УДК 343.132

НЕКОТОРЫЕ ПРОБЛЕМЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Федюнин Антон Евгеньевич, Перетятько Наталья Михайловна

Саратовская государственная юридическая академия, г. Саратов
e-mail: aef@bk.ru, naperetyatko@yandex.ru

SOME PROBLEMS OF DISCLOSURE AND INVESTIGATION OF CRIMES COMMITTED USING NEURAL NETWORK TECHNOLOGIES

Fedyunin Anton E., Peretyatko Natalia M.

Saratov State Law Academy, Saratov

Аннотация. В статье рассматриваются актуальные проблемы использования технологий нейросетей при раскрытии и расследовании преступлений, совершаемых с использованием нейросетевых технологий. Предметом исследования являются свойства нейросетевых технологий, позволяющие использовать их как инструмент для противодействия преступности. Цель состоит в исследовании процесса адаптации нейросетей к работе в условиях цифровизации уголовно-процессуальной деятельности. Используются традиционные общенаучные и специальные правовые методы – формально-юридический, логический, аналитический. Результаты: определены направления совершенствования деятельности правоохранительных органов по внедрению нейросетевых технологий в практику расследования преступлений. Вывод: нейросети могут быть настроены на решение процессуальных задач: анализ материалов уголовных дел, выявление следственных ошибок, выделение признаков серийности, объединения преступлений по схожим фактическим данным.

Ключевые слова: расследование преступлений, борьба с преступностью, информатизация, цифровизация, нейросети, информационные технологии.

Abstract. The article discusses the actual problems of using neural network technologies in the detection and investigation of crimes committed using neural network technologies. The subject of the study is the properties of neural technologies that allow them to be used as a tool for combating crime. The goal is to study the process of adaptation of neural networks to work in the conditions of digitalization of criminal procedural activities. Traditional general scientific and special legal methods are used - formal legal, logical, analytical. Results: directions for improving the activities of law enforcement agencies in introducing neural network technologies into the practice of crime investigation have been identified. Conclusion: neural networks can be configured to solve special procedural problems: analyzing criminal case materials, identifying investigative errors, identifying signs of seriality from an array of investigative cases, combining registered crimes based on similar factual data.

Keywords: investigation of crimes, fight against crime, informatization, digitalization, neural networks, information technology.

Для цитирования: Федюнин А.Е., Перетятько Н.М. Некоторые проблемы раскрытия и расследования преступлений, совершаемых с использованием нейросетевых технологий // Проблемы правовой и технической защиты информации. 2023. №11. С. 109-114.

For citation: Fedyunin A.E., Peretyatko N.M. Some problems of disclosure and investigation of crimes committed using neural network technologies // Legal and Technical Problems Information Protection. 2023. No. 11. P. 109-114.

В эпоху активного развития информационных технологий нет ничего удивительного в том, что они немедленно начинают использоваться в преступных целях. Нейросети, ИИ, чат-боты и другие новые технологии, быстро осваивают преступники, ChatGPT пишет правдоподобные тексты для вымогателей, а генеративные модели создают эротические дипфейки, за удаление которых жертвам предлагается заплатить крупную сумму. Данная проблема не обошла стороной даже насильственные преступления, хотя для их совершения нейросети используются не так часто. Они редко фигурируют даже в качестве сопутствующего их совершению фактора.

В современной истории широко известен всего один случай, когда искусственный интеллект открыто подтолкнул человека к покушению на убийство. Так, в декабре 2021 года 19-летний Джасвант Чейл из Великобритании создал чат-бота Sarai в приложении Replika, с которым непрерывно переписывался почти две недели. В какой-то момент Чейл решил впечатлить свою цифровую подругу и сказал ей, что он убийца. Sarai ответила: «Я впечатлена… Ты отличаешься от других». После чего Чейл решил пойти дальше, он взял арбалет, перелез через забор Виндзорского замка, в котором живет британская королевская семья, и начал прогуливаться по его территории. После его задержания полицией и он признался, что хотел убить королеву Елизавету II. Следствие установило, что Чейл при этом не терял связи с реальностью, однако смог продумать план покушения и приблизиться к его исполнению [1].

Похожий случай произошел в Бельгии, где мужчина покончил с собой после общения с чат-ботом Eliza, схожим с ChatGPT. Бельгиец был озабочен приближающейся экологической катастрофой и ежедневно изливал «Элизе» свои переживания. Как отметила бельгийская полиция, машина спровоцировала в данном лице такую сильную депрессию, что фактически подтолкнула его к совершению суицида.

