УДК 343.98(045)

Н.И. Старостенко

АНАЛИЗ ТЕНДЕНЦИЙ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ

Усилия профильных ведомств и регуляторов финансово рынка не всегда позволяют в полной мере успешно снижать массив преступлений, связанных с применением информационно-телекоммуникационных технологий. Риски совершения подобных деяний напрямую сопряжены с дистанционным характером осуществления противоправных действий, а также с фактами утечки конфиденциальных данных граждан. Дистанционные хищения, составляющие около 70% от общего числа преступлений указанного вида, имеют особую специфику, выраженную в применении в ходе реализации корыстного умысла определенных психологических приемов, которые в специальной литературе называют методами социальной инженерии, а также различных программных средств и технологий, в том числе технологий искусственного интеллекта. Внедрение в противоправную деятельность указанных инструментов изменило характер данной преступности, открыло новые криминальные возможности для преступников, упростило достижение ими корыстных целей, а также усовершенствовало существующие способы подготовки, совершения, а также сокрытия данных преступлений. В статье сделан вывод о том, что прогнозирование подобной преступности позволит своевременно предпринять меры по предупреждению преступлений анализируемого вида, выработать приемы и средства обнаружения цифровых следов противоправной деятельности и современные подходы к производству отдельных следственных действий. Полученные результаты исследования могут использоваться для дальнейшего изучения вопросов, связанных с использованием искусственного интеллекта в преступной деятельности.

Ключевые слова: криминалистика, преступления, мошенничество, расследование преступлений, социальная инженерия, методы социальной инженерии, информационно-телекоммуникационные технологии, искусственный интеллект.

DOI: 10.35634/2412-9593-2024-34-2-339-344

В настоящее время современное состояние преступности в Российской Федерации характеризуется устойчивым ростом преступных проявлений, связанных с использованием в противоправной деятельности информационно-телекоммуникационных технологий. Так, по данным официальной статистики МВД России, число зарегистрированных преступлений указанного вида за период с января по ноябрь 2023 г. по сравнению с аналогичным периодом 2022 года возросло на 30,8 %. Вместе с тем около 70 % от общего числа противоправных деяний, совершенных с применением информационно-телекоммуникационных технологий, составляют хищения [1]. Как видим, виртуальный мир меняет уклад механизмов совершения преступлений различного вида, способствует переходу от традиционных, простых способов их совершения к более сложным дистанционным формам. На расширенном заседании коллегии МВД России, состоявшемся в марте 2023 г., Президент Российской Федерации В.В. Путин обратил особое внимание на то, что одним из безусловных приоритетов работы сотрудников правоохранительных органов остается борьба с преступлениями, совершаемыми с использованием информационных технологий [2].

Несмотря на усилия профильных ведомств и регуляторов финансового рынка, появление новых методов защиты от дистанционных действий злоумышленников, а также формирование усовершенствованных подходов к раскрытию и расследованию преступных схем в информационном пространстве, все же постоянное развитие информационных технологий, а также внедрение новых программных средств в повседневную деятельность общества не позволяют в полной мере успешно снижать массив подобных противоправных проявлений.

Нельзя не согласиться с В.С. Овчинским, который отмечает, что преступность необратимо уходит и действует через киберпространство, а новые технологии меняют мир. При этом главным фактором изменений становится научно-техническая революция и внедрение искусственного интеллекта (ИИ) во все сферы деятельности человека. Кроме того, в большей части изменению подвергнута организованная преступность. Эксперты прогнозируют, что в ближайшее время организованная преступность превратится в глобальную криминальную многопрофильную корпорацию, использующую все новейшие достижения науки и техники, включая ИИ, дроны, социальный инжиниринг [3].

Действительно, способы совершения подобных преступлений имеют тенденции к дальнейшей трансформации, вызванной применением в преступной деятельности искусственного интеллекта (ИИ) – технологий, свойство которых ориентировано на выполнение автоматизированных интеллектуальных задач, которые традиционно считаются прерогативой человека [4]. Например, расширяется генерирование фальсифицированного контента, когда программа синтезирует изображение лица конкретного человека и заменяет им указанное лицо в обрабатываемом видеофрагменте [5; 6]. Применяются технологии синтеза, способные произносить заданные фразы голосом конкретного человека после обработки его индивидуального речевого образца. Прогнозируется, что в ближайшее время поддельные аудио- и видеозаписи, создаваемые с применением ИИ, станут неотличимы от реальных [7].

