

Элементы искусственного интеллекта в контексте национальной безопасности

Н. И. Попова^{1}, И. В. Локтев¹*

¹ Новосибирский военный институт ордена Жукова имени генерала армии И. К. Яковлева войск национальной гвардии Российской Федерации, г. Новосибирск, Российская Федерация
* e-mail: kryne_ni@mail.ru

Аннотация. В работе описаны этапы развития искусственного интеллекта, рассмотрены перспективные технологические направления, связанные с его применением в различных сферах человеческой деятельности. Выявлены основные принципы развития искусственного интеллекта в свете национальной безопасности. Рассмотрены примеры применения искусственного интеллекта в вооружённых силах. Определены перспективные направления развития искусственного интеллекта.

Ключевые слова: искусственный интеллект, национальная безопасность, машинное обучение, цифровые направления

Elements of artificial Intelligence in the context of national security

N. I. Popova^{1}, I. V. Loktev¹*

¹ Novosibirsk Military Institute of the Order of Zhukov named after General of the Army I. K. Yakovlev of the National Guard Troops of the Russian Federation, Novosibirsk, Russian Federation
* e-mail: kryne_ni@mail.ru

Abstract. The paper describes the stages of development of artificial intelligence, considers promising technological areas related to its application in various fields of human activity. The main principles of the development of artificial intelligence in the light of national security are revealed. Examples of the use of artificial intelligence in the armed forces are considered. Perspective directions of development of artificial intelligence are determined.

Keywords: artificial intelligence, national security, machine learning, digital trends

Вопросы, связанные с искусственным интеллектом, стали возникать во второй половине прошлого столетия. В исследованиях данной области несколько раз происходила смена парадигм.

В середине семидесятых годов прошлого столетия возник вопрос, связанный с организацией хранения накопленных человечеством знаний и формирования на их основе «экспертных систем», которые в свою очередь помогали решать узкоспециализированные задачи конкретной предметной области, знания о которой были в ней заложены. Описание задачи формулировались человеком.

В дальнейшем меняется подход к понятию сути мышления – поиск решения конкретной задачи есть процесс манипулирования знаниями, хранящимися в системе. В процессе развития данного направления стало очевидным, что в процессе обучения человек получает большой объем информации, которую весьма

проблематично вручную заложить в систему. На данном этапе развития искусственного интеллекта человек описывает не конкретную задачу, а некоторую предметную область, содержащую несколько задач.

В восьмидесятых годах появляется новое направление – машинное обучение. Основной задачей данного направления стало оптимизация поиска решения, т.е. интеллект стал пониматься не как готовый продукт, способный решать задачи посредством манипулирования полученными знаниями, а как построение эвристик поиска. Данное понимание способствовало снятию ограничений, связанных с «узкостью» предметной области. Это привело к появлению «воплощенных систем» в которых информация служит основой знаний необходимых для решения той или иной задачи. В «воплощенных системах» описание определенной предметной области частично осуществляется самой системой в рамках задорного направления.

В дальнейшем «воплощенные системы» должны включать в себя синтез методов, полученных в рамках изолированных направлений различных предметных областей (систем речевого общения, компьютерного зрения, машинного перевода, биометрическая идентификация и т.д.). Получение более широкого доступа к информации за счет помещения «воплощенных систем» в конкретное социальное, физическое и информационное пространство.

В настоящее время искусственный интеллект в промышленности Российской Федерации нашёл свое применение в виде экспертных систем, робототехники, систем технического зрения, информационно-аналитических систем.

Согласно указу Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», под искусственным интеллектом понимается: «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений» [1, с. 5700].

В указе № 490 определяются принципы развития и использования технологий искусственного интеллекта, одними из которых является:

- обеспечение защиты граждан и государства;
- безопасность граждан;
- технологический суверенитет;
- поддержка конкуренции и т.д.

Исходя из представленных выше принципов развитие искусственного интеллекта в условиях цифровизации всех сфер деятельности имеет принципиальное значение тесно связано с национальной безопасностью.

Согласно стратегии национальной безопасности Российской Федерации (от 31.12.2015 г №683): «национальная безопасность – состояние защищённости

личности, общества и государства от внутренних и внешних угроз. Включает в себя оборону страны и все виды безопасности и прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности» [2, с. 212].

