



КОД БЕЗОПАСНОСТИ

Аппаратно-программный комплекс шифрования

Континент

Версия 3.М2

Руководство администратора

Обновление программного обеспечения



КОД БЕЗОПАСНОСТИ

© Компания "Код Безопасности", 2019. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес: **115127, Россия, Москва, а/я 66
ООО "Код Безопасности"**

Телефон: **8 495 982-30-20**

E-mail: **info@securitycode.ru**

Web: **<https://www.securitycode.ru>**

Оглавление

Введение	4
Общий порядок действий	5
Подготовка к обновлению программного обеспечения	6
Обновление программного обеспечения ЦУС	7
Конфигурирование базы данных журналов	9
Запись ключей сетевого устройства на носитель	10
Обновление программного обеспечения сетевого устройства	11
Документация	12

Введение

Данный документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования «Континент». Версия 3.М2" (далее — комплекс). В документе приводится общий порядок замены программного обеспечения комплекса версии 3.М на программное обеспечение (далее — ПО) версии 3.М2, 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. Информация о продуктах компании "Код Безопасности" представлена на сайте <https://www.securitycode.ru/products/>.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-800-505-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": <https://www.securitycode.ru/services/techsupport/>.

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 <https://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 не обновленные узлы, остается работоспособным.

Также гарантируется совместная работа узлов обновленной и не обновленной версии.

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

1. Подготовка к обновлению программного обеспечения комплекса (см. стр.6).
2. Обновление программного обеспечения ЦУС (см. стр.7).
3. Конфигурирование базы данных журналов (см. стр.9).
4. Запись ключей сетевых устройств на носители (см. стр.10).
5. Обновление программного обеспечения сетевых устройств (см. стр.11).

Одновременно с ПО ЦУС выполняют обновление программы управления ЦУС.

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 не обновленных версий имеет следующие особенности:

- на сетевых устройствах не обновленных версий сохраняется работоспособность функций, настроенных до обновления ПО ЦУС;
- на сетевых устройствах не обновленных версий настройка новых функций обновленного ПО ЦУС недоступна;
- не рекомендуется вносить изменения в настройки сетевых устройств не обновленных версий; если изменения необходимы, их следует выполнить до обновления ПО ЦУС или после обновления ПО сетевого устройства;
- на сетевом устройстве не рекомендуется создавать и изменять правила фильтрации и трансляции до обновления ПО сетевого устройства до версии 3.М2;
- не рекомендуется создавать и изменять сетевые объекты с привязанными криптошлюзами, не обновленными до версии 3.М2;
- для сетевых устройств не обновленных версий сохраняется возможность переустановки парных связей;
- возможность смены ключей сетевого устройства в случае их компрометации или истечения срока действия сохраняется.

Внимание! В ходе обновления ПО комплекса не рекомендуется выполнять смену ключей парных связей между сетевыми устройствами с обновленным до версии 3.М2 и не обновленным (версии 3.М) программным обеспечением.

Подготовка к обновлению программного обеспечения

Перед обновлением ПО комплекса необходимо выполнить подготовительные действия.

Для подготовки к обновлению:

1. Задокументируйте все настройки комплекса (номера сетевых устройств, IP-адреса интерфейсов, подключенные сети, действующие правила фильтрации и маршрутизации). Эти данные могут понадобиться в случае неудачного обновления базы данных из резервной копии.
2. Если в сетевых устройствах комплекса используются VLAN-интерфейсы, на каждом из таких устройств необходимо переименовать зарегистрированные VLAN-интерфейсы. Новое наименование интерфейса должно иметь вид: Vlan№, где № — присваиваемый администратором номер. Рекомендуется присваивать интерфейсам устройства номера последовательно, начиная с 0. Например Vlan0, Vlan1, Vlan2 и т.д. Для этого в свойствах сетевого устройства на вкладке "Интерфейсы" активируйте закладку "VLAN" и в поле "Название" введите новое наименование (см. [1], раздел "VLAN-интерфейсы").
3. Выполните резервное копирование конфигурации ЦУС (см. [1]). Рекомендуется создать не менее двух резервных копий конфигурации ЦУС.
4. Сохраните идентификатор администратора, соответствующий версии ПО 3.М и использовавшийся при создании резервных копий. После восстановления конфигурации из резервной копии запуск программы управления осуществляются с использованием старого идентификатора.
5. В программе управления ЦУС для каждого зарегистрированного сетевого устройства сохраните его конфигурацию на отчуждаемый носитель (USB-флеш-накопитель) (см. [1], раздел "Запись конфигурации сетевого устройства на носитель").
6. 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]).
7. Проверьте правила фильтрации и правила трансляции. Правила, использующие сервис ipv6-istr, удалите или откорректируйте, чтобы исключить применение в них данного сервиса.

