ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ БОРЬБЫ С КИБЕРАТАКАМИ

Красношлык К. Ю., студ. (гр. ФІ-72, ФТІ КПИ им. Игоря Сикорского);
Мітюк Л. О., к.т.н., доц.(каф. ОТГБ КПИ им. Игоря Сикорского)

Скорость процессов и объемы данных, используемых в киберпространстве, уже давно не могут регулироваться человеком без значительной автоматизации. В наше время сложно разработать программное обеспечение с эффективной защитой от развивающихся сетевых атак и при этом использовать обычные фиксированные алгоритмы. Эта проблема решается путем применения методов искусственного интеллекта, которые могут обеспечить достаточную адаптируемость и обучаемость инструментам защиты. Также это подразумевает динамическое изменение среды объекта защиты, высокую осведомленность о текущем состоянии системы и сверхвысокую скорость реакции на новые угрозы. Данные качества свидетельствуют про огромные перспективы дальнейших исследований в этой области.

Искусственный интеллект (ИИ) - это область научных исследований, которая зародилась незадолго после создания первого компьютера. Мы уже стали свидетелями решения многих интеллектуальных проблем компьютерами, например, таких как хорошая игра в шахматы [1]. Этому предшествовало три условия: увеличение компьютерных мощностей, разработка действительно хороших поисковых алгоритмов, и хорошо организованные базовые знания, которые включают в себя всю возможную информацию о шахматах. По существу, проблема с шахматами могла быть решена, так как являлась очень специфической и решалась так называемым узконаправленным (слабым) искусственным интеллектом. Совершенно другой задачей является перевод с одного естественного языка на другой, это в свою очередь требует уже общего (сильного) искусственного интеллекта. Некоторые успехи в отдельных приложениях уже заметны, например переводчик от компании Google, который использует самообучаемый алгоритм машинного перевода, достаточный для перевода слов и словосочетаний, но почти бесполезный, когда дело касается более сложных конструкций, для которых уже необходим общий искусственный интеллект [2].

После рассмотрения информации из открытых источников о применении искусственного интеллекта в киберзащите, можно сделать вывод, что на сегодняшний день уже существует большое кол-во приложений в этой среде [3]. И в первую очередь, это приложения с искусственными нейронными сетями для осуществления безопасности от угроз любого рода.

Становится понятно, что некоторые угрозы нарушения безопасности люди не в состоянии предотвратить без использования методов ИИ, большое

количество которых уже разработаны. Рассмотрим некоторые типы методов ИИ, таких как нейронные сети, машинное обучение, экспертные системы.

Нейронные сети - это система соединенных и взаимодействующих между собой искусственных нейронов. И если число данных нейронов большое, то у сетей проявляются способности к машинному обучению и возможность с их помощью решать задачи принятия решений. В то же время данные системы обладают невероятной скоростью работы. Все эти качества являются очень полезными во время кибер-атак, когда оперативное выявление угрозы, ее классификация и выбор ответного действия играют решающую роль в дальнейшем существовании объекта защиты. Нейронные сети уже неоднократно демонстрировали свои преимущества в реальных условиях: обнаружение враждебного программного обеспечения, компьютерных червей, классификация угроз, предотвращение возможных атак. Также была замечена их невиданная скорость, в случае реализации сетей за счет аппаратных средств или с помощью процессора видеокарты [4]. А возвращения к истокам создания модели нейронных сетей, к реальным биологическим нейронам, и добавление их природных свойств, продолжают улучшать свойства нейросетей и по сей день. В первую очередь продемонстрированы хорошие показатели в адаптации к «развивающимся» кибератакам.

