УДК 004.77

Методы обнаружения сетевых атак

Шардыко П.П., Апанасович С.В.
Белорусский национальный технический университет

Система обнаружения атак, или система обнаружения вторжений – это система, осуществляющая сбор информации с множества системных и сетевых источников, анализирующая полученную информацию на предмет признаков вторжений (атак).

Существует множество современных методов обнаружения атак, однако, их использование в системах имеет ограничения, связанные с устойчивостью и воспроизводимостью результатов.

Современные методы обнаружения атак используют некоторую форму анализа контролируемого пространства на основе правил или статистического подхода. В качестве контролируемого пространства могут выступать журналы регистрации или сетевой трафик. Анализ опирается на набор заранее определённых правил, которые создаются администратором или самой системой обнаружения атак.

Любое разделение атаки во времени или среди нескольких злоумышленников является трудным для обнаружения при помощи экспертных систем. Из-за большого разнообразия атак и хакеров даже специальные постоянные обновления правил экспертной системы никогда не дадут гарантии точной идентификации всего диапазона атак.

Использование возможностей нейронных сетей является одним из способов преодоления указанных проблем экспертных систем. В отличие от экспертных систем, которые могут дать пользователю определённый ответ о соответствии рассматриваемых характеристик заложенным правилам, нейронная сеть проводит анализ информации и предоставляет возможность оценить, согласуются ли данные с характеристиками, которые она научена распознавать. Степень соответствия нейросетевого представления может достигать 100 %, достоверность выбора полностью зависит от качества системы, т.е. возможности анализа параметров поставленной задачи.

Разработка техники обнаружения и распознавания атак, основанной на искусственных нейронных сетях позволяет избежать проблем, характерных для большинства подходов, поскольку нейросетевая система способна с высоким качеством обнаруживать как известные, так и новые атаки за счет способности к обобщению и адаптации. Кроме того, такая система сможет обновляться как стандартным способом – базы обученных детекторов от разработчика – так и обучаться самостоятельно.