Форпост

Система обнаружения компьютерных атак (IDS - Intrusion detection system, в переводе с анг. русскоязычный термин — СОВ/СОА) «ФОРПОСТ» версии 2.0. предназначена для автоматического выявления воздействий на контролируемую данным средством автоматизированную информационную систему, которые могут быть классифицированы как компьютерные атаки или вторжения, и блокирования развития выявленных компьютерных атак.

Ключевые возможности:

- обнаружение компьютерных атак направленных на информационные ресурсы автоматизированной информационной системы, серверы телематических служб (WEB, FTP, электронная почта, СУБД и пр.) и рабочие станции, размещенные в защищаемых сегментах ИС, за счёт анализа сетевого трафика на 2 -7 уровнях сетевой модели стека сетевых протоколов OSI/ISO (ГОСТ Р ИСО/МЭК 7498-1-99),;
- полноценная работа СОА в вычислительных системах:
  - использующих технологию Ethernet 802.1Q;
  - использующих каналы связи с применением технологии MPLS;
- производительность по обработке сетевого трафика:
  - сборка ФСБ 2.0.60 до 1 Гбит/с, для съёма сетевого трафика используется 1 сетевой интерфейс;
  - сборка ФСТЭК 2.0.65 до 6 Гбит/с, для съёма сетевого трафика в режиме Full Duplex используется 2 сетевых интерфейса
- защита информационного обмена между территориально распределёнными компонентами СОВ/СОА "Форпост" с помощью средств криптографической защиты информации (СКЗИ), в том числе отечественных, до класса КС 3 включительно;
- предотвращение развития сетевых компьютерных атак путем блокирования источников атак на активном сетевом оборудовании, удаленно управляемым по защищенному каналу управления, организованному с использованием средств криптографической защиты информации (СКЗИ), в том числе отечественных, до класса КС 3 включительно;
- блокировка источников компьютерных атак:
  - сборка ФСБ 2.0.60 по команде оператора СОА;
  - сборка ФСТЭК 2.0.65 как автоматически, так и по команде оператора СОА;
- контроль целостности файлов серверов и АРМов защищаемой автоматизированной информационной системы, в том числе файлов не только ОС, но и файлов, содержащих информацию, на которой и базируются информационные ресурсы;
- отслеживание действий нарушителей по отношению к информации и правам пользователей, на серверах и АРМах защищаемой автоматизированной информационной системы;
- оценка успешности компьютерной атаки и выявление успешных попыток скомпрометировать информацию в защищаемой автоматизированной информационной системы;
- отслеживание появления новых сообщений системных журналов информационных ресурсов защищаемой автоматизированной информационной системы;
- генерацию отчетов на основе содержимого журналов СОА;
- наличие программных модулей интеграции:
  - с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, создаваемой в соответствии с Указом Президента Российской Федерации N 31с от 15 января 2013 г;
  - внешними SIEM системами;
- возможность неограниченной иерархической интеграции между системами обнаружения компьютерных атак на базе СОА "Форпост" версии 2.0;
- возможность централизованного обновления базы сигнатур компьютерных атак в иерархических системах на базе СОА "Форпост" версии 2.0.

Сертификат ФСТЭК № 2845 (требования к СОВ (сети третьего класса защиты ИТ.СОВ.С3.ПЗ)) от 18.03.2013. Действителен до 18.03.2019.

Наши контактные данные:

ул. Ленина, д.20, (четвертый этаж), каб. 422, 423. Остановка "Яблонька".
e-mail: info@ooo-skb.ru (ссылка для отправки email);
тел. 8 (3812) 53-20-18