СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРОТИВОДЕЙСТВИЯ АТАКАМ

А.И. Понамарчук

Современные информационные технологии приводят к появлению систем, содержащих критически важные ресурсы, стоимость которых во много раз превосходит стоимость самих систем. В таких системах существует вероятность реализации угроз информационной безопасности, основанная на наличии уязвимостей. Одним из технических способов обеспечения информационной безопасности является применение систем обнаружения(IDS) и противодействия атакам (IPS).

Обнаружение вторжений — активный процесс, помогающий при превентивной идентификации активных угроз посредством оповещений и предупреждений. Разработка и ввод в эксплуатацию подобных систем требует решения ряда задач, которые можно

объединить под общим названием — анализ защищенности систем телекоммуникаций от атак. Функционирование IPS основано на модуле анализа, использующего один из возможных алгоритмов распознавания (сигнатурный, статистический, адаптивный). Алгоритм распознавания обязан обеспечивать следующие функции: контроль и анализ активности пользователей и вычислительных систем, аудит конфигураций системы и уязвимостей, распознавание характера активности, обнаружение характерных последовательностей аномалий, эффективность, масштабируемость и пр. для минимизации ложных срабатываний и оптимизации системы обнаружения в целом, применяются различные типа корреляции, каждый из которых осуществляет отдельные функции. На основе этого, разработаны рекомендации по применению системы обнаружения и противодействия атакам.