УДК 343.988:004.8

Бегишев И. Р.

ВИКТИМОЛОГИЧЕСКИЕ РИСКИ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Бегишев Ильдар Рустамович
доктор юридических наук, доцент,
заслуженный юрист Республики Татарстан,
главный научный сотрудник Научно-исследовательского института цифровых технологий и права;
профессор кафедры уголовного права и процесса Казанского инновационного университета имени В.Г. Тимирясова, г. Казань, Россия
begishev@mail.ru
https://orcid.org/0000-0001-5619-4025

Аннотация. В статье рассматриваются актуальные виктимологические риски, возникающие в связи с развитием и внедрением технологий искусственного интеллекта. Проведен комплексный анализ потенциальных угроз, которым подвергаются индивиды, общество и государство в результате использования систем искусственного интеллекта как в легальной, так и в противоправной деятельности. Особое внимание уделяется причинному комплексу формирования криминогенных ситуаций, детерминированных применением искусственного интеллекта, и виктимизации, обусловленной неблагоприятными условиями цифровой социализации. Обосновывается необходимость совершенствования правового регулирования в данной сфере, разработки надежных механизмов безопасности и этических стандартов для защиты потенциальных жертв. Предложены направления совершенствования виктимологической профилактики преступлений, связанных с искусственным интеллектом.

Ключевые слова: виктимология, искусственный интеллект, виктимологические риски, цифровая трансформация, виктимизация, криминогенные ситуации, цифровые технологии

VICTIMOLOGICAL RISKS OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Begishev Ildar Rustamovich
Doctor of Law, Associate Professor,
Honored Lawyer of the Republic of Tatarstan, Chief Researcher of the Research Institute of Digital Technologies and Law;
Professor of the Department of Criminal Law and Process, Kazan Innovation University named after V.G. Timiryasov.
begishev@mail.ru
https://orcid.org/0000-0001-5619-4025

Abstract. The article deals with actual victimological risks arising in connection with the development and implementation of artificial intelligence technologies. A comprehensive analysis of potential threats to which individuals, society and the state are exposed as a result of the use of artificial intelligence systems in both legal and illegal activities is carried out. Special attention is paid to the causal complex of formation of criminogenic situations determined by the use of artificial intelligence and victimization caused by unfavorable conditions of digital socialization. The necessity to improve legal regulation in this sphere, to develop reliable security mechanisms and ethical standards for the protection of potential victims is substantiated. The directions of improvement of victimization prevention of crimes related to artificial intelligence are proposed.

Keywords: victimology, artificial intelligence, victimological risks, digital transformation, victimization, criminogenic situations, digital technologies

Введение

Развитие и широкое внедрение технологий искусственного интеллекта формирует новую социально-правовую реальность, которая характеризуется не только возникновением беспрецедентных возможностей для общества, но и появлением качественно новых рисков виктимологического характера. В условиях цифровой трансформации социальных отношений формируется особый причинный комплекс виктимизации, обусловленный как техническими особенностями функционирования систем искусственного интеллекта, так и социальными, психологическими и правовыми аспектами их применения.

П.Н. Кобец справедливо отмечает, что «появление технологий искусственного интеллекта повышает виктимологические риски из-за потенциального вреда для общества, что требует улучшения мер безопасности и надежной законодательной базы для урегулирования юридической ответственности за ущерб, причиненный этими технологиями» [5]. При этом объектами виктимизации могут выступать не только отдельные индивиды, но и социальные группы, общество в целом, а также государственные и коммерческие структуры.

В современных условиях цифровизации анализ виктимологических рисков технологий искусственного интеллекта приобретает особую актуальность в связи с необходимостью создания эффективной системы противодействия новым формам противоправного поведения и обеспечения защиты потенциальных жертв от негативного воздействия данных технологий.

Основная часть

Категория «виктимологический риск» в контексте технологий искусственного интеллекта представляет собой вероятность причинения вреда объектам виктимизации вследствие функционирования систем искусственного интеллекта или их использования в противоправных целях. Д.В. Будко предлагает концепцию риск-ориентированного подхода к развитию технологий искусственного интеллекта, определяя факторы риска, связанные с данными технологиями, и подчеркивая, что «подход, основанный на рисках, эффективно снижает угрозы, связанные с технологиями искусственного интеллекта» [3].

