

Научная статья

УДК 343.9

EDN HYQOLW

DOI 10.17150/2500-4255.2025.19(1).96-106



## ВОЗМОЖНОСТИ КРИМИНАЛИСТИЧЕСКОГО РЕЧЕВЕДЕНИЯ В ПРОТИВОДЕЙСТВИИ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

**Е.И. Галяшина, К.М. Богатырев***Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), г. Москва,  
Российская Федерация*

### Информация о статье

Дата поступления

4 октября 2024 г.

Дата принятия в печать

23 февраля 2025 г.

Дата онлайн-размещения

21 марта 2025 г.

### Ключевые слова

Информация; информационная  
безопасность; знаковые следы;  
преступление; криминалистическая  
техника; криминалистическое  
речеведение; криминалистические  
средства; искусственный интеллект;  
нейросеть; генеративный ИИ

**Аннотация.** В статье с криминалистических позиций изучены риски, связанные с возникновением и распространением новой информационной технологии — генеративного искусственного интеллекта, использующегося для быстрого и эффективного создания различных информационных продуктов. Данная технология (особенно в свете потенциала ее развития и множественности возможного применения) оценивается неоднозначно в связи с высокой степенью общественной опасности ее использования в преступной деятельности и военных целях. Рассмотрены имеющиеся в литературе подходы к разновидностям использования генеративного искусственного интеллекта для совершения преступлений, приведена авторская позиция по возможной уголовно-правовой квалификации таких деяний, освещены основные направления возможного совершенствования законодательства. В результате исследования авторы пришли к выводу о том, что риски причинения вреда охраняемым законом общественным отношениям в результате использования генеративного искусственного интеллекта имеют место преимущественно в рамках компьютерно-опосредованной коммуникации. Представляется, что чаще всего данная технология используется для осуществления преступлений, совершаемых посредством обмана и манипулирования информацией, — мошенничеств, распространения недостоверной информации, вовлечения в экстремистскую (в том числе террористическую) деятельность и т.д. Этому способствуют широкие возможности генеративного искусственного интеллекта по созданию различных информационных продуктов: текстов, аудио- и видеозаписей, изображений, программ и т.д. Вместе с тем работа генеративного искусственного интеллекта подразумевает специфический механизм следообразования и выражается в криминалистически (в первую очередь — диагностически) значимых признаках. Установление этих признаков возможно за счет применения криминалистических знаний и использования криминалистических средств. Представляется, что наиболее релевантными источниками данных ресурсов научно-технического обеспечения правоохранительной деятельности в настоящее время является новая частная криминалистическая теория — криминалистическое речеведение.

Original article

## THE POTENTIAL OF FORENSIC SPEECH SCIENCE TO COUNTERACT CRIMES COMMITTED USING GENERATIVE ARTIFICIAL INTELLIGENCE

**Elena I. Galyashina, Konstantin M. Bogatyrev***Kutafin Moscow State Law University (MSAL), Moscow, the Russian Federation*

### Article info

Received

2024 October 4

Accepted

2025 February 23

Available online

2025 March 21

**Abstract.** The authors research the criminalistic aspects of risks associated with the emergence and spread of a new information technology, namely, generative artificial intelligence used to create various information products quickly and effectively. The assessments of this technology are controversial (especially in view of its potential diverse applications) due to a high public danger of its application in criminal activities or for military purposes. The authors examine the approaches of different researchers to using generative artificial intelligence to commit crimes, present their own position regarding the possible criminal law qualification of such actions, and

**Keywords**

Information; information security; iconic traces; crime; forensic technology; forensic speech science; forensic tools; artificial intelligence; neural network; generative AI

describe possible directions of improving the legislation. The conducted research allowed the authors to conclude that the risks of damaging public relations protected by the law via the use of generative artificial intelligence are mainly associated with computer-mediated communication. It seems that this technology is most often used to commit crimes through deception and information manipulation, such as fraud, spread of disinformation, involvement into extremist (including terrorist) activities, etc. It is facilitated by the wide possibilities of using artificial intelligence to create various information products: text, audio- and video-recordings, images, software, etc. At the same time, the work of generative artificial intelligence involves a specific mechanism of trace formation and is manifested in the forensically (primarily — diagnostically) relevant features. It is possible to establish these features through the use of criminalistic knowledge and means. It seems that the most relevant current source of the resources providing research support for the law enforcement work is a new special criminalistic theory — criminalistic speech science.

**Введение в проблематику**

XXI в. обещал стать временем прорывных технологий, кардинально повышающих уровень и улучшающих качество жизни всего человечества. Такого рода ожидания оправдываются лишь отчасти: научно-технический прогресс действительно обеспечивает стремительное развитие технической компоненты нашей жизни, однако пока новые технологии являются обоюдоострым мечом, к тому же доступным далеко не всем. Системы национальной, региональной и глобальной безопасности находятся в критической зависимости от новых военных, транспортных, медицинских, промышленных и сельскохозяйственных технологий, но едва ли не ключевую роль играют технологии информационные. «Кто владеет информацией, тот владеет миром». Этот афоризм из XIX в. в высшей степени актуален и для дня сегодняшнего, когда в результате повсеместного внедрения средств массовой коммуникации в масштабах планеты сформировалась принципиально иная среда обитания человека — так называемая новая информационная реальность [1, с. 6].

Вместе с тем эта реальность, сформировавшаяся на функционирующих в сети Интернет информационных ресурсах, не является раз и навсегда данной. Она находится в процессе постоянной трансформации (или в категориях диалектической логики — в становлении): от первоначальной текстовой формы — к поликодовой, т.е. сочетающей разные системы передачи информации, и далее — к мультимодальной. Основным же драйвером развития в текущем десятилетии (2020-е гг.) уже общепризнанно стали большие языковые модели и иные системы генеративного искусственного интеллекта (ИИ). Последний понимается как комплекс технологических решений, позволяющий имитиро-

вать когнитивные функции человека, включая самообучение и поиск решений без заранее заданного алгоритма, и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека<sup>1</sup>, создаваемые по модели искусственных нейронных сетей.

