Academic Journal of Digital Economics and Stability

ISSN 2697-2212 Online: https://academicjournal.io

Special Issue on "Innovative Economy: Challenges, Analysis and Prospects for Development"
Published in Aug-2021

Application of Methods of Artificial Intelligence for Protecting Information on Information Networks

Gulyamov Saidakhror Saidakhmedovich[1]

Holboyev Bohodir Murodovich, Ph.D[2]

Аннотация. Статья посвящена анализу проблематики использования искусственного интеллекта (ИИ). Так, управление данными, обрабатываемыми роботами, представляет большую проблему не только с точки зрения законодательства об обработке персональных данных, но и с точки зрения типа данных, их объема. На основании проведенного в статье анализа следует заключить, что ИИ предполагает решение не только информационных вопросов, проблем защиты информации и информационной безопасности, защиты системы ИИ от проникновений, но и вопросов обучения ИИ, характеристик и систематизации самих данных в программах, критериев их обработки. Все эти проблемы требуют нормативного решения и определения.

Ключевые слова: искусственный интеллект, устойчивая нейронная сеть, самообучение, обнаружение угроз, вредоносные программы, перцептрон.

[1]Academician, Doctor of Economics, Prof., Head of the Department of the Research Institute for Statistical Research and Personnel Retraining

[2]Associate professor, head of the department of "Digital Economics and Mathematical Disciplines" Tashkent branch of the Russian Economic University named after G.V. Plekhanov

ISSN 2697-2212 Online: https://academicjournal.io

Введение. В Постановлении Президента Республики Узбекистан от 28 апреля 2020 года «О мерах по широкому внедрению цифровой экономики и электронного правительства» одной из дополнительных задач дальнейшего развития цифровой экономики и электронного правительства определено ускоренное формирование цифровой экономики, предусмотрев увеличение ее доли в валовом внутреннем продукте страны к 2023 году в 2 раза, в том числе путем внедрения комплекса информационных систем в управление производством, широкого использования программных продуктов при ведении отчетности в финансово-хозяйственной деятельности, а также автоматизации технологических процессов.

Технологии искусственного интеллекта сегодня интенсивно развиваются, в том числе из-за развития технологий устойчивых нейронных сетей и инфраструктур облачных вычислений, технологий нечетких систем, энтропийного управления, роевого интеллекта, эволюционных вычислений и мн. др. Стратегия развития отрасли информационных технологий в Узбекистане предполагает, что интеллектуальные системы становятся основой для анализа больших массивов данных и извлечении знаний, включая новые методы и алгоритмы для сбора, хранения и систем обработки больших объемов данных, машинного обучения, а также при защите информации в компьютерных сетях.

Как известно, большинство современных систем сетевой безопасности не имеют возможности самообучения и оперируют только заложенными в них вручную правилами и появление нежелательной программы, использующего новые уязвимости, повышает требования к системам сетевой безопасности. Применение методов искусственного интеллекта (ИИ) позволяет ввести в системы защиты свойство самообучения и обеспечивает обнаружение угроз.

В целях обеспечения защищенности компьютерных сетей были созданы системы, которые классифицируют сетевую активност различных программ. В случае совпадения с ситуацией, определенной экспертом, такие системы предлагают пользователю прекратит действия возможно вредоносной программы и откатит произведенные им изменения.

Обзор литературы. В докладе, /XX Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 9–12 апр. 2019 г. / Г.И. Абдрахманова, К. О. Вишневский, Л.М. Гохберг и др.; науч. ред. Л.М.Гохберг; Нац. исслед. ун-т «Высшая школа экономики».- М.: Изд. дом Высшей школы экономики, 2019.– 82 с., подготовленном коллективом Института статистических исследований и экономики знаний (ИСИЭЗ) НИУ ВШЭ, представлены ключевые аспекты развития цифровой экономики - тренды развития цифровых технологий, изменения под их влиянием условий жизни человека, цифровизация государственного управления и сферы науки, трансформация рынка труда и спроса на компетенции кадров. Рассмотрены международные и российские практики государственной поддержки развития цифровой экономики. Впервые представлены оригинальные подходы к статистическому измерению цифровой экономики, экспериментальные расчеты объема и структуры затрат на ее развитие в России, оценки вклада цифровой экономики в экономический рост.