Безусловно, внедрение в противоправную деятельность указанных инструментов может менять характер преступности, открывать новые криминальные возможности, облегчать достижение целей, совершенствовать способы подготовки, совершения и сокрытия преступных действий, реализуемых в сфере информационно-телекоммуникационных технологий.

Необходимо подчеркнуть, что развитие искусственного интеллекта уже сегодня требует адекватного правового регулирования, способного спрогнозировать риски его применения и предусмотреть ответственность в случае причинения вреда общественным отношениям [8]. Важно и то, что прогнозирование подобной преступности позволит своевременно предпринять меры по предупреждению преступлений анализируемого вида, выработать приемы и средства обнаружения цифровых следов противоправной деятельности и современные подходы к производству отдельных следственных действий.

На данный момент значительное внимание общественности привлекает выпуск и широкое использование технологий ChatGPT – большой языковой модели (LLM), разработанной OpenAI [9]. Одно из самых существенных преимуществ технологий обозначенного вида связано с возможностью получать ответ на любой поставленный чат-боту вопрос, быстро собирать и интерпретировать искомую информацию в сети Интернет без необходимости ручного поиска и обобщения огромного объема сведений, задаваемых в поисковых системах. В этой связи стоит отметить положительное значение ChatGPT, поскольку его использование позволит глубже погружаться в интересующую тему, может значительно ускорить процесс обучения, помочь гораздо быстрее освоиться в новой области знаний.

В то же время распространение технологий анализируемого вида вызывает обеспокоенность у учёных и правоприменителей относительно внедрения и применения их в процессе совершения преступлений. Так, по данным Европола, всего через несколько недель после публичного выпуска ChatGPT преступники адаптировали новые технологии в своей деятельности, продумывая конкретные криминальные способы их использования. Также в отчете «ChatGPT The impact of Large Language Models on Law Enforcement» детально рассматривается данная проблематика, уделяется внимание некоторым аспектам влияния больших языковых моделей на совершенствование преступной деятельности, а также последствиям их использования злоумышленниками [10].

Согласно указанному отчету, можно выделить следующие направления криминального использования ChatGPT: при хищениях с применением методов социальной инженерии, в террористической деятельности, в области криминальной пропаганды и дезинформации в сети Интернет.

Рассмотрим применение ChatGPT при совершении хищений с применением методов социальной инженерии. Прежде всего стоит указать, что методы социальной инженерии – это совокупность психологических приемов, технических действий по применению программных средств, технологий в процессе подготовки, непосредственного совершения и сокрытия преступления, направленных на оказание психологического воздействия на сознание и поведение людей, создание условий, необходимых для дистанционного хищения чужого имущества [11].

Использование указанных методов социальной инженерии позволяет преступнику создать такие условия, при которых жертва самостоятельно выполняет перевод денежных средств на определенный банковский счет, принадлежащий третьим лицам, либо под контролем преступников совершает иные финансовые операции; добровольно предоставляет преступникам удаленный доступ или управление электронным устройством либо передает код из SMS-сообщений от банка, подтверждающий финансовую операцию, реквизиты банковской карты, в том числе код, логины и пароли от сервиса дистанционного банковского обслуживания, а также иную информацию, необходимую для хищения чужого имущества.

К методам социальной инженерии относятся психологические приемы манипуляции, связанные с использованием специально подготовленного сценария или текста, предусматривающего исполнение определенной роли при осуществлении преступных действий в целях оказания воздействия на психоэмоциональное состояние жертвы для изменения ее восприятия и убеждения в необходимости срочного принятия решения в ограниченный период времени; а также технологические приемы манипуляции, направленные на создание поддельного интернет-сайта, фишинговой ссылки и (или) использование определенных программных средств для дистанционного воздействия на жертву, обеспечивающих сокрытие преступных действий.

Изучение судебной и следственной практики подтвердило, что одновременное применение преступниками в ходе достижения корыстных целей методов социальной инженерии и информационно-телекоммуникационных технологий препятствует своевременному установлению данных о личности преступника и способе совершения преступления, что зачастую приводит к трудностям при собирании следов, проведении отдельных следственных действий, а также при организации криминалистического взаимодействия на первоначальном этапе расследования данных хищений.

