Continent Documentation

Выпуск 0.1.1

g00dvin

нояб. 22, 2021

АПКШ Континент - программно-аппаратный комплекс для поддержания сетевого нейтралитета производства компании Код Безопасности. Официальный сайт производителя находится здесь.

Внимание:

- Документация описывает версию 3.7, в дальнейшем будет так же 3.9 и 4, но пока вот так
- Вся информация, представленная здесь, носит ознакомительный характер
- Мнение авторов может не совпадать с мнением производителя
- Страдание - залог успеха
- Аббревиатуры тут не расшифровываются, так и живем
- Обсуждение в Telegram - https://t.me/apksh

Глава 1

Общая информация

Содержание

1.1 Текущие версии ПО

Версии ПО 3.5 и 3.6 не поддерживаются Производителем и не имеют действующих сертификатов Регуляторов.

На текущий момент актуальной является версия АПКШ Континент 3.7.7 (сертификаты ФСБ до класса КС3 и ФСТЭК по МЭ А3,СОВ3).

Версия 3.9 на данный момент имеет сертификат ФСБ до класса КС2 и сертификат ФСТЭК по МЭ А4 и СОВ4.

Версия 4 станет доступна для бета-теста ближе к лету 2019 года, следите за новостями на сайте Производителя.

Таблица 1: Версии ПО

Версия	Статус	Текущий сертифицированный билд
3.5	EOL	3.5.74.0
3.6	EOL	3.6.90.4
3.7	**Текущая**	**3.7.7.671 (ФСБ, ФСТЭК)**
3.9	**Текущая**	**3.9.2808 (ФСБ, ФСТЭК)**
4	В разработке	Не зафиксировано

1.2 Сертификаты соответствия

Сертификаты соответствия (версия 3.7.7.671):

- **ФСТЭК России:**
  - №3008 (МЭ А3, СОВ3) - действителен до 1 ноября 2019, исполнения 1,2.
- **ФСБ России:**
  - СФ-124/2871 (КС2) - действителен до 25 марата 2019, исполнение 2
  - СФ-124/2918 (КС3) - действителен до 07 июля 2019, исполнение 3
  - СФ-124/3704 (КС2) - действителен до 15 мая 2021, исполнение 4,5
  - СФ-124/3018 (КС3) - действителен до 16 декабря 2019, исполнение 6
  - СФ-124/3373 (КС3) - действителен до 15 мая 2021 года, исполнение 1
  - СФ-124/3454 (КС2) - действителен до 15 мая 2021 года, исполнение 7
  - СФ-124/3455 (КС3) - действителен до 15 мая 2021 года, исполнение 8
  - СФ-525/3138 (МСЭ4) - действителен до 19 мая 2020, исполнения 1-6

Сертификаты соответствия (версия 3.9.0.2808):

- **ФСБ России:**
  - СФ-124/3664 (КС2) - действителен до 28 марта 2022, исполнение 1
  - №4145 (МЭ А4, СОВ4) - действителен до 17 июля 2024

1.3 Исполнения ФСБ и ФСТЭК

АПКШ Континент сертифицирован по требования ФСБ к СКЗИ и МЭ, так и по требованиям ФСТЭК к МЭ и СОВ (НДВ сейчас входит в МЭ/СОВ).

Примечание: АПКШ Континент, один из немногих продуктов на рынке, сертификационный в рамках одного билда по требованиям ФСБ и по требованиям ФСТЭК!

Исторически «исполнения» - термин ФСБ. Используется для поэтапной сертификации компонентов комплекса и служат для разделения на классы СКЗИ. * КС2 - исполнение 4 (пример артикула - HSEC-3.7-IPC10-CM-KC2-SP1Y) * КС2 - исполнение 5, СД с КриптоПро CSP 4.0 (пример артикула - HSEC-3.7-IPC100-CM-ACS-CSP4.0-KC2-SP1Y) * КС3 - исполнение 6 (пример артикула - HSEC-3.7-IPC100-CM-ACS-KC3-SP1Y)

Когда мы говорим об исполнениях ФСТЭК, речь идет двух исполнениях: * Первое исполнение по ФСТЭК - классический Континент 3.7, который мы все знаем, основанный на FreeBSD. * Второе исполнение по ФСТЭК - Континент СОВ, пу сути это уже версия 4, но только с функциями СОВ, без VPN и МЭ.

Подсказка: Определить исполнение можно просто, для этого надо узнать индекс исполнения в регистрационном номере ФСБ данного образца СКЗИ. Регистрационный номер указан в паспорте АПКШ Континент и имеет вид №351Д6-000001, где Д6 это исполнение 6.