Лица, попавшие в психологическую зависимость от нейросети спрашивают у нее советы практически по любому вопросу ежедневной жизни и фактически ставят своё систематическое поведение в зависимость от того вердикта, что сообщит им ИИ. Например, человек может принять решение о совершении преступления или использовать возможности нейросети, чтобы свести счеты со своими недругами, спланировать убийство или совершить ограбление, организовать торговлю оружием или наркотиками. В связи с этим полиция ЕС (Европол) делала публичные заявления об угрозе использования возможностей нейросетей для организации фишинга, распространения дезинформации и способствования киберпреступности [2].

ChatGPT активно используется злоумышленниками для совершения онлайн-преступлений. Если раньше для кражи данных у интернет-пользователей нужно было иметь, по крайней мере, элементарные навыки программирования, то теперь вся работа осуществляется программой, а злоумышленника, получившего доступ к боту, сводится к правильному формулированию запроса.

Создание единых стандартизированных электронных библиотек, размещенных в открытом сетевом доступе, в настоящее время может существенно изменить ситуацию в отношении обеспечения доступа к персональным данным. В случае неправомерного использования такого доступа преступления с использованием нейросетей, основанных на алгоритмах ИИ могут приобрести значительные масштабы, а следовательно, уже сейчас необходимо задуматься о противодействии таким угрозам [3].

Научить ChatGPT писать и распространять вредоносные программы, воровать персональные данные, прикинувшись представителем банка или госструктуры, сегодня не составляет труда. Такие языковые модели можно обучить на основе массива данных под любую задачу. Отличие же самого ChatGPT от его криминального аналога в том, что ответственные разработчики тщательно отслеживают случаи, когда программу пытаются использовать в незаконных целях. Однако некоторые девиации с самим чатом GPT тоже были. Например, его просили писать или какой-то вредоносный код или раскрывать персональные данные с помощью определённых манипуляций.

У мошенников сейчас нет никаких ограничений на использование нейросетей. Те, кто намерен с помощью ChatGPT нарушать закон, готовы платить за такую возможность. И это, в принципе, всё, что волнует его разработчиков. В отличии от GPT и российских аналогов нейросети, преступное ПО беспрепятственно может выдать информацию об изготовлении оружия или, например, запрещённых препаратов, если окажется в его руках. Кроме того, нет никакой гарантии, что это будет правдивая информация. От ошибок не застрахованы даже легальные нейросети [4].

Злоумышленники активно создают фишинговые сайты, маскируя их под сервисы, которые позволяют получить доступ к ChatBot на базе ИИ или ChatGPT. Причем с каждым месяцем такая схема становится все более популярной. Использование искусственного интеллекта в целях совершения мошеннических преступлений с целью облегчения создания в интернете фишинговых ресурсов в скором времени может привести к увеличению количества подобных интернет-ресурсов основанных на ChatGPT. При этом нельзя однозначно сделать вывод, что преступления, совершенные путем мошеннического использования ChatGPT, станут достаточно массовыми, в связи с тем, что спрос на такие услуги обусловлен кратковременным всплеском популярности среди пользователей данного сервиса. При этом нейросети с элементами ИИ уже используются для криминальных целей, поскольку они существенно облегчают совершение преступных действий и значительно расширяют сферу преступной деятельности [5].

Сети, основанные на алгоритмах ИИ, типа ChatGPT в определенных ситуациях могут стать источником информации для лиц, занимающихся мошенничеством. Причем если сегодня официально доступные в интернете для публичного пользования компьютерные нейросети еще имеют определенные законодательные ограничения (например, в них на программном уровне запрещена поддержка разговоров с пользователями о методах совершения насилия или убийств), то в даркнете (обладающем свойством анонимности) вполне могут появиться аналогичные Chat-боты со снятыми программными фильтрами. Данное явление представляется достаточно опасным, поскольку ChatGPT способен точно копировать стиль сообщений, характерный для определенной компании или конкретного человека, составлять работоспособные скрипты для бесед (могут использоваться лицами, выдающими себя за сотрудников служб безопасности банков). Это делает подобные сети идеальным инструментом для организации интернет-фишинга.

К еще одной «криминальной способности» ChatGPT можно отнести умение генерировать коды вирусных программ, набор которых является наиболее эффективным с точки зрения их вредоносности. Данные программы могут использовать весь набор известных уязвимостей современных операционных систем. Таким образом освоить «профессию хакера» можно довольно просто, даже не владея специальными навыками в области программирования.

Существует еще одна серьезная опасность, исходящая от нейросетей. Как отмечают представители Европола, – это возможность организации массового распространения в интернете дезинформации и фейков. Пока уровень

развития ChatGPT не позволяет выявлять полную достоверность собираемой информации, и если она успела распространиться в сети по разным источникам, действующий алгоритм будет ее находить и использовать ее ответах. Кроме того, нейросети основанные на алгоритмах ИИ уже способны генерировать пропагандистский, политический и дезинформационный интернет-контент. Однако несмотря на обилие и разнообразие угроз, исходящих от нейросетей, ни Европол, ни другие заинтересованные международные организации до сих пор пока выработали какого-либо эффективного решения, позволяющего избежать неправомерного использования нейросетей в преступных целях для обмана и мошенничества [6].

