BC/NW 2012; №1 (20): 9.4

**МЕТОДЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ**

С.А. Петров, П.Б. Хорев

Национальный Исследовательский Университет Московский энергетический институт

В настоящее время компьютерные сети представляют собой большие распределенные системы программ и устройств, взаимодействующие между собой с целью обмена, хранения и обработки информации. Компьютерная сеть – прекрасная возможность для развития бизнеса компании. Сети объединяют разные типы устройств, соединенных различными каналами связи. Усложнение структуры сетей, повышение нагрузки на них, регулярное появление новых методов нарушения работы, способы ограничения доступа к данным законных владельцев и целостности информации, превращение сферы создания нежелательного программного обеспечения из любительского занятия в прибыльный бизнес определяют необходимость серьезного отношения к вопросам сетевой безопасности.

Применение методов искусственного интеллекта (ИИ) позволяет ввести в системы защиты свойство самообучения и обеспечивает обнаружение угроз «на лету». В докладе приводится обзор методов ИИ, используемых для защиты компьютерных сетей. Рассматриваются многоагентные системы и системы защиты и анализа защищенности сетей, основанные на агентах [1]. Описываются продукционные системы и их использование для построения систем защиты и обнаружения известных уязвимостей в проверяемой системе по формальным признакам, выявленным экспертами [2]. Рассмотрен пример построения спам-фильтра на основе теоремы Байеса [3]. Описан подход к определению различных атак и адаптации к новым типам угроз на основе нейронных сетей [4]. И, наконец, выполнен обзор относительно новой технологии ИИ – метода опорных векторов, пока ещё мало применяемой для защиты сетей, но имеющей большие перспективы в этой сфере [5].

Литература

1. **Котенко И. В., Уланов А. В.** Кооперативная работа команд агентов при защите от сетевых атак нарушения доступности. Электронный ресурс: [www.comsec.spb.ru](http://www.comsec.spb.ru)
2. **Зайцев О.** Сайт «Информационная безопасность» Электронный ресурс: [www.z-oleg.com](http://www.z-oleg.com)
3. **Лаборатория Касперского**: технология фильтрации спама. Электронный ресурс: [www.spamtest.ru](http://www.spamtest.ru)
4. **Зайцев О.** Нейросети в системах безопасности. IT-Спец. – 2007. – № 6.
5. **Lashkov P., Schäfer C., Kotenko I.** Intrusion Detection in Unlabeled Data with Quarter-Sphere Support Vector Machine [www.comsec.spb.ru](http://www.comsec.spb.ru)