Обновление программного обеспечения 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.

Для обновления ПО ЦУС:

1. Выполните инициализацию ЦУС (см. [2], раздел "Инициализация и подключение ЦУС"). Процедура инициализации включает в себя установку ПО новой версии.
2. На АРМ администратора удалите программу управления ЦУС старой версии (см. [1]).
После удаления программы управления перезагрузите компьютер.
3. Удалите стандартными средствами Windows СУБД, используемую для сбора и хранения журналов.
4. Повторно установите СУБД для сбора и хранения журналов.
5. На АРМ администратора установите программу управления ЦУС новой версии (см. [1]).
6. Запустите программу управления (см. [1]).
На экране появится запрос на ввод пароля.
7. 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".

8. Откройте в окне объектов контекстное меню объекта "Центр управления сетью" и активируйте команду "Загрузить файл конфигурации". На экране появится стандартный диалог выбора файла.
9. 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".

10. Извлеките из считывателя ключевой носитель администратора, созданный при последней инициализации ЦУС. Данный ключевой носитель больше не понадобится.
11. Предъявите старый ключевой носитель администратора, относящийся к загруженной конфигурации ЦУС.

- 12.** Установите соединение программы управления с ЦУС. Для этого активируйте в меню "ЦУС" команду "Установить соединение".

На экране появится запрос на ввод пароля.

- 13.** Если файл резервной копии, указанный в п. 7, был создан в версии 3.М, не вводя пароля нажмите кнопку "ОК".

Если файл резервной копии был создан в версии 3.М2, 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 конфигурированию базы данных журналов.

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.

Конфигурирование базы данных журналов

Конфигурирование выполняют на АРМ администратора средствами компонента "Конфигуратор БД журналов ЦУС". Описание работы по конфигурированию базы данных приведено в документе [3].

Запись ключей сетевого устройства на носитель

При инициализации, выполняемой в ходе обновления ПО сетевого устройства, необходимо загрузить в сетевое устройство комплект ключей, хранящийся на внешнем носителе. Комплект ключей должен быть записан на внешний носитель средствами ПУ ЦУС версии 3.М2.

Внимание! Загружаемые в сетевое устройство ключи не должны быть просрочены. Поэтому перед записью ключей на носитель у каждого сетевого устройства необходимо проверить значение параметра "Время смены ключей", отображаемое в общей таблице состояния КШ (см. [1], раздел "Мониторинг состояния комплекса"). Проверку выполняют в ПУ ЦУС обновленной версии. Если ключи просрочены, следует выполнить плановую смену ключей (см. [1]).

Описание процедуры записи ключей приведено в документе [1] (см. раздел "Запись ключей сетевого устройства на носитель").

Обновление программного обеспечения сетевого устройства

Для обновления ПО сетевого устройства до версии 3.М2 необходима лицензия на обновление. При этом количество обновляемых сетевых устройств комплекса не может превышать количество, указанное в лицензии на обновление.

Внимание! Для обновления ПО сетевого устройства необходимо иметь:

1. Внешний носитель с записанным на него конфигурационным файлом криптошлюза/криптокоммутатора. При этом может быть использован конфигурационный файл, записанный средствами ПУ ЦУС как версии 3.М, так и версии 3.М2 (см. [1], раздел "Запись конфигурации сетевого устройства на носитель").
2. Ключевой носитель с комплектом ключей сетевого устройства, записанным средствами обновленной до версии 3.М2 ПУ ЦУС (см. стр.10).

Для обновления ПО сетевого устройства:

1. Выполните процедуру инициализации ПАК "Соболь". В настройках общих параметров у параметра "Версия криптографической схемы" установите значение "2.0" (см. эксплуатационную документацию ПАК "Соболь").
2. Выполните установку ПО сетевого устройства версии 3.М2 (см. [2], раздел "Установка программного обеспечения").
3. Выполните инициализацию и подключение сетевого устройства (см. [2], раздел "Инициализация и подключение сетевого устройства"). При инициализации используйте подготовленные файл конфигурации и комплект ключей.
4. В ПУ ЦУС выполните для данного сетевого устройства смену ключей парной связи (см. [1], подраздел "Смена ключей парной связи").

Документация

- | |
|---|
| 1. Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Централизованное управление комплексом |
| 2. Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Локальное управление сетевыми устройствами |
| 3. Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аудит |
| 4. Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аутентификация пользователя |