



Код безопасности

Аппаратно-программный комплекс шифрования

# Континент

## Версия 3.7



### Инструкция

Загрузка базы решающих правил

## Список сокращений

АПКШ	Аппаратно-программный комплекс шифрования
БД	База данных
БРП	База решающих правил
ДКА, ДА	Детектор (компьютерных) атак
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПУ	Программа управления
СОВ	Система обнаружения вторжений (компьютерных атак)
ЦУС	Центр управления сетью криптографических шлюзов

## Введение

Данная инструкция предназначена для администраторов изделия "Аппаратно-программный комплекс шифрования «Континент». Версия 3.7". В ней содержатся сведения, необходимые администраторам для загрузки в БД ЦУС базы решающих правил системы обнаружения вторжений (СОВ).

**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](mailto: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](mailto: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](mailto:education@securitycode.ru)).

# Загрузка базы решающих правил в БД ЦУС версии 3.7

Для загрузки базы решающих правил необходимо выполнение следующих условий:

- В БД ЦУС зарегистрирована лицензия на обновление базы решающих правил.
- Установлен агент обновлений.
- Поддерживаются соединения ПУ ЦУС – ЦУС и ЦУС – ДА.

## Для загрузки базы решающих правил:

1. В главном меню ПУ ЦУС выберите команду "ЦУС | Сертификаты для обновления БРП".

На экране появится диалог "Управление сертификатами обновлений БРП".

2. Вставьте в дисковод диск с БРП.

3. В диалоге "Управление сертификатами обновлений БРП" нажмите кнопку "Добавить".

На экране появится стандартный диалог выбора файла.

4. Укажите вставленный диск с БРП, раскройте папку "БРП" и выберите файл сертификата ids\_update.cer.

Нажмите кнопку "Открыть".

В диалоге "Управление сертификатами обновлений БРП" появится добавленный сертификат.

5. Нажмите кнопку "Закреть".

6. В окне объектов ПУ ЦУС раскройте папку "База решающих правил" и в панели инструментов нажмите кнопку "Загрузить файл обновлений БРП".

На экране появится стандартный диалог выбора каталога.

7. Укажите каталог "БРП" на вставленном в дисковод диске и нажмите кнопку "ОК".

Начнется загрузка обновлений и после ее завершения на экране появится соответствующее сообщение.

8. Нажмите кнопку "ОК" в окне сообщения.

Загруженные правила отобразятся в окне "База решающих правил".

9. В окне объектов раскройте папку "Детекторы атак" и выберите в списке ДА, которому необходимо назначить правило (или правила).

10. В дополнительном окне "Привязка правил СОВ к детектору атак" установите отметки у правил, которые необходимо назначить выбранному детектору атак.

**Примечание.** Для выделения списка правил выделите первое правило, прокрутите список до последнего правила, нажмите клавишу <Shift> и выделите последнее правило. Далее для установки отметки у всех выделенных правил нажмите клавишу <Пробел>.

11. Нажмите кнопку "Сохранить" на панели инструментов дополнительного окна и дождитесь сообщения "Выполнена привязка к детектору атак".

12. Нажмите кнопку "ОК" в окне сообщения.

Окно сообщения закроется.

13. Повторите п.п. 9 - 12 для детекторов атак, которым необходимо назначить правила.