10. *Анахов, С. В.* Особенности реализации научно-образовательной политики в рамках национальной технологической инициативы / С. В. Анахов. Текст: непосредственный // Новые информационные технологии в образовании и науке. 2019. № 2. С. 5–15.

11. *EDUCAUSE* Horizon Report 2019. URL: https://www.educause.edu/horizonreport. Text: electronic.

УДК 004.8
DOI:10.17853/2587-6910-2020-03-15-18

ВОПРОСЫ БЕЗОПАСНОСТИ МОЛОДЕЖИ В УСЛОВИЯХ МЕНЯЮЩЕГОСЯ ОКРУЖЕНИЯ СОВРЕМЕННОГО МИРА

YOUTH SAFETY ISSUES IN THE CONDITIONS OF THE CHANGING ENVIRONMENT OF THE MODERN WORLD

Диана Александровна Богданова

кандидат педагогических наук,
старший научный сотрудник

d.a.bogdanova@mail.ru

Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия

Diana Aleksandrovna Bogdanova

Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia

Аннотация. *Поднята проблема защиты интересов детей и молодежи в условиях активного проникновения систем искусственного интеллекта в жизнь современного общества. Сформулированы вопросы, ответы на которые помогут подготовить подрастающее поколение к решению задач конфиденциальности и безопасности при использовании в Сети приложений, работающих на основе искусственного интеллекта, даны базовые правила профилактики.*

Ключевые слова: *Интернет-риски, искусственный интеллект, игрушки на основе искусственного интеллекта, персональные данные, цифровое гражданство, цифровые следы, мобильные приложения на основе искусственного интеллекта, Интернет-безопасность, ответственность взрослых.*

Abstract. *The article is devoted to the problem of protecting children and youth in conditions of the active penetration of artificial intelligence systems into the life of modern society. Based on the analysis of publications, questions to be answered are formulated, which will help to prepare children and youth for resolving privacy and safety issues in situations associated with the use of applications based on artificial intelligence, as well as basic prevention rules.*

Keywords: *Internet risks, artificial intelligence, toys using artificial intelligence, personal data, digital citizenship, digital footprints, mobile applications using artificial intelligence, Internet safety, adults responsibility.*

В течение последних лет технологии, основанные на использовании искусственного интеллекта (ИИ), активно формируют важные части цифровой экономики и затрагивают основные области нашего общества, объединенного сетью Интернет. Будь то транспорт, производство или социальная справедливость, ИИ оказывает глубокое влияние на деятельность людей и трансформирует будущее как видимыми, так и скрытыми способами. Перспективы технологий на основе искусственного интеллекта безграничны, и выгоды от их применения варьируются от повышения эффективности до беспрецедентного улучшения качества жизни.

Инновации внедряются ускоренными темпами не только в профессиональной рабочей среде. Исследований о положительном влиянии на детей и подростков систем на основе ИИ к настоящему времени проведено сравнительно немного [1]. Однако очевидно, что искусственный интеллект играет все более важную роль в сферах образования, обучения и здравоохранения. Например, Hello Barbie и Cozmo — это всего лишь игрушки на основе ИИ, которые открывают детям новые игровые творческие возможности, а некоторые способствуют повышению грамотности, формированию социальных навыков и развитию речи. В рамках формального образования такие основанные на системах ИИ технологии, как интеллектуальные системы обучения, индивидуальные траектории обучения и интеллектуальная виртуальная реальность могут улучшить результаты занятий, предложив разнообразный увлекательный интерактивный опыт для детей и молодежи [2]. В неформальной среде обучения, как, например, на платформе Scratch MIT Media Lab, молодые люди получают возможность разрабатывать и программировать интерактивные игры на основе ИИ, симуляторы, чат-роботов и виртуальных роботов, что влияет на развитие творчества, получение знаний и самовыражение.