Высокая степень общественной опасности указанных противоправных деяний подтверждается их спецификой, поскольку совершить их могут лица, обладающие знаниями в области психологии, а также умениями собирать необходимую информацию о жертвах для реализации корыстных целей. Вместе с тем особенности способа совершения преступлений данной категории обусловлены созданием злоумышленниками специально разработанных алгоритмов и сценариев обмана, рассчитанных на их многократное применение в отношении граждан.

Следует подчеркнуть, что в рассматриваемом аспекте технологии нейросети ChatGPT могут применяться ими при создании текстов, обращений к жертвам, сценариев взаимодействия для введения их в заблуждение относительно преступных намерений. Так, в руках преступника ChatGPT может создавать текст для сообщений, направленный на манипулирование людьми с целью разглашения ими конфиденциальной информации или выполнения определенных действий с использованием банковского счета (карты).

Можно отметить, что в целом ChatGPT может представлять угрозу для информационной безопасности общества. По мнению специалистов защиты информации компании «Газинформсервис», с помощью чат-ботов злоумышленники могут получить персональную и коммерческую тайну от пользователей двумя способами: 1) когда пользователь самостоятельно проявит неосторожность и сообщит данные чат-боту; 2) при получении чат-ботом информации о пользователе при аутентификации через социальные сети [12].

Вместе с тем большую опасность названные технологии представляют при использовании их преступниками в сочетании с Osint (Open Source Intelligence) при сборе информации из открытых (общедоступных) источников. В отчете международной аналитической компании по страхованию от киберпреступлений специалистами выделяются тенденции преступности, связанной с применением при совершении хищений методов социальной инженерии, а также приема «масштабного социального профилирования» (Social profiling at scale) [13]. Иными словами, возможности ИИ могут способствовать собиранию злоумышленниками данных о жертвах при помощи OSINT-технологий (автоматизированных технологий для получения информации о людях из профилей в социальных сетях, исходя из активности в Интернете, из общедоступных документов и других источников), то есть создавать исчерпывающий профиль потенциальной жертвы, включающий в себя сведения о ее интересах, увлечениях, информацию о родственниках и друзьях и др. [14]. Знание такой информации позволяет создать перечень вопросов для ChatGPT, а полученные при этом ответы – разработать алгоритмы, предусматривающие оказание психологического воздействия на конкретного человека.

Более того, преступники используют ChatGPT при осуществлении рассылок фишинговых ссылок. Опасность применения нейросети при генерировании текстов для рассылок по определенному заданию заключается в том, что ее использование может сделать содержание обращений к жертвам убедительным, создать более персонализированный текст, учитывающий особенности личности адресата. В то же время рассматриваемые технологии могут способствовать преступным действиям злоумышленника не только при вступлении во взаимодействие с жертвами, но и при дальнейшем общении, поскольку возможности ChatGPT позволяют за считанные секунды сгенерировать ответ на поставленный вопрос.

Важно отметить, что контекст поддельного электронного письма может быть легко сгенерирован в зависимости от потребностей субъекта угрозы, начиная от мошеннических инвестиционных возможностей и заканчивая компрометацией деловой электронной почты и мошенничеством с исполнением роли руководителя конкретной организации [15]. Действительно, функционал, которым располагает ChatGPT, используется злоумышленниками для подражания стилю речи специалиста в определенной области. Этой возможностью преступники злоупотребляют в широких масштабах, поскольку это позволяет им ввести большее количество потенциальных жертв в заблуждение и склонить их к доверию преступным структурам.

Как видим, новый способ обмана с применением нейросети ChatGPT может облегчать работу преступников, а именно автоматизировать методы социальной инженерии при рассылке фишинговых ссылок, создании алгоритмов для общения с жертвами, текста поддельных интернет-сайтов, что с большой долей вероятности, несомненно, приведет к увеличению количества таких ресурсов.

В дополнении к преступной деятельности, описанной выше, стоит сказать, что функционал ChatGPT используется злоумышленниками в ряде случаев при совершении преступлений террористической направленности, поскольку рассматриваемые инструменты преступники адаптировали для общего сбора дополнительной информации, которая может способствовать организации террористической деятельности.

Д. Холл, независимый обозреватель закона о терроризме и один из известных юристов в Великобритании, отметил, что ботов, таких как ChatGPT, можно научить распространять террористическую идеологию среди экстремистов [16]. Думается, что указанную позицию можно считать вполне оправданной, поскольку ChatGPT, получая новую информацию в определенной предметной области, «обучается», т.е. в период своего функционирования становится всё более совершенным, и в дальнейшем может создавать модели по определенному текстовому описанию, запрашивать данные от внешних источников, производить их анализ.