В своем исследовании И.А. Алешковский, А.А. Гребенюк иИ.Н. Сидороввыявляют социальные риски и негативные последствия диффузии технологий искусственного интеллекта, акцентируя внимание на «росте киберпреступности и киберугроз, которые представляют серьезную угрозу для конфиденциальности и безопасности людей, что требует тщательной оценки и управления этими возникающими социальными рисками» [2].

Развитие технологий искусственного интеллекта детерминирует возникновение специфических виктимологических проблем, которые проявляются в различных сферах общественной жизни. П.Н. Кобец характеризует «виктимологические риски технологий искусственного интеллекта как новые уязвимости и угрозы, приводящие к росту виктимизации из-за неблагоприятных условий социализации» [6].

В свою очередь В.Ф. Лапшин указывает на глобальные риски неконтролируемого развития искусственного интеллекта и предлагает установить «уголовную ответственность за создание технологий автономного интеллекта» [7]. По его мнению, «бесконтрольное распространение искусственного интеллекта создает значительные риски для общества» [7], которые могут проявляться в различных формах виктимизации.

В системе здравоохранения А.А. Шутова выявляет «уголовные риски в технологиях искусственного интеллекта, которые могут подорвать доверие и безопасность пациентов» [11]. Автор подчеркивает необходимость правового регулирования для эффективного противодействия данным рискам.

Особую озабоченность вызывают виктимологические аспекты цифровой трансформации общества. А.А. Павлова и А.А. Николаева обращают внимание на «высокие криминологические риски, связанные с информационно-коммуникационными технологиями, включая искусственный интеллект» [9]. Авторы подчеркивают «необходимость разработки надежных механизмов безопасности для защиты пользователей от потенциальной виктимизации в меняющемся цифровом ландшафте» [9].

На основе проведенного исследования нами разработана классификация виктимологических рисков технологий искусственного интеллекта (таблица 1).

Таблица 1. Классификация виктимологических рисков технологий искусственного интеллекта

Категория риска	Характеристика	Примеры проявления	Потенциальные жертвы
Нарушение конфиденциальности и приватности	Риски, связанные с несанкционированным доступом, обработкой и распространением персональных данных	Утечка важных данных, нарушение врачебной тайны, незаконное профилирование пользователей	Физические лица, пациенты медицинских учреждений, пользователи цифровых сервисов
Алгоритмическая дискриминация	Риски предвзятости и дискриминации при принятии решений системами искусственного интеллекта	Отказ в кредитовании, трудоустройстве, медицинском обслуживании на основе алгоритмических решений	Представители социально уязвимых групп, этнических меньшинств, маргинализированные сообщества
Дезинформация и манипуляция общественным сознанием	Риски создания и распространения ложной информации с использованием искусственного интеллекта	Deepfake-видео, фейковые новости, искусственно сгенерированные дезинформационные кампании	Общество в целом, политические деятели, публичные лица
Автоматизированный фишинг и социальная инженерия	Риски использования искусственного интеллектадля массовой персонализированной социальной инженерии	ИИ-генерируемые фишинговые письма, голосовые клоны, таргетированные атаки	Пользователи интернета, держатели банковских карт, клиенты финансовых организаций
Использование искусственного интеллекта-как инструмента совершения преступлений	Риски применениеискусственного интеллектав качестве средства или орудия преступного посягательства	Автоматизированный взлом систем безопасности, DDoS-атаки, использование роботизированных устройств в террористических целях	Физические и юридические лица, объекты критической инфраструктуры, государственные органы
Автономные системы с разрушительным потенциалом	Риски, связанные с функционированием автономных систем вооружения и других систем с потенциалом причинения физического вреда	Боевые дроны, автономные системы вооружения, промышленные роботы с небезопасным режимом функционирования	Гражданское население, военнослужащие, промышленные рабочие

Представленная классификация виктимологических рисков технологий искусственного интеллекта демонстрирует многообразие и комплексный характер современных угроз, обусловленных внедрением и использованием систем искусственного интеллекта. Данная систематизация основана на функциональном признаке и характере негативного воздействия технологий искусственного интеллекта на объекты виктимизации. Следует отметить, что в условиях стремительного развития данных технологий предложенные категории рисков могут расширяться и трансформироваться, требуя постоянного мониторинга и правового регулирования. Особую проблему представляет

юридическая квалификация ущерба, причиненного в результате функционирования систем искусственного интеллекта, и установление правосубъектности в случаях причинения вреда. Полагаю, что эффективное противодействие указанным рискам возможно только при комплексном подходе, сочетающем меры правового, технологического и организационного характера. Предложенная классификация может быть использована как при теоретическом осмыслении виктимологических аспектов технологий искусственного интеллекта, так и при разработке практических мер по минимизации соответствующих рисков и обеспечению защиты потенциальных жертв.