Данная сфера показывает взрывной рост: за прошедшее с 2014 г. десятилетие во Всемирную организацию интеллектуальной собственности (ВОИС) было подано 54 тыс. патентных заявок на генеративный искусственный интеллект, четверть которых — за последние полтора года (после того, как компанией OpenAI в конце 2022 г. была представлена ChatGPT, ставшая «первой ласточкой» новой эпохи)<sup>2</sup>. Данные технологии могут быть приложены к любой сфере, поэтому все, у кого есть такая возможность, занялись их внедрением (в немалой степени из-за боязни проиграть в конкурентной борьбе). К примеру, недавно в Японии разработали ИИ-цифрового посредника, который перерабатывает речь разгневанных клиентов колл-центров, подавляя эмоции и тем самым делая их речь менее агрессивной<sup>3</sup>.

Перспективы и риски данной технологии пока не ясны в полной мере. По возможностям и

<sup>1</sup> О развитии искусственного интеллекта в Российской Федерации : указ Президента РФ от 10 окт. 2019 г. № 490 // Собрание законодательства РФ. 2019. № 41. Ст. 5700.

<sup>2</sup> Китай запатентовал в 6 раз больше изобретений с ИИ, чем США // ХАЙТЕК+. URL: <https://hightech.plus/2024/07/04/kitai-zapatenoval-v-6-raz-bolshe-izobretenii-s-ii-chem-ssha> (дата обращения: 04.07.2024).

<sup>3</sup> In Japan, SoftBank's 'emotion-cancelling' AI filter aims to protect workers from angry customers // South China Morning Post. URL: <https://www.scmp.com/week-asia/people/article/3266515/japan-softbanks-emotion-cancelling-ai-filter-aims-protect-workers-angry-customers> (дата обращения: 14.06.2024).

эффективности применения в совокупности с количеством создаваемых угроз данную технологию можно метафорически сравнить с джинном, выпущенным из бутылки: самообучающийся ИИ может выполнить любое наше желание, но результат может быть совсем не тем, что мы хотим получить; кроме того, никто не знает, что этот «джинн» наделает, когда станет «свободным». На вызывающие беспокойство обстоятельства обращают внимание отраслевые специалисты. Так, генеральный директор ООО «Лаборатория Наносемантика» С.И. Ашманов применительно к ChatGPT описал, как обученная только лишь продолжать или дополнять текст нейросеть внезапно показала свойства, которые не только не закладывались, но даже и не ожидались от нее (например, навыки переформулирования текста, решения математических задач и т.д.).<sup>4</sup> Приводя в пример «слишком быстрое развитие» GPT, некоторые исследователи предлагают принять серьезные меры по управлению развитием ИИ: приостановить (ввести мораторий) или же отказаться от развития подобных технологий вовсе, мотивируя подобные предложения угрозой выхода таких систем из-под контроля людей с возможным последующим уничтожением человечества<sup>5</sup>. Хотя подобные предположения кому-то могут показаться технофобской, неолуддитской паникой, факты участия ChatGPT (как первого и наиболее показательного примера такой технологии) в хакерских атаках<sup>6</sup> или даже в выборах — в качестве кандидата<sup>7</sup>, позволяют получить представления о негативной стороне технологии.

<sup>4</sup> Разработчики нейросетей об отрасли // PRO Hi-Tech. YouTube. URL: <https://www.youtube.com/watch?v=XYbqey-bdII> (дата обращения: 14.06.2024).

<sup>5</sup> «Все умрут, включая детей». Как искусственный интеллект изменит интернет и почему этого боится даже Илон Маск // LENTA.RU. URL: <https://lenta.ru/articles/2023/04/06/evilgpt> (дата обращения: 14.06.2024); Бывшие сотрудники OpenAI считают, что ее деятельность угрожает человечеству // ХАЙТЕК+. URL: <https://hightech.plus/2024/06/05/bivshie-sotrudniki-openai-schitayut-cto-ee-deyatelnost-ugrozhaet-chelovechestvu> (дата обращения: 02.07.2024).

<sup>6</sup> Автономные боты GPT-4 научились взламывать сайты через неизвестные уязвимости // ХАЙТЕК+. URL: <https://hightech.plus/2024/06/10/avtonomnie-boti-gpt-4-nauchilis-vzlamivat-saiti-cherез-neizvestnie-uyazvimosti> (дата обращения: 12.06.2024).

<sup>7</sup> OpenAI отключила ИИ, который боролся за пост мэра одного из городов Вайоминга // ХАЙТЕК+. URL: <https://hightech.plus/2024/06/28/openai-otklyuchila-ii-kotorii-borolsya-za-post-mera-odnogo-iz-gorodov-vaiominga> (дата обращения: 02.07.2024).

Нейросети, обученные для создания текстов, программ, изображений, видео и иного контента, могут не блистать качеством результата, однако их сильная сторона заключается в его большом объеме и низкой цене (на этом фоне имеет место волнение представителей творческих профессий, особенно в свете заявлений разработчиков ИИ о том, что они изначально не были нужны<sup>8</sup>). Такой «творческий потенциал» уже запустил, а затем серьезнейшим образом повлиял на процесс трансформации интернета. Прежде всего, в плане содержания — произошла его фейковизация [2, с. 100]: площадки наводнил информационный шум (мусор) — низкокачественный, недостоверный контент, количество которого растет в геометрической прогрессии (что особенно критично для поисковых сервисов, торговых площадок и средств массовой коммуникации, таких как почтовые сервисы, соцсети, мессенджеры и т.д.)<sup>9</sup>. Рассуждая в понятиях Томаса Гоббса, современный интернет стал полем информационной войны всех против всех [3] (людей и ИИ друг с другом и между собой), ключевым оружием в которой стал навык проверки достоверности информации (фактчекинга).

