Код Безопасности

Аппаратно-программный комплекс шифрования

Континент
Версия 3.7

Руководство администратора

Обновление программного обеспечения

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Введение

Данный документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования «Континент». Версия 3.7" (далее — комплекс). В документе приводится общий порядок замены программного обеспечения комплекса версий 3.5 и 3.6 на программное обеспечение версии 3.7, а также ссылки на описание необходимых процедур.

Более подробная информация об администрировании компонентов комплекса содержится в документах, перечисленных в конце этого руководства. Ссылки на эти документы заключены в квадратные скобки и выглядят так: [**1**].

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-495-982-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": http://www.securitycode.ru/products/technical-support/.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Общий порядок действий

Выполнение процедур обновления программного обеспечения накладывает определенные ограничения на управление комплексом в штатном режиме и поэтому должно быть завершено в минимально допустимые сроки.

Следует также иметь в виду, что во время проведения процедур обновления работа VPN и межсетевого экрана не прекращается. При этом VPN, включающий в себя обновленные и необновленные узлы, остается работоспособным.

Также гарантируется совместная работа узлов обновленной и необновленной версии.

Замену программного обеспечения старых версий на более новую версию выполняют в следующем порядке:

1. Подготовка к обновлению ПО (см. стр.**6**).
2. Обновление ПО ЦУС (см. стр.**7**).
3. Обновление ПО сетевого устройства (см. стр.**9**).
4. Обновление Программы управления сервером доступа (см. стр.**11**).
5. Обновление ПО абонентского пункта (стр.**12**).

Одновременно с ПО ЦУС выполняют обновление программы управления ЦУС, а также ПО сервера доступа.

Внимание! При обновлении ПО необходимо обновить BIOS аппаратной платформы. Версии BIOS для обновления находятся на установочном диске в папке BIOS.

После обновления ПО ЦУС совместная работа ЦУС с сетевыми устройствами необновленных версий имеет следующие особенности:

- на сетевых устройствах необновленных версий сохраняется работоспособность функций, настроенных до обновления ПО ЦУС;
- на сетевых устройствах необновленных версий настройка новых функций обновленного ПО ЦУС недоступна;
- не рекомендуется вносить изменения в настройки сетевых устройств необновленных версий; если изменения необходимы, их следует выполнить до обновления ПО ЦУС или после обновления ПО сетевого устройства;
- для сетевых устройств необновленных версий сохраняется возможность переустановки парных связей;
- возможность смены ключей сетевого устройства в случае их компрометации или истечения срока действия сохраняется.

Подготовка к обновлению ПО

Перед обновлением ПО комплекса необходимо выполнить подготовительные действия.

Для подготовки к обновлению:

1. Задокументируйте все настройки комплекса (номера КШ, IP-адреса интерфейсов, подключенные сети, действующие правила фильтрации и маршрутизации). Эти данные могут понадобиться в случае неудачного обновления базы данных из резервной копии.
2. Выполните резервное копирование конфигурации ЦУС (см. [**1**]). Рекомендуется создать не менее двух резервных копий конфигурации ЦУС.
3. Выполните резервное копирование базы данных сервера доступа (см. документ "АПКШ "Континент". Сервер доступа. Руководство по администрированию"). Рекомендуется создать не менее двух резервных копий базы данных.
4. При использовании межсетевых экранов или других устройств, осуществляющих фильтрацию IP- пакетов и находящихся на пути служебного трафика комплекса, необходимо создать для этих устройств правила, которые разрешают прохождение служебных пакетов по новым протоколам и портам, указанным в приложении (см. [**1**]).
5. Проверьте правила фильтрации и правила трансляции. Правила, использующие сервис ipv6-icmp, удалите или откорректируйте, чтобы исключить применение в них данного сервиса.

Обновление ПО ЦУС

При обновлении ПО ЦУС используется резервная копия (файл конфигурации), сохраненная при подготовке к обновлению и соответствующая более ранней версии ПО.

Внимание! При установке ПО ЦУС будет создан новый идентификатор администратора комплекса. Этот идентификатор предназначен только для первого запуска программы управления ЦУС новой версии. Обязательно сохраните старый идентификатор администратора, соответствующий обновляемой версии ПО и использовавшийся при создании резервных копий. После восстановления конфигурации из резервной копии запуск Программы управления осуществляют с использованием старого идентификатора.