Однако сложное взаимодействие между наборами данных и алгоритмами, которые используют эти технологии, вызывает немало жизненно важных вопросов относительно прозрачности, подотчетности, конфиденциальности пользователей. Более того, технологии на основе использования систем ИИ (и их зависимость от больших баз данных) вызывают серьезные опасения по поводу безопасности, поскольку современная молодежь делится с другими своими персональными данными как сознательно (используя платформы социальных сетей, публикуя фотографии), так и неосознанно (ставя лайки, делая покупки в Интернете).

Основная цель многих систем ИИ состоит в том, чтобы, алгоритмически обнаруживая закономерности в больших объемах данных, строить прогнозы и делать выводы об отдельных лицах и целых группах. Эти прогнозы варьируются от относительно безобидных, таких как рекомендуемые на YouTube видео, основанные на истории просмотров, до потенциально вредных и опасных, например, информация об употреблении алкоголя или наркотиков, выдаваемая на основании лайков и обновлений статуса пользователей в Сети. Кроме того, огромные объемы данных, собранные системой ИИ, могут оказаться доступными для третьих лиц и использоваться в незаконных или эксплуататорских целях, как это произошло с Cambridge Analytica. Впрочем, даже люди, имеющие разрешенный начальный доступ к данным системы ИИ, могут в своих интересах принимать решения, ограничивающие текущие или будущие возможности молодежи.

Сложное взаимодействие между наборами данных и алгоритмами, которые питают «черный ящик» систем ИИ, особенно когда эти системы подключены к Интернету, приводит к множеству проблем, касающихся предвзятости и дискриминации, прозрачности и подотчетности, конфиденциальности и безопасности молодежи [3]. Решать их необходимо всем заинтересованным сторонам.

Во-первых, разработчикам, так как риск нарушения конфиденциальности молодежи возрастает, если компании, которые разрабатывают основанные на искусственном интеллекте технологии, не имеют четкого представления о том, какие пользовательские данные они собирают, где эти данные хранятся, кто имеет к ним доступ и что может с ними сделать. Широкий спектр личной информации о молодых пользователях может быть записан и сохранен при взаимодействии с системой ИИ даже в результате разговора между подростком и цифровым личным помощником или записи географического местоположения при использовании

домашнего приложения [4]. Поэтому крайне важно, чтобы технологии разрабатывались с осознанием ответственности и обеспечивали конфиденциальность пользователей.

Во-вторых, необходимо вооружить молодых людей знаниями для эффективного решения вопросов конфиденциальности и безопасности в ситуациях, связанных с использованием приложений, работающих на основе ИИ.

В-третьих, требуется вмешательство законодателей, регулирующих организаций или других лиц, принимающих решения в вопросах детской и подростковой безопасности. Например, в США законы и нормативные акты, регламентирующие конфиденциальность цифровых данных молодежи, обычно дают полномочия на согласие о сборе этих данных родителям или опекунам. В сфере образования согласие на обмен данными об обучающихся дает школа. Таким образом, сама молодежь в рамках закона не имеет никаких юридических прав соглашаться или не соглашаться с тем, что личные данные собираются или используются системой ИИ.

В связи с этим возникает целый ряд вопросов, настоятельно требующих ответа.

1. Поскольку технологии, основанные на ИИ, меняют наше отношение к собственной защищенности в цифровом мире, каким образом привлекать заинтересованные стороны (политиков, педагогов, родителей, опекунов, самих молодых людей) к разработке образовательных структур, учитывающих взаимодействие между системой ИИ и онлайн-безопасностью и конфиденциальностью?

2. Каковы возможности добровольного или обязательного образования в области цифрового гражданства как средства, позволяющего молодежи защищать свою конфиденциальность и безопасность личных данных при взаимодействии с ИИ?

3. Какими полномочиями можно наделить молодежь для разрешения разногласий между взрослыми заинтересованными сторонами, принимающими решения, и опытом молодых людей в отношении вопросов конфиденциальности и безопасности в контексте образовательных технологий? В случаях воздействия на частную жизнь и безопасность участие каких заинтересованных сторон может потребоваться, по каким каналам и каким образом молодой человек может сам принять участие в разрешении проблемы?

