ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И НЕКОТОРЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ РОССИИ

© 2019 г. А.А. Кокошин

Московский государственный университет им. М.В. Ломоносова, Москва, Россия

E-mail: dekanat@fmp.msu.ru

Поступила в редакцию 03.12.2018 г.
Поступила после доработки 03.12.2018 г.
Принята к публикации 25.12.2018 г.

В статье в сжатом виде представлены некоторые случаи применения систем искусственного интеллекта (интеллектуальных систем) в целях надёжного предупреждения и оптимальной реакции на техногенные и природные чрезвычайные ситуации, решения комплекса задач информационной безопасности и кибербезопасности, повышения боеспособности Вооружённых сил.

Ключевые слова: системы и технологии искусственного интеллекта, обучение на прецедентах, техногенные и природные чрезвычайные ситуации, информационная безопасность и кибербезопасность, боеспособность Вооружённых сил.

DOI: https://doi.org/10.31857/S0869-5873895437-439

При оценке перспектив исследований в области искусственного интеллекта (ИИ) необходимо учитывать как долгосрочные, так и среднесрочные тенденции в этой сфере. Сегодня мы переживаем третью волну в развитии искусственного интеллекта, которая характеризуется весьма высокой степенью оптимизма относительно возможностей информационно-коммуникационных технологий и систем. Во многом это связано с развитием широкого спектра таких технологий и соответствующих разделов математики.

Работы в области искусственного интеллекта ведутся в некоторых странах по крайней мере со второй половины 1950-х годов. За это время они прошли через ряд подъёмов и спадов, в том числе применительно к проблемам безопасности. Нельзя не упомянуть, что многие специалисты обоснованно обращают внимание на целый ряд существенных рисков и проблем, которые возникают при бурном развитии этого направления. А значит, изучению рисков при создании систем ИИ, особенно автономных, должны быть посвящены специальные исследования и разработки.

По определению академика РАН И.А. Соколова, искусственный интеллект – междисциплинарная наука на стыке математики, информатики, лингвистики и когнитивных наук. Методы искусственного интеллекта применяются в тех областях, где приходится действовать, не имея точных инструментов решения проблемы, и к тем задачам, для которых отсутствует или неприемлем по временны́м ограничениям заранее заданный алгоритм решения. Академик РАН К.В. Рудаков говорил о том, что для использования методов и математических подходов искусственного интеллекта наличие адекватной математической модели предметной области не является необходимым, чем во многом, по его мнению, и определяется широта спектра приложений технологий и систем ИИ.

Традиционно к числу задач, решаемых системами и технологиями искусственного интеллекта, относятся: обработка текстов, распознавание изображений и видео, обработка аудиозаписей (в том числе речи), обработка электронных сигналов и иных массивов информации с дальнейшим выделением и представлением знаний, поддержка принятия решений. Развитие систем искусственного интеллекта для указанных направлений в растущей мере связано с рядом общественных и гуманитарных наук, в том числе с социологией, психологией, политологией, правоведением, теорией управления. Этот факт нередко недоучитывается, особенно при постановке задач, в частности в области систем поддержки принятия решения.

Системы ИИ способны обучаться на прецедентах в непредвиденных ситуациях. С этой точ-

КОКОШИН Андрей Афанасьевич – академик РАН, декан факультета мировой политики МГУ им. М.В. Ломоносова, 6-й секретарь Совета безопасности РФ.

ки зрения исключительно важно формирование как можно более детального и исчерпывающего набора описаний прецедентов. Во многих случаях это весьма сложная ресурсоёмкая задача, требующая тесного взаимодействия учёных и специалистов разного профиля. Для эффективной работы систем искусственного интеллекта в сфере безопасности необходима первичная обработка огромных объёмов информации, структурированных в разных вариантах, что требует тесного взаимодействия как разработчиков и операторов систем ИИ, так и специалистов-аналитиков.

В соответствии с НИР «Разработка прогноза реализации приоритета научно-технического развития, определённого пунктом 20д Стратегии научно-технологического развития Российской Федерации "Противодействие техногенным, биогенным, социокультурным угрозам, терроризму и идеологическому экстремизму, а также киберугрозам и иным источникам опасности для общества, экономики и государства"» выделены прикладные области использования искусственного интеллекта в сфере безопасности.

Повышение эффективности правоохранительной деятельности, в том числе применительно к борьбе с экстремизмом и терроризмом. Существенное значение в рамках противодействия терроризму и идеологическому экстремизму приобрели работы над совершенствованием технологий и обработки больших массивов данных, обеспечивающих оперативность и комплексность рассмотрения соответствующих проблем. Весьма важен анализ и прогнозирование развития социокультурной среды в целях обеспечения поиска связей между различными субъектами, явлениями и событиями с применением ИИ. Соответствующие системы искусственного интеллекта могли бы выявлять субъектов, потенциально опасных для общества в том числе по внешним поведенческим признакам.

