КОД безопасности

Комплекс безопасности

Континент
Версия 4

Руководство администратора

Установка и обновление ПО комплекса

АМБС.26.20.40.140.001 90 2

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

Список сокращений

ДСЧ	Датчик случайных чисел
МК	Менеджер конфигурации
ОС	Операционная система
ПО	Программное обеспечение
РМ	Рабочее место
УБ	Узел безопасности
ЦУС	Центр управления сетью
CSP	Cryptography Service Provider
IP	Internet Protocol

Введение

Документ предназначен для администраторов изделия "Комплекс безопасности "Континент". Версия 4" (далее — комплекс). В нем содержатся сведения, необходимые администраторам для установки и обновления ПО комплекса.

Дополнительные сведения, необходимые администратору комплекса, содержатся в документах [**1**]–[**5**].

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

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.

Установка Менеджера конфигурации

Установку и удаление МК и CSP может выполнить только пользователь, наделенный правами локального администратора данного компьютера.

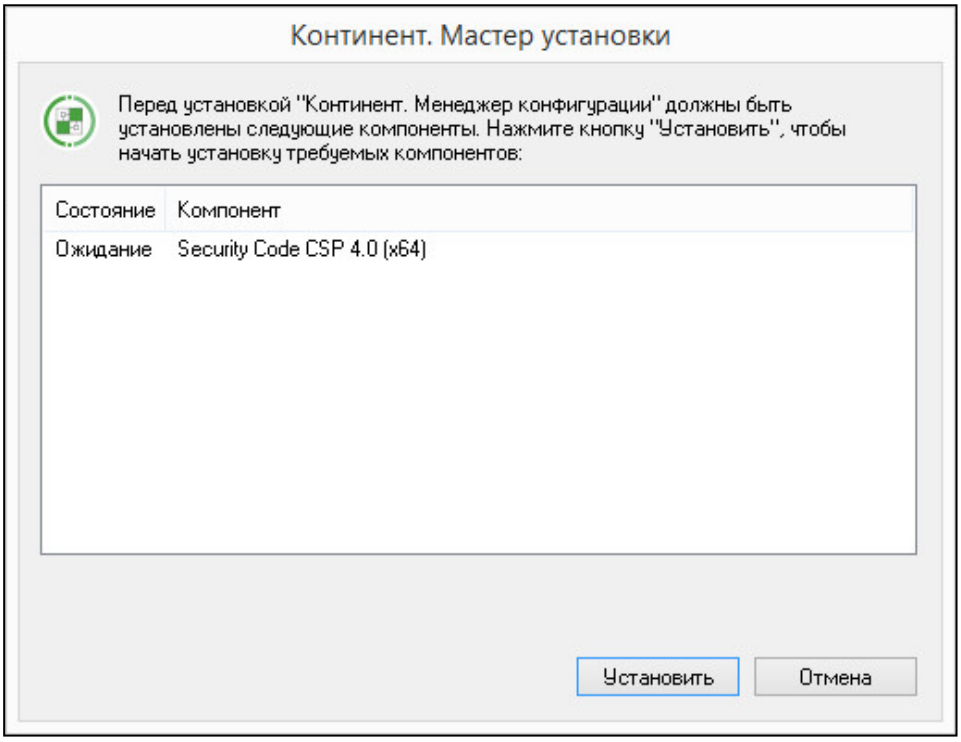
Перед запуском программы установки завершите работу всех приложений.

При установке МК отключите компьютер, на который устанавливается МК, от сети либо заблокируйте с него доступ в интернет.

Для установки МК:

1. Запустите на исполнение:
   - файл \Setup\Continent\MS\Rus\x86\Setup.exe — для 32-разрядной ОС;
   - файл \Setup\Continent\MS\Rus\x64\Setup.exe — для 64-разрядной ОС.

