

УГОЛОВНО-ПРАВОВЫЕ НАУКИ/CRIMINAL LAW SCIENCES

DOI: https://doi.org/10.60797/IRJ.2026.168.90 EDN: QCLNZW

КИБЕРПРЕСТУПЛЕНИЯ И ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Научная статья

Кобрисев Е.А.[1, *], Новикова Л.В.[2]

[1, 2] Владимирский государственный университет имени А.Г. и Н.Г. Столетовых, Владимир, Российская Федерация

* Корреспондирующий автор (egorkobrisev[at]yandex.ru)

Предложена: 23.11.2025; Принята: 15.06.2026; Опубликована: 17.06.2026

Аннотация

В данной статье рассматривается вопрос использования искусственного интеллекта в рамках киберпреступлений. Вместе с тем искусственный интеллект обладает не только способностью к генерации контента, но и к его оценке с точки зрения подлинности и достоверности. В связи с этим ИИ становится эффективным инструментом противодействия преступным действиям в цифровой среде. Киберпреступность в контексте развития искусственного интеллекта представляет собой одну из наиболее сложных и динамично развивающихся угроз современности. Использование ИИ в преступных целях значительно расширяет масштабы, методы и последствия противоправной деятельности, что требует переосмысления традиционных подходов к уголовно-правовому регулированию и обеспечению информационной безопасности. Современная правоприменительная практика сталкивается с трудностями в квалификации таких деяний и в определении степени ответственности субъектов, участвующих в создании и эксплуатации интеллектуальных систем.

Ключевые слова: цифровая трансформация, киберпространство, киберпреступления, искусственный интеллект, расследование преступлений.

CYBERCRIMES AND THE USE OF ARTIFICIAL INTELLIGENCE

Research article

Kobrisev E.A.[1, *], Novikova L.V.[2]

[1, 2] Vladimir State University named after Alexander and Nikolay Stoletovs, Vladimir, Russian Federation

* Corresponding author (egorkobrisev[at]yandex.ru)

Suggested: 23.11.2025; Accepted: 15.06.2026; Published: 17.06.2026

Abstract

This article discusses the use of artificial intelligence in the context of cybercrimes. However, artificial intelligence is not only capable of generating content, but also of evaluating it in terms of authenticity and reliability. Therefore, AI becomes an effective tool for countering criminal activities in the digital environment. Cybercrime, in the context of the development of artificial intelligence, represents one of the most complex and rapidly evolving threats of our time. The use of AI for criminal purposes significantly expands the scale, methods and consequences of unlawful activity, which calls for a rethinking of traditional approaches to criminal law regulation and the safeguarding of information security. Current law enforcement practice faces difficulties in classifying such acts and in determining the degree of liability of those involved in the creation and operation of intelligent systems.

Keywords: digital transformation, cyberspace, cybercrimes, artificial intelligence, and crime investigation.

Введение

В условиях стремительной цифровизации общественных, экономических и государственных процессов киберпространство становится неотъемлемой средой функционирования современного общества. Расширение использования информационно-коммуникационных технологий, развитие облачных сервисов, интернета вещей и систем больших данных обусловливают не только новые возможности для устойчивого развития, но и формирование принципиально новых угроз. Одной из наиболее значимых проблем современности выступают киберпреступления, эволюция которых тесно связана с внедрением и распространением технологий искусственного интеллекта.

Киберпреступность как социально-правовое и технологическое явление характеризуется высокой степенью динамичности, транснациональностью и адаптивностью к изменениям цифровой среды. Использование алгоритмов машинного обучения, нейронных сетей и автоматизированных систем анализа данных позволяет злоумышленникам существенно повышать эффективность атак, автоматизировать процессы подбора уязвимостей, создавать реалистичные фишинговые сообщения и генерировать поддельный медиаконтент. Особую опасность представляют технологии генеративного ИИ, обеспечивающие создание так называемых «глубоких фейков», а также интеллектуальные боты, способные имитировать поведение человека в сетевом взаимодействии.

Актуальность исследования обусловлена тем, что интеграция искусственного интеллекта в преступления в сфере компьютерной информации трансформирует характер угроз, делая их более масштабными, скрытными и трудно выявляемыми. Современные информационные системы, включая финансовый сектор, критическую инфраструктуру, государственные платформы электронного управления и частный бизнес, оказываются уязвимыми перед атаками,

основанными на самообучающихся алгоритмах. При этом традиционные методы киберзащиты зачастую оказываются недостаточно эффективными в условиях противодействия интеллектуализированным угрозам.