О том, что генеративный ИИ является продуктом двойного назначения, пригодным для использования в военных целях, свидетельствует пересмотренная стратегия НАТО в области искусственного интеллекта, в которой отмечается, что для НАТО жизненно важно (везде, где это применимо, и как можно скорее) использовать генеративный ИИ, способный практически в неограниченном объеме создавать сложный текст, компьютерный код, реалистичные изображения и аудио и иной контент, все больше неотличимый от созданного человеком<sup>10</sup>. Вместе с тем подчеркиваются и проблемы для безопасности, такие как дезинформация и информационные операции с использованием ИИ,

<sup>8</sup> Мира Мурати из OpenAI: «ИИ уничтожит творческие специальности, которых не должно быть» // ХАЙТЕК+. URL: <https://hightech.plus/2024/06/27/miramurati-iz-openai-ii-unichtozhit-te-tvorcheskiespecialnosti-kotorih-ne-dolzno-bit> (дата обращения: 02.07.2024).

<sup>9</sup> На наших глазах ИИ убивает старый интернет. Но новый обещает быть хуже // Хабр. URL: <https://habr.com/ru/companies/itglobalcom/articles/747488> (дата обращения: 02.07.2024).

<sup>10</sup> Summary of NATO's revised Artificial Intelligence (AI) strategy // North Atlantic Treaty Organization. URL: [https://www.nato.int/cps/en/natohq/official\\_texts\\_227237.htm](https://www.nato.int/cps/en/natohq/official_texts_227237.htm) (дата обращения: 10.07.2024).

которые могут повлиять на результаты выборов, посеять разногласия и смятение в Альянсе, демобилизовать и деморализовать общества и военные силы во время конфликтов, а также снизить доверие к институтам и властям, имеющим важное значение для НАТО.

Сами технологии ИИ достоверность оценить не способны. Точнее, эта способность напрямую зависит от тех данных, на которых она была обучена, и сформировавшейся на их основе «картины мира» ИИ; к примеру, на некоторую тематику может быть в целом наложен запрет. При этом они уже вплотную приблизились к черте, когда их возможности позволяют им сформировать «второй», фейковый интернет, полностью состоящий из создаваемых ими недостоверных информационных продуктов и способный занять место «оригинального» интернета. В этой связи не следует удивляться возникновению таких культурных феноменов, как «теория мертвого интернета», согласно которой он уже давно является безлюдным пространством, наполненным ботами, создаваемым и размещаемым ими контентом<sup>11</sup>.

Какие-то из рассмотренных выше проблем являются реальными, какие-то — гипотетическими ситуациями, представляющими широкий простор для дискуссий, размышлений и мысленных экспериментов. Вместе с тем следует также помнить о том, что в калейдоскопе связанных с нейросетями угроз и рисков по-прежнему имеет место и человеческий фактор: с момента своего создания генеративные ИИ стали активно использоваться представителями криминального мира — мошенниками, хакерами, плагиаторами, экстремистами и иными нарушителями закона.

#### Методология исследования

Работа носит комплексный характер, осуществляется в рамках юридико-лингвистического подхода. Исходя из подхода методологического плюрализма, в качестве основы исследования принята философская методология позитивизма и постпозитивизма как наиболее проработанная и актуальная, с использованием по мере необходимости общепринятого в криминологической науке диалектического метода.

<sup>11</sup> «Эта штука пугает». Что такое теория мертвого интернета и почему ее сторонники верят, что в сети не осталось живых людей // LENTA.RU. URL: [https://lenta.ru/articles/2022/11/23/dead\\_internet\\_theory](https://lenta.ru/articles/2022/11/23/dead_internet_theory) (дата обращения: 14.06.2024).

Помимо указанных, используются логические приемы (анализ, синтез, индукция, дедукция и др.); общенаучные (описание, сравнение, абстрагирование, систематизация, формализация и др.), а также частнонаучные методы (лингвистический, семантический анализ и др.).

#### Преступления, совершаемые с использованием генеративного ИИ

Научный коллектив из Университетского колледжа Лондона в своей работе [4] привел актуальное на 2020 г. видение существующих и возможных в будущем нарушений, связанных с преступным использованием ИИ. Нарушения делятся на группы по степени опасности с учетом объема причиняемого вреда, преступной прибыли, возможности использования технологии и сложности противодействия ей:

##### 1. Высокая степень опасности:

- аудио- и видеоимитации (подделки);
- создание недостоверных (фейковых) новостей;
- крупномасштабный шантаж с использованием собранной или созданной ИИ информации;
- нарушения работы ИИ, являющегося частью критической информационной инфраструктуры;
- фишинговые атаки с использованием искусственного интеллекта;
- использование беспилотных автомобилей под управлением ИИ в качестве оружия.

##### 2. Средняя степень опасности:

- использование ИИ для взлома учетных записей и кибератак на информационные ресурсы;
- использование в противоправных целях ударных дронов и иной военной техники, функционирующей на основе ИИ;
- «онлайн-выселение», т.е. блокировка доступа к важным информационным ресурсам и сервисам;
- обход системы распознавания лиц;
- манипулирование финансовыми рынками с помощью ИИ;
- манипулирование данными машинного обучения, приводящее к искажению работы ИИ;
- мошенничество при торговле программами, маскируемыми под решения на основе ИИ (в данном случае последние выступают не в качестве средств совершения преступления или объекта посягательства, а в качестве контекста коммуникативной ситуации, способствующей обману).



### 3. Низкая степень опасности:

– использование существующих предвзятостей ИИ (на что обращают внимание и отечественные ученые [5]);

– создание поддельных отзывов;

– преследование людей с помощью ИИ;

– подделка предметов искусства, музыкальных и иных произведений.

Отметим, что элементы приведенного выше перечня возможных угроз являются взаимопересекающимися, а кроме того — подготовленными в рамках междисциплинарного подхода (что имеет место и в литературе [6]), не в полной мере соотношенного с возможной юридической квалификацией. Сказывается и то, что данная публикация [6] была подготовлена еще до нейросетевого бума, в связи с чем в ней содержится общий анализ возможного противоправного использования ИИ без особого внимания именно генеративным нейросетям (как мы понимаем, из приведенных выше угроз с ними связаны те, которые реализуются посредством создания или обработки информационных продуктов, в особенности — распространение недостоверной информации под видом достоверных сведений). И пока одни исследователи уделяют больше внимания проблематике этичности и допустимости использования ИИ в различных сферах общественной жизни (например, в сфере безопасности, для осуществления пограничного контроля [7; 8] и т.д.), мы сосредоточимся на анализе противоправных действий, совершаемых с использованием нейросетей (преимущественно в рамках компьютерно-опосредованной коммуникации).

