



Ребус·СОВ

Программный комплекс обнаружения вторжений

«Ребус-СОВ»

www.rebus-sov.ru
rebus-sov.pf



СЕРТИФИЦИРОВАН
ФСТЭК России

научно-исследовательский институт
ЦЕНТРПРОГРАММСИСТЕМ

Назначение и область применения ПК «Ребус-СОВ»

Программный комплекс обнаружения вторжений «Ребус-СОВ» (сокращенное наименование – ПК «Ребус-СОВ») предназначен для обнаружения и блокирования угроз безопасности информации, относящихся к вторжениям (преднамеренный несанкционированный доступ или специальные воздействия на информацию).

ПК «Ребус-СОВ» функционирует на уровне сети и узлов информационной системы с целью предотвращения деструктивного воздействия

- со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей;
- со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

ПК «Ребус-СОВ» может использоваться на объектах вычислительной техники в качестве элемента системы защиты информации информационных систем, функционирующих на базе вычислительных сетей и обрабатывающих сведения, содержащие государственную тайну и (или) конфиденциальную информацию, включая персональные данные.

С помощью ПК «Ребус-СОВ» могут решаться следующие задачи:

- обнаружение вторжений в информационной системе;
- регистрация обнаруженных вторжений;
- анализ обнаруженных вторжений;
- реагирование на обнаруженные вторжения;
- контроль состояния СОВ;
- управление доступом к данным и функциям СОВ.

Для решения указанных задач ПК «Ребус-СОВ» выполняет следующие функции:

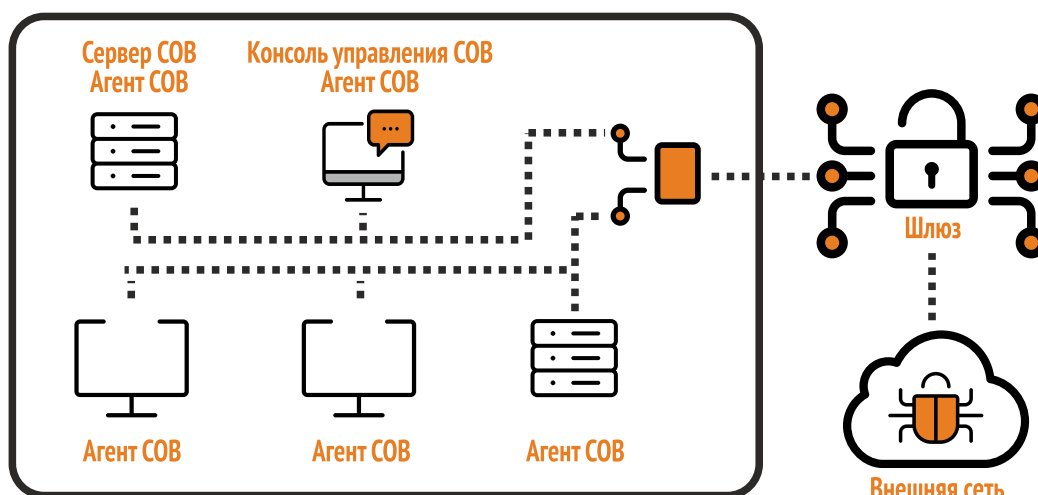
- обнаружение вторжений на основе анализа сетевого трафика, проходящего через контролируемый узел ИС (станцию), в режиме, близком к реальному масштабу времени (сигнатурный анализ, статистический анализ, контроль состава локальной вычислительной сети);
- обнаружение вторжений на основе сигнатурного анализа журналов аудита ОС и прикладного ПО;
- обнаружение вторжений на основе анализа журналов аудита АПКЗИ «Ребус-М»;
- оперативное отображение информации о вторжениях, обнаруженных на контролируемых станциях;
- оперативное реагирование на выявленные вторжения в ручном и автоматическом режимах;
- отображение состояния агентских станций;
- визуализация собранной статистики о вторжениях;
- централизованное управление блокировкой станций и сетевого трафика;
- формирование отчетов с возможностью фильтрации выводимой информации.

ПК «Ребус-СОВ» может использоваться на ЭВМ, объединенных в вычислительную сеть и функционирующих под управлением ОС семейства Windows, ОС MSBC 5.0 и ОССН «Astra Linux Special Edition» (релизы «Смоленск» и «Ленинград»).

Составные части ПК «Ребус-СОВ»:

- консоль управления СОВ;
- сервер СОВ;
- агент СОВ;
- средство сбора данных и обнаружения вторжений;
- средство противодействия вторжениям.