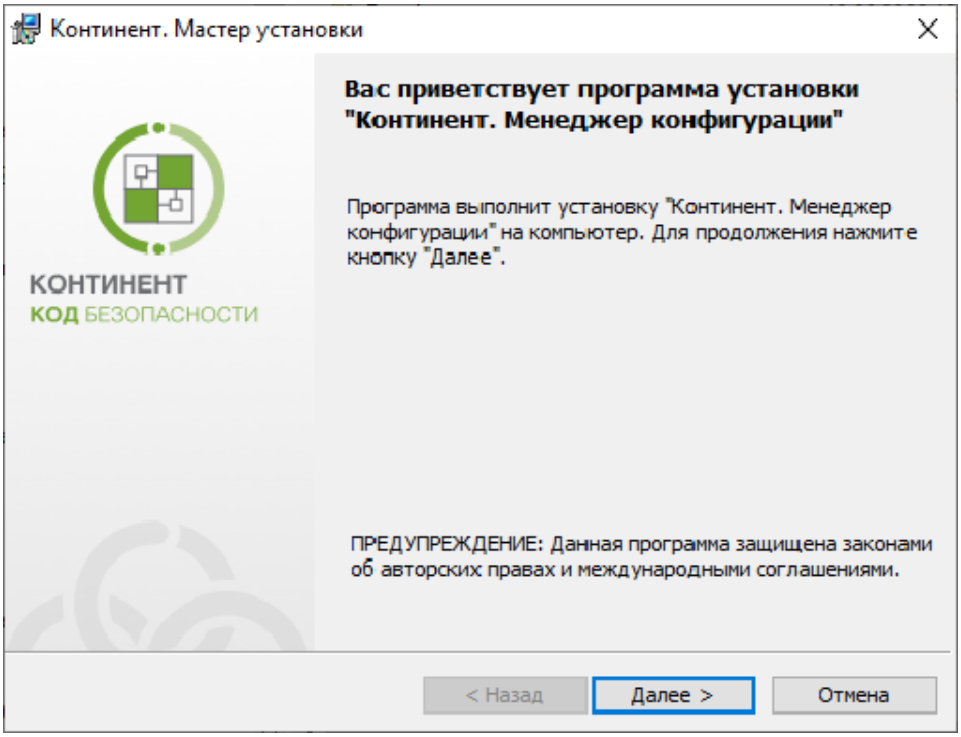
   На экране появится окно со списком дополнительных компонентов, которые должны быть установлены до начала установки МК.



Примечание. Если на компьютере уже установлен сторонний криптопровайдер (КриптоПро CSP), утилита установки не будет предлагать установить компонент "Security Code CSP". Выбор криптопровайдера выполняется после установки МК (см. [**4**]).

2. Нажмите кнопку "Установить".

   После завершения установки дополнительных компонентов на экране появится стартовое окно программы установки МК.



3. Ознакомьтесь с информацией, содержащейся в стартовом окне, и нажмите кнопку "Далее >" для продолжения установки.

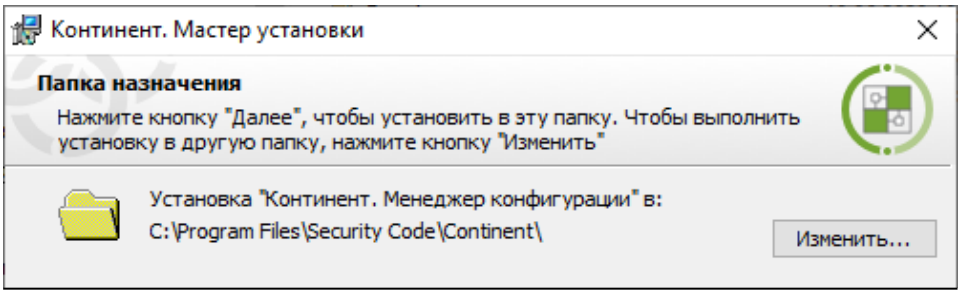
   Появится окно с текстом лицензионного соглашения.

4. Изучите содержание лицензионного соглашения, прочитав его до конца. Если вы согласны с условиями лицензионного соглашения, установите отметку в поле "Я принимаю условия лицензионного соглашения", затем нажмите кнопку "Далее >".

   На экране появится окно "Папка назначения" для определения папки установки программы "Континент. Менеджер конфигурации".

5. При необходимости измените папку установки и нажмите кнопку "Далее >".

   Для выбора папки используйте кнопку "Изменить...".



   По умолчанию программа установки копирует файлы на системный диск в папку ..\Program Files\Security Code\Continent.

6. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится финальное окно мастера установки МК.

   Примечание. Для корректировки параметров установки используйте кнопку "< Назад".

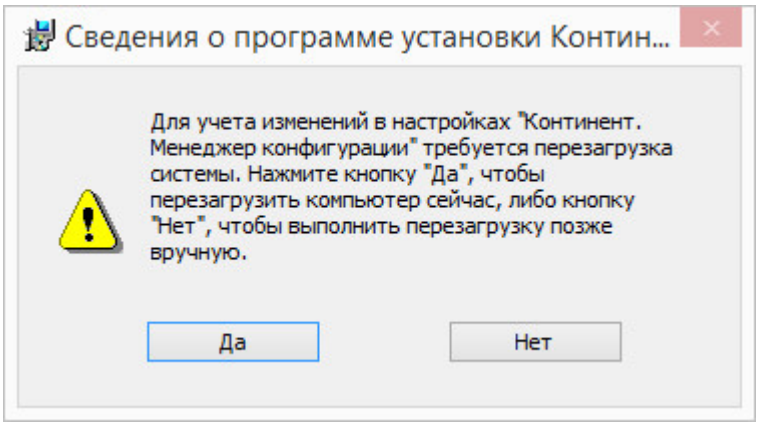
7. Для начала установки программы нажмите кнопку "Установить".

   Программа установки приступит к копированию файлов на жесткий диск компьютера. Ход выполнения процесса копирования отображается на экране в специальном окне.

   Примечание. Если программа установки в процессе копирования не обнаружит файл, заявленный в комплекте поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. Скопируйте еще раз файлы с установочного диска и повторите установку. Если это не приведет к желаемому результату, обратитесь к поставщику комплекса.

После установки МК на экране появится информационное окно об успешной установке приложения.

8. Для завершения установки нажмите кнопку "Готово". При этом появится окно с предложением перезагрузить компьютер.



9. Перезагрузите компьютер.

   После перезагрузки на рабочем столе появится ярлык МК, а в меню "Пуск" ОС Windows появится группа "Код Безопасности" с командами — "Менеджер конфигурации", "Код Безопасности CSP" и "Восстановление Код Безопасности CSP".

Примечание. Не допускается беспрерывная работа с МК в течение 7 суток без перезапуска.

Обновление программного обеспечения

Обновление ПО комплекса выполняют в следующем порядке:

1. Загрузка файлов обновления в репозиторий (см. ниже).
2. Обновление ПО ЦУС (процедура аналогична процедуре обновления УБ, см. стр. **11**).
3. Обновление МК (см. стр. **13**).
4. Обновление ПО УБ защищаемой сети (см. стр. **11**).

В случае сбоя при обновлении ПО узла безопасности произойдет автоматическое восстановление последней рабочей версии ПО. Повторите процедуру обновления ПО этого узла безопасности еще раз.

Примечание. Информация о версиях ПО на компонентах комплекса отображается в подразделе "Администрирование | Обновления" МК.

Управление репозиторием обновлений

Загрузить файлы обновления в репозиторий можно двумя способами — с сервера обновлений (в том числе без участия администратора) или из локального источника.

