УДК 004.8

Нейросетевая структура обнаружения сетевых вторжений на информационную систему

Автор: Левкович С.С. (levkovich_stas@mail.ru), Исаева А.В., Соловьев Д.В., Мельничук П., Бондаренко И.Б., Гатчин Ю.А., Нагуськин В.В.
Научный руководитель: Гатчин Юрий Арменакович, Университет ИТМО, Санкт-Петербург

В настоящее время растут возможности и перспективы использования алгоритмов искусственного интеллекта, а именно, алгоритмов искусственных нейронных сетей в задачах обеспечения информационной безопасности информационных систем. Высокую эффективность нейросетевые алгоритмы показывают в решении задач, которые либо не могут быть формализованы, либо формализованы, но на настоящий момент отсутствует математический аппарат для их решения, либо же при наличии математического аппарата, точность решений таких задач не удовлетворяет по времени, массе, энергии и д.р. Такая особенность нейронных сетей и ложится в основу решения широкого спектра задач по информационной безопасности современных информационных систем. Как показывает практика, в последние годы крайне быстро увеличивается количество и характер атак на информационные ресурсы, попытки нанесения материального ущерба путем реализации таких атак, нарушение целостности и конфиденциальности информации, а также доступности. Применение же алгоритмов ИНС позволяет в целом качественно повысить уровень ИБ ИС.

На сегодняшний день математический аппарат искусственных сетей переживает, пожалуй, второй качественный этап своего развития. В области информационной безопасности применение математического аппарата нейросетей еще более масштабно. Нейросети уверенно показывают свои способности в задачах автоматизации аудита ИБ, фильтрации спам-сообщений, обнаружении вторжений и атак на информационную систему. Технология глубинного машинного обучения – новый этап в развитии применения аппарата нейросетей в антивирусных средствах. Известно, что на данный момент большинство продуктов работает по принципу постфактум при обнаружении и уничтожению вирусных угроз. А с помощью глубинного машинного обучения антивирусные средства смогут работать на опережение. Это качественно новый уровень и переоценить вклад нейросетей в эту область сложно.

Потребность в своевременном обнаружении и классификации таких атак, обусловлена задачами минимизации возможных последствий, урона для самой информационной системы и пользователей этой ИС. На данный момент существует способ обнаружения DDoS-атаки путем анализа структуры трафика, выявления аномалий в его структуре. Широко используемые файрволы и системы обнаружения вторжения не являются эффективными в вопросах детектирования таких атак, а также противодействия им, особенно в случаях использования большого объема трафика.

В представленной работе были основательно изучены способы и механизмы организации атак, направленных на отказ в обслуживании информационной системой. Как показала практика, такой вид атаки является самым распространенным среди злоумышленников в последнее время. Крупными целями злоумышленников осуществляющих такие атаки были ресурсы интернет-магазинов, средств массовой информации, информационные сайты, интернет-биржы, игровые сайты, сайты с объявлениями о продаже недвижимости, правительственные ресурсы, платежные системы и банки.

В дальнейшем был разработан программно-аппаратный комплекс для организации и изучения способов и механизмов таких атак на практике. На этом этапе были применены современные средства виртуализации, так как организация реального, а не "виртуального" программно-аппаратного стенда была бы слишком затратна и заняла бы много времени на

настройку оборудования. Стенд показал, что даже использование последних версий программных продуктов не является панацеей. В том числе использования безопасных протоколов HTTPS, шифрования SSL и механизмов виртуальных частных сетей.

На основе полученных результатов была сформирована структура нейросетевой системы обнаружения атак на информационную систему. Предложенный алгоритм показал свою эффективность в вопросе обнаружения низкоинтенсивных распределенных атак на отказ в обслуживании. Количество ложных срабатываний составило 3,16 процента, а количество фиксаций пропущенных атак 1,23 процента. Особенностью этой структуры является включение нейросетевого модуля обнаружения атаки и модуля базы знаний, хранящего не только известные сигнатуры атак, но и нейросетевые структуры.

Автор Левкович С.С.

Научный руководитель Гатчин Ю.А.

Заведующий кафедрой Заколдаев Д.А.