ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И КИБЕРБЕЗОПАСНОСТЬ В СОВРЕМЕННОЙ ПОЛИТИКЕ

Козлов С.А. *студент группы ИУЗ-41Б*
Московский государственный технический университет им Н. Э. Баумана

Научный руководитель: ***Гришнова Е.Е.****, доктор политических наук, профессор кафедры «Информационная аналитика и политические технологии»*

Аннотация: В работе автором рассматривается влияние новых технологий – искусственный интеллект и кибербезопасность – на современное общество и политику. Рассмотрены истоки новых технологий, этапы их развития. Выявлены новые перспективы современной политики в условиях их применения.

Ключевые слова: Искусственный интеллект, кибербезопасность, информационная безопасность.

В XXI веке огромное влияние на общество оказывает информация. Особое место занимают искусственный интеллект и кибербезопасность. В данной статье предполагается рассмотреть влияние этих технологий на современную политику.

Для начала следует упомянуть о тех научных дисциплинам, которые внесли большой вклад в развитие данной области. Философия оказала большое влияние, так как помогла ответить на некоторые общеметодологические вопросы, например, откуда приходят знания или каким образом знания ведут к действиям? По своей сути, философы сформулировали основные идеи искусственного интеллекта. Математика помогла логически точно формализовать идеи философов. Формальная логика, в первую очередь логика первого порядка, предоставила формальный способ представления знаний и выстраивания правильных рассуждений. Теория вероятностей и статистика помогли искусственному интеллекту рассуждать в условиях неопределённости или неизвестности. А, появившаяся относительно недавно, теория вычислимости или теория рекурсивных функций смогла выделить те задачи, которые невозможно решить с помощью компьютера за короткое время. Большое влияние оказали экономика и исследования в сфере управленческих решений, так как они предоставили алгоритмы оптимизации в принятии решений, в том числе в условиях неопределённости. Нейронауки – область научных исследований, посвященная изучению нервной системы, в особенности, мозга. Изучение работы нейронов помогли лучше разобраться в работе человеческого мышления. Психология также оказала влияние в сфере изучения мотивации поведение людей и особенностей их коммуникации

друг с другом. Если нейронауки изучают работу мозга на физико-химическом уровне, то психология (в формате когнитивной психологии) изучает мышление человека с учётом того, что наша психика функционирует как информационная система, которая обрабатывает, анализирует и интерпретирует внешний мир. Когнитивные психологи изучают различные аспекты мышления, включая логическое рассуждение, принятие решений, анализ проблем и творческое мышление. Они исследуют как люди формируют концепции, категории и схемы для организации информации.

Несомненно, на появление искусственного интеллекта оказало влияние развитие компьютерной техники. Именно с использованием компьютерных и программных средств осуществляются вычисления, необходимые искусственному интеллекту. Согласно эмпирическому закону Мура, производительность компьютеров удваивается почти каждые 18 месяцев. Значительное влияние оказала теория управления, доказывая то, что система должна обладать определенным механизмом, регулирующим поведение системы в условиях воздействия внешних факторов.

Также на развитие искусственного интеллекта большое влияние оказала лингвистика, ведь возможность человека составлять новые предложения с определённым смыслом из отдельных слов является важной частью человеческого мышления. Также лингвистика отвечает за обработку и распознание естественного (человеческого) языка [2].

Можно выделить определенные периоды развития искусственного интеллекта:

- начальный этап (1943–1956) – первые нейронные сети, системы математических доказательств и основы обучения машин;
- первые крупные достижения (1952–1969) – создание программы общего решателя задач, решающая задачи, аналогично тому, как это делает человек, разработана программа игры в шашки, разработка языка программирования Lisp;
- проблемы (1966–1975) – нехватка вычислительной мощности, прекращение финансирования исследований;
- экспертные системы (1969–1986) – создание систем, с привлечением экспертов для коррекции алгоритмов, внедрение искусственного интеллекта во многие предприятия;
- возвращение к нейронным сетям (1986 – настоящее время);
- вероятностные рассуждения и машинное обучение (1987 – настоящее время) – появление систем распознавания речи, изображений, появление модели байесовских сетей, возвращение к робототехнике;

- большие данные (2001 – настоящее время) – революция в области компьютерного зрения, возвращение коммерческого интереса;
- глубокое обучение (2011 – настоящее время).