Научная новизна данной темы заключается в комплексном анализе взаимосвязи преступлений в сфере компьютерной информации и технологий искусственного интеллекта с позиций междисциплинарного подхода, объединяющего правовые, технические и социальные аспекты. Особое внимание уделяется двойственной природе ИИ как инструмента как совершения преступлений, так и противодействия им. В рамках исследования предполагается выявление ключевых тенденций трансформации киберугроз под влиянием интеллектуальных технологий, а также формирование направлений совершенствования механизмов правового регулирования и технологической защиты.

Методологическую основу исследования составляют общенаучные и специальные методы познания. В работе использованы методы анализа, синтеза, индукции и дедукции, а также системный подход, позволивший рассмотреть киберпреступность как комплексное социально-техническое явление, связанное с развитием технологий искусственного интеллекта.

Среди специальных методов применены формально-юридический метод для анализа нормативно-правового регулирования, сравнительно-правовой метод для сопоставления отечественного и зарубежного опыта, а также криминологический анализ для изучения структуры и динамики преступлений в сфере компьютерной информации.

Эмпирическую базу исследования составили статистические данные, материалы судебной практики и научные публикации. Для выявления особенностей использования искусственного интеллекта в киберпреступной деятельности применён кейс-метод, основанный на анализе конкретных примеров.

Основные результаты

Быстрое развитие информационных сетей в рамках прикладных наук и компьютерных технологий приводит к росту числа преступлений, связанных с компьютерами [4].

В этой связи нарастает большое опасение в рамках киберпространства.

Киберпреступления в 2025 г. увеличились примерно в четыре раза. Об этом сообщила пресс-служба Совета безопасности Российской Федерации после заседания межведомственной комиссии по информационной безопасности, состоявшегося 16 сентября 2025 года [10].

Однако общий прирост преступлений в сфере компьютерной информации снизился, но дистанционные кражи и компьютерные преступления остаются также на высоком уровне. Это на 27% выше, чем в 2024 году. При этом две трети из них нацелены на критическую информационную инфраструктуру [10].

Однако более весомую опасность представляют преступления в сфере компьютерной информации, связанные с искусственным интеллектом.

Современные технологии искусственного интеллекта позволяют создавать контент столь высокого уровня реалистичности, что его практически невозможно отличить от подлинных материалов, произведённых человеком. Подобные синтетические данные, включая так называемые дипфейки, становятся всё более доступными для массового использования. Однако широкое распространение этих технологий привело к активному внедрению их в арсенал киберпреступников, что существенно усилило риски для информационной безопасности как отдельных граждан, так и коммерческих структур по всему миру.

Одним из проявлений данной тенденции является использование генеративных моделей для создания поддельных изображений и видеозаписей известных личностей с целью манипулирования общественным мнением. Так, осенью прошлого года актёр Том Хэнкс сообщил в социальных сетях о распространении видеоролика с его искусственно сгенерированным образом, рекламирующего стоматологические услуги, к созданию которого он не имел никакого отношения [11].

По мнению экспертов, дальнейшее развитие и доступность генеративных технологий искусственного интеллекта могут стать одним из ключевых факторов, стимулирующих рост киберпреступности в ближайшей перспективе [6].

В результате усложнения и расширения функциональных возможностей систем искусственного интеллекта фишинговые атаки приобретают более высокий уровень изощрённости. Злоумышленники переходят от практики массовой рассылки единого подключения для всех получателей к использованию серии персонализированных обращений, формируемых нейросетевыми моделями на основе комплексного анализа данных о пользователях, включая сведения, полученные из социальных сетей [4].

За год число фишинговых инцидентов в России удвоилось [12]. В 2022 году получили широкое распространение сценарии таргетированного фишинга, в которых использовались имитированные коммуникации от имени известных брендов, предложения о выгодных покупках в интернет-магазинах и лотереи или розыгрыши призов под видом официальных кампаний крупных компаний [12].

Злоумышленники используют методы искусственного интеллекта для снижения заметности своих действий в информационном пространстве. Применение методов машинного обучения обеспечивает преимущество при адаптации атакующих техник к существующим средствам защиты и способствует выявлению новых векторов обхода инфраструктурных контрмер. Киберпреступники овладели приёмами маскировки вредоносного поведения под легитимные компоненты ИТ-систем и интеграции вредоносного кода в официально распространяемое программное обеспечение. В результате подготовка атак упрощается, а вероятность их успешной реализации возрастает.