Как любой инструмент, генеративные технологии ИИ могут быть использованы для достижения как благих, так и предосудительных целей. Хотя разработчики и предпринимают меры по ограничению возможностей их применения в противоправных целях (к примеру, для поиска и анализа информации, оборот которой ограничен законом), способность ИИ к самообучению и постоянный «творческий поиск» злоумышленников приводят к возникновению и обнаружению новых способов взлома, обхода подобных программных ограничений — так называемых джейлбрейков (англ. *jailbreak* — побег из тюрьмы).

Кроме того, некоторые генеративные технологии ИИ изначально создаются для криминальной деятельности, яркий пример — не имевший этических границ или ограничений

WormGPT, обученный на массиве данных, связанных с вредоносным программным обеспечением<sup>12</sup>. В научных обзорах, посвященных проблематике противоправного применения генеративного ИИ, отмечается, что после того, как технология WormGPT была закрыта для использования, преступники сосредоточились не на разработке собственных новых нейросетей (так как это долго, дорого и рискованно), а на использовании для совершения преступлений возможностей уже существующих и широко доступных генеративных технологий ИИ (таких, как ChatGPT).

Выделяют следующие способы их использования преступниками:

– создание писем для фишинговых рассылок;

– создание глубоких подделок (дипфейков);

– обход систем идентификации человека по биометрическим данным;

– поиск опубликованных или получение новых персональных данных и иной конфиденциальной информации о человеке (доксинг); в том числе за счет решения генеративным ИИ диагностических задач, направленных на установление пола, возраста, местоположения и иных параметров [9];

– осуществление коммуникации между преступниками из разных стран и налаживание связей в рамках транснациональной преступности<sup>13</sup>.

Деяния, совершаемые с использованием генеративных ИИ, могут быть квалифицированы как преступления в соответствии со ст. 110–110.2, 119, 128.1, 135, 137, 138, 146, ч. 1 ст. 148, ст. 150, 158–159, 163, 183, 185.6, 205.1, 205.2, 205.4, 205.5, 207–207.3, 212, 221, 229, 230, 233, 239, 242, 242.1, 272–273, 274.1, 275–276, 280, 280.1, 280.3, 280.4, 281.1, 282–282.2, 282.4, 283.1, 284.1, 284.2, 288, 296, 297, 298.1, 306, 307, 310, 319, 336, 354, 354.1, 361 Уголовного кодекса Российской Федерации. Преимущественно речь идет о корыстных преступлениях (в первую очередь, о мошенничестве) и преступлениях, связанных с незаконным оборотом недостоверной и иной информации, оборот которой

<sup>12</sup> WormGPT — The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks // SlashNext. URL: <https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks> (дата обращения: 14.06.2024).

<sup>13</sup> Five ways criminals are using AI // MIT Technology Review. URL: <https://www.technologyreview.com/2024/05/21/1092625/five-ways-criminals-are-using-ai> (дата обращения: 14.06.2024).

ограничен или запрещен. Как можно заметить, перечень весьма объемный, и это без учета того, что генеративные нейросети могут быть элементом механизма иных преступлений (например, использоваться при подготовке или сокрытии убийств, террористических актов и т.д.), а также административных правонарушений и гражданских деликтов. Вместе с тем активно дискутируется вопрос о необходимости совершенствования имеющегося правового (в том числе уголовно-правового) регулирования для адекватной правовой оценки действительной общественной опасности действий, совершенных с использованием ИИ [10, с. 129].

Технологические изменения и связанная с ними трансформация преступности обуславливают потребность в определении виновного лица, обосновании оптимальных форм криминализации новых общественно опасных деяний. Относительно первого обстоятельства поднимается вопрос о возможности привлечения ИИ в качестве субъекта противоправных действий к ответственности в той или иной форме. Мнения по данному вопросу разнятся: хотя в литературе указывают на то, что некоторые нарушения жестко связаны с ИИ и являются непосредственными результатами выполняемых ими действий в отсутствие иных активных виновных субъектов [11], отсутствие у обученной нейросети разума и следующей из него свободы воли большинством авторов признается основанием для невозможности признания ИИ субъектом преступления. Одни исследователи признают возможным приобретение искусственным интеллектом правосубъектности в средне- и долгосрочной перспективе (когда искусственный интеллект станет сопоставим с естественным) с сохранением ответственности иных лиц, в том числе создателей и пользователей [12–14], другие же считают, что ответственность за работу «машин» (обученной нейросети), воспринимаемой лишь как инструмент, должен нести работающий с ней человек [15].

Оценивая первую позицию как гипотетически возможную, а вторую — как констатирующую уже существующую ситуацию, мы склонны согласиться с позицией о том, что, пока законом не установлено иное регулирование, ответственность за результаты использования ИИ в качестве инструмента несет ее создатель или пользователь [16]; в таком случае ИИ с криминологической точки зрения рассматривается как орудие преступления либо объект посягатель-

ства, а его использование — как особая разновидность высокотехнологичного способа совершения преступления.

Последний признак предлагается использовать при дифференциации уголовной ответственности (так как совершение преступления с использованием ИИ представляется потенциально более общественно опасным). Имеются как сторонники [17, с. 179], так и противники [18, с. 21] такого шага. Соглашаясь с мнением о необходимости актуализации уголовного закона в части противодействия противоправному использованию ИИ и признавая более перспективным не введение новых статей, а закрепление новых квалифицирующих признаков, мы разделяем осторожность относительно введения в оборот новых широко сформулированных специальных юридических терминов. Представляется желательным более точное регулирование, направленное на противодействие наиболее опасным разновидностям использования ИИ. В этом мы солидарны с исследователями, предлагающими криминализовать противоправное использование результатов применения ИИ (таких, как дипфейки [2, с. 103]).