Таблица исполнений приведена в формуляре на комплекс, но мы же не звери, чтобы отправлять тебя туда и покажем ее тут:

Таблица 2: Исполнения АПКШ Континент 3.7 по ФСБ

Исп.	Класс	Обяз-ные комп-нты	Необяз-ные комп-нты	СКЗИ М-506А-XP или СЗИ SN 7	СКЗИ КриптоПро CSP 4.0	Сборка 3.7.7.671 3.7.7.671 3.7.7.671
1	КС3	ЦУС ПУ ЦУС	КШ АРМ ГК	+	-	3.7.3.536 3.7.5.426 3.7.5.493 3.7.6.602 3.7.7.671
2	КС2	ЦУС ПУ ЦУС	КШ АРМ ГК	-	-	3.7.3.536 3.7.5.426 3.7.5.493 3.7.6.602 3.7.7.671
3	КС3	ЦУС ПУ ЦУС	КШ КК АРМ ГК	+	-	3.7.3.536 3.7.5.426 3.7.5.493 3.7.6.602 3.7.7.671
4	КС2	ЦУС ПУ ЦУС или ЦУС, СД ПУ ЦУС	КШ КК СД АРМ ГК ПУ СД	-	-	3.7.5.426 3.7.5.493 3.7.6.602 3.7.7.671
5	КС2	ЦУС ПУ ЦУС или ЦУС, СД ПУ ЦУС	КШ КК СД АРМ ГК ПУ СД	-	+	3.7.5.493 3.7.6.602 3.7.7.671
6	КС3	ЦУС ПУ ЦУС или ЦУС, СД ПУ ЦУС	КШ КК СД АРМ ГК ПУ СД	+	-	3.7.5.493 3.7.6.602 3.7.7.671

На данный момент производителем отгружаются исполнения 4,5,6,7 и 8.

Примечание: Исполнения 7 и 8 это экспортный вариант АПКШ Континент, который разрешен к вывозу с территории РФ!

1.4 Состав комплекса

В состав комплекса входят несколько компонентов:

- *ПУ ЦУС*
- *ЦУС (ЦУС-СД)*
- *КШ (КШ-СД)*
- *СД*
- *КК*
- *ДА*
- *АРМ ГК*
- *Континент АП*

1.4.1 ПУ ЦУС

ПУ ЦУС - программа управления ЦУС. Основной инструмент администратор Континента для управления и мониторинга устройств комплекса. ПУ ЦУС позволяет производить следующие действия:

- создание устройств комплекса
- конфигурация системных параметров устройств
- формирование топологии и параметров VPN
- управление политикой межсетевого экранирования и трансляции адресов
- управление учетными записями администраторов
- оперативный мониторинг устройств комплекта
- управление ключевой информацией
- дистанционное обновление ПО устройств комплекса

1.4.2 ЦУС (ЦУС-СД)

ЦУС - Центр управления сетью. Сердце сети АПКШ Континент. Без ЦУСа не бывает сети, даже если в сети одно устройство это всегда будет ЦУС. ЦУС реализуется в виде отдельно устройства, по сути своей это КШ с дополнительным модулем (netcenter). Дополнительно может содержать модуль СД (Сервер доступа)

Подсказка: Достаточно запомнить следующую мантру и повторять ее время от времени: **Любой ЦУС это КШ, но не любой КШ это ЦУС**

ЦУС выполняет следующие функции:

- оперативное управление устройствами комплекса
- создание, изменение, удаление конфигураций и ключей устройств комплекса
- хранение конфигурации комплекса
- сбор журналов с устройств и передача их агенту журналов для записи в БД
- дистанционное обновление ПО устройств комплекса
- мониторинг устройств комплекса

1.4.3 КШ (КШ-СД)

КШ - Криптошлюз. Основное устройство комплекса. Дополнительно может содержать модуль СД (Сервер доступа) КШ выполняет следующие функции:

- шифрование трафика (VPN)
- межсетевое экранирование (FW + NAT)
- маршрутизация (статическая, динамическая, Multi-WAN)
- аутентификация пользователей (агентский способ)

1.4.4 СД

СД - Сервер доступа. Является дополнительным модулем, устанавливаем на КШ или же на ЦУС (который такой же КШ, просто с модулем ЦУСа). СД имеет свою собственную базу конфигурации и управляется при помощи отдельного компонента ПУ (ПУ СД) СД выполняет следующие функции:

- управление внутренним корневым центром сертификации
- интеграция с КриптоПро УЦ
- управление учетными записями пользователей Континент АП (аутентификация, авторизация)

1.4.5 КК

КК - Криптокоммутатор. Отдельное устройство комплекса, позволяющее организовать L2 VPN. Удобен для организации схем с использованием роутеров и динамической маршрутизации между ними. Может пробрасывать транки, а так же служебные кадры LACP. Транзитный трафик подвержен фрагментации, так как не позволяет туннелируемым устройствам использовать Path MTU Discovery.

