ФИЛЬТРАЦИЯ ЛОЖНЫХ СИГНАЛОВ ТРЕВОГИ С ПОМОЩЬЮ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

В.В. АНИЩЕНКО, Ю.В. ЗЕМЦОВ

В последнее время наблюдалась тенденция к использованию методов интеллектуального анализа данных в области обнаружения атак на продукты и системы информационных технологий. Предлагаемые подходы чаще всего базировались на применении того или иного алгоритма интеллектуального анализа данных для обнаружения аномалий, которые связывались со злонамеренной активностью. В некоторых работах предлагалось даже заменить существующие методы выявления атак методами обнаружения аномальной активности, основанными на технологии интеллектуального анализа данных. Однако, за исключением отдельных узких областей, таких как обнаружение широко распространенных "червей", практического применения подобные подходы не получили. Связанно это главным образом с их невысокой эффективностью, а также сложностью сбора данных, пригодных для последующего анализа.

В тоже время, основанные на правилах методы выявления атак, являющиеся наиболее эффективными на сегодняшний день, имеют существенный недостаток, заключающийся в общем характере этих правил, что приводит к большому количеству ложных срабатываний. Уменьшение количества ложных сигналов тревоги обычно достигается за счет ухудшения качества обнаружения.

В данной работе предлагается оригинальный подход к редуцированию количества ложных срабатываний для систем обнаружения атак, основанных на правилах. Суть подхода состоит в использовании технологии интеллектуального анализа не для самого процесса выявления атак,

а исключительно для фильтрации ложных сигналов тревоги. Проводя интеллектуальный анализ данных, сгенерированных системой обнаружения атак за время обучения, можно выявить схожие группы сигналов тревоги (базовые кластеры). Затем, вычисляя отклонения групп сигналов тревоги, выявленных за последующие периоды времени от базовых кластеров, можно выделить сигналы тревоги, которые действительно представляют интерес.