УДК 343.211.5
ББК Х408.14
DOI: 10.14529/law200420

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ

А. В. Минбалеев[1,2]
[1] Московский государственный юридический университет им. О. Е. Кутафина (МГЮА), г. Москва,
[2] Южно-Уральский государственный университет, г. Челябинск

Статья посвящена исследованию проблем использования искусственного интеллекта в противодействии киберпреступности. Искусственный интеллект используется и в целях совершения киберпреступлений, например, в случаях совершения атак на уязвимые информационные системы. Искусственный интеллект явно необходимо использовать и в противодействии киберпреступности и обеспечении кибербезопасности. Машинное обучение уже активно используется для прогнозирования новых угроз и вредоносных программ на основе существующих шаблонов. Сегодня методы машинного обучения используются в целях мониторинга деятельности системы и человека с целью выявления потенциальных вредоносных отклонений, прогнозирования вредоносных приложений и вредоносных сайтов.Все эти возможности должны лечь в основу развития действующего законодательства и средств противодействия киберпреступности. Законодателю необходимо учитывать возможное использование ИИ, в частности при совершенствовании ряда составов преступлений в сфере компьютерной информации, мошенничества и др. Необходимо усиливать требования при использовании технологий ИИ при обработке больших объемов данных с точки зрения возможности обеспечения кибербезопасности. Автором в статье выделены основные тенденции в сфере технологий искусственного интеллекта и кибербезопасности в условиях пандемии коронавирусной инфекции COVID-19.

Ключевые слова: кибербезопасность, киберпреступность, искусственный интеллект, противодействие.

Кибербезопасность[1] максимально взаимоувязана с возможностями для автоматизации искусственного интеллекта (далее – ИИ). Создание новых инструментов ИИ для расширения возможностей людей должно тесно взаимодействовать с защитой их конфиденциальности и сохранением безопасности их информации, в том числе в киберпространстве. ИИ традиционно уже достаточно давно используется для борьбы со спамом и обнаружения вредоносных программ. ИИ используется и в целях совершения киберпреступлений, например, в случаях совершения атак на уязвимые информационные системы, поскольку это позволяет увеличить скорость атаки, снизить затраты на подготовку и совершение преступлений, а также избежать необходимости привлечения большого количества специалистов в сфере IT, ресурс которых достаточно ограничен, тем более применительно к нелегальной сфере [1].

Помимо эффективности использования ресурсов, технологии ИИ создают психологическую дистанцию между злоумышленником и его жертвой. Ряд киберпреступлений традиционно предполагает взаимодействие с другими людьми и часто их присутствие, что ограничивало анонимность преступника и часто сдерживало его. ИИ, функционируя автономно, снимает эти барьеры и увеличивает анонимность, а также дистанцию. Так, в рамках фишинговых схем традиционно преступникам приходилось достаточно много уделять внимания созданию мотивационных писем, которые побуждали пользователей пройти по предлагаемой веб-ссылке, что позволяло загрузить вредоносное программное обеспечение на устройство пользователя. Проводимые исследования предполагают анализ особенностей той или иной группы людей, их потребительские интересы, посещение ими тех или иных сайтов, коммуникации с другими пользователями и группами. Появление технело-

[1] Работа выполнена при финансовой поддержке Совета по грантам Президента Российской Федерации (грант МД-2209.2020.6) «Развитие системы правовых средств обеспечения кибербезопасности в Российской Федерации».

гий ИИ и больших данных в киберпространстве кардинальным образом меняет ситуацию. Исследование больших наборов данных с помощью ИИ помогает злоумышленникам расставлять приоритеты для своих жертв на основе поведения в сети Интернет и их социальных статусов и ролей, правовых статусов. Используя ИИ, преступники систематизируют данные, доступные в общественном достоянии, различные конфиденциальные данные, незаконно распространенные в сети Интернет, для индивидуализации жертвы за считанные секунды без каких-либо человеческих усилий. Доверие строится путем вовлечения людей в более длительные диалоги в течение продолжительных периодов времени в социальных сетях, которые не требуют человеческих усилий. Используемые же чат-боты поддерживают тесное взаимодействие и даже имитируют реальные контакты, стиль и риторику общения. Прогностические модели ИИ позволяют определить уровень платежеспособности пользователей и определить готовность платить выкуп, скорректировать размер выплаты требуемой злоумышленниками для удаления программ-вымогателей. Машинное обучение, используемое для идентификации жертв и разведки, значительно сокращает вложения злоумышленником в ресурсы, а шансы обогатиться возрастают в разы [1].

ИИ активно используется для имитации голоса и видеоизображений лиц, очень распространенным становится создание так называемых дипфейков (deepfake) благодаря быстрому развитию синтеза речи и видеоизображений. Современные нейронные технологии, основанные на использовании ИИ, активно «оперируют и видеоконтентом: генерируют движущиеся пейзажи, убирают объекты или же заставляют танцевать людей на фото» [2]. Такие технологии часто используются в мошеннических целях, в том числе при получении паролей, кодов доступа и т.п.