1.4.6 ДА

ДА - Детектор атак. Отдельное устройство комплекса, в версии 3.7 работает в режиме IDS. Поддерживает как вендорские сигнатуры, так и сигнатуры, созданные администратором. Вендорские сигнатуры обновляются дистанционно с сервера обновлений БРП производителя. Поддерживает интеграцию с КШ, при назначении на КШ SPAN-интерфейса.

1.4.7 АРМ ГК

АРМ ГК - Автоматизированные рабочее место генерации ключей. Используется для генерации ключей, сроком жизни три года. Сертифицирован ФСБ, сложен в эксплуатации.

1.4.8 Континент АП

Континент АП - Абонентский пункт. Клиентское ПО, позволяющее удаленному пользователю подключаться к СД с использованием сертификатов X.509 и получать доступ к защищаемым ресурсам.

1.5 Аппаратные платформы

АПКШ Континент поставляется как предустановленное ПО на собственных аппаратных платформах.

Таблица 3: Аппаратные платформы АПКШ Континент

Модель	Шасси	Поддерживаемые версии ПО
IPC10	S088	3.7, 3.9
IPC10	LN010A	3.7, 3.9, 4
IPC10	S185	3.9, 4
IPC25	GA630	3.5, 3.6
IPC25	9830	3.5, 3.6
IPC25	92D9	3.6, 3.7, 3.9
IPC25	S115	3.7, 3.9, 4*
IPC50	LN010C	3.9, 4
IPC100	G560	3.5, 3.6
IPC100	92E3	3.6, 3.7, 3.9
IPC100	S102	3.6, 3.7, 3.9, 4*
IPC400	IBM9297	3.6, 3.7, 3.9
IPC400	S021	3.6, 3.7, 3.9, 4*
IPC500	LN015B	3.7, 3.9, 4
IPC500F	LN015C	3.9, 4
IPC600	DV030A	3.9, 4
IPC800F	DV030B	3.9, 4
IPC1000	IBM9297	3.6, 3.7
IPC1000F	IBM9297	3.6, 3.7
IPC1000F2	IBM9297	3.6, 3.7
IPC1010	IBM9297	3.6, 3.7
IPC1000	S021	3.6, 3.7, 3.9, 4*
IPC1000F	S021	3.6, 3.7, 3.9, 4*
IPC1000F2	S021	3.6, 3.7, 3.9, 4*
IPC1000	DV031A	3.9, 4
IPC1000F	DV031B	3.9, 4
IPC1000F2	DV031C	3.9, 4
IPC3000F	S021	3.6, 3.7, 3.9, 4*

Продолжается на следующей странице

Таблица 3 – продолжение с предыдущей страницы

Модель	Шасси	Поддерживаемые версии ПО
IPC3034	S021	3.6, 3.7, 3.9, 4*
IPC3034F	S021	3.6, 3.7, 3.9, 4*
IPC3000F	LN021	3.9, 4
IPC3000FC	LN021A	3.9, 4
IPC3000NF2	LN021E	3.9, 4
IPC3034F	LN021C	3.9, 4
IPC3000	LN021D	3.9, 4
IPC5000FC	S145	3.9, 4

Внимание: * - требуется приобретение комплекта модернизации RAM и HDD, подробности уточнять у производителя

Глава 2

Быстрый старт

АПКШ Континент поставляется с предустановленной текущей тиражируемой версией ПО. В некоторых случая может потребоваться ее переустановка (понижение или повышение версии, восстановление работоспособности, установка отладочной версии по и т.д.).