В настоящее время технологии искусственного интеллекта применяются в следующих сферах:

– в промышленности: при повышении эффективности разработки новых продуктов, автоматизированной оценки поставщиков и при анализе требований к деталям и комплектующим, автоматизации сборочных линий, снижение количества ошибок и т.д.;

– в социальной сфере: повышение качества муниципальных и государственных услуг на здравоохранение, образование и т.д.;

– в государственной сфере: налоговое администрирование, формирование прогнозов федерального бюджета, организации взаимодействия органов власти и т.д.;

– в финансовом секторе: автоматизация взаимодействия с клиентами, представление персональных предложений, одобрение кредитов и т.д.;

– в электроэнергетике: оценка надежности энергогенерирующего оборудования, автоматизированное обслуживание клиентов, снижение потерь и предотвращение кражи электроэнергии и т.д.;

– в транспортной сфере: применение автопилотов, обеспечение безопасности движения и т.д.;

– в оборонно-промышленном комплексе.

Процент использования искусственного интеллекта в российских компаниях представлен на рисунке 1.

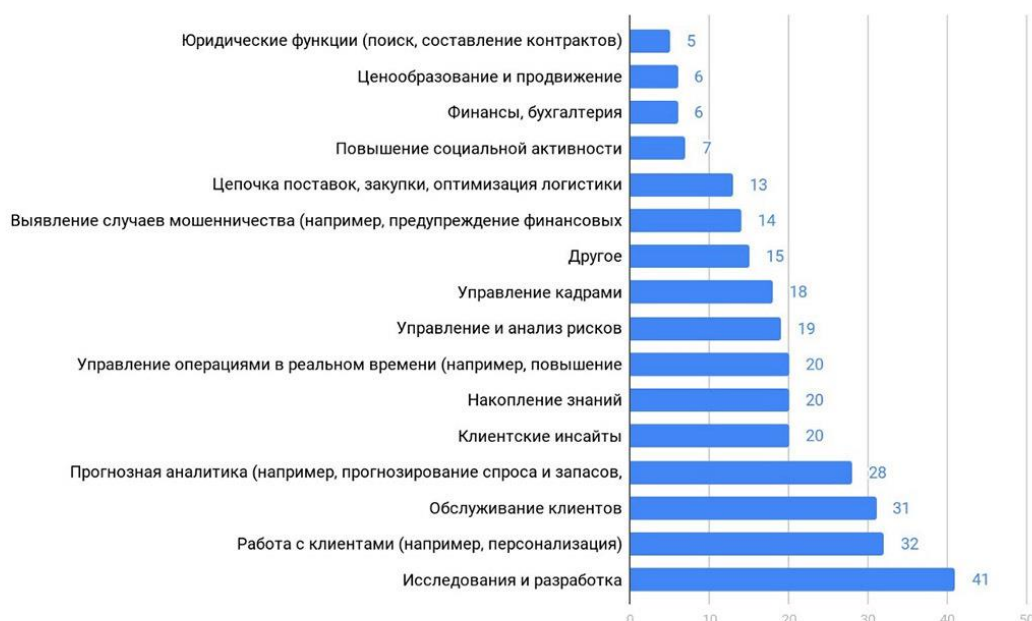


Рис. 1. Процент применения искусственного интеллекта в российских компаниях

Следует отметить, что подход к развитию искусственного интеллекта в разных странах различен: одни страны ведут ключевые разработки в данной сфере исключительно в мирных целях и лишь потом рассматривают применение данных технологий в военных разработках, другие, наоборот, однако в настоящее время все развитые страны ведут сбор и анализ разведанных, используют роботов, беспилотники для осуществления определенных операций, осуществляют кибероперации.

В российской федерации большое внимание уделяется разработке технологий искусственного интеллекта в военно-промышленном комплексе [3].

В настоящее время на вооружении российской армии находится более 2000 беспилотных летательных аппаратов («Орлан-10», «Альтиус-У», «Орион»), разработана линейка беспилотных наземных систем, включающие в себя малые системы, большие танковые системы («Уран-9», «Соратник», «Уран-6», «Сфера»).

В рамках форума «Искусственный интеллект: проблемы и решения», который проходил в мае 2018 года министр обороны России Сергей Шойгу призвал гражданских и военных конструкторов страны объединить усилия по разработке технологий искусственного интеллекта для обеспечения национальной безопасности страны.

