в сертификате должна быть представлена в виде URL: http://<IP-адрес ресурса, на котором находится CRL>/<путь к списку отзыва>/<имя списка отзыва>.crl. В противном случае корректная проверка отозванных сертификатов не гарантируется.

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 МБ 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. При высокой нагрузке КШ, реализующего функции МЭ и/или VPN, не рекомендуется использовать СД на этом КШ.

4.7. 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 только те сертификаты, которые соответствуют 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".

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.

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