Содержание

2.1 Инсталляция на аппаратную платформу

При инсталляции ПО на аппаратную платформу используются два источника инсталляции:

- CD-диск (входит в комплекте поставки оборудования)
- USB Flash drive (так же входит в состав поставки)

Самый распространенный способ - это установка через USB Flash drive. В этом случае на носитель необходимо записать образ USB Flash drive из комплекта поставки. Образы находятся на CD-диске в директории Setup\Continent\FLASH\IMAGES, имеют расширение .flash и записываются на USB Flash drive при помощи таких утилит как:

- dd (Linux, BSD)
- Win32DiskImager (Windows)
- Rufus (Windows)
- balenaEtcher (Windows, Linux, MacOS)

Примечание: Для распознавания файла образа в **balenaEtcher** необходимо изменить расширение с .flash на .img (cgw_release.flash -> cgw_release.img)

По факту каждый образ это raw image жесткого диска с двумя разделами. Первый раздел FAT размером 8 МБ. Предназначен для сохранения ключей администратора ЦУС или же конфигурации и ключей КШ. Второй раздел UFS (FreeBSD). Содержит необходимые для установки ПО файлы. Созданный таким образом USB Flash drive будет являться загрузочным устройством и позволит произвести установку ПО на аппаратную платформу АПКШ.

Каждый образ установочного ПО содержит требуемый функционал для конкретной реализации ПО:

- arm_release.flash - АРМ ГК (Генерации Ключей)
- cgw.aserv_release.flash - КШ-СД
- cgw_release.flash - КШ
- csw_release.flash - КК
- ids_release.flash - ДА
- ncc.aserv_release.flash - ЦУС-СД
- ncc_release.flash - ЦУС

Внимание: При переустановке ПО на аппаратную платформу АПМДЗ «Соболь» будет выдавать предупреждение о том, что изменился загрузочный диск, на запрос о изменении загрузочного диска следует ответить *«НЕТ»*, в ином случае Соболь при загрузке уже с диска опять выдаст это предупреждение. Так же после переустановке ПО сбросится настройка «Время автоматического входа в систему», следует установить этот параметр в значение, отличное от 0, иначе устройство будет требовать предъявление iButton при каждой загрузке. Пункт «Время автоматического входа в систему» может быть недоступен для редактирования, в этом случае необходимо создать пользователя AUTOLOAD в меню управления пользователям АПМДЗ «Соболь».

2.2 Инсталляция на виртуальную машину

Для того, чтобы установить ПО Континент на виртуальную машину используется специальный ISO-образ. Данный образ содержит в инсталляционных файлах все возможные компоненты комплекса (ЦУС, КШ, КК, ДА, ЦУС-СД, КШ-СД, АРМ ГК). Основное отличие данного ISO-образа это эмуляция Соболя, по факту же данный образ может использоваться для установки на x86-совместимое

аппаратное обеспечение. Важно понимать, что в этом случае мы никогда не получим формальное соответствие формуляру (актуально для версии 3.7 и ниже). При установке на виртуальную платформу необходимо выбирать гостевую систему FreeBSD (32 bit) ниже 10 версии.

Для оптимизации потребления ресурсов гипервизора рекомендуется использовать следующие параметры в файле /boot/loader.rc:

- set hint.p4tcc.0.disabled=1
- set hint.acpi_throttle.0.disabled=1
- set hint.apic.0.clock=0
- set kern.hz=50

Важно: Начиная с версии 3.9 для установки на реальную платформу и на гипервизор используется один установочный диск, который самостоятельно определяет в каком режиме он будет работать.

2.3 Строка инициализации

Строка инициализации используется для создания устройства в ПУ ЦУС, это способ сообщить ПУ ЦУС идентификационный номер устройства, а так же количество и тип сетевых интерфейсов.

Внимание: При ошибке в строке инициализации в дальнейшем будет невозможно загрузить конфигурацию на устройство, так что стоит быть предельно внимательным при ее вводе.

Строка инициализации для оборудования, поставляемого производителем приведена в Паспорте. Так же строку инициализации можно увидеть при инсталляции ПО (строка инициализации появляется после ввода идентификатора устройства. В некоторых случая строка инициализации может уйти за границы экрана, в этом случае необходимо нажать Scroll Lock и прокрутить экран вверх при помощи клавиш с указателями).

Внимание: Следует быть внимательным, при установке на виртуальную машину, поскольку в некоторых гипервизорах могут использоваться различные типы интерфейсов! К примеру в VirtualBox используются интерфейсы le. Так же стоит обратить внимание, если количество интерфейсов в строке инициализации отличается от фактического количества интерфейсов на аппаратной платформе, это может быть признаком выхода интерфейса из строя, и как следствие ОС не может его обнаружить.