Для обновления ПО ЦУС:

1. Выполните инициализацию ЦУС (см. [**2**], раздел "Инициализация и подключение КШ с ЦУС"). Процедура инициализации включает в себя установку ПО новой версии.

   Если обновление ПО осуществляется на КШ с установленным сервером доступа, в ходе инициализации программой будет предложено выполнить инициализацию сервера доступа. Процедура инициализации сервера доступа описана в [**2**] (см. раздел "Инициализация сервера доступа").

2. На АРМ администратора удалите программу управления ЦУС старой версии (см. [**1**]).

   После удаления программы управления перезагрузите компьютер.

3. На АРМ администратора установите программу управления ЦУС новой версии (см. [**1**].

4. Запустите программу управления (см. [**1**]).

   На экране появится запрос на ввод пароля.

5. Введите пароль, указанный при инициализации ЦУС.

   При этом запуске программы управления используйте носитель с вновь созданным административным ключом (новый идентификатор администратора).

   Примечание. При вводе неправильного пароля или предъявлении неверных ключей выводится сообщение "Ошибка соединения с ЦУС. Неожиданное завершение потока данных. Возможно неверные ключи или пароль".

6. Откройте в окне объектов контекстное меню объекта "Центр управления сетью" и активируйте команду "Загрузить файл конфигурации". На экране появится стандартный диалог выбора файла.

7. Выберите нужную папку и укажите имя файла резервной копии, сохраненного при подготовке к обновлению ПО. Нажмите кнопку "Открыть". Начнется процедура восстановления базы данных ЦУС, при успешном завершении которой на экране появится соответствующее сообщение. Закройте окно этого сообщения.

   ЦУС приступит к загрузке сохраненной конфигурации и затем автоматически перезагрузится. После окончания перезагрузки на экране монитора ЦУС появится сообщение:

   ```
   Успешный запуск <дата> <время>
   ```

   При перезагрузке ЦУС соединение ЦУС с программой управления будет разорвано. В строке сообщений главного окна программы управления появится сообщение "Произошла потеря соединения с ЦУС. Необходимо переподключение".

8. Извлеките из считывателя ключевой носитель администратора, созданный при последней инициализации ЦУС. Данный ключевой носитель больше не понадобится.

9. Предъявите старый ключевой носитель администратора, относящийся к загруженной конфигурации ЦУС.

10. Установите соединение программы управления с ЦУС. Для этого активируйте в меню "ЦУС" команду "Установить соединение".

На экране появится запрос на ввод пароля.

11. Укажите пароль для расшифровки ключей администратора и нажмите кнопку "ОК".

Защищенное соединение программы управления с ЦУС будет установлено, и в основном окне программы управления отобразится восстановленная конфигурация комплекса. Перейдите к обновлению ПО сетевых устройств.

Примечание. Если при установке соединения произошел сбой и на экран выведено сообщение о невозможности соединения с ЦУС, проверьте параметры соединения с ЦУС, работоспособность самого ЦУС и повторите попытку соединения еще раз.

Внимание! После загрузки конфигурации КШ с ЦУС отображается в ПУ ЦУС как отключенный. Для корректного отображения необходимо добавить лицензию на обновление КШ.

Обновление ПО сетевого устройства

Для обновления ПО сетевого устройства до версии 3.7 необходима лицензия на обновление. При этом количество обновляемых сетевых устройств комплекса не может превышать количество, указанное в лицензии на обновление.

При обновлении ПО КШ следует учитывать следующие условия:

- Дистанционное обновление ПО КШ с версии 3.5 до 3.7 возможно только в том случае, если раннее не было выполнено дистанционное обновление с 3.x до 3.5. В остальных случаях возможно только ручное обновление.
- Дистанционное обновление ПО с версии 3.6 до 3.7 возможно только в том случае, если раннее не было выполнено дистанционного обновления с 3.x до 3.6. В остальных случаях возможно только ручное обновление ПО.

Дистанционное обновление ПО сетевого устройства

Дистанционное обновление ПО выполняют средствами программы управления при наличии лицензии на обновление ПО сетевого устройства.