В свою очередь Г.М. Аглямова отмечает возможные ошибки при использовании искусственного интеллекта для предупреждения преступности, «подчеркивая виктимологические риски, такие как ошибочная идентификация и предвзятость, которые могут привести к неправомерным обвинениям или игнорированию реальных жертв» [1]. Данная проблема требует междисциплинарного исследования и разработки комплексных мер по минимизации указанных рисков в парадигме виктимологической профилактики.

Виктимологическая профилактика рисков искусственного интеллекта представляет собой систему мер, направленных на снижение вероятности виктимизации потенциальных жертв в результате функционирования систем искусственного интеллекта или их использования в противоправных целях.

В рамках виктимологической профилактики представляется необходимым разработать комплекс мер, включающих:

1. Совершенствование правового регулирования создания и применения технологий искусственного интеллекта.

2. Разработку технических и технологических мер защиты потенциальных жертв от негативного воздействия технологий искусственного интеллекта.

3. Повышение осведомленности населения о виктимологических рисках технологий искусственного интеллекта.

4. Формирование культуры безопасного использования технологий искусственного интеллекта.

В контексте виктимологической профилактики рисков искусственного интеллекта особого внимания заслуживает анализ потенциала использования данных технологий для предупреждения преступности [4; 8; 10].

Заключение

Проведенное исследование позволяет сделать вывод о том, что виктимологические риски технологий искусственного интеллекта представляют собой сложную и многоаспектную проблему, требующую комплексного подхода к ее решению. Данные риски характеризуются высокой степенью общественной опасности и способностью причинять значительный вред человеку, обществу и государству.

Систематизация виктимологических рисков технологий искусственного интеллекта позволяет выделить несколько ключевых групп, включая риски нарушения приватности, дискриминации, манипуляции общественным со-

знанием, автоматизированного фишинга, создания deepfake-контента и использования искусственного интеллекта в качестве инструмента совершения преступлений.

В научном сообществе ведется активная дискуссия относительно правовой оценки виктимологических рисков технологий искусственного интеллекта, при этом большинство исследователей сходятся во мнении о необходимости разработки эффективных мер правового регулирования и технологической профилактики данных рисков.

Виктимологическая профилактика рисков искусственного интеллекта должна включать меры правового, технологического, организационного и просветительского характера, направленные на снижение вероятности виктимизации потенциальных жертв.

Дальнейшее развитие технологий искусственного интеллекта требует постоянного мониторинга и анализа возникающих виктимологических рисков, а также совершенствования системы их профилактики с учетом изменяющихся социально-правовых и технологических условий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аглямова Г.М. Виктимологические аспекты использования искусственного интеллекта в предупреждении преступности // Юридический мир. 2024. № 1. С. 50-54. DOI: https://doi.org/10.18572/1811-1475-2024-1-50-54

2. Алешковский И.А. Социальные риски и негативные последствия распространения технологий искусственного интеллекта / И.А. Алешковский, А.А. Гребенюк, И.Н. Сидоров // Электронный научно-образовательный журнал "История". 2022. Т. 13, № 4(114). DOI: https://doi.org/10.18254/S207987840019849-2

3. Будко Д.В. Концепция риск-ориентированного подхода в условиях развития технологий искусственного интеллекта // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 3(57). С. 49-58. DOI: https://doi.org/10.37973/VESTNIKKUI-2024-57-6

4. Бхатт Н. Преступления в эпоху искусственного интеллекта: гибридный подход к ответственности и безопасности в цифровую эру // Journal of Digital Technologies and Law. 2025. Т. 3, № 1. С. 65-88. DOI: https://doi.org/10.21202/jdtl.2025.3.

5. Кобец П.Н. Причинный комплекс возникновения криминальных рисков, вызванныхприменением технологий искусственного интеллекта, и превентивные меры по их предупреждению // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 1 (61). С. 80–85. DOI: https://doi.org/10.36511/2078-5356-2024-1-80-85

6. Кобец П.Н. Характеристики виктимологических проблем, вызванных развитием технологий искусственного интеллекта, способствующих росту жертв неблагоприятных условий социализации // Виктимология. 2024. Т. 11, № 1. С. 13-24. DOI: https://doi.org/10.47475/2411-0590-2024-11-1-13-24.