Надёжное предупреждение и оптимальная реакция на техногенные и природные чрезвычайные ситуации (ЧС):

• выявление угроз возникновения ЧС на основе обработки неформализованной информации из социальных медиа, сообщений добровольцев и т. п.;

• обнаружение признаков ЧС с использованием видовой информации (аэрофотосъёмка, камеры наружного наблюдения, автомобильные видеорегистраторы, иные средства фото- и видеофиксации;

• определение границ районов ЧС с использованием видовой информации;

• поиск людей и объектов в районах ЧС, в том числе под завалами, в горно-лесистой местности, в других сложных условиях;

• в области природных воздействий значительная часть проблем, требующих изучения, связана с механизмами подобных воздействий, прогнозированием и моделированием угроз, например, гидрологического (наводнения, затопления территорий и др.), геолого-геоморфологического (землетрясения, вулканы, сели, оползни, лавины и др.), метеорологического характера, а также природных пожаров.

Всё бóльшую актуальность приобретают методы и средства жёсткой, функциональной и комбинированной защиты сложных технических систем.

Решение обширного комплекса задач информационной безопасности и кибербезопасности. В США, например, пытаются создать программное обеспечение, которое позволяет определять ботов, занимающихся дезинформацией в сети, выявлять те или иные информационные кампании в социальных сетях, оценивать их эффективность.

Огромное значение имеют системы искусственного интеллекта для кибервойн, в том числе для распознавания на ранней стадии возможных кибератак как по военным, так и по гражданским целям, для обнаружения аномалий в киберпространстве. Применительно к ведению информационного противоборства системы ИИ помогают подбирать важную информационную стратегию и тактику работы в социальных сетях.

В соответствии с Доктриной информационной безопасности РФ 2016 г. понятие "информационная безопасность" является максимально полным, охватывающим информационно-психологический аспект, кибербезопасность, защиту информации и др. (п. 23 Доктрины). Тем не менее специалисты проводят различие между кибервойнами и информационными войнами. По словам президента Российской академии ракетных и артиллерийских наук В.М. Буренка, кибервойна – "это целенаправленное деструктивное воздействие информационных потоков в виде программных кодов на материальные объекты и их системы, их разрушение, нарушение функционирования или перехват управления ими". Информационные же войны – "это контентные войны, имеющие своей целью изменение массового, группового и индивидуального сознания". В процессе таких войн идёт борьба за умы, ценности, поведенческие характеристики людей. Справедливо утверждается, что информационные войны велись задолго до появления киберпространства.

Повышение боеспособности Вооружённых сил по широкому спектру их функций и задач. Многочисленные исследования, оценки авторитетных учёных и специалистов свидетельствуют, что в области искусственного интеллекта наступает новый этап, который может знаменоваться заметными прорывными результатами в военной сфере.

Выдвигаются гипотезы о том, что широкое внедрение систем ИИ приведёт к революционным изменениям, сопоставимым с появлением боевой авиации или даже атомного оружия. Но эта гипотеза нуждается в тщательной научно-исследовательской проработке. Значительный интерес представляет применение ИИ в различных звеньях всего контура принятия решения – от получения и обработки информации до выработки решения на основе анализа разных вариантов, реализации решения, включая контроль за его исполнением. В целом системы и средства искусственного интеллекта призваны обеспечить упреждающее выполнение всего цикла управления на высоком уровне.

Перечень задач, которые могут быть решены применительно к сфере безопасности и обороны с использованием технологий и систем ИИ, далеко не исчерпывается указанными выше направлениями. Но именно эти направления, на которых акцентируют внимание многие эксперты, должны войти в перечень, который необходимо активно формировать уже сегодня с учётом достижений в области искусственного интеллекта.

ARTIFICIAL INTELLIGENCE AND SOME ISSUES OF RUSSIAN SECURITY PROVISION

© 2019 A.A. Kokoshin

Lomonosov Moscow State University, Moscow, Russia

E-mail: dekanat@fmp.msu.ru

Received: 03.12.2018
Revised version received: 03.12.2018
Accepted: 25.12.2018

Some cases of using Artificial Intelligence systems are analyzed in order to give reliable warning and optimal response to man-made and natural emergencies. The author considers the set of tasks of information and cyber security, of increasing the combat capability of the armed forces.

Keywords: systems and technologies of artificial intelligence, case study, man-made and natural emergencies, informational and cyber security, combat capability of armed forces.