Типовая схема применения ПК «Ребус-СОВ» на уровне узла



Преимущества использования «Ребус-СОВ»:

- функционирование на уровне как сети, так и узла;
- поддержка ОС Microsoft Windows, MCBC 5.0, Astra Linux Special Edition;
- поддержка платформ x86 и «Эльбрус»;
- функционирование в гетерогенных сетях;
- выявление вторжений по данным аудита АПКЗИ «Ребус-М»;
- контроль нештатных сетевых подключений в сети;
- гибкая настройка автоматической реакции на вторжения;
- расширяемая схема, позволяющая подключать дополнительные модули сбора данных и их анализа, а также реагирования, непосредственно на объекте без модификации исполняемых модулей изделия;
- программная реализация, позволяющая использование на уже существующей на объектах технике;
- взаимодействие с межсетевыми экранами, поддерживающими подключение по SSH (Dionis-NX, АПК «Маршрутизатор доступа» и т.д.);
- гибкая настройка анализатора сетевого трафика с возможностью выбора сетевых интерфейсов и работы в режиме разрыва канала;
- возможность взаимодействия с ГосСОПКА;
- возможность выдачи событий аудита в SIEM;
- возможности автоматического обновления баз решающих правил с доверенных источников.

Соответствие требованиям нормативных документов ФСТЭК России:

- требования к системам обнаружения вторжений;
- требования к уровням доверия - по 2-му уровню;
- профиль защиты систем обнаружения вторжений уровня сети 2-го класса защиты. ИТ.СОВ.С2.ПЗ;
- профиль защиты систем обнаружения вторжений уровня узла 2-го класса защиты. ИТ.СОВ.У2.ПЗ.

Сертификат соответствия ФСТЭК России № 4394.

ПК «Ребус-СОВ» является отечественной разработкой и включен в Единый реестр российских программ для электронных вычислительных машин и баз данных
(Приказ Минсвязи России № 421 от 15.08.2017 г.).

Способы обнаружения вторжений и противодействия им



Способы обнаружения вторжений

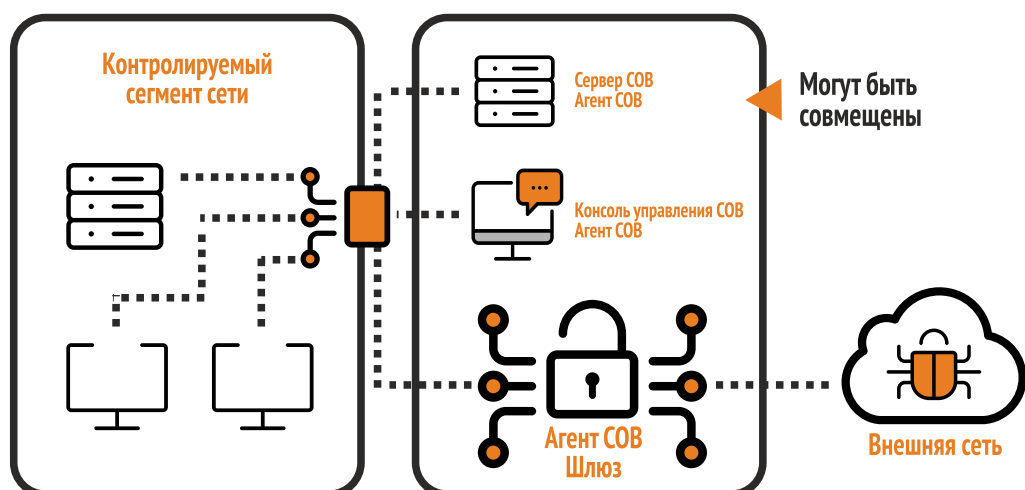
- ▶ Анализ сетевого трафика
- ▶ Анализ статистики сетевого трафика
- ▶ Контроль состава ЛВС
- ▶ Анализ журналов аудита ОС и ПО
- ▶ Анализ журналов аудита АПКЗИ «Ребус-М»



Способы противодействия вторжениям

- ▶ Блокировка станции
- ▶ Блокировка сетевого трафика
- ▶ Управление межсетевым экраном

Типовая схема применения ПК «Ребус-СОВ» на уровне сети



Акционерное общество
Научно-исследовательский институт
«Центрпрограммсистем»

+7 (4822) 39-91-74

г. Тверь, проспект Николая Корыткова, д. 3а

zi@cps.tver.ru
www.rebus-sov.ru
ребус-сов.рф