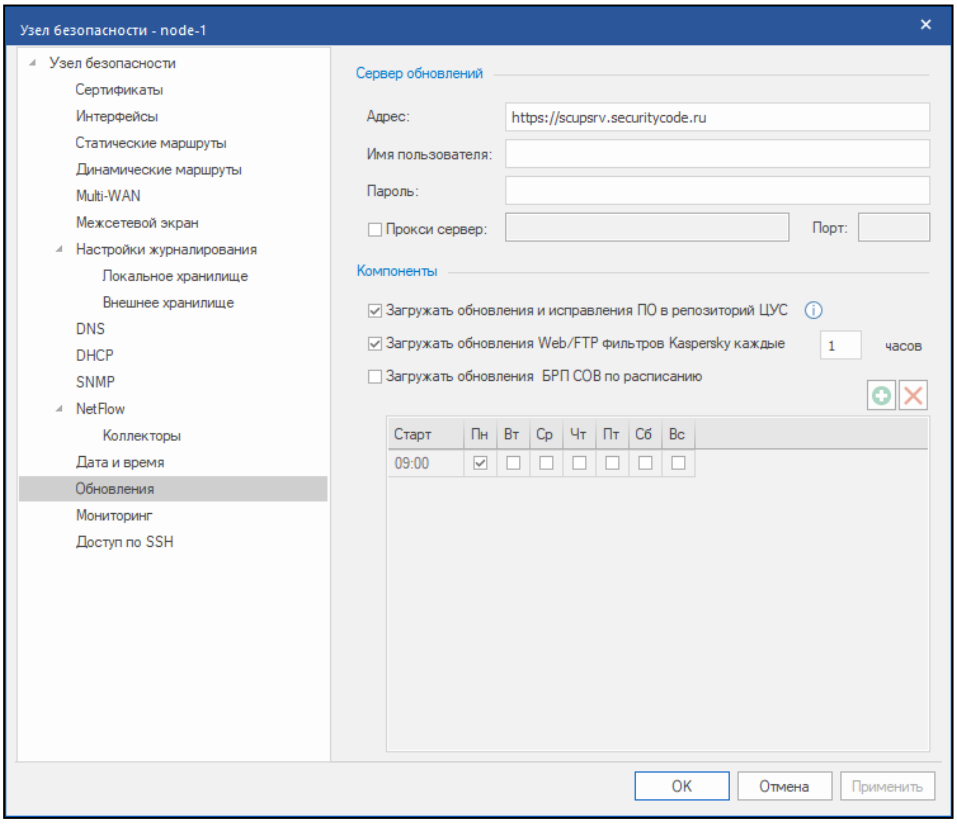
Настройка доступа к серверу обновлений осуществляется в МК только для ЦУС.

Для настройки параметров сервера обновлений:

1. Перезагрузите устройство, на котором установлен МК.
2. Откройте МК и перейдите в раздел "Структура".
3. В списке узлов безопасности выберите ЦУС и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно "Свойства узла".
4. Выберите в левой части окна в разделе "Узел безопасности" подраздел "Обновления".

   В правой части окна появятся параметры обновлений.



5. Для настройки параметров подключения к серверу обновлений выполните следующие действия:
   - Укажите учетные данные пользователя.

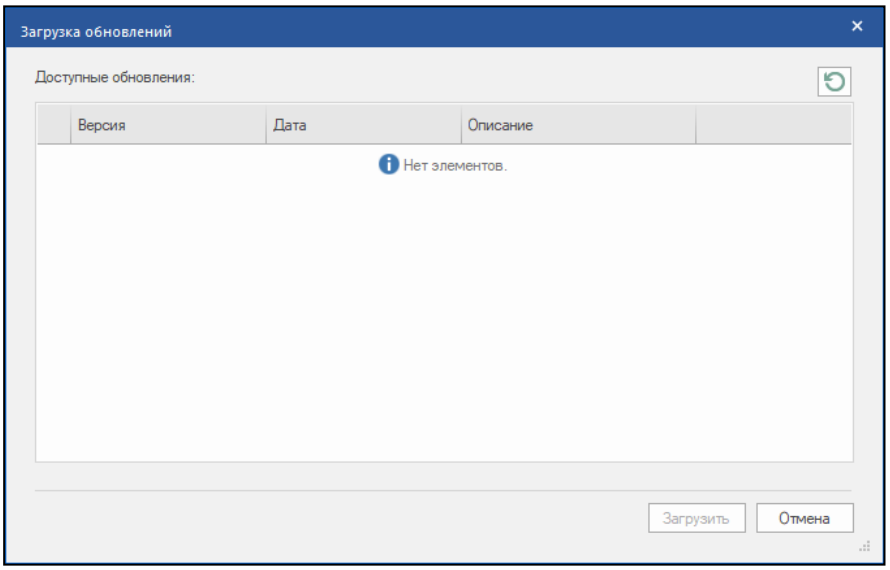
     Примечание. Для получения учетных данных пользователя обратитесь в службу технической поддержки (см. стр. 5).
   - При необходимости использования прокси-сервера укажите его IP-адрес и порт подключения.
6. Для включения автоматической загрузки обновлений и исправлений ПО в репозиторий ЦУС установите отметку в соответствующем поле.
7. Нажмите кнопку "ОК".
8. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте ЦУС и его подчиненные УБ и нажмите кнопку "ОК".

