КОД БЕЗОПАСНОСТИ

Программный комплекс

Континент-СОВ
Версия 4

Инструкция

Загрузка базы решающих правил

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**

Список сокращений

БД	База данных
БРП	База решающих правил
ДА	Детектор (компьютерных) атак
МК	Менеджер конфигурации
СОВ	Система обнаружения вторжений (компьютерных атак)
ЦУС	Центр управления сетью

Введение

Документ предназначен для администраторов изделия "Программный комплекс "Континент-СОВ". Версия 4" (далее — комплекс). В нем содержатся сведения о загрузке в базу данных центра управления сетью базы решающих правил системы обнаружения вторжений.

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 8-495-982-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": https://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 https://www.securitycode.ru/company/education/training- courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Установка базы решающих правил

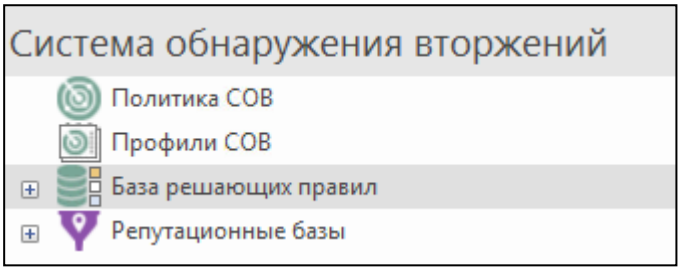
При обновлении ПО комплекса с версии 4.0.1 на 4.0.2 рекомендуется предварительно удалить старый набор БРП из БД ЦУС и со всех ДА.

Очистку и установку БРП выполняют в Менеджере конфигурации (МК). Для установки используется архивный файл, полученный от поставщика БРП.

Примечание. Типовое имя файла БРП – ids_update.json.gz.

Для удаления набора БРП в версии 4.0.1:

1. Откройте МК, перейдите в раздел "Система обнаружения вторжений" и войдите в подраздел "База решающих правил".

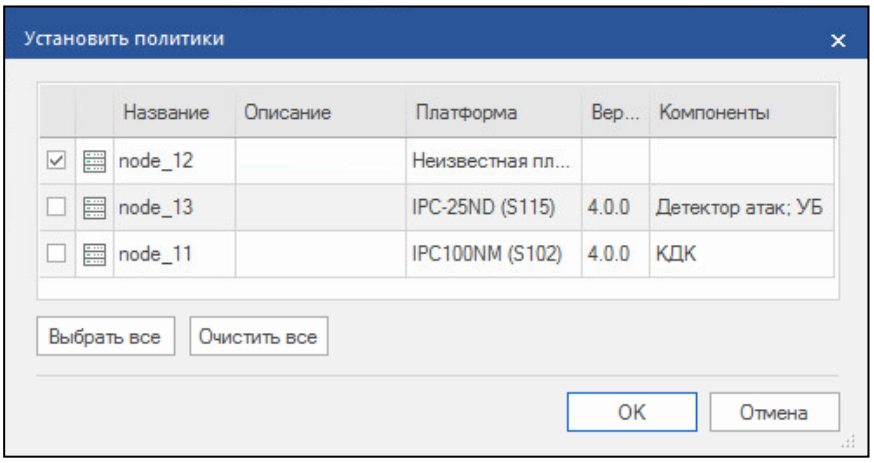


2. Выберите любое решающее правило в области отображения информации и нажмите "Ctrl" + "A". В панели инструментов нажмите кнопку "Удалить".

   Появится окно с сообщением о подтверждении удаления правил.

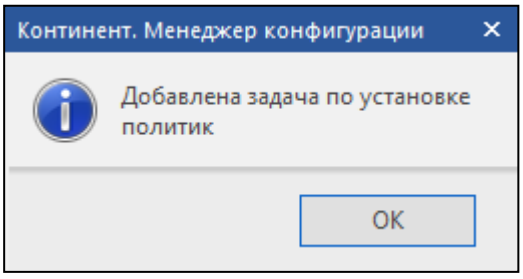
3. Нажмите кнопку "Да" в окне сообщения.
4. В главном окне МК перейдите в раздел "Структура" и нажмите кнопку "Установить политику".

   Откроется окно для установки политик на узлы сети.



5. В окне установки политик отметьте все узлы безопасности (в левой колонке) с обновляемым ПО. Далее нажмите кнопку "ОК".

   Задача по установке политик на выбранные узлы будет добавлена на ЦУС, после чего на экране появится соответствующее сообщение.

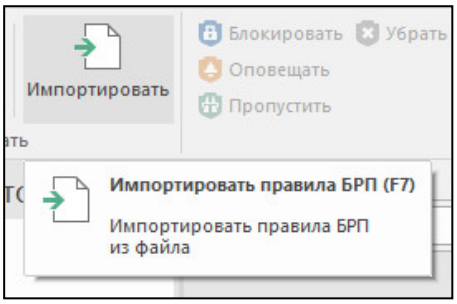


6. Нажмите кнопку "ОК" в окне сообщения.

Примечание. Статус задачи можно увидеть в разделе "Администрирование | Задачи". Для контроля ее выполнения в реальном времени нужно нажать на флажок в нижнем правом углу МК. В всплывающем окне будет показан прогресс выполнения текущих задач.

Для установки БРП:

1. Подготовьте файл архива с БРП. Если он находится на сменном носителе — подключите носитель к рабочему месту с установленным МК.
2. Откройте МК, перейдите в раздел "Система обнаружения вторжений" и войдите в подраздел "База решающих правил".
3. В панели инструментов нажмите кнопку "Импортировать".

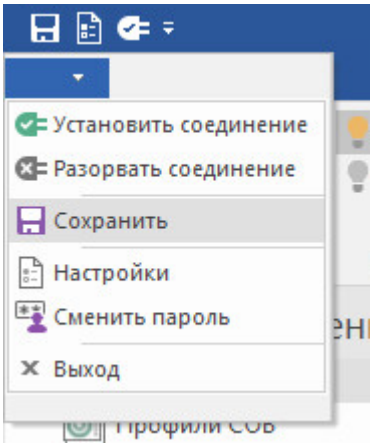


На экране появится стандартное окно выбора файла.

4. Выберите файл архива с БРП и выполните загрузку.

Будет выполнена загрузка БРП и на экране появится сообщение: "Файл загружен."

5. Нажмите кнопку "ОК" в окне сообщения.
6. Если на ЦУС установлено ПО версии 4.0.2.1731 или новее, нажмите кнопку вызова меню в левом верхнем углу окна МК и выберите пункт "Сохранить".



Изменения в конфигурации ЦУС будут применены.

7. В главном окне МК перейдите в раздел "Структура" и нажмите кнопку "Установить политику".

Откроется окно для установки политик узлам сети.

8. Установите отметки у тех узлов (ЦУС и ДА), на которые должна быть загружена новый набор БРП, и нажмите кнопку "ОК" в окне запроса.

Если в данный момент на ЦУС никакие другие задачи не выполняются, начнется выполнение добавленной задачи.

9. Для просмотра сведений о поставленных задачах нажмите на значок в нижнем правом углу главного окна МК. В правой части экрана отобразится список задач, отсортированный по времени их добавления. Статус "выполнена" будет свидетельствовать о завершении процедуры установки политик.

После установки политик загруженные правила отобразятся в окне МК.

Примечание. Если загруженные правила не отобразились — нажмите кнопку "Обновить" на панели инструментов.