Одним из первых зафиксированных случаев применения технологий искусственного интеллекта в масштабных кибератаках принято считать распространение вредоносного программного обеспечения CryptoLocker, функционировавшего при поддержке однорангового ботнета Gameover ZeuS. Указанный ботнет использовал зашифрованные каналы связи для взаимодействия с центрами управления и контроля. Предполагается, что в его архитектуре применялись самообучающиеся алгоритмы управления, точный тип и принципы функционирования которых на данный момент достоверно не установлены [5, С. 597].

В результате международной операции Tovar ботнет Gameover ZeuS был изолирован от центров управления, однако доступ к самим управляющим серверам получить не удалось, что исключило возможность детального анализа соответствующего программного обеспечения. Тем не менее совокупность косвенных признаков — таких как высокая устойчивость системы к контрвзлому, способность избегать прямых атак, адаптивность поведения и высокая скорость принятия решений — указывает на вероятное использование элементов нейросетевых технологий в механизмах управления данным вредоносным комплексом.

Правительства и правоохранительные органы по всему миру ведут активную борьбу с фишинговыми кампаниями, проводят обучающие кампании и предупреждают пользователей о возможных угрозах. Это помогает снизить риск попадания в ловушку фишинговых атак и защитить пользователей от потери их личных данных [8].

Вместе с тем искусственный интеллект является и «индикатором» расследования преступлений в рамках компьютерных систем.

Искусственный интеллект (ИИ) обладает не только способностью к генерации контента, но и к его оценке с точки зрения подлинности и достоверности. В связи с этим ИИ становится эффективным инструментом противодействия преступным действиям в цифровой среде. Одним из ключевых факторов успешного отражения кибератаки является время реакции. Применение ИИ позволяет автоматизировать часть аналитических задач и ускорить процесс сбора информации об инциденте [3].

Так, языковые модели на основе ИИ способны обрабатывать события информационной безопасности (ИБ) и устанавливать между ними причинно-следственные связи. Это обеспечивает переход от простого уведомления о происшествии к формированию структурированного описания инцидента, включая рекомендации по реагированию и выявлению возможных векторов распространения угрозы. Роль специалиста при этом сводится к анализу полученных данных и принятию решений на их основе [3].

В числе инструментов противодействия киберпреступности, особое место занимает технология "Threat Hunting" — проактивный поиск угроз, при котором ИИ используется для выбора релевантных индикаторов компрометации из множества источников и поддержки процесса выдвижения аналитических гипотез. Кроме того, значимую роль играет "UEBA (User and Entity Behavior Analytics)" — технология выявления аномалий, основанная на ИИ-анализе поведения пользователей, устройств и приложений [2]. Подобные решения позволяют фиксировать отклонения от нормальной активности и оперативно информировать специалистов об обнаруженных подозрительных действиях.

Противодействие преступлениям, совершаемым с использованием высоких технологий, невозможно без надлежащего правового регулирования. Действующее уголовное законодательство лишь частично охватывает вопросы, связанные с созданием и применением вредоносных систем искусственного интеллекта. Учитывая тесную взаимосвязь данного явления с областью компьютерной информации, особое внимание следует уделить положениям главы 28 Уголовного кодекса Российской Федерации, включающей четыре статьи. Они предусматривают уголовную ответственность за неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; а также за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации [1].

Согласно статье 273 УК РФ, запрещается создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств её защиты [1].

В Уголовном кодексе Российской Федерации отягчающие обстоятельства закреплены в статье 63 и образуют исчерпывающий перечень, не подлежащий расширительному толкованию, что подтверждается разъяснениями Постановления Пленума Верховного Суда РФ № 58 от 22 декабря 2015 г. Вместе с тем действующее уголовное законодательство в полной мере не отражает качественно новые угрозы, обусловленные использованием технологий искусственного интеллекта.

Современные цифровые инструменты существенно трансформируют характер преступной деятельности, обеспечивая увеличение как масштабов, так и тяжести наступающих последствий. В частности, речь идет о мошенничестве, совершаемом с применением технологий синтеза изображения и голоса (deepfake), позволяющих имитировать личность потерпевшего либо третьих лиц [2].