Пока же подобного рода регулирование отсутствует, поэтому указанные обстоятельства не получают надлежащей уголовно-правовой оценки. Вместе с тем наличие ИИ в механизме преступления имеет высокую криминологическую (в первую очередь диагностическую) значимость, поэтому, вне зависимости от закрепления квалифицирующих признаков в законе (и, соответственно, вхождения в предмет доказывания), при подозрении на использование ИИ обстоятельства, которые могут на это указывать, должны быть надлежащим образом изучены для получения всей возможной криминологически значимой информации.

#### **Криминологическое речеведение и преступления, совершаемые с использованием генеративного ИИ**

Криминологика обладает объемным инструментарием научно-технических средств, позволяющих устанавливать факт использования ИИ при планировании, совершении и сокрытии следов преступления, совершаемых посредством речевых действий. Учитывая особую среду совершения (информационное пространство) и коммуникативный (мультимодальный) характер таких действий, наряду с техническими исследованиями (аудио- и видеозаписей,

документов и т.д.) большое значение приобретают исследования следов подобной преступной деятельности, осуществляемые с позиций криминалистического речеведения.

Последнее представляется частной криминалистической теорией, консолидирующей и развивающей положения уже существующих отраслей криминалистической техники (криминалистической фоноскопии, криминалистического автороведения и др.), а также, по необходимости, разрабатывающей новые положения относительно задач, которые в русле традиционной криминалистики ранее не ставились и не решались. Наиболее показательный пример — лингвистические исследования, получившие широкое распространение в 1990-х гг. Криминалистическое речеведение позволяет совершенствовать не только техническое, но и тактическое и даже методическое криминалистическое обеспечение борьбы с преступлениями, совершаемыми посредством речевых действий. Криминалистическое и судебное речеведение [19] тесно связаны, но при этом имеют и существенные отличия. Не имея возможности в рамках данной статьи рассмотреть эту взаимосвязь подробно (что будет сделано авторами в отдельной публикации), здесь отметим, что, хотя речь выступает общим объектом изучения, данные научные области различаются по своему предмету, объекту, целям, функциям и задачам.

Ввиду того что совершаемые с использованием генеративного ИИ действия отражаются в информационных продуктах, распространяемых с использованием цифровой электроники среди неопределенного круга лиц через функционирующие на основе информационно-телекоммуникационных сетей (как отмечается в литературе, такие результаты использования генеративных ИИ, как дипфейк, вряд ли вообще можно представить вне сетевого пространства [2, с. 103]) средства массовой коммуникации (социальные сети, такие как «ВКонтакте», «Одноклассники»; системы мгновенного обмена сообщениями — Telegram, WhatsApp, Viber; иные ресурсы — форумы, видеохостинги, почтовые сервисы и т.д.), можно говорить о сходстве механизма данных преступлений, в том числе в части слеодообразования. Исследование с позиций криминалистического речеведения содержащихся в сгенерированных ИИ информационных продуктах следов преступлений данной группы в числе прочего позволяет охарактеризовать источник их происхождения как искусствен-

ный (текст или аудио, видео или письменное сообщение, созданное самообучающейся компьютерной программой). В качестве примера можно привести следующие диагностические признаки текста, полученного в результате использования генеративного ИИ:

- повторы словосочетаний и слов;
- повторение одной и той же мысли в разных предложениях;
- отсутствие когерентности текста (нарушена его связность);
- поверхностные (семантически опустошенные) примеры;
- искажение фактов, присутствие недостоверной информации и т.д.

Ввиду наличия проблем, которые могут возникать при расследовании преступлений рассматриваемой категории из-за необходимости работать с нетипичными источниками криминалистически значимой информации, необходимо активное использование как специальных знаний в области речеведения (применение их носителями в предусмотренных законом формах), так и разрабатываемых на их основе или с их использованием криминалистических средств. К числу таких криминалистических средств, разрабатываемых субъектами применения специальных речеведческих знаний, можно отнести [20, с. 101–103]:

- методики и алгоритмы работы с информационными продуктами в цифровой форме;
- криминалистические диагностические комплексы (КДК) [21];
- средства распознавания копий (в том числе замаскированных) речевых продуктов противоправного характера (актуально для выявления материалов, внесенных в список экстремистских, фейковой информации и т.д.);
- программы, позволяющие осуществлять автоматизированное предварительное исследование источников криминалистически значимой информации (имеющих цифровую форму представления речевых и иных информационных продуктов);
- автоматизированные системы выявления преступлений, совершаемых в цифровой среде (мониторинг — система постоянного наблюдения и парсинг — автоматизированный сбор и структурирование информации);
- автоматизированные системы цифрового профилирования лиц (определение их социально-демографических характеристик), в том числе совершающих преступления в цифровой

медиасреде, на основе имеющейся в сети Интернет общедоступной информации;

– базы данных, связанные с перечисленными выше криминалистическими средствами [22];  
– иные перспективные разработки.

Более предметно описать систему средств криминалистического речеведения, пригодных для противодействия преступлениям, совершаемым с использованием генеративного ИИ, возможно будет в дальнейшем, по достижении полноценного становления данной частной криминалистической теории. Однако уже сейчас можно с уверенностью утверждать о наличии широких возможностей в применении знаний в области криминалистического речеведения для описания и изучения значимых признаков такого рода противоправных действий.

В правоохранительной деятельности применение перечисленных средств может сочетаться с использованием инновационных криминалистических средств, в том числе специально разработанных ИИ, которые также активно внедряются в правоохранительную деятельность [23] и могут использоваться в том числе для обнаружения и противодействия преступлениям, совершаемым с использованием генеративного ИИ.

### Заключение

Криминалистика, будучи прикладной юридической наукой синтетической природы, агрегирующей и адаптирующей передовые достижения иных (в первую очередь естественных и точных) наук для решения своих задач по обеспечению эффективной правоохранительной деятельности, связанной с раскрытием, расследованием и предупреждением преступлений, находится на острие перспективных исследований и в настоящее время, в условиях меняющегося мира и связанных с его изменениями больших вызовов, способна выполнять для иных наук юридического цикла методологическую функцию по формированию концептуальных подходов к новым (или существенно трансформировавшимся) явлениям.