На сегодняшний день искусственный интеллект используется повсеместно. Уже сейчас он способен решать такие задачи, как автоматическое управление транспортными средствами, автономное планирование и составление расписаний, машинный перевод текстов, распознавание и синтезирование речи, составление рекомендаций, ведение игр, распознавание и синтезирование изображений, диагностика заболеваний. Так что с недавних пор область искусственного интеллекта является бурно развивающейся и крайне перспективной [6].

Теперь кратко охарактеризуем кибербезопасность. Защита информации использовалась ещё с древних времён: ещё в Древнем Египте и Древнем Риме. По свидетельству Геродота кодирование информации применялось уже в V веке до нашей эры. А самым известным примером криптографии является «шифр Цезаря». Рассмотрим развитие средств защиты информации в России:

- XVII век – использование дезинформации, шифрования переписок, введение ответственности за разглашение информации, шпионаж и государственную измену;
- XVIII век – расширение состава защищаемой информации;
- XIX век – появление цензуры, коммерческой тайны, законодательства в области патентов и авторского права;
- начало XX века – расширение состава защищаемой информации, военно-промышленная тайна, появление средств защиты информации, передаваемой по радиотелеграфной связи;
- 1917–1945 годы – отмена коммерческой тайны, увеличение объёма сведений, составляющих гостайну, централизация управления защитой госсекретов, усиление ответственности за утечки информации;
- 1945–1975 годы – расширение объёма и тематики защищаемой информации, категорирование по степени секретности;
- 1975–1995 – появление новых носителей информации, средств её обработки и передачи, широкое применение средств технической разведки, разработка теоретических моделей безопасности [6].

С развитием технологий обработки, хранения и передачи информации постоянно возникают задачи по обеспечению безопасности данных. Можно предположить, что теория информационной безопасности будет развиваться и будет востребована постоянно. Более того, инфор-

мационная безопасность является одной из самой быстроразвивающихся областей науки.

В современном мире информация выступает в роли ведущего фактора общественного производства. В связи с этим, современный этап развития общества часто называют «информационным обществом». Особую роль в развитии теории информационной безопасности играют центры информационной безопасности. Это государственные и частные коммерческие организации, проводящие теоретические исследования, разрабатывающие практические решения в области защиты информации, а также осуществляющие прогнозирование. Приоритетные направления деятельности центров информационной безопасности: информационно-аналитические, оперативного реагирования, консультационные, научно-исследовательские, центры сертификации. Фактические центры информационной безопасности определяют направления дальнейшего развития соответствующей области знания. Предметной областью информационной безопасности является: информация и её свойства; угрозы безопасности информации и её собственности; политика безопасности и модели безопасности; способы, методы и средства защиты информации; классификация систем защиты; требования к защищённости информационных систем; методология оценки защищённости информационных систем и проектирование защиты; конкретные системы защиты информации, применяемые в различных органах управления, учреждениях и на предприятиях различных форм собственности [3].

К числу перспективных направлений стоит отнести: формализацию положений теории информационной безопасности; разработку моделей безопасности, более удобных для практического использования и анализа защищённости; разработку средств и методов противодействия угрозам информационной войны; вопросов обеспечения безопасности в глобальных информационных сетях, например, в сети Интернет; разработку системы безопасности электронной коммерции; системы безопасности обработки информации мобильными пользователями [3].

Что касается непосредственного влияния данных технологий на современную политику, то следует отметить, что современные методы защиты информации имеют столь надежный характер, что преступникам гораздо проще манипуляциями заставить людей самостоятельно раскрыть информацию, чем осуществлять попытки взлома.

Государственная информация, отличаясь особо важным для всего общества характером, нуждается в надежной защите. Фактически информационная безопасность является элементом национальной безопасности. Под ней понимается состояние защищённости жизненно важных национальных интересов от внутренних и внешних угроз, при котором обеспечивается реализация конституционных прав и свобод граждан Российской

Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации.

Из-за того, что информация используется практически во всех важных областях жизнедеятельности общества, то обеспечение информационной безопасности является основным показателем национальной безопасности. Информационная безопасность занимает ведущее место в ее обеспечении. Таким образом, обеспечение информационной безопасности должно стать ключевым фактором современной политики. Без него невозможно решить задачи достижения качественного уровня жизни и обеспечения защищённости прав и свобод граждан.