4. Как согласовать цель сбора данных с защитой личной информации при использовании технологии распознавания образов? Обладая значительным потенциалом для обеспечения безопасности молодежи, например, помощь при воссоединении пропавших детей с близкими, она создает серьезные проблемы с конфиденциальностью из-за усиления слежки и, следовательно, сбора личных данных, вплоть до слежки в масштабах школы [5].

5. Способна ли молодежь, которая нередко находится на передовом крае внедрения новейших цифровых технологий, отказаться от использования некоторых потенциально опасных систем искусственного интеллекта? Если нет, то как донести информацию о краткосрочных и долгосрочных последствиях, которые эти технологии могут иметь для безопасности жизни?

6. Как использовать искусственный интеллект при создании образовательных процессов более богатых в социально-эмоциональном плане (например, с помощью персонажей на основе ИИ в виртуальной среде), как для молодежи, так и для взрослых, которые ее обучают?

7. Как более активно внедрять устройства с системами искусственного интеллекта за пределами образовательной сферы в целях обеспечения равных возможностей для уязвимой категории обучающихся при защите их личной жизни?

В настоящее время вокруг концепции цифрового гражданства существует несколько конструкций, касающихся конфиденциальности и безопасности в Интернете. В отдельных случаях они способствовали проведению реформы образования (сингапурский план, законодательные инициативы в США). Однако даже самые оптимистичные прогнозы о достоинствах новейших ИИ-технологий для улучшения качества жизни, должны учитывать и устранять ряд важных барьеров, не говоря уже о более фундаментальных проблемах с предположениями о роли технологии в обществе. Например, всегда есть различия между перспективой сервиса и его реализацией в контекстных реальных приложениях. Несмотря на возможности, которые открывают эти технологии, существует реальный риск того, что без вдумчивого вме-

шательства они могут фактически усугубить структурный, экономический, социальный и политический дисбаланс. Могут еще больше усилить неравенство, основанное на таких демографических переменных, как пол, возраст, религия, местонахождение, а также образовательный и (или) социально-экономический статус [6].

Список литературы

1. *Богданова, Д. А.* Социальные роботы и дети / Д. А. Богданова. Текст: непосредственный // Информатика и образование. 2018. № 4. С. 56–60.
2. *Najar, A. S.* Learning with intelligent tutors and worked examples: selecting learning activities adaptively leads to better learning outcomes than a fixed curriculum / A. S. Najar, A. Mitrovic, B. M. McLaren. Text: electronic // User Modeling and User-Adapted Interaction The Journal of Personalization Research. № 5. Vol. 26. URL: https://www.cs.cmu.edu/~bmclaren/pubs/NajarMitrovicMcLaren-LearningWithITSAndWorkedExamples-UMUAI2016.pdf.
3. *Ahar, A.* Why inclusion matters for the future of artificial intelligence / A. Ahar, S. Cortesi. Text: electronic // Harvard business school. 2018. April, 26. URL: https://digital.hbs.edu/artificial-intelligence-machine-learning/inclusion-matters-future-artificial-intelligence/.
4. *Shulevitz, J.* Alexa, should we trust you? / J. Shulevitz. Text: electronic // The Atlantic. URL: https://www.theatlantic.com/magazine/archive/2018/11/alexa-how-will-you-change-us/570844/ November 2018 issue.
5. *Stolzoff, S.* Schools are using AI to track their students / S. Stolzoff. Text: electronic // Quartz. URL: https://qz.com/1318758/schools-are-using-ai-to-track-what-students-write-on-their-computers/2018August19.
6. *Wykstra, S.* Developing a More Diverse AI / S. Wykstra. Text: electronic // What's Next — Stanford Social Innovation Review URL: https://perma.cc/52U2-FUM9 Winter 2019.