Вместе с тем учитывая возможности ChatGPT в оказании помощи при составлении сценариев и алгоритмов выполнения определенных действий, следует подчеркнуть, что данные функции могут быть использованы преступниками при подготовке радикалов к совершению террористических действий.

Вместе с тем существует точка зрения, согласно которой ChatGPT может способствовать распространять дезинформацию в сети Интернет в неконтролируемых масштабах. В 80% случаев чатбот с ИИ делал красноречивые, ложные и вводящие в заблуждение заявления о важных темах в новостях, включая информацию о пандемии COVID-19, о специальной военной операции, о скулшутинге [17] и т.д.

Кроме того, отмечается, что при помощи ChatGPT злоумышленники создают вредоносный код. Несмотря на то, что инструменты являются лишь базовыми (т.е. с их помощью могут создаваться несложные приложения для достижения преступных целей в сети), все же это представляет угрозу кибербезопасности общества в связи с тем, что это позволяет пользователю, без наличия специальных технических знаний, использовать данные технологии для совершения преступных действий. В то же время более «продвинутый пользователь» может использовать эти улучшенные возможности для дальнейшего совершенствования или даже автоматизации изощренных способов совершения преступлений.

С учетом этого добавим, что, несмотря на то, что ChatGPT достаточно функционален, появляются более совершенные чат-боты, такие как Claude («Клод» — это название новой похожей нейросети), который, по мнению аналитиков, по своим возможностям превзойдёт GPT по всем параметрам, т.е. исследуемые технологии могут стать еще более уникальными, что приведет к получению от чат-бота более точных ответов на поисковые запросы.

Отметим, что рассмотренные технологии находятся в неограниченном доступе в сети Интернет, злоумышленник может установить их на устройство и использовать при совершении преступлений. В то же время анализ судебно-следственной практики не выявил фактов многократного использования обозначенных технологий при совершении преступлений в России, но их существование, активная разработка и внедрение позволяют сделать вывод об их соответствии потребностям злоумышленников, а также прогнозировать в ближайшем будущем их широкое применение в преступных целях.

Подводя общий итог, отметим следующее. Сегодня особенно важно осознавать угрозы, которые могут нанести современные программные средства и технологии, и предпринимать необходимые упре-

дительные действия для предупреждения преступности анализируемого вида. Изучение возможностей злонамеренного применения инструментов ИИ помогает прогнозировать способ совершения преступлений, выявлять его особенности, формы использования для достижения противоправных целей.

Обозначенные вопросы заслуживают глубокого осмысления научным сообществом, а в дальнейшем нуждаются в постоянной корректировке с учетом совершенствования данных технологий и особенностей применения ИИ в преступной деятельности. Учитывая потенциальный вред, который может возникнуть в результате злонамеренного использования ChatGPT, крайне важно повысить осведомленность общественности по этому вопросу. Добавим также, что появление технологий, способствующих осуществлению преступной деятельности, побуждает повысить компетентность сотрудников правоохранительных органов в данной области, поскольку правоприменители должны обладать соответствующими знаниями о данной преступности, уметь оценивать контент, создаваемый генеративными моделями ИИ. В этой связи необходимо скорректировать существующие и разработать научно-практические рекомендации, учитывающие современные подходы к выявлению, раскрытию и расследованию преступлений анализируемого вида.