В статье Пономаревой С. В. Представлено применение в промышленности инновационных приложений, базирующихся на искусственном интеллекте (в рамках развития концепции цифровой экономики). Научная статья посвящена отдельным аспектам применения инновационных приложений в отечественной промышленности в целом и в высокотехнологичных компаниях в частности, базирующихся на искусственном

ISSN 2697-2212 Online: https://academicjournal.io

интеллекте. В рамках осуществленного исследования, представлены критерии, (Цифровая трансформация экономики и промышленности: сборник трудов научно- практической конференции с зарубежным участием (Санкт-Петербург, 20-22 июня 2019 г.): СПБПУ, 2019. - С. 130-138.

В статье Селеменева А. В. Применение искусственных иммунных систем для обнаружения сетевых вторжений. Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. - 2019. - № 2. - С. 49-56.) рассматривается решение задачи обнаружения вредоносной информации при помощи алгоритма отрицательного отбора, активно использующегося в искусственных иммунных системах. Отрицательный отбор в иммунной системе используется для распознавания чужеродных антигенов путем удаления тех клеток (антител), которые реагируют на собственные антигены. Этот процесс называется распознаванием «свой-чужой». В статье представлен модифицированный алгоритм отрицательного отбора и проведен вычислительный эксперимент с иммунной системой, обнаруживающей сетевые вторжения. Вычислительный эксперимент, демонстрирующий ответную защитную реакцию системы при обнаружении аномального объекта. На конкретном примере рассмотрено применение алгоритма отрицательного отбора.

В статье Щуриной С. В. Искусственный интеллект как технологическая инновация для ускорения развития экономики. (Ж. Экономика. Налоги. Право. - 2019. – Т.: 12, № 3. – С. 125-133.) делаются выводы о том, что искусственный интеллект является прорывной технологией, имеющей большой потенциал. Активное внедрение искусственного интеллекта в компаниях значительно повышает их эффективность, конкурентоспособность, развивает отраслевые рынки, стимулирует создание новых технологий, повышает качество продукции и увеличивает объем производства. В общем плане искусственный интеллект формирует дополнительные импульсы, способствующие развитию России и ее вхождению в число пяти крупнейших экономик мира.

Методы исследований: При написании статьи нами были использованы такие методы как метод анализа и синтеза исследуемых материалов.

Обсуждение результатов: Однако большинство современных систем сетевой безопасности не имеют возможности самообучения и оперируют только заложенными в них вручную правилами. Частое появление нежелательной программы, использующего новые уязвимости, повысило требования к системам сетевой безопасности. Применение методов искусственного интеллекта (ИИ) позволяет ввести в системы защиты свойство самообучения и обеспечивает обнаружение угроз. Искусственная нейронная сет (НС) является упрощенной моделью мозга и представляет набор нейронов, соединенных между собой определенным образом[1]. Нейронные сети позволяют решат различные практические задачи, связанные, в основном, с распознаванием и классификацией образов. Несомненными преимуществами НС является то, что они могут автоматически приобретать знания в процессе обучения и обладают способностью к обобщению. Основным элементом сети является искусственный нейрон является математическая модел биологической нервной клетки. Нейронные сети - это более сложный аналог

[1] Доклад XX Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 9–12 апр. 2019 г./ Г.И. Абдрахманова, К.О. Вишневский, Л. М. Гохберг и др.; науч. ред. Л.М.Гохберг; Нац. исслед. ун-т «Высшая школа экономики».- М.: Изд. дом Высшей школы экономики, 2019.– 82 с.,