Для принудительной загрузки обновлений в репозиторий:

Примечание. Перед выполнением процедуры необходимо задать все параметры для подключения к серверу обновлений.

1. Откройте МК, перейдите в раздел "Администрирование" и выберите подраздел "Обновления".
2. В списке узлов безопасности выберите нужный узел и нажмите кнопку "Загрузка" на панели инструментов.

   На экране появится окно "Загрузка обновлений".



3. Нажмите кнопку  для получения актуального списка доступных обновлений.

   Будет выполнен запрос к серверу обновлений и, при наличии доступных обновлений, на экране отобразится список ПО.
4. Выберите требуемую версию ПО из списка и нажмите кнопку "Загрузить".

   После загрузки файла с сервера в репозиторий в списке обновлений отобразится новая версия ПО.

Для импорта файла обновления ПО из локального источника:

1. Откройте МК, перейдите в подраздел "Администрирование | Обновления" и нажмите кнопку "Импорт" на панели инструментов.

   На экране появится стандартное окно открытия файла.
2. Укажите файл обновления с расширением *.tgz.signed (при импорте с установочного диска с ПО файлы обновления обычно лежат в корневом каталоге).

Начнется процесс загрузки файла обновления в базу ЦУС. После успешной загрузки появится соответствующее информационное окно.

3. Нажмите кнопку "ОК".

   В репозитории обновлений появится файл обновления с указанием его типа, версии и размера.

Для удаления файла обновления из репозитория:

1. Откройте МК, перейдите в подраздел "Администрирование | Обновления", выделите ненужный файл обновления и нажмите кнопку "Удалить" на панели инструментов.

   На экране появится окно подтверждения удаления.

2. Нажмите кнопку "Да".

   Файл с обновлением будет удален из репозитория.

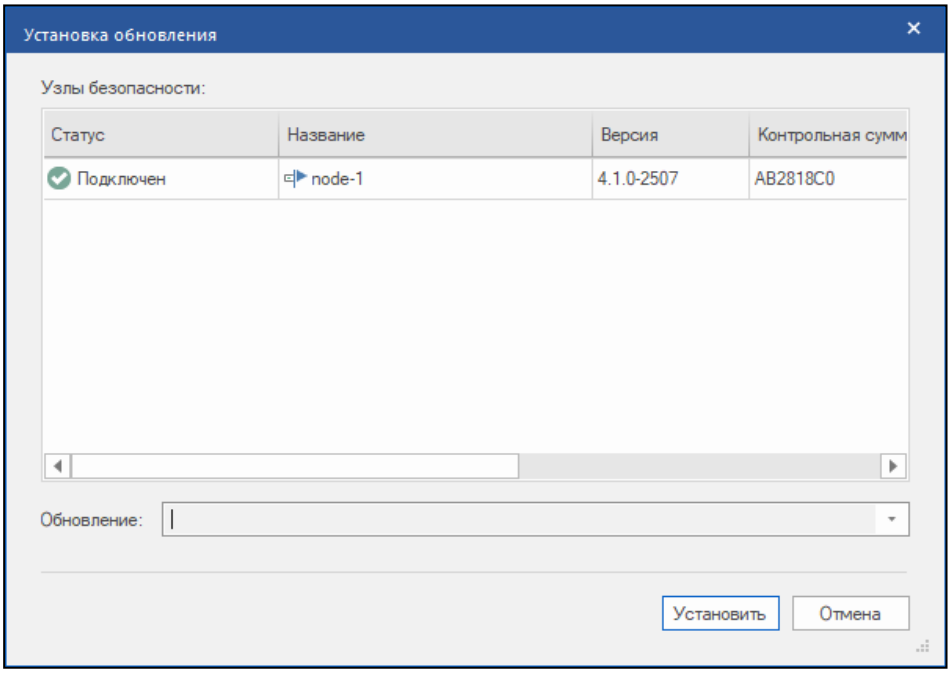
Обновление ПО УБ

Внимание! Перед обновлением/откатом ПО рекомендуется создать резервную копию (бэкап) настроек узла, а в случае обновления ПО ЦУС — и его подчиненных узлов.