В этом контексте представляется значимым внесение в сентябре 2024 г. в Государственную Думу Российской Федерации законопроекта № 718538-8, предусматривающего установление квалифицирующего признака использования технологий дипфейка при совершении мошенничества. Указанная инициатива получила положительное заключение Верховного Суда Российской Федерации.

Дополнительно, Александр Бастрыкин обосновал целесообразность включения использования искусственного интеллекта в перечень отягчающих обстоятельств, по аналогии с применением оружия либо совершением преступления в особых условиях. Аналогичная позиция была поддержана Михаилом Мишустиным, указавшим на необходимость учета применения технологий искусственного интеллекта при назначении наказания.

Практика общественной опасности деяний, совершаемых с использованием высоких технологий

Зарубежная правоприменительная и законодательная практика свидетельствует о формировании устойчивого понимания необходимости специального регулирования ответственности за преступления, совершаемые с использованием технологий искусственного интеллекта. Так, во Франции с 2023 г. на уровне уголовного законодательства усилена ответственность за деяния, связанные с применением ИИ-технологий, включая создание и распространение deepfake-контента (ст. 226-8-1 Уголовного кодекса Франции).

В Соединённых Штатах Америки при отсутствии прямого нормативного закрепления соответствующих положений Министерство юстиции США выработало рекомендации для прокуроров, предусматривающие необходимость добиваться ужесточения наказаний за преступления, совершённые с применением технологий

искусственного интеллекта, исходя из их повышенной общественной опасности (DOJ guidelines, 2024). Показательным является дело United States v. Vasquez (2024), рассмотренное окружным судом Южного округа Калифорнии, в рамках которого использование deepfake-технологий было признано обстоятельством, отягчающим наказание, что повлекло его существенное усиление.

В Китае с января 2023 г. действует нормативный акт "Deep Synthesis Management Regulations", устанавливающий строгие требования к использованию технологий глубокого синтеза, а также предусматривающий ответственность, включая уголовную, за их противоправное применение.

С точки зрения современного правового и технологического анализа, искусственный интеллект может быть отнесён к категории сложных, но всё же компьютерных программ, обладающих особым уровнем автономности и функциональной сложности.

А.И. Коробеев, Р.И. Дремлюга и Я.О. Кучина справедливо отмечают, что чрезмерное сдерживание технологического развития, его излишняя бюрократизация и искусственное торможение приводят к росту киберпреступности [7, С. 417-419]. В подобных условиях деятельность, которая могла бы осуществляться в правовом поле и находиться под государственным контролем, перемещается в теневой сектор. Это отвлекает внимание правоохранительных органов от действительно значимых угроз и затрудняет определение того, идет ли речь о трансформации уже существующих преступных практик с использованием новых технологий либо общество сталкивается с принципиально новой угрозой, требующей формирования особых направлений в уголовной политике, праве, криминологии и сфере безопасности.

Заключение

Киберпреступность в контексте развития искусственного интеллекта представляет собой одну из наиболее сложных и динамично развивающихся угроз современности. Использование ИИ в преступных целях значительно расширяет масштабы, методы и последствия противоправной деятельности, что требует переосмысления традиционных подходов к уголовно-правовому регулированию и обеспечению информационной безопасности. Современная правоприменительная практика сталкивается с трудностями в квалификации таких деяний и в определении степени ответственности субъектов, участвующих в создании и эксплуатации интеллектуальных систем [9].

Для эффективного противодействия данной категории преступлений необходим комплексный подход, включающий совершенствование уголовного законодательства, развитие международного сотрудничества, повышение цифровой грамотности и формирование этических стандартов разработки и применения искусственного интеллекта. Только при условии сбалансированного взаимодействия технологий, права и безопасности возможно минимизировать риски, связанные с киберпреступностью в эпоху интеллектуальных систем.

Конфликт интересов

Не указан.

Рецензия

Волков Ю.В., Уральский государственный юридический университет им. В.Ф. Яковлева, Екатеринбург Российская Федерация
DOI: https://doi.org/10.60797/IRJ.2026.168.90.1

Conflict of Interest

None declared.