ISSN 2697-2212 Online: https://academicjournal.io

эмпирических формул, которые ранее широко применялись для проектирования техники. В отличие от эмпирических формул, создаваемых учеными и инженерами, нейронные сети самообучаются и иногда само создаются в процессе обучения, однако они всегда имеют некий процент ошибок, поэтому невозможно сделать нейронную сеть, которая будет предсказывать результат на 100%. Следовательно, нейронная сеть в большинстве случаев предсказывает правильно, основываясь на жизненном опыте (то есть на тех данных, которых она обучена). Для разных видов (топологий) нейронных сетей количество «угаданных случаев» различно, и именно им определяется эффективность работы нейронной сети[2]. Например, распознавание изображений сейчас находится на уровне 97–98%. Тип распознаваемых объектов и эффективность работы сети зависят от типа нейронной сети. Как показали исследования, применение НС для решения задачи включает два этапа: обучение и распознавания. На этапе обучения на вход НС подается обучающая выборка, состоящая из заранее отобранных и подготовленных входных и выходных векторов. В соответствии с выбранным алгоритмом обучения (например, метод обратного распространения ошибки или метод сопряженных градиентов) происходит настройка весовых коэффициентов, в результате которой при подаче на вход НС обучающего вектора на выходе появляется заданный выходной вектор, обозначающий класс входного вектора.

Для распознавания объектов и определению эффективности работы сети необходимо использовать определенные методы[3]:

1. Сверхточные (используются для распознавания локальных паттернов, таких как распознавание изображений, языковых паттернов, а также для распознавания сочетаний промышленных параметров (например, сочетание параметров работы оборудования: данные температуры, давления, вибрация, деформации и т. д.). Это наиболее эффективные на данный момент сети, с их использованием связано большинство внедряемых сейчас технологий. Например, распознавание графического и видеоизображения, предиктивный анализ состояния нагруженного промышленного оборудования, паттерны языка и рынка ценных бумаг.
2. Рекуррентные (используются для анализа различных последовательностей. На данный момент они не стол успешны, как сверхточные. Например, распознавание текста, речи, включая онлайн-перевод, распознавание информации с рынка ценных бумаг (но с учетом нерегулярности последовательности), распознавание изменения различных показателей, например, температуры час за часом, день за днем и т. д.).
3. Многосвязные или перцептрон. (Оценивают влияние любого входного параметра на предсказываемый ответ/ответы.

На этапе распознавания на НС поступает заранее неизвестный входной вектор, а на выходе появляется вектор как результат распознавания, в соответствии с которым

[2]Пономарева С. В. Применение в промышленности инновационных приложений, базирующихся на искусственном интеллекте (в рамках развития концепции цифровой экономики. сборник трудов научно-практической конференции с зарубежным участием (Санкт-Петербург, 20-22 июня 2019 г.): СПбПУ, 2019. - С. 130-138.

[3]Селеменева А. В. Применение искусственных иммунных систем для обнаружения сетевых вторжений. Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. - 2019. - № 2. - С. 49-56.