В Российской Федерации действует «Доктрина информационной безопасности Российской Федерации», введённая Указом Президента РФ № 646 от 05.12.2016 [9]. Она являет собой систему официальных взглядов на обеспечение информационной безопасности РФ в информационной сфере [1, 3].

В области искусственного интеллекта должна вестись адекватная политика. Одной из важных проблем ИИ является его возможность синтезирования изображений, речи и даже видеоматериалов. С такими возможностями, могут быть созданы компрометирующие материалы, которые могут повлиять не только на имидж политических лидеров, но и на ситуацию внутри стран, и на систему межгосударственных и международных отношений. Инструментарий несет значительные риски, что требует решения задачи защиты общества от разрушительного его воздействия, чтобы не допустить массовых волнений в обществе из-за дезинформации, искусственно созданной с помощью ИИ.

Также важен вопрос доверия искусственному интеллекту. Например, известно, что ИИ используется в медицине для диагностики заболеваний, к примеру, система Lyna, определяющая метастатический рак молочной железы с точностью около 99,6%. Тем не менее комбинация ИИ + экспертный медик работает гораздо эффективнее.

Из-за того, что ИИ используется для принятия оптимальных решений в том числе в сфере политики, необходимо критически относиться к ответам ИИ, не относясь к ним, как к единственно правильному пути разрешения проблемы. Из-за того, что ИИ часто проектируется для достижения конкретной цели, упор идёт именно на цель, а не на средства достижения и мораль, поэтому ИИ зачастую может выдать неэтические пути решения проблем. Так что государства должны ограничивать применение искусственного интеллекта при принятии важных решений [4, 8, 9].

В заключение, можно отметить, что особое внимание следует направить на необходимость обеспечения адекватности политики в услови-

ях все нарастающего внедрения в нее искусственного интеллекта. В силу этого требуется продуманное и выверенное отношение к использованию искусственного интеллекта в политике. Наряду с этим следует признать, что область искусственного интеллекта является очень перспективной и быстроразвивающейся, поэтому ограничительные меры не должны препятствовать её позитивному развитию. Данные моменты следует учитывать при разработке эффективной системы кибербезопасности. В целом, очевидно, что современные государства должны будут развивать информационную безопасность с привлечением искусственного интеллекта для обеспечения надежного политического, экономического и технологического суверенитета.

Литература и источники

1. Анохин М.Г. Современные технологии эффективной политики. М.: РУДН, 2008. 239 с.
2. Бочарников И.В. Развитие современных глобализационных процессов: перспективы, проблемы и риски. В сборнике: Современная Россия в мировом политическом процессе: глобальное и региональное измерение. Материалы международной научно-практической конференции. Под общей редакцией А.Я. Касюка, И.К. Харичкина. 2019. С. 171–182.
3. Вострецова Е.В. Основы информационной безопасности. Екатеринбург: Урал. ун-т, 2019. 204 с.
4. Гришин О.Е. Политические цифровые технологии: о сути явления // Культура и природа политической власти: теория и практика: сборник научных трудов. Екатеринбург: УрГПУ, 2023. С. 221–225.
5. Гришнова Е.Е. Особенности современного политологического анализа развития институциональной структуры политической системы // Этносоциум и межнациональная культура. 2012. № 11 (53). С. 23–29.
6. Рассел С., Норвиг П. Искусственный интеллект. Современный подход. Том 1. Решение проблем: знания и рассуждения. – 4-е изд. Санкт-Петербург: ООО «Диалектика», 2021. 704 с.
7. Ремарчук В.Н. Управление смыслами как инструмент современной политики: технологии, вероятные последствия // Этносоциум и межнациональная культура. 2019. № 2 (128). С. 9–21.
8. Сиденко О.А., Сосунов Д.В., Щеглова Д.В., Гармонова А.В., Савенков Г.В., Глухова А.В., Маврин О.В. Современные технологии в публичной политике. Воронеж: Издательский дом ВГУ, 2018. 228 с.
9. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
10. Content of the process of formation of students' speech abilities at the university / Ovsyannikova O.A., Mishcherina M.A., Bocharnikov I.V. В сборнике: E3S Web of Conferences. 8. Сер. "Innovative Technologies in Science and Education, ITSE 2020" 2020. С. 18106.