Строка инициализации имеет простой и понятный формат, например:

Таблица 1: **000027103igb0*02BDigb1*02BDigb2*02BDffff**

00002710	3	igb0*02BDigb1*02BDigb2*02BD	ffff

- **00002710** - идентификатор криптошлюза в HEX, длиной восемь символов, дополняется нулями в начале
- **3** - количество сетевых интерфейсов устройства, далее и до конца строки идет перечисление интерфейсов и их режимов работы

- **igb0*02BDigb1*02BDigb2*02BD** - наименование сетевых интерфейсов, как их определяет операционная система, режим работы (скорость, дуплекс), * отделяет интерфейсы
- **ffff** - признак окончания строки инициализации

Интерфейсы и режим работы:

- em0 (медь) - 02BD
- igb (оптика) - 3001
- igb (медь) - 02BD
- ix (оптика 10G) - 0001
- ixl (оптика криптоускоритель) - 2E801

Онлайн генератор строки инициализации

2.4 Настройка VPN

2.4.1 Настройка L3 VPN между КШ

Настройка L3 VPN между КШ это самая распространенная задача, выполняемая администратором комплекса. Для создания данного типа VPN необходимо выполнить следующие действия:

1. создание сетевых объектов
2. создание парных связей
3. создание правил фильтрации

Создание сетевых объектов

Шифрование трафика в комплексе возможно только между сетевыми объектами с типом **Защищаемый**.

Привязка сетевого объекта должна производится к внутреннему интерфейсу или к интерфейсу с типом «Любой» криптошлюза, за которым этот сетевой объект находится.

После создания сетевого объекта он может быть использован в правилах фильтрации. Подробнее о сетевых объектах и их типов читайте тут (link!).

Создание парных связей

Парные связи позволяют крипошлюзам узнавать о защищаемых сетевых объектах парных криптошлюзов.

При создании парной связи между криптошлюзами они строят между собой VPN по дефолтному порту UDP 10000 и начинают обмениваться keepalive-сообщениями. Если криптошлюз не получает данные сообщения от парного криптошлюза, то в ПУ ЦУС напротив него в колонке VPN будет отображаться восклицательный знак.

Создание правил фильтрации

После того, как сетевые объекты и парные связи созданы единственное, что останавливает прохождение трафика по VPN-каналу это межсетевой экран криптошлюза.

Необходимо создать правила фильтрации на основе созданных межсетевых объектов описав в них требуемые разрешения для прохождения трафика. Подробнее о правилах фильтрации и управлении межсетевым экраном читайте тут (link!).

2.4.2 Настройка L2 VPN между КК

L2 VPN при использовании криптокоммутаторов позволяет прозрачно объединять физические порты криптокоммутатров в единый L2-сегмент. Для конфигурации L2 VPN необходимо выполнить следующие действия:

- настройки интерфейсов коммутации
- конфигурация виртуального коммутатора

Настройка интерфейсов коммутации

Интерфейс коммутации - физический или логический интерфейс (VLAN) КК, который отправляет все присланные на него кадры в виртуальный коммутатор. Для задания интерфейса коммутации необходимо открыть свойства КК, перейти на вкладку **Интерфейсы**, выбрать нужный интерфейс и назначить ему тип «Порт криптокоммутатора». У КК должен так же быть минимум один внешний интерфейс, который используется для передачи VPN-трафика и управления устройством.

Конфигурация виртуального коммутатора

Для того, чтобы порты криптокоммутатора передавали трафик защищаемых хостов внутри VPN необходимо создать виртуальный криптокоммутатор. В общем случае можно сказать, что виртуальный коммутатор на логическом уровне объединяет все порты криптокоммутаторов, которые в него включены в единый L2-сегмент. Для создания виртуального коммутатора необходимо задать его имя и добавить из списка доступные порты необходимых КК. Если чекбокс *Автоматически создавать парные связи* активен, то с свойствах каждого КК не потребуется вручную указывать парные для него КК.

2.4.3 Настройка удаленного доступа VPN между СД и АП

Для организации защищенного соединения удаленного пользователя и доступа его к защищенным ресурсам внутренней сети используется связка Континент АП и СД (Сервер доступа).

Примечание: Не стоит забывать, что СД это дополнительный модуль, устанавливаемый на КШ и по факту он живет своей жизнью, не привязываясь к IP-адресам или идентификатору КШ.

Для организации удаленного доступа производятся действия на АРМ пользователя и на СД.

На АРМ пользователя:

- установка ПО «Континент АП»
- создание закрытого ключа пользователя (опционально)

- импорт сертификата пользователя (опционально с импортом закрытого ключа), выпущенный на СД
- создание соединения с СД

На СД:

- создание объекта защищаемой сети
- создание правил межсетевого экрана
- создание пользователя и выпуск сертификата пользователя
- назначение пользователю правил межсетевого экрана

Более детально конфигурация данного типа VPN будет рассмотрена в соответствующем разделе.