СПИСОК ЛИТЕРАТУРЫ

1. Официальный сайт МВД России. Краткая характеристика состояния преступности в Российской Федерации за январь-ноябрь 2023 года. URL: https://мвд.рф/reports/item/45293174/ (дата обращения: 11.01.2024).
2. Официальный сайт Президента Российской Федерации. Расширенное заседание коллегии МВД России. URL: http://kremlin.ru/events/president/news/70744 (дата обращения: 12.01.2024).
3. Овчинский В.С., Ларина Е.С., «Искусственный интеллект. Большие данные. Преступность»: Новые технологии меняют мир.
4. Аверкин А.Н., Гаазе-Рапопорт М.Г., Поспелов Д.А. Толковый словарь по искусственному интеллекту. М.:Радио и связь, 1992. 256 с.
5. Chesney R., Citron D. Deepfakes: A looming crisis for national security, democracy and privacy? Lawfare, February 21, 2018. URL: https://www.lawfareblog.com/deep-fakes-looming-crisis-national-security-democracy-and-privacy (дата обращения: 22.01.2024);
6. *Bendel O.* The synthetization of human voices // AI and Society. March 2019, Vol. 34. Issue 1. URL: https://doi.org/10.1007/s00146-017-0748-x (дата обращения: 22.01.2024).
7. Осипенко А.Л. Оперативно-розыскная деятельность в информационном обществе: адаптация к условиям цифровой реальности // Научный вестник Омской академии МВД России. 2019. №4 (75). С. 38-46.
8. Грачева Ю.В., Арямов А.А. Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы российского права. 2020. Т. 15. № 6. С. 169–178.
9. Introducing ChatGPT. URL: https://openai.com/blog/chatgpt (дата обращения: 10.02.2024).
10. Europol. ChatGPT – the impact of Large Language Models on Law Enforcement. URL: https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement (дата обращения: 19.02.2024).
11. Старостенко Н.И. Понятие и виды методов социальной инженерии, применяемых при совершении преступлений в сфере информационно-телекоммуникационных технологий // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 1(61). С. 152–159.
12. «Газинформсервис» информирует: из-за чат-ботов начали происходить утечки данных. URL: https://www.novostiitkanala.ru/news/detail.php?ID=168011(дата обращения: 15.02.2024).
13. Thomson D. Social Engineering Blurring reality and fake: A guide for the insurance professional. URL: https://www.actuarialpost.co.uk/downloads/cat_1/Cybercube - The Future of Social Engineering.pdf (дата обращения: 10.02.2024).
14. Rosengren K. Contribution of Open-Source intelligence to Social Engineering Cyberattacks [Электронный ресурс]. URL: https://www.theseus.fi/bitstream/handle/10024/754826/ Rosengren_Kim.pdf?sequence=2&isAllowed=y (дата обращения: 10.02.2024).
15. WithSecure 2023, Creatively malicious prompt engineering, accessible at. URL: https://labs.withsecure.com/publications/creatively-malicious-prompt-engineering. (дата обращения 03.02.2024).
16. AI Chatbots like ChatGPT can be used to groom young men into terrorists, says top UK lawyer. URL: https://www.firstpost.com/world/chatgpt-can-be-used-to-groom-young-men-into-terrorists-says-top-uk-lawyer-12434072.html (дата обращения: 03.02.2024).
17. The Next Great Misinformation Superspreader: How ChatGPT Could Spread Toxic Misinformation At Unprecedented Scale URL: https://www.newsguardtech.com/misinformation-monitor/jan-2023 (дата обращения: 20.02.2024).

Поступила в редакцию 05.02.2024

Старостенко Нина Игоревна, кандидат юридических наук, преподаватель кафедры криминалистики
Краснодарский университет МВД России
350005, Россия, г. Краснодар, ул. Ярославская 128
E-mail: nstarostenko1996@mail.ru

N.I. Starostenko
ANALYSIS OF TRENDS IN THE USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL ACTIVITIES

DOI: 10.35634/2412-9593-2024-34-2-339-344

The efforts of relevant agencies and financial market regulators do not always make it possible to fully successfully reduce the array of crimes related to the use of information and telecommunication technologies. The risks of committing such acts are directly related to the remote nature of the illegal actions, as well as the facts of leakage of confidential data of citizens. Remote theft, which makes up about 70% of the total number of crimes of this type, has a special specificity, expressed in the use of certain psychological techniques during the implementation of mercenary intent, which in the specialized literature are called methods of social engineering, as well as various software tools and technologies, including artificial intelligence technologies. The introduction of these tools into illegal activities has changed the nature of this crime, opened up new criminal opportunities for criminals, simplified their achievement of selfish goals, and improved existing methods of preparing, committing, and concealing these crimes. The article concludes that forecasting such crime will allow timely measures to be taken to prevent crimes of the analyzed type, to develop techniques and means for detecting digital traces of illegal activity and modern approaches to the production of individual investigative actions. The obtained research results can be used for further study of issues related to the use of artificial intelligence in criminal activities.

Keywords: criminology, crime, fraud, crime investigation, social engineering, social engineering methods, information and telecommunication technologies, artificial intelligence.

Received 05.02.2024

Starostenko N.I., Candidate of Law, Lecturer at the Department of Criminalistics
Krasnodar University of the Ministry of Internal Affairs of Russia
Yaroslavskaya st., 128, Krasnodar, Russia, 350005
E-mail: nstarostenko1996@mail.ru