ИИ явно необходимо использовать и в противодействии киберпреступности, обеспечении кибербезопасности. Машинное обучение уже активно используется для прогнозирования новых угроз и вредоносных программ на основе существующих шаблонов. Сегодня методы машинного обучения используются в целях мониторинга деятельности информационной системы и человека с целью выявления потенциальных вредоносных отклонений, прогнозирования вредоносных приложений, вредоносных сайтов.

Многочисленные естественные вычислительные методы ИИ (вычислительный интеллект, нейронные сети, интеллектуальные агенты, искусственный иммунитет, машинное обучение, интеллектуальный анализ данных, распознавание образов и др.) играют все более важную роль в обнаружении и предотвращении киберпреступлений. ИИ позволяет разрабатывать автономные вычислительные решения, способные адаптироваться к их контексту использования, используя методы самоуправления, самонастройки, самодиагностики и самоконтроля [3].

Все эти возможности должны лечь в основу развития законодательства и средств противодействия киберпреступности. Законодателю важно учитывать возможное использование ИИ, в частности при совершенствовании ряда составов преступлений в сфере компьютерной информации, мошенничества и др. Необходимо усиливать требования при использовании технологий ИИ в процессе обработки больших объемов данных с точки зрения возможности обеспечения кибербезопасности.

Особое значение в противодействии киберпреступности технологии ИИ приобретают в условиях распространяемой пандемии коронавирусной инфекции COVID-19. Связано это с массовым переходом к использованию информационных технологий в процессе взаимодействия между людьми. Здесь можно выделить несколько тенденций:

– рост киберпреступности, поскольку произошло многократное увеличение финансовых транзакций в электронной среде, а также передач персональных данных и иной информации ограниченного доступа. Электронное взаимодействие привело и к массовому использованию технологий больших данных с использованием ИИ. Соответственно эти возможности были использованы как субъектами, осуществляющими обработку больших объемов данных, так и киберпреступниками при осуществлении кибератак в отношении органов государственной власти, отдельных хозяйствующих субъектов и физических лиц;

– технологии ИИ позволяют как анализировать складывающуюся практику, прежде всего по DDos-атакам, так и спрогнозировать модель поведения злоумышленников, сфор-

мировать модель угроз, разработать меры по противодействию им;

– государства все чаще начинают использовать цифровые технологии для отслеживания преступлений в сети Интернет и с использованием сети, использовать цифровые следы для розыска киберпреступников;

– технологии ИИ активнее стали использоваться за последний год пандемии и при оценке угроз и уязвимостей пользователей, что позволило давать им дополнительные рекомендации по недопущению виктимного поведения в интернет-среде, а также необходимости принятия дополнительных мер защиты от кибератак.

Влияние пандемии COVID-19 на киберпреступность было наиболее заметным по сравнению с другими видами преступной деятельности. Преступники, занимающиеся киберпреступностью, в условиях инфодемии смогли быстро адаптироваться и извлечь выгоду из тревоги и страхов пользователей. Так запускаются массово кампании по фишингу и использованию программ-вымогателей, ожидается, что масштабы фишинга будут только расти. С начала пандемии в целом было небольшое увеличение количества распределенных атак типа «отказ в обслуживании» (DDoS). Однако сегодня мы можем говорить об их резком увеличении. Значительное увеличение удаленно работающих из дома людей способствует повышению пропускной способности трафика, в связи с чем увеличивается лимит трафика в организациях, что позволяет злоумышленникам эффективно реализовывать DDoS-атаки. В начале пандемии имела места активная регистрация вредоносных доменов, связанных со словами «корона» и «COVID». Сегодня эти зарегистрированные доменные имена образуют костяк для многих криминальных операций по всему миру. Увеличение покупок в сети Интернет в условиях пандемии повлекло и резкий рост теневой интернет-торговли. Так, в даркнете наблюдается рост торговых площадок и иных платформ для распространения незаконных товаров и услуг. Уменьшение дефицитных лекарств на официальных сайтах также увеличивает риск подтолкнуть покупателей к поиску альтернативных предложений в даркнете [4]. Дезинформация и иные виды инфодемии вокруг COVID-19 продолжают распространяться по всему миру с потенциально опасными последствиями в виде интернет-мошенничества с лекарствами, оказанием медицинских услуг и т.п. [5]

Для предотвращения противоправных действий в сети Интернет и борьбы с ними сегодня эффективно внедряются технологии ИИ. Особенно активно они используются в противодействии фейковой информации и инфодемии. Ряд международных организаций, в том числе с использованием ИИ, отслеживают дезинформацию и фейковые новости о COVID-19, регулярно публикуя обновления, опровергающие такие утверждения. Так, Всемирная организация здравоохранения отслеживает ложные утверждения о COVID-19 на своем сайте, который регулярно обновляется. Основное внимание уделяется утверждениям о природе вируса и возможных мерах лечения и профилактики [6]. Распространение фейковых новостей и дезинформации во многих случаях не считается уголовным преступлением.