Глава 3

Обновление ПО

В жизни каждого администратора АПКШ Континент наступает тот момент, когда необходимо произвести обновление ПО.

Примечание: ЦУС (он же КШ с ЦУСом) обновляется только локально!

Содержание

Обновления ПО можно разделить на:

- обновление мажорной версии (обновление с 3.6 на 3.7)
- обновление минорной версии (обновление с 3.7.5 на 3.7.7)

Внимание: Лицензия на обновление ПО требуется только в случае обновления на мажорную версию! Обновление с 3.6 на 3.7, с 3.7 на 3.9 и так далее!

3.1 Файлы обновления

Локальное обновление, это по сути просто инсталляция ПО на платформу. При локальном обновлении используются *образы USB Flash Drive* версии, на которую производится обновление АПКШ Континент.

При дистанционном обновлении используются архивы, находящиеся на CD-диске с новой версией ПО, указанные ниже:

- preupdate.tar - специальный пакет обновления, который устанавливается в том случае, если невозможно загрузить update_all_release.tar
- update_all_release.tar - пакет обновления АПКШ Континент для всех устройств комплекса. Релизная версия.
- update_2deb_release.tar - пакет обновления АПКШ Континент для всех устройств комплекса. Отладочная версия.

3.2 Обновление мажорной версии

При обновление мажорной версии ПО, к примеру обновление сети с версии 3.6.90.4 на версию 3.7.7.761 следует выполнить следующие действия:

- убедиться в наличии лицензии на обновление (приобретается вместе с правом на обновление, без нее не удастся обновить устройства комплекса после обновления ЦУСа)
- внимательно ознакомится с документом Release Notes (в нем описаны все нюансы обновления и измененный функционал)
- сохранить резервную копию БД ЦУС *ЦУС* → *Сохранить конфигурацию* (сделать копию дважды и сохранить ее в нескольких местах)
- выполнить рекомендации из Release Notes на текущей версии ПО
- сохранить резервную копию БД ЦУС (сделать копию дважды и сохранить ее в нескольких местах)
- произвести смену ключей всех устройств комплекса (в случае, если ключи истекли)
- сохранить резервную копию БД ЦУС (сделать копию дважды и сохранить ее в нескольких местах)
- проверить восстановление из резервной копии БД ЦУС, сохраненной на предыдущем шаге (при возможности)
- сохранить ключ администратора (не удалять его и не переписывать при инициализации новой версии ПО)
- установить ПО новой версии на ЦУС, установить новую версию ПУ ЦУС
- произвести инициализацию ЦУС (можно использовать временные параметры, после восстановления БД ЦУС на новой версии все настройки восстановятся в соответствии со старой конфигурацией, такие как адреса интерфейсов, маршрутизация, ключи администратора)
- подключится ПУ ЦУС к ЦУС и восстановить БД ЦУС из последней сохраненной резервной копии (ЦУС автоматически перезагрузится после восстановления БД)
- подключится ПУ ЦУС к ЦУС с ключом администратора версии 3.6
- добавить лицензии на обновление ПО
- загрузить файл дистанционного обновления (ПУ ЦУС - Свойства - Обновление)
- **обновить устройства комплекса:**
  - дистанционно (в свойствах устройства перейти на вкладку «Версии ПО» и выполнить обновление указав платформу устройства)
  - локально (сохранить конфигурацию и ключи устройства в ПУ ЦУС на USB Flash, установить на устройство новую версию ПО локально, залить конфигурацию и ключи)

- после обновления всех устройств комплекса сохранить резервную копию БД ЦУС новой версии (сделать копию дважды и сохранить ее в нескольких местах)

Внимание: При обновлении с версий 3.5 и 3.6 на версию 3.7 возможна ситуация, когда дистанционное обновление ПО не устанавливается на устройства. В большинстве случаев это связанно с тем, что корневой раздел устройства заполнен. В случае ошибки демонов создаются отладочные дампы процессов или ядра, начиная с версии 3.7.5.493 их создание отключено. В данном случае следует поставить обновление **preupdate.tar** которое выполнит очистку свободного места на диске и позволит загрузить пакет обновления. Другим выходом из ситуации является локальное обновление ПО, рекомендуется по возможности использовать его при мажорных обновлениях.

