УДК 004
ББК 32.81

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ОБНАРУЖЕНИЯ АТАК НА ОСНОВЕ МНОГОАГЕНТНОГО ПОДХОДА

А.В. Никишова

Рассмотрены особенности современных атак. Предложена модель системы обнаружения атак, учитывающая эти особенности. Данная система обнаружения атак реализует сбор информации на нескольких уровнях информационной системы и использует для анализа системы искусственного интеллекта (нейронные сети).

Ключевые слова: *атака, система обнаружения атак, нейронная сеть, интеллектуальный агент, многоагентная система.*

На кафедре информационной безопасности ВолГУ проводятся исследования в рамках темы «Многоагентная интеллектуальная система обнаружения атак на информационную систему». В них принимают участие студенты III, IV и V курсов в ходе выполнения курсовых и дипломных работ.

Системы обнаружения атак применяются как дополнение к разработанной и примененной политике безопасности, которые являются относительно статическими.

В связи с широким распространением сетей общего пользования все большее число компьютеров подвергается атакам. Согласно статистике «Лаборатории Касперского» за 2010 г., несмотря на стабилизацию количества новых атакующих воздействий (см. рис. 1), общее количество инцидентов продолжает увеличиваться. В 2010 г. общее число зафиксированных инцидентов типа атаки через Интернет и локальные инциденты превысили 1,9 миллиарда.

В настоящее время основными особенностями атак является то, что:

- происходит постоянное увеличение сложности атакующих воздействий, их технологический уровень значительно вырос даже по сравнению с прошлым годом. Зачастую атаки имеют многошаговый алгоритм действий и распределенный характер;

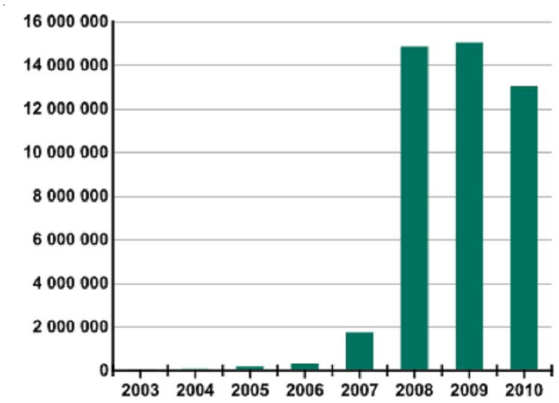

Рис. 1. Число новых атакующих воздействий, обнаруженных «Лабораторией Касперского»

- большинство атак изначально осуществляется через браузер – при помощи множества уязвимостей и в самих браузерах, и в сторонних приложениях, взаимодействующих с ними. Это приводит к тому, что зачастую одна и та же вредоносная программа может распространяться при помощи десятка различных уязвимостей, – что ведет к пропорциональному росту количества разновидностей атак.

Для учета этих особенностей современные системы обнаружения атак (СОА) должны выполнять распределенный сбор и анализ информации, а также интеллектуальный ее анализ. Кроме того, обнаруживать новые атакующие воздействия, число которых, по данным статистики, велико.

Как показывает анализ современных бесплатных СОА, ни одна из них в полной мере не удовлетворяет поставленным требованиям, однако тенденция показывает, что большинство из них выполняют анализ на нескольких уровнях информационной системы или обладают возможностью расширяться. Кроме этого, осуществляются попытки реализовать возможность СОА адаптироваться к новым видам атакующих воздействий.

Исходя из анализа различных методов, применяемых для анализа данных при выявлении атакующих воздействий, нейронные сети и генетические алгоритмы являются наиболее предпочтительными для решения поставленной задачи. В рамках данного исследования применяются нейронные сети.

Так как сбор данных необходимо проводить на нескольких уровнях и информационной системы, то были выбраны следующие источники информации, анализ которой позволит выявлять атакующие воздействия:

- данные о сетевых пакетах;
- сведения журнала маршрутизатора;
- сведения журнала безопасности операционной системы;
- сведения из реестра операционной системы;
- сведения о процессах операционной системы.