Для обновления ПО сетевого устройства:

1. Поочередно на всех сетевых устройствах замените ПО старой версии на ПО новой версии. Замену ПО осуществляют дистанционно из Программы управления ЦУС (см. [**1**]).

   Примечание. Если обновление ПО сетевого устройства не выполняется, проверьте работоспособность канала связи. Если канал связи работоспособен, а обновление ПО по-прежнему не происходит, выполните обновление ПО сетевого устройства вручную (см. стр. 9).

2. Обязательно проверьте и при необходимости отредактируйте список сетевых объектов и список правил фильтрации (см. [**1**]). Редактирование списков осуществляют в Программе управления ЦУС.
3. Убедитесь в правильности настроек штатного режима работы комплекса "Континент".

   Примечание. Обязательно проверьте и при необходимости отредактируйте часовой пояс, в котором эксплуатируется сетевое устройство. Редактирование часового пояса осуществляют в Программе управления ЦУС (см. [**1**], Настройка общих параметров сетевого устройства).

Ручное обновление ПО сетевого устройства

Ручное обновление ПО выполняют при отсутствии возможности дистанционного обновления.

Ручное обновление может быть выполнено без лицензии на обновление, однако в этом случае в ПУ ЦУС сетевое устройство будет отображаться как отключенное, а в его журнале появится сообщение об отстутствии лицензии.

Для обновления ПО сетевого устройства:

1. Запишите конфигурацию и ключи сетевого устройства на носитель (см. [**1**]). Запись конфигурации осуществляют в Программе управления новой версии.
2. Выполните процедуру инициализации ПАК "Соболь". В настройках общих параметров у параметра "Версия криптографической схемы" установите значение "2.0" (см. эксплуатационную документацию ПАК "Соболь").
3. Установите программное обеспечение сетевого устройства (см. [**2**]).
4. Выполните инициализацию сетевого устройства (см. [**2**]).
5. Выполните инициализацию сервера доступа (при наличии) (см. [**2**]).

Примечание. При инициализации сервера доступа создается идентификатор администратора сервера доступа. Этот идентификатор предназначен для запуска Программы управления сервера доступа новой версии.

Ручное обновление ПО кластера сетевых устройств

Для обновления ПО кластера сетевых устройств:

1. Выполните процедуры записи конфигурации основного и резервного устройств, а также ключей устройства на носитель (см. [**1**], раздел "Запись конфигурации сетевого устройства на носитель"). Запись конфигурации осуществляют в программе управления ЦУС новой версии.
2. Выключите питание основного и резервного устройств.
3. На основном устройстве выполните процедуру инициализации ПАК "Соболь". В настройках общих параметров у параметра "Версия криптографической схемы" установите значение "2.0" (см. эксплуатационную документацию ПАК "Соболь").
4. На основном устройстве выполните **пп. 1–19** процедуры установки программного обеспечения (см. [**2**], "Установка программного обеспечения").

   Дождитесь загрузки операционной системы и появления сообщения:

   ```
   Криптографический шлюз "Континент"
   Конфигурация: КШ
   Вставьте носитель с конфигурацией и нажмите Enter
   ```

5. Загрузите конфигурацию основного устройства. Для этого выполните **п.п. 5-9** процедуры инициализации сетевого устройства (см. [**2**], "Инициализация и подключение сетевого устройства").

   Имя предъявляемого на USB-флеш-накопителе конфигурационного файла должно быть "gate.cfg" (без кавычек).

6. На резервном устройстве выполните процедуру инициализации ПАК "Соболь". В настройках общих параметров у параметра "Версия криптографической схемы" установите значение "2.0" (см. эксплуатационную документацию ПАК "Соболь").
7. На резервном устройстве выполните **п.п. 1 - 19** процедуры установки программного обеспечения (см. [**2**], "Установка программного обеспечения").

   Дождитесь загрузки операционной системы и появления сообщения, приведенного выше.
8. Загрузите конфигурацию резервного устройства. Для этого выполните **п.п. 5 - 9** процедуры инициализации сетевого устройства (см. [**2**], "Инициализация и подключение сетевого устройства").

   См. примечание к п.5.