Для установки обновления ПО:

1. Перезагрузите УБ и устройство, на котором установлен МК.
2. Откройте МК и перейдите в подраздел "Администрирование | Обновления".
3. В списке узлов безопасности выберите нужный узел и нажмите кнопку "Установить обновление" на панели инструментов.

   На экране появится окно "Установка обновления".



4. Выберите нужную версию обновления ПО из раскрывающегося списка поля "Обновление" и нажмите кнопку "Установить" в окне запроса.

   На экране появится сообщение о добавлении новой задачи.

Внимание! После обновления ПО узел безопасности автоматически перезагрузится. В случае обновления ПО ЦУС соединение с МК будет разорвано, после окончания перезагрузки ЦУС необходимо заново установить соединение между МК и ЦУС.
После обновления ПО версии 4.0.3 до 4.1 необходимо установить политику на УБ.

Для установки обновления ПО ЦУС с подключенным РЦУС:

1. Выполните установку обновления ПО ЦУС (см. стр. **11**).

   Примечание. Одновременное обновление активного и резервного ЦУС невозможно. Необходимо дождаться завершения установки обновлений.

   ЦУС автоматически перегрузится и перейдет в статус "Резервный". Подключение МК к ЦУС будет разорвано.
2. Подождите несколько минут и заново установите соединение между МК и ЦУС.
3. Перейдите в раздел "Структура".
4. В списке УБ выделите обновленный ЦУС, правой кнопкой мыши вызовите контекстное меню и выберите пункт "Резервирование — Назначить ЦУС активным".
5. В открывшемся окне нажмите кнопку "Да" для подтверждения операции.

   Появится сообщение об изменении статуса ЦУС. Подключение МК к ЦУС будет разорвано.
6. Подождите несколько минут и заново установите соединение между МК и ЦУС.
7. Выполните установку обновления ПО РЦУС (см. стр. **11**).
8. Дождитесь завершения перезагрузки РЦУС после обновления ПО.
9. Перейдите в раздел "Структура".
10. В списке УБ выделите РЦУС, для множественного выбора используйте клавишу Ctrl.
11. Правой кнопкой мыши вызовите контекстное меню и выберите пункт "Резервирование — Синхронизировать ЦУС".
12. В открывшемся окне нажмите кнопку "Да" для подтверждения операции.

    Начнется процедура синхронизации. На экране будет отображаться прогресс-бар выполнения, который закроется по окончании процедуры.
13. Статус РЦУС в списке УБ изменится на "Синхронизирован".

Для отмены последнего обновления ПО:

1. Откройте МК и перейдите в подраздел "Администрирование | Обновления".
2. В списке узлов безопасности выберите нужные узлы и нажмите кнопку "Отменить последнее обновление" на панели инструментов.

   На экране появится запрос на подтверждение операции.
3. Нажмите кнопку "Да".

   Будет восстановлена версия ПО УБ до обновления, после чего на экране появится соответствующее информационное окно.

   При отмене последнего обновления ПО ЦУС на экране появится сообщение о добавлении новой задачи.
4. Нажмите кнопку "ОК" в окне сообщения.

   Примечание. Будет восстановлена активная на момент обновления конфигурация УБ.

Обновление ПО УБ кластера

Обновление ПО УБ кластера необходимо проводить в следующем порядке:

1. Выполните обновление ПО компонента кластера со статусом "В ожидании".
2. Назначьте обновленный УБ активным.
3. Выполните обновление ПО компонента кластера со статусом "В ожидании".
4. Установите политику на кластер, затем назначьте требуемый УБ активным.

Примечание.
УБ со статусом "В ожидании" может сменить статус на "Не готов к работе" сразу после обновления. В этом случае для завершения обновления необходимо выполнить следующие действия:

- Установите политику на кластер. При этом на еще не обновленный ("Активный") узел кластера данная политика не установится. После установки политики уже обновленный УБ автоматически станет активным, еще не обновленный УБ соответственно получит статус "В ожидании".
- Выполните обновление ПО УБ "В ожидании" (на который не установилась политика), после обновления он также может иметь статус "Не готов к работе".
- Установите политику на кластер.