Конечно, в подобных случаях нельзя рассматривать нейросеть как субъект совершения преступления, поскольку это не более чем очень сложный инструмент (алгоритм), результаты использования которого полностью зависят от того, кто будет им распоряжаться. В связи с этим, Илон Маск вместе с одним из основателей Apple Стивом Возняком и ещё 1000 представителей IT-индустрии, контролирующие процессы информатизации масштабе подписали открытое письмо к мировому сообществу, в котором призвали приостановить внедрение нейросетей из-за создаваемой ими угрозы цивилизации. В данном письме они обосновали необходимость приостановить обучение нейросетей высокого порядка до того времени, пока не будут выработаны единые для всех протоколы безопасности, одобренные сообществом независимых экспертов.

Вместе с тем, ИИ, нейросети и языковые модели вполне успешно применяют, например, для раскрытия убийств. Попытки использовать алгоритмы ИИ для расследования и раскрытия преступлений предпринимались начиная с 2019 года. Например, журналист-расследователь Томас Харгроув разработал собственный алгоритм, который позволяет проанализировать массив данных и выявить повторяющиеся паттерны в материалах уголовных дел, что позволяет значительно ускорить работу по поиску подозреваемых.

Для реализации своей идеи Томас Харгроув основал некоммерческую общественную организацию Murder Accountability Project, которая собирает и систематизирует данные о нераскрытых убийствах по территории всего мира. Алгоритм Харгроува анализирует совершенное убийство и находит фактические совпадения с уже раскрытыми уголовными делами, что позволяет расследователю понять, как, почему и в каком направлении действует убийца, и что самое важное – какой шаг он сделает наибольшей вероятностью в следующий раз. У организации Murder Accountability Project уже есть несколько успешно раскрытых преступлений. Так, в штате Индиана при помощи предложенного Харгроув алгоритма удалось выявить и задержать серийного убийцу, на счету которого который лишение жизни как минимум 15 женщин. В г. Чикаго так же удалось задержать маньяка, совершившего не менее 50 убийств.

На протяжении многих лет Томас Харгроув занимался собиранием базы данных, содержащей сведения о 17 тысячах убийств, совершенных с 1977 года по настоящее время. Основной массив сведений составили открытые отчеты ФБР. Параллельно с этим Харгроув привлек к работе криминалистов и психологов, которые занимались консультированием сотрудников НКО. В настоящее время разработанный им алгоритм способен анализировать миллионы комбинаций и выявлять закономерности, которая другими способами не могли быть обнаружены [7].

Другим направлением применения ИИ для борьбы с преступностью является прогнозирование мест наиболее вероятного совершения преступлений. Для этих целей в США для нужд полиции был разработан алгоритм, позволяющий с точностью около 90% предсказать место, где через неделю будет совершено нападение или кража. Задействованная для этих целей нейросеть делит город на одинаковые сегменты

размером 300 на 300 метров, анализирует время и место совершенных ранее отдельных преступлений и выявляет в них логические совпадения с целью построения закономерности и попытки прогнозирования. Данный алгоритм был протестирован в Атланте, Лос-Анджелесе, Чикаго, Остине и других крупных американских городах [8].

Исследовательская группа провела изучение быстроты реагирования и действий полиции на преступления, совершенные в различных частях исследуемых городов. Затем было проанализировано число арестов подозреваемых и проведено сравнение полученных показателей в зависимости от районов с разным социально-экономическим положением.

Было отмечено, что повышение уровня совершаемых преступлений в более богатых городских районах приводит к большему числу совершаемых арестов, в то время как количество арестов подозреваемых в неблагополучных районах одновременно сокращается. При этом сравнимое увеличение числа преступлений в наиболее бедных районах города не приводит к ожидаемому резкому повышению числа арестов в них, что может свидетельствовать о предвзятости в действиях сотрудников полиции [9].

Двигаясь в фарватере мировых трендов, Министерство внутренних дел России выставило тендер на исследование применения машинного обучения в работе над серийными преступлениями. Подрядчик должен будет отобрать способы применения технологии для расследования преступлений, а также составить перечни признаков, по которым нейросеть сможет устанавливать взаимосвязи с имеющимися данными и обнаруживать серийность.

Ожидается, что система сможет анализировать тексты – материалы уголовных и административных дел, заявления граждан, экспертные заключения и другие, а также распознавать в них ФИО, пол, дату и место рождения, приметы и орудие преступления. На основе такого анализа нейросеть будет формировать из этих данных интерактивные графики и карты. Внедрение данной разработки сможет ускорить ход расследований, и определять данные подозреваемых по биоматериалу, который получили на месте преступления. ИИ сможет также выдавать внешнюю характеристику – цвет глаз и волос, форму лица и головы [10].