9. Проверьте версию ПО. Для этого в ПУ ЦУС в окне объектов выберите кластер с обновленным ПО, вызовите диалоговое окно "Свойства <сетевого устройства>" и перейдите на вкладку "Версия ПО".
10. Перезагрузите кластер (см. [**1**], раздел "Перезагрузка сетевого устройства").

Обновление Программы управления сервером доступа

Обновление ПО сервера доступа осуществляется в полном соответствии с обновлением ПО сетевого устройства (см. стр.**9**).

Примечание. При инициализации сервера доступа создается идентификатор администратора сервера доступа. Этот идентификатор предназначен для запуска Программы управления сервером доступа новой версии.

Для обновления Программы управления ее необходимо установить заново с установочного диска, содержащего ПО новой версии.

Внимание! Перед выполнением переустановки обязательно завершите работу программы управления и программы просмотра журнала, иначе переустановка завершится с ошибкой.

Для обновления Программы управления СД:

1. Удалите Программу управления СД с компьютера (см. [**5**]).
2. Установите Программу управления СД на компьютер (см. [**5**]). При установке используйте установочный диск, содержащий ПО новой версии. В ходе установки настройте параметры соединения Программы управления с сервером доступа.
3. Запустите Программу управления СД и установите соединение с сервером доступа.

   На экране появится запрос на ввод пароля.
4. Введите пароль, указанный при инициализации сервера доступа.
5. После успешного соединения с сервером доступа выберите в разделе "Настройки сервера" команду "Восстановить" и укажите файл резервной копии базы данных, созданной на этапе подготовки к обновлению ПО.

   Произойдет восстановление базы данных и появится сообщение о его успешном завершении и необходимости переподключиться к СД со старыми ключами.
6. Предъявите носитель со старыми ключами и затем нажмите кнопку "Установка/разрыв связи с сервером".

   Появится запрос на ввод пароля.
7. Укажите пароль для расшифровки ключей администратора и нажмите кнопку "OK".

   Произойдет соединение с сервером доступа.

Обновление Абонентского пункта

Для обновления Абонентского пункта версии 3.5 и выше:

1. Установите Абонентский пункт на компьютер (см. [**9**]). При установке используйте установочный диск, содержащий ПО новой версии.

   Программа установки удалит ПО старой версии автоматически. После удаления старой версии появится запрос на перезагрузку компьютера. Перезагрузите компьютер. После перезагрузки программа установки автоматически продолжит свою работу.

2. Восстановите ранее установленные сертификаты (см. [**10**]).

Для обновления Абонентского пункта версии 3.3:

1. Удалите с компьютера программное обеспечение старой версии средствами операционной системы (см. [**9**]).
2. Установите Абонентский пункт на компьютер (см. [**9**]). При установке используйте установочный диск, содержащий ПО новой версии.
3. Восстановите ранее установленные сертификаты (см. [**10**]).

Документация

1.	Аппаратно-программный комплекс шифрования "Континент". Централизованное управление комплексом. Руководство администратора
2.	Аппаратно-программный комплекс шифрования "Континент". Локальное управление сетевыми устройствами. Руководство администратора
3.	Аппаратно-программный комплекс шифрования "Континент". Аудит. Руководство администратора
4.	Аппаратно-программный комплекс шифрования "Континент". Аутентификация пользователя. Руководство администратора
5.	Аппаратно-программный комплекс шифрования "Континент". Сервер доступа. Руководство администратора
6.	Аппаратно-программный комплекс шифрования "Континент". Программа мониторинга КШ. Руководство пользователя
7.	Аппаратно-программный комплекс шифрования "Континент". Тестирование каналов связи. Руководство администратора
8.	Аппаратно-программный комплекс шифрования "Континент". Обновление программного обеспечения. Руководство администратора
9.	Средство криптографической защиты информации "Континент-АП". Руководство администратора. Windows
10.	Средство криптографической защиты информации "Континент-АП". Руководство пользователя. Windows
11.	Аппаратно-программный комплекс шифрования "Континент". Автоматизированное рабочее место генерации ключей. Руководство администратора
12.	Аппаратно-программный комплекс шифрования "Континент". Система обнаружения вторжений. Руководство администратора

Примечание. Набор документов, входящих в комплект поставки, может отличаться от указанного списка.