Распространение дезинформации может исходить от самых разных субъектов, включая киберпреступников, ищущих финансовую выгоду [4].

Таким образом, кибер-инфраструктуры сегодня очень уязвимы для вторжений и других угроз кибербезопасности. Современных технологий и активного участия человека недостаточно для мониторинга и защиты этих инфраструктур. В связи с этим явно существует потребность в более сложных системах обеспечения кибербезопасности, которые должны быть гибкими, адаптируемыми и надежными, а также способными обнаруживать широкий спектр угроз и принимать разумные решения в режиме реального времени. Разработка новых методов ИИ играет все более важную роль в современном киберпространстве и позволяет эффективно раскрывать и предотвращать преступления.

Литература

1. Zinatullin L. Artificial Intelligence and Cybersecurity: Attacking and Defending. URL: https://www.tripwire.com/state-of-security /featured/artificial-intelligence-cybersecurity-attacking-defending/.

2. Валяева, А. Как делают deepfake-видео и почему лучше говорить «face swap» / А. Валяева. URL: https://vc.ru/ml/94457-kak-delayut-deepfake-video-i-pochemu-luchshe-govorit-face-swap.

3. Dilek S., Çakır H., Aydin M. Applications of artificial intelligencet echniques to combating

cyber crimes: review // International Journal of Artificial Intelligence & Applications (IJAIA), 2015, Vol. 6, No. 1, January. URL: https://arxiv.org/ftp/arxiv/papers/1502/1502.

4. Catching the virus cybercrime, disinformation and the COVID-19 pandemic.

5. Правовое регулирование искусственного интеллекта в условиях пандемии и инфодемии / под общ. ред. В. В. Блажеева, М. А. Егоровой. – М.: Проспект, 2020. – 240 с.

6. Coronavirus disease (COVID-19) advice for the public: Mythbusters. URL: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters.

Минбалеев Алексей Владимирович – доктор юридических наук, профессор, зав. кафедрой информационного права и цифровых технологий, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), г. Москва; профессор кафедры теории государства и права, конституционного и административного права, Южно-Уральский государственный университет, г. Челябинск. E-mail: alexmin@bk.ru.

Статья поступила в редакцию 18 октября 2020 г.

DOI: 10.14529/law200420

PROBLEMS OF USING ARTIFICIAL INTELLIGENCE IN COUNTERING CYBERCRIME

A. V. Minvaleev[1,2]

[1] Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation,

[2] South Ural State University, Chelyabinsk, Russian Federation

The article is devoted to the study of the problems of using artificial intelligence in countering cybercrime. Artificial intelligence is also used to commit cybercrimes, for example, in cases of attacks on vulnerable information systems. Artificial intelligence clearly needs to be used in countering cybercrime and ensuring cybersecurity. Machine learning is already being actively used to predict new threats and malware based on existing patterns. Today, machine learning methods are used to monitor system and human activity in order to identify potential malicious deviations, predict malicious applications and malicious sites. All these possibilities should form the basis for the development of existing legislation and means of countering cybercrime. The legislator needs to take into account the possible use of AI, in particular when improving a number of crimes in the field of computer information, fraud, etc. It is necessary to strengthen the requirements for the use of AI technologies when processing large amounts of data in terms of the possibility of ensuring cybersecurity. The author highlights the main trends in the field of artificial intelligence and cybersecurity technologies in the context of the COVID-19 coronavirus infection pandemic.

Keywords: cybersecurity, cybercrime, artificial intelligence, counteraction.

References

2. Valyayeva A. *Kak delayut deepfake-video i pochemu luchshe govorit' «face swap»* [How to make deepfake videos and why it's better to say "face swap»]. Available at: https://vc.ru/ml/94457-kak-delayut-deepfake-video-i-pochemu-luchshe-govorit-face-swap.

5. Blazheyev V. V., Egorova M. A. *Pravovoye regulirovaniye iskusstvennogo intellekta v usloviyakh pandemii i infodemii* [Legal regulation of artificial intelligence in the context of the pandemic and infogenie]. Moscow, 2020, 240 p.

Aleksey Vladimirovich Minbaleev – Doctor of Sciences (Law), Professor, head Department of Information Law and Digital Technologies of Kutafin Moscow State Law University (MSAL), Moscow; Professor of the Department of Theory of State and Law, Constitutional and Administrative Law, South Ural State University, Chelyabinsk, Russian Federation. E-mail: alexmin@bk.ru.

Received 18 October 2020.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Минбалеев, А. В. Проблемы использования искусственного интеллекта в противодействии киберпреступности / А. В. Минбалеев // Вестник ЮУрГУ. Серия «Право». – 2020. – Т. 20, № 4. – С. 116–120. DOI: 10.14529/law200420.

FOR CITATION

Minvaleev, A. V. Problems of using artificial intelligence in countering cybercrime. *Bulletin of the South Ural State University. Ser. Law*, 2020, vol. 20, no. 4, pp. 116–120. (in Russ.) DOI: 10.14529/law200420.