Отмену последнего обновления ПО УБ кластера необходимо проводить в следующем порядке:

1. Выполните отмену обновления ПО компонента кластера со статусом "В ожидании" (см. стр. **12**).

   Статус УБ изменится на "Не готов к работе".
2. Остановите активный УБ после отображения статуса "Исправный, обновленный".
3. Выполните отмену обновления ПО остановленного УБ (см. стр. **12**).
4. Убедитесь, что статусы УБ изменились на значение "Исправный", затем установите политику на кластер.

Обновление Менеджера конфигурации

Для обновления ПО на РМ администратора:

1. На панели управления ОС Windows на РМ администратора выберите элемент "Программы и компоненты", вызовите контекстное меню программы "Континент. Менеджер конфигурации" и выберите в нем команду "Изменить".
2. В открывшемся окне сервисной программы нажмите кнопку "Далее".
3. В окне обслуживания программ выберите "Удалить" и нажмите кнопку "Далее".
4. В открывшемся окне удаления программы нажмите кнопку "Удалить".

   Начнется процесс деинсталляции ПО.
5. После завершения процесса деинсталляции нажмите кнопку "Готово".
6. В появившемся запросе на перезагрузку ПК выберите "Да".

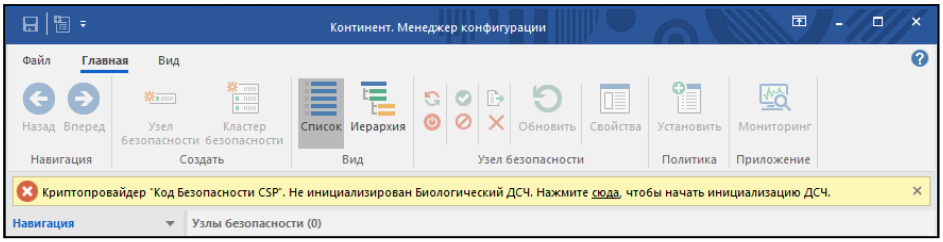
   Будет выполнена перезагрузка РМ администратора для завершения процесса деинсталляции.
7. На панели управления выберите элемент "Программы и компоненты", вызовите контекстное меню программы "Код Безопасности CSP" и выберите в нем команду "Удалить".
8. В открывшемся окне сервисной программы нажмите кнопку "Да".

   Начнется процесс деинсталляции ПО.
9. После завершения процесса деинсталляции в появившемся запросе на перезагрузку ПК выберите "Да".

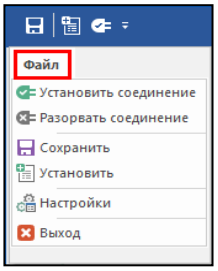
   Будет выполнена перезагрузка РМ администратора для завершения процесса деинсталляции.
10. Поместите установочный диск с дистрибутивом МК в устройство чтения компакт-дисков и перейдите в директорию \Setup\Continent\MS\Rus, а затем выберите директорию, соответствующую разрядности ОС РМ администратора.

    Примечание. В случае если дистрибутив МК получен при критическом обновлении ПО по сети интернет, перейдите к директории, содержащей файл дистрибутива.
11. Установите МК (см. стр. **6**).

Примечание. При первом запуске МК после его обновления в главном окне может быть отображено информационное сообщение о необходимости выполнить инициализацию биологического ДСЧ.



Нажмите по ссылке для начала процесса инициализации ДСЧ и следуйте указаниям на экране. Дождитесь завершения процесса накопления энтропии, а затем нажмите кнопку "Файл" в левом верхнем углу МК и в раскрывшемся списке выберите команду "Установить соединение".



Документация

1. Комплекс безопасности "Континент". Версия 4. Руководство администратора. Межсетевое экранирование.
2. Комплекс безопасности "Континент". Версия 4. Руководство администратора. Обнаружение и предотвращение вторжений.
3. Комплекс безопасности "Континент". Версия 4. Руководство администратора. Мониторинг и аудит.
4. Комплекс безопасности "Континент". Версия 4. Руководство администратора. Управление комплексом.
5. Комплекс безопасности "Континент". Версия 4. Руководство администратора. Сетевые функции.