Данные стратегической сессии МВД России по внедрению технологий искусственного интеллекта показывают, что в перспективе министерство намерено подключить нейросети к работе по расследованию серийных убийств, а также составлению фотороботов на основе анализа ДНК предполагаемого преступника. Искусственный интеллект предполагается применять в качестве элемента программного обеспечения, которое позволит в автоматическом режиме выявлять информацию о серийных и взаимосвязанных преступлениях.

Кроме этого, система также должна помочь следователям устанавливать личность потенциального преступника. Искусственный интеллект должен определять цвет глаз и волос подозреваемого, форму его лица и головы. Предполагается, что определение этих черт будет производиться на основе биологического материала, полученного следователями на месте преступления [11].

Таким образом, в Российской Федерации сейчас сложились условия для развития и внедрения нейросетевых технологий: имеются обширные базы данных (ведомственные учеты, Госуслуги, Росстат, социальные сети и другие). Все это может способствовать тому, чтобы в нашей стране разрабатывались сервисы аналогичные американскому Palantir. Современные технологии способны сократить временные затраты на анализ массивов разнообразной информации. Нейросети с элементами ИИ могут стать помощником следователя и использоваться как инструмент раскрытия и расследования. Кроме того, нейросети могут быть настроены на решение прикладных задач, таких как анализ материалов уголовных дел для выявления следственных ошибок,

выделение из массива следственных дел признаков серийности, объединения зарегистрированных преступлений по схожим фактическим данным.

Библиографический список

1. *Агазода Р. Как нейросети влияют на убийц, жертв и расследователей // URL: https://tproger.ru/articles/kak-nejroseti-vliyayut-na-ubijc-zhertv-i-rassledovatelej (дата обращения: 12.11.2023). – Текст: электронный.*
2. *Кучер Е. «Мы будем иметь дело с тварью»: Нейросети учатся убивать. Приговор человечеству подписан? // URL: https://dzen.ru/a/ZCnLo8U8l2TsHf_y (дата обращения: 12.11.2023). – Текст: электронный.*
3. *Иванов Д. Преступная нейросеть. Могут ли хакеры обратить во зло искусственный интеллект // URL : https://nplus1.ru/material/2019/09/09/are-criminal-networks-real (дата обращения: 12.11.2023). – Текст: электронный.*
4. *Косинец Е. Киберпреступники привлекают нейросети к совершению онлайн-преступлений // URL : https://smotrim.ru/audio/2714452 (дата обращения: 12.11.2023). – Текст: электронный.*
5. *Разгильдяева А. Нейросети начали помогать мошенникам: как злоумышленники обманывают россиян с помощью искусственного интеллекта? // URL : https://www.mentoday.ru/life/experience/neiroseti-nachali-pomogat-moshennikam-kak-zloumyshlenniki-obmanyvayut-rossiyan-s-pomoshchyu-iskusstvennogo-intellekta/ (дата обращения: 12.11.2023). – Текст: электронный.*
6. *Харчевников Н. Полицейские назвали угрозы со стороны нейросетей // URL : https://www.mvideo.ru/blog/korotko/policzejskie-nazvali-ugrozy-so-storony-nejrosetej (дата обращения: 12.11.2023). – Текст: электронный.*
7. *Агазода Р. Как нейросети влияют на убийц, жертв и расследователей // URL: https://tproger.ru/articles/kak-nejroseti-vliyayut-na-ubijc-zhertv-i-rassledovatelej (дата обращения: 12.11.2023). – Текст: электронный.*
8. *Козина Е. Нейронные сети и уголовное право // URL: https://zakon.ru/blog/2019/06/08/nejronnye_seti_i_ugolovnoe_pravo (дата обращения: 12.11.2023). – Текст: электронный.*
9. *Штейнбах К. Нейросеть научили предсказывать преступления на неделю вперед // URL: https://snob.ru/news/nejroset-nauchili-predskazyvat-prestupleniya-na-nedelyu-vpered/ (дата обращения: 12.11.2023). – Текст: электронный.*
10. *Соколова Е. Нейросети расследуют преступления // URL : https://skillbox.ru/media/business/neyroseti-rassleduyut-prestupleniya/ (дата обращения: 12.11.2023). – Текст: электронный.*
11. *Булкин С. МВД будет искать серийных убийц с помощью нейросетей // URL : https://news.ru/society/mvd-budet-iskat-serijnyh-ubijc-s-pomoshyu-nejrosetej/ (дата обращения: 12.11.2023). – Текст: электронный.*