Review

Volkov Y.V., Ural State Law University nm. V.F. Yakovlev, Ekaterinburg Russian Federation
DOI: https://doi.org/10.60797/IRJ.2026.168.90.1

Список литературы / References

1. Уголовный кодекс Российской Федерации : федеральный закон от 13.06.1996 № 63-ФЗ // Собрание законодательства Российской Федерации. — 1996. — № 25. — Ст. 2954.

2. Abbott R. Punishing artificial intelligence: legal fiction or science fiction / R. Abbott, A. Sarch // University of California, Davis, Law Review. — 2019. — Vol. 53. — P. 323–384.

3. Ализаде В.А. Судебная практика по делам о преступлениях преступных сообществ (преступных организаций) в сфере незаконного оборота наркотиков, совершенных с использованием информационно-телекоммуникационной сети Интернет и криптовалюты / В.А. Ализаде, А.Г. Волеводз // Библиотека криминалиста. — 2017. — № 6 (35). — С. 281–299.

4. Волынский А.Ф. Компьютерная криминалистика в системе уголовно-правовой защиты традиционной и цифровой экономики / А.Ф. Волынский. — Москва, 2020. — С. 84.

5. Исаков А.А. Искусственный интеллект и расследование киберпреступлений / А.А. Исаков // Вестник науки. — 2023. — Т. 3. — № 5 (62). — С. 597–603. — URL: https://www.вестник-науки.рф/article/8275 (дата обращения: 31.10.2025).

6. Клишков В.Б. Киберпреступность: понятие, признаки, основные направления противодействия / В.Б. Клишков, Е.В. Стебенева, М.А. Яковлева // Вестник Нижегородского университета им. Н.И. Лобачевского. — 2022. — № 4. — С. 106–114. — DOI: 10.52452/19931778_2022_4_106. — EDN WWFAEM.

7. Коробеев А.И. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации / А.И. Коробеев, Р.И. Дремлюга, Я.О. Кучина // Всероссийский криминологический журнал. — 2019. — Т. 13. — № 3. — С. 416–425.

8. Мирончик А.С. Хищения в электронной среде как разновидность информационных преступлений: проблемы разграничения и квалификации / А.С. Мирончик, А.В. Суслопаров // Юридические исследования. — 2019. — № 9. — С. 17–30. — DOI: 10.25136/2409-7136.2019.9.30745. — EDN ONIEJG.

9. Тирранен В.А. Искусственный интеллект и нейронные сети как инструмент современной киберпреступности / В.А. Тирранен // Уголовное право: стратегия развития в XXI веке : материалы XVI Международной научно-практической конференции (24-25 января 2019 г.). — Москва: РГ-Пресс, 2019. — С. 135–140.

10. Число кибератак на информационную инфраструктуру России выросло в четыре раза // Коммерсантъ. — 2025. — URL: https://www.kommersant.ru/doc/8101273?ysclid=mosz5b4jss200186584 (дата обращения: 31.10.2025).

11. Москвичев А. Том Хэнкс пожаловался на использование в рекламе своего образа, созданного ИИ / А. Москвичев // Сноб. — 2023. — URL: https://snob.ru/news/tom-henks-pozhalovalsya-na-ispolzovanie-v-reklame-svoego-obraza-sozdannogo-ii/?ysclid=mmavclhd7x24376844 (дата обращения: 31.10.2025).

12. Тренды фишинговых атак на организации в 2022–2023 годах // Positive Technologies. — 2024. — URL: https://ptsecurity.com/research/analytics/phishing-attacks-on-organizations-in-2022-2023/?ysclid=mosz7qnf3g8096155 (дата обращения: 31.10.2025).

Список литературы на английском языке / References in English

1. Ugolovnyj kodeks Rossijskoj Federacii [Criminal Code of the Russian Federation] : federal law No. 63-FZ of 13.06.1996 // Sobranie zakonodatel'stva Rossijskoj Federacii [Collection of Legislation of the Russian Federation]. — 1996. — № 25. — Art. 2954. [in Russian]

2. Abbott R. Punishing artificial intelligence: legal fiction or science fiction / R. Abbott, A. Sarch // University of California, Davis, Law Review. — 2019. — Vol. 53. — P. 323–384.

