КОД БЕЗОПАСНОСТИ

Аппаратно-программный комплекс шифрования

Континент
Версия 3.9

Руководство администратора

Загрузка базы решающих правил

RU.88338853.501430.022 90 11

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

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

Введение

Руководство предназначено для администраторов изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.9" . В нем содержатся сведения, необходимые администраторам для загрузки в БД ЦУС 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 8-800-505-30-20 или по электронной почте support@securitycode.ru . Страница службы технической поддержки на сайте компании "Код Безопасности": https://www.securitycode.ru/services/tech-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).

Загрузка базы решающих правил в БД ЦУС версии 3.9

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. Вставьте в дисковод диск с БРП.
2. В окне объектов ПУ ЦУС раскройте папку "Сертификаты" и в панели инструментов нажмите кнопку "Импортировать сертификат".

   На экране появится окно мастера "Импорт сертификата".
3. На странице мастера "Импорт сертификата из файла" в поле "Файл сертификата" нажмите кнопку "...".

   Откроется стандартный диалог выбора файла.
4. Укажите вставленный диск с БРП, раскройте папку "БРП" и выберите файл сертификата ids_update.cer.

   Нажмите кнопку "Открыть".
5. На странице мастера "Импорт сертификата из файла" в поле "Назначение" выберите значение "Обновление БРП".

   Нажмите кнопку "Далее".

   Откроется страница мастера "Привязка сертификата обновления БРП".
6. Оставьте значения по умолчанию и нажмите кнопку "Готово".

   В списке сертификатов появится добавленный сертификат.
7. 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.
8. Укажите каталог "БРП" на вставленном в дисковод диске и нажмите кнопку "ОК".

   Начнется загрузка обновлений и после ее завершения на экране появится соответствующее сообщение.
9. Нажмите кнопку "ОК" в окне сообщения.

   Загруженные правила отобразятся в окне "База решающих правил".
10. В окне объектов раскройте папку "Детекторы атак" и выберите в списке ДА, которому необходимо назначить правило (или правила).
11. В дополнительном окне "Привязка правил 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>.
12. Нажмите кнопку "Сохранить" на панели инструментов дополнительного окна и дождитесь сообщения "Выполнена привязка правил к детектору атак".

13. Нажмите кнопку "ОК" в окне сообщения.

Окно сообщения закроется.

14. Повторите пп. **10–13** для детекторов атак, которым необходимо назначить правила.