КОМБИНИРОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ АТАК

В.А. Дмитриев, Е.П. Максимович

К характерным недостаткам разных отдельных методов обнаружения атак относятся: недопустимо высокий уровень ложных срабатываний и пропусков атак; слабые возможности по обнаружению новых атак; частая невозможность определения атаки на начальных этапах; трудность определения атакующего, цели атаки; отсутствие оценок точности и адекватности результатов работы; невозможность определения «старых» атак, использующих новые стратегии; слабые возможности по автоматическому обнаружению сложных координированных атак. В виду этого актуальным подходом к повышению эффективности систем обнаружения атак является использование комбинации нескольких методов обнаружения атак, нивелирующих недостатки друг друга.

В настоящее время подавляющее большинство реальных систем обнаружения атак делятся по способам выявления атак на системы обнаружения аномалий и системы обнаружения злоупотреблений. Обнаружение злоупотреблений позволяет идентифицировать несанкционированные действия, если имеется их точное представление в виде характерных идентифицирующих свойств) атак (сигнатур, экспертных правил). Данные методы являются точным и обоснованным средством выявления известных типов атак, но не пригодны для идентификации новых атак либо модификаций известных атак. Обнаружение аномалий на основе методов интеллектуального анализа данных (нейронные сети, деревья решений, индуктивные выводы, методы рассуждения по аналогии, нечеткие логические выводы, генетические алгоритмы, методы искусственных иммунных систем) – важное средство

обнаружения незнакомых атак, но принимаемые ими решения базируются не использовании эвристичных процедур, что не гарантирует их точности и однозначности.

Перспективным направлением при проектировании систем обнаружения атак представляется в настоящее время реализация подходов, совмещающих в себе преимущества сигнатурных и эвристических методов. Кроме того, анализируется целесообразность использования сигнатур, основанных не только на конкретном эксплоите (программном коде, автоматизирующем проведение атаки), но и на уязвимости сетевых протоколов и атакуемых систем.

Возможность эффективной практической реализации подходов, основанных на использовании комбинации нескольких алгоритмов обнаружения атак, обусловлена достигнутым в настоящее время уровнем развития компьютерной техники, телекоммуникационных средств, информационно-коммуникационных технологий.