3. Alizade V.A. Sudebnaja praktika po delam o prestuplenijah prestupnyh soobshhestv (prestupnyh organizacij) v sfere nezakonnogo oborota narkotikov, sovershennyh s ispol'zovaniem informacionno-telekommunikacionnoj seti Internet i kriptovaljuty [Judicial practice in cases of crimes of criminal communities (criminal organizations) in the sphere of illicit drug trafficking committed using the information and telecommunications network Internet and cryptocurrency] / V.A. Alizade, A.G. Volevodz // Biblioteka kriminalista [Criminalist's Library]. — 2017. — № 6 (35). — P. 281–299. [in Russian]

4. Volynskij A.F. Komp'juternaja kriminalistika v sisteme ugolovno-pravovoj zashhity tradicionnoj i cifrovoj jekonomiki [Computer forensics in the system of criminal law protection of traditional and digital economy] / A.F. Volynskij. — Moscow, 2020. — P. 84. [in Russian]

5. Isakov A.A. Iskusstvennyj intellekt i rassledovanie kiberprestuplenij [Artificial intelligence and cybercrime investigation] / A.A. Isakov // Vestnik nauki [Bulletin of Science]. — 2023. — Vol. 3. — № 5 (62). — P. 597–603. — URL: https://www.вестник-науки.рф/article/8275 (accessed: 31.10.2025). [in Russian]

6. Klishkov V.B. Kiberprestupnost': ponjatie, priznaki, osnovnye napravlenija protivodejstvija [Cybercrime: concept, signs, main directions of counteraction] / V.B. Klishkov, E.V. Stebeneva, M.A. Jakovleva // Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo [Bulletin of Nizhny Novgorod University named after N.I. Lobachevsky]. — 2022. — № 4. — P. 106–114. — DOI: 10.52452/19931778_2022_4_106. — EDN WWFAEM. [in Russian]

7. Korobeev A.I. Kiberprestupnost' v Rossijskoj Federacii: kriminologicheskij i ugolovno-pravovoj analiz situacii [Cybercrime in the Russian Federation: criminological and criminal law analysis of the situation] / A.I. Korobeev, R.I. Dremljuga, Ja.O. Kuchina // Vserossijskij kriminologicheskij zhurnal [All-Russian Criminological Journal]. — 2019. — Vol. 13. — № 3. — P. 416–425. [in Russian]

8. Mironchik A.S. Hishhenija v jelektronnoj srede kak raznovidnost' informacionnyh prestuplenij: problemy razgranichenija i kvalifikacii [Theft in the electronic environment as a type of information crime: problems of differentiation and qualification] / A.S. Mironchik, A.V. Susloparov // Juridicheskie issledovanija [Legal Research]. — 2019. — № 9. — P. 17–30. — DOI: 10.25136/2409-7136.2019.9.30745. — EDN ONIEJG. [in Russian]

9. Tirranen V.A. Iskusstvennyj intellekt i nejronnye seti kak instrument sovremennoj kiberprestupnosti [Artificial intelligence and neural networks as a tool of modern cybercrime] / V.A. Tirranen // Ugolovnoe pravo: strategija razvitija v XXI veke : materialy XVI Mezhdunarodnoj nauchno-prakticheskoj konferencii (24-25 janvarja 2019 g.) [Criminal law: development strategy in the XXI century : materials of the XVI International Scientific and Practical Conference (January 24-25, 2019)]. — Moscow: RG-Press, 2019. — P. 135–140. [in Russian]

10. Chislo kiberatak na informacionnuju infrastrukturu Rossii vyroslo v chetyre raza [The number of cyber attacks on Russia's information infrastructure has grown fourfold] // Kommersant". — 2025. — URL: https://www.kommersant.ru/doc/8101273?ysclid=mosz5b4jss200186584 (accessed: 31.10.2025). [in Russian]

11. Moskvichev A. Tom Hjenks pozhALOVALsja na ispol'zovanie v reklame svoego obraza, sozdannogo II [Tom Hanks complained about the use of his AI-generated image in advertising] / A. Moskvichev // Snob. — 2023. — URL: https://snob.ru/news/tom-henks-pozhalovalsya-na-ispolzovanie-v-reklame-svoego-obraza-sozdannogo-ii/?ysclid=mmavclhd7x24376844 (accessed: 31.10.2025). [in Russian]

12. Trendy fishingovyh atak na organizacii v 2022–2023 godah [Trends of phishing attacks on organizations in 2022–2023] // Positive Technologies. — 2024. — URL: https://ptsecurity.com/research/analytics/phishing-attacks-on-organizations-in-2022-2023/?ysclid=mosz7qnf3g8096155 (accessed: 31.10.2025). [in Russian]