К такого рода новым явлениям, нуждающимся в подробном и основательном юридическом осмыслении, может быть в высшей степени обоснованно отнесен ИИ, в том числе генеративный ИИ. Несмотря на большое количество научной литературы по данной проблематике, а также наличие нормативно-правового регулирования (в том числе актов стратегического планирования), пока идет лишь формирование

концептуальных основ и базовых подходов к исследуемой проблематике (которая также находится в постоянной динамике, день ото дня прирастая новыми технологиями). Замечательной иллюстрацией тому служит дискуссия о терминологическом аппарате; в частности, несмотря на наличие закрепленного в Указе Президента Российской Федерации от 10 октября 2019 г. № 490 (и даже на уровне федерального закона<sup>14</sup>) определения понятия «искусственный интеллект», содержательное наполнение данного термина до сих пор вызывает оживленную дискуссию в научных кругах [24].

Генеративный ИИ же стал прорывом, продемонстрировавшим всему миру, что искусственный интеллект — это элемент уже не столько научной фантастики, сколько реальной современной жизни. Данная технология имеет широкие возможности как для правомерного, так и для противоправного применения (в том числе потенциально — независимо от человеческой воли). Риски причинения вреда охраняемым законом общественным отношениям в результате использования генеративного искусственного интеллекта имеют место преимущественно в рамках компьютерно-опосредованной коммуникации; эти риски меняют ландшафт угроз и нуждаются в своевременном осмыслении. Представляется, что чаще всего данная технология используется для осуществления преступлений, совершаемых посредством обмана и манипулирования информацией, — мошенничеств, распространения недостоверной информации, вовлечения в экстремистскую, в том числе террористическую, деятельность и т.д. Этому способствуют широкие возможности генеративного искусственного интеллекта по созданию различных информационных продуктов с помощью компьютерных моделей (технологий): текстов, аудио- и видеозаписей, изображений, компьютерных программ и т.д., в том числе вымышленного (ложного) содержания.

Вместе с тем работа генеративного искусственного интеллекта подразумевает специфический механизм следообразования при

<sup>14</sup> О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в ст. 6 и 10 Федерального закона «О персональных данных» : Федер. закон от 24 апр. 2020 г. № 123-ФЗ // Собрание законодательства РФ. 2020. № 17. Ст. 2701.



совершении преступлений в ходе компьютерно-опосредованной коммуникации и выражается в криминалистически (в первую очередь диагностически) значимых признаках (криминалистических диагностических комплексах). Установление этих признаков возможно за счет применения криминалистических знаний

и использования криминалистических средств. Представляется, что в качестве наиболее перспективного и релевантного источника данных ресурсов научно-технического обеспечения правоохранительной деятельности может выступать частная криминалистическая теория — криминалистическое речеведение.

#### СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Колин К.К. Информатизация общества и социальная информатика / К.К. Колин. — EDN KVRPBZ // Вестник Челябинской государственной академии культуры и искусств. — 2009. — № 3 (19). — С. 6–14.
2. Ефремова М.А. Дипфейк (deepfake) и уголовный закон / М.А. Ефремова, Е.А. Рускевич. — DOI 10.37973/VESTNIKUI-2024-56-13. — EDN LXAWLM // Вестник Казанского юридического института МВД России. — 2024. — Т. 15, № 2 (56). — С. 97–105.
3. Гоббс Т. Левиафан / Т. Гоббс. — Москва : АСТ, 2021. — 800 с.
4. AI-enabled future crime / M. Caldwell, J.T.A. Andrews, T. Tanay, L.D. Griffin. — DOI 10.1186/s40163-020-00123-8. — EDN DNBTIW // Crime Science. — 2020. — Vol. 9, no. 14. — P. 1–13.
5. Харитонов Ю.С. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права / Ю.С. Харитонов, В.С. Савина, Ф. Паньини. — DOI 10.17072/1995-4190-2021-53-488-515. — EDN EUKCPY // Вестник Пермского университета. Юридические науки. — 2021. — № 53. — С. 488–515.
6. Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions / T.C. King, N. Aggarwal, M. Taddeo, L. Floridi. — DOI 10.1007/s11948-018-00081-0 // Science and Engineering Ethics. — 2020. — Vol. 26. — P. 89–120.
7. Малышкин А.В. Интегрирование искусственного интеллекта в общественную жизнь: некоторые этические и правовые проблемы / А.В. Малышкин. — DOI 10.21638/spbu14.2019.303. — EDN HBIOXR // Вестник Санкт-Петербургского университета. Право. — 2019. — Т. 10, № 3. — С. 444–460.
8. Milivojevic S. Artificial intelligence, illegalised mobility and lucrative alchemy of border utopia / S. Milivojevic. — DOI 10.1177/17488958221123855 // Criminology & Criminal Justice. — 2022. — URL: <https://journals.sagepub.com/doi/10.1177/17488958221123855>.
9. Beyond Memorization: Violating Privacy Via Inference with Large Language Models / R. Staab, M. Vero, M. Balunović, M. Vechev // Published as a conference paper at ICLR 2024. — URL: <https://arxiv.org/pdf/2310.07298v2>.
10. Филипова И.А. Правовое регулирование искусственного интеллекта : 2-е изд., обновл. и доп. / И.А. Филипова. — Нижний Новгород : Изд-во ННГУ, 2022. — 275 с. — EDN VLVYJA.
11. Nerantzi E. 'Hard AI Crime': The Deterrence Turn / E. Nerantzi, G. Sartor. — DOI 10.1093/ojls/ggae018 // Oxford Journal of Legal Studies — 2024. — Vol. 7, no. 3. — P. 1–29.
12. Лаптев В.А. Понятие искусственного интеллекта и юридическая ответственность за его работу / В.А. Лаптев. — DOI 10.17323/2072-8166.2019.2.79.102. — EDN GQATHO // Право. Журнал Высшей школы экономики. — 2019. — № 2. — С. 79–102.
13. Мосечкин И.Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления / И.Н. Мосечкин. — DOI 10.21638/spbu14.2019.304. — EDN BGASBE // Вестник Санкт-Петербургского университета. Право. — 2019. — Т. 10, № 3. — С. 461–476.
14. Даниленко Ю.А. Использование искусственного интеллекта в преступных целях: уголовно-правовая характеристика / Ю.А. Даниленко. — EDN NXVLSM // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. — 2023. — Т. 9, № 4. — С. 232–240.
15. Sunde I.M. A new thing under the sun?: Crime in the digitized society / I.M. Sunde // NSfK's 58. Research Seminar: New challenges in criminology: Can old theories be used to explain or understand new crimes? / ed. I.A. Kinnunen. — Bifröst, 2016. — P. 60–79.
16. Čerka P. Liability for damages caused by artificial intelligence / P. Čerka, J. Grigienė, G. Sirbikytė. — DOI 10.1016/j.clsr.2015.03.008 // Computer Law & Security Review. — 2015. — Vol. 31, no. 3. — P. 376–389.
17. Архипцев И.Н. К вопросу о правовом обеспечении предупреждения преступлений, совершаемых с использованием искусственного интеллекта и технологий, созданных на его основе в Российской Федерации / И.Н. Архипцев, А.В. Сарычев, А.В. Мотузов. — DOI 10.15688/lc.jvolsu.2022.2.23. — EDN PZAJAG // Правовая парадигма. — 2022. — Т. 21, № 2. — С. 175–181.
18. Осипенко А.Л. Технологии искусственного интеллекта в преступной деятельности: новые угрозы и вызовы / А.Л. Осипенко. — EDN FIRGNI // Общество и право. — 2023. — № 4 (86). — С. 15–25.
19. Галяшина Е.И. Судебное речеведение : учебник / Е.И. Галяшина. — Москва : Норма, 2020. — 320 с. — EDN NLRDPS.
20. Богатырев К.М. Знания в области речевого действия в системе криминалистических средств противодействия преступлениям в цифровой медиасреде : дис. ... канд. юрид. наук / К.М. Богатырев. — Москва, 2023. — 242 с. — EDN QQKWDT.
21. Галяшина Е.И. Типовые криминалистические диагностические комплексы криминогенных речевых действий / Е.И. Галяшина, В.Д. Никишин, К.М. Богатырев. — DOI 10.25724/VAMVD.RXYZ. — EDN QSAXPL // Судебная экспертиза. — 2021. — № 1 (65). — С. 16–31.
22. Степаненко Д.А. Формирование криминологических баз данных с использованием технологий блокчейна / Д.А. Степаненко. — EDN CRIDJP // Евразийский юридический журнал. — 2022. — № 10 (173). — С. 436–437.