7. Лапшин В.Ф. Технология искусственного интеллекта как потенциальная угроза для охраняемой уголовным законом общественной безопасности // Российский девиантологический журнал. 2022. Т. 2, № 4. С. 374-385. DOI: https://doi.org/10.35750/2713-0622-2022-4-374-385

8. Майоров А.В. Виктимология цифровой преступности: концепция научного направления // Виктимология. 2024. Т. 11, № 1. С. 7-12. DOI: https://doi.org/10.47475/2411-0590-2024-11-1-7-12

9. Павлова А.А. Виктимологические аспекты цифровой трансформации общества / А.А. Павлова, А.А. Николаева // Вестник Северо-Восточного федерального университета имени М. К. Аммосова. 2024. № 1. С. 44-46. DOI: https://doi.org/10.25587/2587-5612-2024-1-44-46

10. Спайропулос Ф. Новые подходы к исследованию ИИ-преступности: конституирование цифровой криминологии // Journal of Digital Technologies andLaw. 2024. Т. 2, № 3. С. 636-656. DOI: https://doi.org/10.21202/jdtl.2024.32

11. Шутова А.А. Криминальные риски применения технологий искусственного интеллекта в здравоохранении // Безопасность бизнеса. 2024. № 1. С. 52-57. DOI: https://doi.org/10.18572/2072-3644-2024-1-52-57

REFERENCES

1. Aglyamova G.M. Victimological aspects of using artificial intelligence in crime prevention // Legal world. 2024. No. 1. P. 50-54. DOI: https://doi.org/10.18572/1811-1475-2024-1-50-54

2. Aleshkovsky I.A. Social risks and negative consequences of the spread of artificial intelligence technologies / I.A. Aleshkovsky, A.A. Grebenyuk, I.N. Sidorov // Electronic scientific and educational journal "History". 2022. Vol. 13, No. 4 (114). DOI: https://doi.org/10.18254/S207987840019849-2

3. Budko D.V. The Concept of a Risk-Oriented Approach in the Context of the Development of Artificial Intelligence Technologies // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2024. Vol. 15, No. 3(57). P. 49-58. DOI: https://doi.org/10.37973/VESTNIKKUI-2024-57-6

4. Bhatt N. Crimes in the Age of Artificial Intelligence: A Hybrid Approach to Liability and Security in the Digital Age // Journal of Digital Technologies and Law. 2025. Vol. 3, No. 1. P. 65-88. DOI: https://doi.org/10.21202/jdtl.2025.3.

5. Kobets P.N. The causal complex of the emergence of criminal risks caused by the use of artificial intelligence technologies, and preventive measures to prevent them // Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2024. No. 1 (61). P. 80–85. DOI: https://doi.org/10.36511/2078-5356-2024-1-80-85

6. Kobets P.N. Characteristics of victimological problems caused by the development of artificial intelligence technologies that contribute to the growth of victims of unfavorable conditions of socialization // Victimology. 2024. Vol. 11, No. 1. P. 13-24. DOI: https://doi.org/10.47475/2411-0590-2024-11-1-13-24.

7. Lapshin V.F. Artificial Intelligence Technology as a Potential Threat to Public Safety Protected by Criminal Law // Russian Deviantological Journal. 2022. Vol. 2, No. 4. Pp. 374-385. DOI: https://doi.org/10.35750/2713-0622-2022-4-374-385

8. Mayorov A.V. Victimology of Digital Crime: the Concept of a Scientific Direction // Victimology. 2024. Vol. 11, No. 1. Pp. 7-12. DOI: https://doi.org/10.47475/2411-0590-2024-11-1-7-12

9. Pavlova A.A. Victimological Aspects of the Digital Transformation of Society / A.A. Pavlova, A.A. Nikolaeva // Bulletin of the North-Eastern Federal University named after M.K. Ammosov. 2024. No. 1. P. 44-46. DOI: https://doi.org/10.25587/2587-5612-2024-1-44-46

10. Spyropoulos F. New approaches to the study of AI crime: constituting digital criminology // Journal of Digital Technologies and Law. 2024. Vol. 2, No. 3. P. 636-656. DOI: https://doi.org/10.21202/jdtl.2024.32

11. Shutova A.A. Criminal risks of using artificial intelligence technologies in healthcare // Business Security. 2024. No. 1. P. 52-57. DOI: https://doi.org/10.18572/2072-3644-2024-1-52-57