3.3 Обновление минорной версии

Обновление минорной версии обычно проходит без проблем и не требует повышенного внимания к нюансам из Release Notes. При обновление минорной версии ПО, к примеру обновление сети с версии 3.7.5.493 на версию 3.7.7.761 следует выполнить следующие действия:

- внимательно ознакомится с документом Release Notes (в нем описаны все нюансы обновления и измененный функционал)
- сохранить резервную копию БД ЦУС (сделать копию дважды и сохранить ее в нескольких местах)
- выполнить рекомендации из Release Notes на текущей версии ПО
- сохранить резервную копию БД ЦУС (сделать копию дважды и сохранить ее в нескольких местах)
- произвести смену ключей всех устройств комплекса (в случае, если ключи истекли)
- сохранить резервную копию БД ЦУС (сделать копию дважды и сохранить ее в нескольких местах)
- проверить восстановление из резервной копии БД ЦУС, сохраненной на предыдущем шаге (при возможности)
- сохранить ключ администратора (не удалять его и не переписывать при инициализации новой версии ПО)
- установить ПО новой версии на ЦУС, установить новую версию ПУ ЦУС
- произвести инициализацию ЦУС (можно использовать временные параметры, после восстановления БД ЦУС на новой версии все настройки восстановятся в соответствии со старой конфигурацией, такие как адреса интерфейсов, маршрутизация, ключи администратора)
- подключится ПУ ЦУС к ЦУС и восстановить БД ЦУС из последней сохраненной резервной копии (ЦУС автоматически перезагрузится после восстановления БД)
- подключится ПУ ЦУС к ЦУС с ключом администратора предыдущей версии
- загрузить файл дистанционного обновления (ПУ ЦУС - Свойства - Обновление)
- **обновить устройства комплекса:**
  - дистанционно (в свойствах устройства перейти на вкладку «Версии ПО» и выполнить обновление указав платформу устройства)
  - локально (сохранить конфигурацию и ключи устройства в ПУ ЦУС на USB Flash, установить на устройство новую версию ПО локально, залить конфигурацию и ключи)
- после обновления всех устройств комплекса сохранить резервную копию БД ЦУС новой версии (сделать копию дважды и сохранить ее в нескольких местах)

3.4 Обновление Сервера Доступа

Обновление СД не привязано к конфигурации интерфейсов, платформе или же к идентификатору клиента. При дистанционном обновлении нет необходимости выполнять дополнительные действия по обновлению СД.

Внимание: Всегда, запомни, всегда делай резервные копии не только базы СД, но и закрытых ключей! Без закрытых ключей СД базу не восстановить и она превратится в тыкву!

Для локального обновления СД необходимо:

- создать резервную копию базы СД через ПУ СД (сделать копию дважды и сохранить ее в нескольких местах)
- сохранить ключ администратора СД
- создать резервную копию закрытого ключа СД через Код Безопасности CSP (так же сохранить его в нескольких местах)
- после того, как устройство обновлено, в локальном меню инициализировать СД
- подключиться ПУ СД к СД с новым ключом администратора, созданным на предыдущем шаге
- восстановить конфигурацию СД из резервной копии

Примечание: Для создания резервной копии закрытого ключа корневого сертификата СД необходимо средствами КБ CSP осуществить перемещение закрытого ключа на носитель (USB Flash), затем средствами ОС скопировать с носителя директорию topsecretkeys. При копировании ключей через КБ CSP (используя его встроенный функционал) копию ключа будет невозможно использовать в СД. Есть такой нюанс.

Глава 4

Стенд в виртуальной среде

4.1 Проверка конфигурации на VM

Опасно: Никто не хочет положить продуктивную среду при обновлении!

Рано или поздно перед каждым из нас встает задача проверки конфигурации при ее обновлении на мажорную или минорную версию. Важно не только прочитать Release Notes, но и в боевой среде проверить как пройдет процесс обновления. Перед тем как произвести обновление ПО, не зависимо от того мажорный это релиз или нет, возникает вполне резонное желание проверить как конфиг с текущей версии ПО применится в новой версии. А так же, очень полезно проверить существуют ограничения на обновления или же все пройдет гладко. Увы, ничто не идеально и проверять нужно всё.

Для версии 3.7 и 3.9 рекомендуется использовать следующие гипервизоры:

- VMWare
- VirtualBox(vbox)

У обоих гипервизоров есть свои особенности и недостатки (TODO: перчислить).

4.1.1 Создание VM для ЦУС

Для обоих гипервизоров выбор профиля ОС одинаков:

- Версия 3.7 - 32-х разрядная версия FreeBSD
- Версия 3.9 - 64-х разрядная версия FreeBSD

Примечание: Если для версии 3.7 выбрать 64-х битный профиль ничего страшного не произойдет.