Одной из самых интересных проблем искусственного интеллекта является его «самообразование», или более точно: «машинное обучение». Система способна получать новые знания путем их накопления, изменения взаимосвязей структуры в базе данных, или путем усовершенствования механизма логического вывода. В результате чего системы ИИ могут получить новые и дополнительные навыки: система постепенно начинает адаптироваться к условиям, в которых находится. Уже существуют методы обучения систем ИИ двух типов: контролируемые (обучение происходит с «учителем») и самообучающиеся. Последний из них хорошо себя зарекомендовал в случае работы с огромными массивами данных [5]. Процесс обучения системы может происходить параллельными алгоритмами, что является актуальным для многоядерных процессоров и им подобных систем. Здесь могут быть использованы генетические алгоритмы и такой раздел дискретной математики, как нечеткая логика. Методики обучения систем безопасности широко используются в механизмах выявления существующих и новых, ранее неизвестных системе, угроз.

Следующим популярным применением ИИ являются экспертные системы [6]. В первую очередь они созданы для поиска ответов на вопросы среди уже известных решений. База решений таких систем является набором экспертных мнений в некоторой области знаний, и может быть дополнена. Другим важнейшим элементом системы является механизм логического вывода, т.е. выбор решения, которое лучше других соответствует запрашиваемым критериям. Процесс дополнения знаний системы может проходить как вручную (добавление библиотеки человеком), так и автоматизировано («самообучение»). Второй способ подразумевает «сотрудничество» системы с пользователем или другими программами, с

которыми система способна обмениваться информацией. Само собой качество работы системы сильно зависит от содержания базы решений системы. Поэтому процесс приобретения знаний должен сопровождаться с высоким качеством получаемых знаний, что является решающим при разработке реальных систем. Экспертные системы нашли свое применение в медицинской диагностике, интернет сервисах, финансовой сфере. В безопасности такие системы способны помочь при выборе конфигураций, направленных на улучшение угрозостойкости, выборе оптимального использования ресурсов и других подобных ситуаций, в которых человек нуждается в экспертных мнениях.

Анализ публикаций [7] показывает, что результаты исследований ИИ нашли широкое применение в кибербезопасности. Наиболее подходящей технологией для многих развивающихся областей являются нейронные сети. Это области поддержки принятия решений, осознавание текущей ситуации и управление имеющимися знаниями. А экспертные системы в будущем могут стать наиболее перспективным направлением.

Уже в скором будущем проблема быстрого роста интеллекта вредоносных программ и усложнения кибератак приведет к неизбежности развития систем киберзащиты с использованием инструментов ИИ. Такие системы будут самообучаемыми, реагировать на любые изменения и обладать высокой скоростью работы. Эти технологии значительно увеличат обороноспособность систем защиты.

Литература

1. Feng-Hsiung Hsu. Behind Deep Blue - Building the Computer that Defeated the World Chess Champion. — Princeton University Press, 2004. — 320 p.
2. The Guardian: Google updates Tensor Flow, its open source artificial intelligence [Электронный ресурс]// - 2016. Режим доступу:https://www.theguardian.com/technology/2016/apr/13/google-updates-tensorflow-open-source-artificial-intelligence
3. Selden H.: Deep Instinct: A New Way to Prevent Malware, With Deep Learning [Электронный ресурс]. – 2016 – Режим доступа: http://www.tomshardware.co.uk/deep-instinct-deep-learning-malware-detection,news-52271.html
4. Swantee Olaf: Self learning computers: giving machines a human brain [Электронный ресурс]/ The Telegraph – 2014. Режим доступа: http://www.telegraph.co.uk/sponsored/technology/4g-mobile/olaf-swantee/11252503/self-learning-computer-think-like-humans.html
5. Abhinav Maurya, Manisha Ankam: Artificial Intelligence And Expert Systems [Электронный ресурс]/ -2011 – Режим доступа: https://www.reviewessays.com/ Technology/Artificial-Intelligence-And-Expert-Systems/34503.html

6. Jie-Hao Chen: DDoS defense system with turing test and neural network[Текст]/ Ming Zhong ; Feng-Jiao Chen ; An-Di Zhang // Department of Software Engineering, Beijing Institute of Technology, Hangzhou, China– 2012 – 38-43 с.

7. Swati Khandelwal: MIT builds Artificial Intelligence system that can detect 85% of Cyber Attacks [Электронный ресурс] / The Hacker News – 2016. Режим доступа: http://thehackernews.com/2016/04/artificial-intelligence-cyber-security.html