23. Степаненко Д.А. Использование систем искусственного интеллекта в правоохранительной деятельности / Д.А. Степаненко, Д.В. Бахтеев, Ю.А. Евстратова. — EDN KUFXLQ // Вестник Санкт-Петербургского военного института войск национальной гвардии. — 2020. — № 2 (11). — С. 104–110.

24. Кирюшина И.К. вопросу о понятии искусственного интеллекта и основах его регулирования в международном и российском праве / И. Кирюшина, Е. Коваленко. — DOI 10.14258/leglin(2023)2907. — EDN XQGZTO // Юрислингвистика. — 2023. — № 29 (40). — С. 42–48.

## REFERENCES

1. Kolin K.K. Computing of the Society and Social Computer Science. *Herald of the Chelyabinsk State Academy of Culture and Arts*, 2009, no. 3, pp. 6–14. (In Russian). EDN: KVRPBZ.

2. Efremova M.A., Russkevich E.A. Deepfake and Criminal Law. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA Russia*, 2024, vol. 15, no. 2, pp. 97–105. (In Russian). EDN: LXAWLM. DOI: 10.37973/VESTNIKKUI-2024-56-13.

3. Hobbes Th. *Leviathan or The Matter, Form and Power of a Commonwealth Ecclesiastical and Civil*. London, Printed for A. Crooke, 1651. 300 p. (Russ. ed.: Hobbes Th. *Leviathan*. Moscow, AKT Publ., 2021. 800 p.).

4. Caldwell M., Andrews J.T.A., Tanay T., Griffin L.D. AI-enabled Future Crime. *Crime Science*, 2020, vol. 9, no. 14, pp. 1–13. EDN: DNBTIW. DOI: 10.1186/s40163-020-00123-8.

5. Kharitonova Yu.S., Savina V.S., Pagnini F. Artificial Intelligence's Algorithmic Bias: Ethical and Legal Issues. *Vestnik Perm'skogo universiteta. Yuridicheskie nauki = Perm University Herald. Juridical Sciences*, 2021, no. 53, pp. 488–515. (In Russian). EDN: EUKCPY. DOI: 10.17072/1995-4190-2021-53-488-515.

6. King T.C., Aggarwal N., Taddeo M., Floridi L. Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. *Science and Engineering Ethics*, 2020, vol. 26, pp. 89–120. DOI: 10.1007/s11948-018-00081-0.

7. Malyshekin A.V. Integration of Artificial Intelligence into Public Life: Some Ethical and Legal Problems. *Vestnik Sankt-Petersburgskogo universiteta. Pravo = Vestnik of Saint-Petersburg University. Law*, 2019, vol. 10, no. 3, pp. 444–460. (In Russian). EDN: HBIOXR. DOI: 10.21638/spbu14.2019.303.

8. Milivojevic S. Artificial Intelligence, Illegalised Mobility and Lucrative Alchemy of Border Utopia. *Criminology & Criminal Justice*, 2022. URL: <https://journals.sagepub.com/doi/10.1177/17488958221123855>. DOI 10.1177/17488958221123855.

9. Staab R., Vero M., M. Balunović M., Vechev M. Beyond Memorization: Violating Privacy via Inference with Large Language Models. *Published as a conference paper at ICLR 2024*. URL: <https://arxiv.org/pdf/2310.07298v2>.

10. Filipova I.A. *Legal Regulation of Artificial Intelligence*. Nizhny Novgorod, Lobachevsky State University of Nizhniy Novgorod Publ., 2022. 275 p. EDN: VLVYJA.

11. Nerantzi E., Sartor G. 'Hard AI Crime': The Deterrence Turn. *Oxford Journal of Legal Studies*, 2024, vol. 7, no. 3, pp. 1–29. DOI: 10.1093/ojls/gqae018.