ISSN 2697-2212 Online: https://academicjournal.io

входной вектор причисляется к одному из известных классов. Таким образом, в случае использования НС в сфере сетевой безопасности, любое действие пользователя или приложения должно быт представлено в виде вектора признаков, которые подаются на вход НС. В результате прохождения сигналов по сети на выходе получается вектор, определяющий, является ли действие вредоносным. Обучение НС производят с помощью существующих пакетов, как пакет Deductor Lite[4]; MATLAB Neural Network Toolbox или известных алгоритмов, например, метод «обратного распространения ошибки». Для качественного обучения такой сети необходимо около 300 обучающих примеров. Следует отметить, что подготовка обучающей выборки является достаточно сложным этапом. Выход НС может быт интерпретирован как процентное соответствие текущих действий действиям хакера. Таким же способом можно организовать определение различных атак и адаптацию к новым типам угроз. Примером использования НС в системах сетевой безопасности является нейроанализатор, входящий в состав антивирусной утилиты AVZ. Нейро - анализатор позволяет исследовать подозрительные файлы и применяется в детекторе клавиатурных хакеров (Keylogger). Использование нейросетевых технологий позволяет придат системам безопасности способност к обучению, обеспечивает высокую точност распознавания. Как показал анализ, его недостатком является сложность анализа, вследствие чего обученная НС представляется пользователю «черным ящиком» с определенным количеством входов и выходов. В отличие от продукционных систем, хранение нейронной сети в компьютерах требует гораздо меньше памяти, а определение вредоносных действий – меньше вычислительных ресурсов. Эффект от этих преимуществ усиливается, если учесть, что разработчики стремятся минимизировать размер обновлений для своих систем безопасности. В появляющихся новых антивирусных утилитах, программах анализа сетевой защищенности, межсетевых экранах наблюдается тенденция увеличения масштаба использования технологий искусственного интеллекта. Этому способствует наличие в них возможности обучения, активное развитие методологии ИИ, увеличение числа и усложнение сетевых угроз. Другой тенденцией является направленность на интеграцию средств защиты различных уровней (например, персональный антивирус и сетевой экран уровня предприятия) с использованием средств ИИ.

Заключение. Подходы и методы ИИ на сегодняшний день далеко не исчерпали свой потенциал. Высока вероятность, что дальнейшие исследования раскроют новые пути применения методов ИИ в сфере сетевой безопасности. Согласно ряду современных подходов к искусственному интеллекту, его можно условно разделит на два типа: так называемый сильный и слабый искусственный интеллект. Слабый и сильный искусственный интеллект обратим внимание на такое потенциальное воплощение сильного ИИ, как «искусственный ученый». Речь идет уже не о сознании, а реализуются принципиально иные подходы: на заданную област знаний выделяется значительный объем максимально достоверных научных публикаций, на основе которых обучаются большие многослойные и параллельные нейронные сети. По нескольким пересекающимся смежным областям знаний обучаются другие нейронные сети, имеющие похожие структуры. Для достижения максимальной эффективности можно использовать методы, характерные для «живой» реальной науки, когда открытия и находки совершаются в ходе

[4]Щурина С. В. Искусственный интеллект как технологическая инновация для ускорения развития экономики. Ж. Экономика. Налоги. Право. - 2019. – Т.: 12, № 3. – С. 125-133.

ISSN 2697-2212 Online: https://academicjournal.io

научной полемики между группами исследователей или научных организаций: не один, а несколько базирующихся на нейронных сетях объектов обучаются на смежных, но не дублирующийся данных, а затем они зацикливаются друг на друга, совместно «обсуждая» поставленные задачи и находя решения, подобно модификации принципа, который впервые был применен компанией AlphaGo.

Список использованной литературы

1. Что такое цифровая экономика? Тренды, компетенции, измерение. Докл. к XX Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 9–12 апр. 2019 г. / Г.И. Абдрахманова, К.О. Вишневский, Л.М. Гохберг и др.; науч. ред. Л.М. Гохберг; Нац. исслед. ун-т «Высшая школа экономики».- М.: Изд. дом Высшей школы экономики, 2019.- 82 с,
2. 2 Пономарева С. В. Применение в промышленности инновационных приложений, базирующихся на искусственном интеллекте (в рамках развития концепции цифровой экономики. сборник трудов научно- практической конференции с зарубежным участием (Санкт-Петербург, 20-22 июня 2019 г.): СПБПУ, 2019. - С. 130-138.
3. Селеменева А. В. Применение искусственных иммунных систем для обнаружения сетевых вторжений. Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. - 2019. - № 2. - С. 49-56.
4. Щурина С. В. Искусственный интеллект как технологическая инновация для ускорения развития экономики. Ж. Экономика. Налоги. Право. - 2019. – Т.: 12, № 3. – С. 125-133.