Применение адаптивных методов анализа данных, подобных нейронным сетям, обладает большим числом ложных срабатываний. Для уменьшения данного показателя в рамках проводимого исследования применяются интеллектуальные агенты, которые взаимодействуют между собой для нахождения совместного решения в рамках состояния всей информационной системы, а не отдельного события. Архитектура данной СОА представлена на рисунке 2.

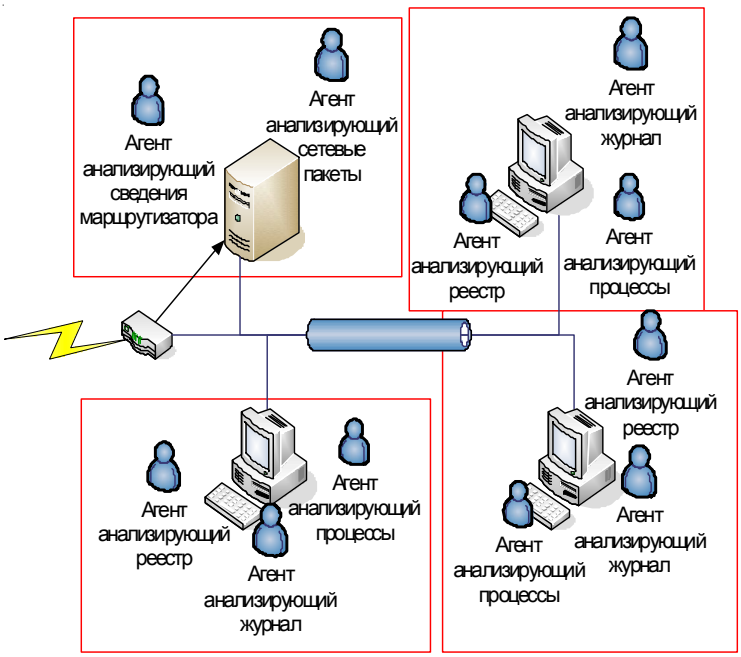

Рис. 2. Архитектура многоагентной СОА

Каждый агент обнаружения атак описывается состоянием (*P*, *B*, *S*, *G*, *I*), где:

- *P* – ощущение. Представляет собой информацию об окружающей среде, собираемую агентом, то есть набор входных данных агента.
- *B* – убеждения. Множество убеждений, то есть сведений и знаний об окружающей агента среде. Убеждения агента представляют собой нейронную сеть. На первом этапе агенты собирают сведения о функционировании информационной системы, и на их основе создается обучающая выборка для нейронной сети.
- *S* – ситуация. Конкретное состояние среды, то есть конкретные значения входных данных и результата классификации их нейронной сетью.
- *G* – цели. Определяется как желаемое состояние среды.
- *I* – намерения. Множество возможных планов действий агента.

Соответственно агенты обнаружения атак обладают следующими базовыми функциями:

- порождение и пересмотр убеждений. Данная функция отвечает за сбор сведений для обучения и в случае необходимости переобучения нейронной сети и само обучение;
- оценка ситуации. Получение результатов оценки собранных сведений об информационной системе нейронной сетью;
- активация цели. В зависимости от значения выхода нейронной сети агент выбирает набор элементарных действий, которые необходимо выполнить в данной ситуации;
- назначение. Агент определяет окончательный план действий, определяя последовательность элементарных действий;
- выполнение. Выполнение агентом выбранных элементарных действий.

Взаимодействие агентов между собой позволяет принимать совместные решения, уменьшая ошибки отдельно взятой нейронной сети.

В настоящее время проводятся экспериментальные исследования на разработанном для данной архитектуры программном комплексе.

INTELLIGENT INTRUSION DETECTION SYSTEM ON BASIS OF MULTI-AGENT APPROACH

A.V. Nikishova

Up-to-date attacks' features have been considered. Intrusion detection system's model that takes into consideration these features has been suggested. This intrusion detection system gathers information in several levels of information system and use artificial intelligence system (neural network) for analysis.

Key words: *attack, intrusion detection system, neural network, intelligent agent, multi-agent system.*