12. Laptev V.A. Artificial Intelligence and Liability for its Work. *Pravo. Zhurnal Vysshey shkoly ekonomiki = Law. Journal of the Higher School of Economics*, 2019, no. 2, pp. 79–102. (In Russian). EDN: GQATHO. DOI: 10.17323/2072-8166.2019.2.79.102.

13. Mosechkin I.N. Artificial Intelligence and Criminal Liability: Problems of Becoming a New Type of Crime Subject. *Vestnik Sankt-Petersburgskogo universiteta. Pravo = Vestnik of Saint-Petersburg University. Law*, 2019, vol. 10, no. 3, pp. 461–476. (In Russian). EDN: BGASBE. DOI: 10.21638/spbu14.2019.304.

14. Danilenko Y.A. The Use of Artificial Intelligence for Criminal Purposes: Criminal and Legal Characteristics. *Uchenye zapiski Krymskogo federal'nogo universiteta im. V.I. Vernadskogo. Yuridicheskie nauki = Scientific Notes of V.I. Vernadsky Crimean Federal University. Juridical Science*, 2023, vol. 9, no. 4, pp. 232–240. (In Russian). EDN: NXVLSM.

15. Sunde I.M. A new thing under the sun?: Crime in the Digitized Society. In Kinnunen I.A. (ed.). *NSfK's 58. Research Seminar: New challenges in Criminology: Can Old Theories Be Used to Explain or Understand New Crimes?* Bifröst, 2016, pp. 60–79.

16. Čerka P., Grigienė J., Širbikytė G. Liability for Damages Caused by Artificial Intelligence. *Computer Law & Security Review*, 2015, vol. 31, no. 3, pp. 376–389. DOI: 10.1016/j.clsr.2015.03.008.

17. Arkhipov I.N., Sarychev A.V., Motuzov A.V. On the Legal Support for the Prevention of Crimes Committed Using Artificial Intelligence and Technologies Created on its Basis in the Russian Federation. *Pravovaya paradigma = Legal Concept*, 2022, vol. 21, no. 2, pp. 175–181. (In Russian). EDN: PZAJAG. DOI: 10.15688/lc.jvolsu.2022.2.23.

18. Osipenko A.L. Artificial Intelligence Technologies in Criminal Activity: New Threats and Challenges. *Obshchestvo i pravo = Society and Law*, 2023, no. 4, pp. 15–25. (In Russian). EDN: FIRGNI.

19. Galyashina E.I. *Judicial Recitation*. Moscow, Norma Publ., 2020. 320 p. EDN: NLRDPS.

20. Bogatyrev K.M. Speech Science Knowledge in the Criminalistic Tools System for Countering Digital Media Crimes. *Cand. Diss. Moscow*, 2023. 242 p. EDN: QQKWDI.

21. Galyashina E.I., Nikishin V.D., Bogatyrev K.M. Typical Forensic Diagnostic Complexes of Criminogenic Speech Actions. *Sudebnaya ekspertiza = Forensic Examination*, 2021, no. 1, pp. 16–31. (In Russian). EDN: QSAXPL. DOI: 10.25724/VAMVD.RXYZ.

22. Stepanenko D.A. Formation of Criminological Databases Using Blockchain Technologies. *Evrasiiskii yuridicheskii zhurnal = Eurasian Law Journal*, 2022, no. 10, pp. 436–437. (In Russian). EDN: CRJDJP.

23. Stepanenko D.A., Bakhteev D.V., Evstratova Yu.A. Use of Artificial Intelligence Systems in Law Enforcement. *Vestnik Sankt-Petersburgskogo voennogo instituta voisk natsional'noi gvardii = Bulletin of the St. Petersburg Military Institute of the National Guard Troops*, 2020, no. 2, pp. 104–110. (In Russian). EDN: KUFXLQ.

24. Kiryushina I., Kovalenko E. On the Concept of Artificial Intelligence and the Basics of its Regulation in International and Russian Law. *Yurislingvistika = Legal Linguistics*, 2023, no. 29, pp. 42–48. (In Russian). EDN: XQGZTO. DOI: 10.14258/leglin(2023)2907.

#### ИНФОРМАЦИЯ ОБ АВТОРАХ

Галышина Елена Игоревна — заведующий кафедрой криминалистики Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, доктор филологических наук, профессор, г. Москва, Российская Федерация; e-mail: eigalyashina@gmail.com.

Богатырев Константин Михайлович — старший преподаватель кафедры криминалистики Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук, г. Москва, Российская Федерация; e-mail: kbog@rambler.ru.

#### ВКЛАД АВТОРОВ

Все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

#### ДЛЯ ЦИТИРОВАНИЯ

Галышина Е.И. Возможности криминалистического речеведения в противодействии преступлениям, совершаемым с использованием генеративного искусственного интеллекта / Е.И. Галышина, К.М. Богатырев. — DOI 10.17150/2500-4255.2025.19(1).96-106. — EDN HYQQLW // Всероссийский криминологический журнал. — 2025. — Т. 19, № 1. — С. 96–106.

#### INFORMATION ABOUT THE AUTHORS

Galyashina, Elena I. — Head, Department of Criminalistics, Kutafin Moscow State Law University (MSAL), Doctor of Law, Doctor of Philology, Professor, Moscow, the Russian Federation; e-mail: eigalyashina@gmail.com.

Bogatyrev, Konstantin M. — Senior Lecturer, Department of Criminalistics, Kutafin Moscow State Law University (MSAL), Ph.D. in Law, Moscow, the Russian Federation; e-mail: kbog@rambler.ru.

#### CONTRIBUTION OF THE AUTHORS

The authors contributed equally to this article. The authors declare no conflicts of interests.

#### FOR CITATION

Galyashina E.I., Bogatyrev K.M. The Potential of Forensic Speech Science to Counteract Crimes Committed Using Generative Artificial Intelligence. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2025, vol. 19, no. 1, pp. 96–106. (In Russian). EDN: HYQQLW. DOI: 10.17150/2500-4255.2025.19(1).96-106.