По результатам форума были определен перечень сквозных цифровых направлений, которые следует развивать в ближайшее время [4]:

- компьютерное зрение;
- обработка естественного языка;
- распознавание и синтез речи;
- рекомендательные системы и интеллектуальные системы поддержки принятия решений;
- нейропротезирование;
- нейроинтерфейсы, нейростимуляция и нейросенсинг.

С каждым годом развитие области, связанной с технологиями искусственного интеллекта, стремительно растут как в государственной, частной, так и в военной сфере и не только в российской федерации, но и по всему миру.

По прогнозу экспертов объем рынка искусственного интеллекта с каждым годом будет только расти и к 2025 году составит 59,7 миллиардов долларов США (рис. 2).

Технологии искусственного интеллекта обладают уникальными характеристиками, позволяющими охватывать все значимые сферы жизнедеятельности человека в том числе и сферу обеспечения национальной безопасности:

- 1) искусственный интеллект позволяет осуществлять интеграцию разрозненных устройств и приложений, для достижения оптимальной производительности и формированию «Интернет-вещей»;
- 2) технологии искусственного интеллекта практически не заметны при интеграции в какой-либо продукт;
- 3) одни и те же технологии искусственного интеллекта могут применяться как в военных, так и в гражданских приложениях.

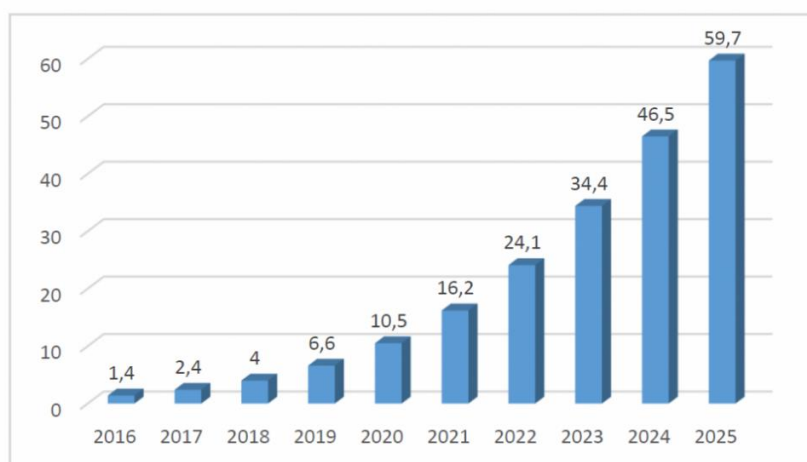


Рис. 2. Объем рынка искусственного интеллекта до 2025 года в миллиардах долларов США

Повсеместное внедрение искусственного интеллекта может не только привести к позитивным изменениям во всех сферах жизнедеятельности человечества в том числе и национальной безопасности, но и создать определенные угрозы.

Например, поведение искусственного интеллекта может быть непредсказуемо при применении уникальных форм манипуляции, при удачном осуществлении кибератаки, при воздействии разрушительных и обманчивых тактик.

В заключении хотелось бы отметить, стремительное развитие искусственного интеллекта и его повсеместное внедрение существенно помогает в осуществлении национальной безопасности, но в тоже время бесконтрольное и бездумное применение данных технологий может и разрушительно воздействовать на человека, общество и государство. Применение технологий искусственного интеллекта в различных сферах человеческой деятельности должно чего контролироваться и регулироваться человеком, обществом, государством, иначе их бездумное внедрение в различного рода конфронтации по разные стороны баррикад может привести к необратимым последствиям в том числе и в сфере национальной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О развитии искусственного интеллекта в Российской Федерации: Указ Президента Российской Федерации от 10.10.2019 № 490 // Собрание законодательства РФ. 2019. № 41, Ст. 5700.
2. О Стратегии национальной безопасности РФ: указ президента РФ от 31 дек. 2015 г. № 683 // Собрание законодательства РФ. 2015. № 1, ч. II. Ст. 212.
3. Национальная безопасность Российской Федерации: проблемы укрепления государственно-правовых основ /В.Г. Вишняков, Л.В. Андрийченко, С.А. Боголюбов и др. // Журнал российского права. 2005. № 2. С. 4
4. Дорожная карта развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект» // [Электронный ресурс] – URL: <https://digitech.ac.gov.ru/upload/iblock/21a/21a0c5dcd903204acb78c486e7eaa54a> (дата обращения: 15.01.2022)

© Н. И. Попова, И. В. Локтев, 2022