Необходимые ресурсы для VM:

- CPU: 1 и более ядро
- RAM: 1024 Мб и более
- HDD: 2 Гб и более
- USB: версия контроллера не ниже v2.0

Примечание: Количество сетевых интерфейсов зависит от того сколько их на вашем реальном ЦУС, и сколько можно добавить в определенном гипервизоре.

В VMWare максимальное количество сетевых интерфесов 8, в VirtualBox зависит от платформы где работает гипервизор (Linux - phpvitualbox более 14, Windows не более 6 интерфейсов). При использовании гипервизора, который не поддерживает большее количество интерфейсов, чем на вашем ЦУС, можно получить определенные ограничения для проверки конфигурации, о них далее.

4.1.2 Установка ПО на VM

В зависимости от версии существуют разные образы для установки на VM. Образы делятся на «vm_release» и «vm_debug», мы рекомендуем сразу устанавливать **debug** версию. Установка проходит в обычном режиме. В качестве ID (КШ №) необходимо указать ID вашего ЦУС.

4.1.3 Подготовка ЦУС

Для того чтобы можно было применить вашу конфигурацию на **виртулаьный** ЦУС необходимо отредактировать интерфейсы в соотвествии с тем как они есть на **реальном** ЦУС. Для этого можно воспользоваться специальным редактором интерфейсов БД ЦУС, распростарняемым в виде OVA-образа виртуальной машины, или внести изменения в ручном режиме при использовании скриптов, о них ниже.

Если гипервизор поддерживает необходимое количество интерфейсов, то это хорошо и вам необходимо минимум телодвижений. Для начала нужно включить «мягкий режим» на ЦУС, или настроить соотвествующие правила фильтрации для доступа на ЦУС по ssh (tcp/22). Реквизиты для доступа на ЦУС по умолчанию в **debug** версии:

- Логин: root
- Пароль: chay6spu3reswefE

После успешного подключения к ЦУС по протоколу SSH нужно перейти в директорию:

```
cd /etc/rc.startup/
```

В ней создать пустой файл:

```
cat /dev/null >/etc/rc.startup/001if
```

И записать в него скрипт который будет переименовывать интерфейсы **до** старта демона/сервиса ЦУС. Пример скрипта для переименовывания интерфейсов под IPC-3000F:

```
cat << end >> /etc/rc.startup/001if
#!/bin/sh
ifconfig em0 name ix0
ifconfig em1 name ix1
ifconfig em2 name igb0
```

(continues on next page)

(продолжение с предыдущей страницы)

```
ifconfig em3 name igb1
ifconfig em4 name igb2
ifconfig em5 name igb3
ifconfig em6 name igb4
ifconfig em7 name igb5
ifconfig em8 name igb6
ifconfig em9 name igb7
ifconfig em10 name em0
ifconfig em11 name em1
ifconfig em12 name ix2
ifconfig em13 name ix3
end
```

Далее нужно сделать скрипт исполняемым:

```
chmod +x /etc/rc.startup/001if
```

После чего перезагрузить КШ коммандой:

```
reboot
```

Если всё прошло гладко, то при выводе списка интерфейсов, через меню Alt+F2, у вас будут те названия, которые вы задавали в скрипте.

Примечание: Если выбранный вами гипервизор не поддерживает нужное количество интерфейсов, их можно создать используя тот же скрипт переименовывания интерфейсов.

Пример:

```
ifconfig tun1 create; ifconfig tun1 name em1
ifconfig tun2 create; ifconfig tun2 name em2
...
```

Внимание: Интерфейсы tun являются не настоящими с точки зрения виртуальной машины.

Если на подобном tun интерфейсе будет назначен какой-либо IP адрес, он не будет доступен в виртуальной сетевой инфраструктуре. В этом случае в скрипте учитывать порядок создания и переименовая интерфейсов. Если невозможно закрыть все условные «пробелы» tun интерфейсами, нужно выбрать более подходящий гипервизор для этих целей.

После перезагрузки виртуальной машины необходимо переинизиализировать ЦУС. По этому можно сразу зайти в меню администратора («Для входа нажмите ENTER»), вход в которое доступен в течении 5 секунд.

В меню администратора нужно зайти в:

3: Управление

4: Переинизиализировать ЦУС

4.1.4 Загрузка конфига в ЦУС

После переинициализации ЦУС нужно подключиться к нему используя ключ который был создан при **инициализации**. Далее загрузить кофинг и после того как ЦУС перезагрузится и применит новую конфигурацию, нужно использовать ключ, который используется для подключения к **реальному** ЦУС или можно создать новый ключ в меню администратора:

4: Настройки безопасности

1: Зарегистрировать нового администратора