УДК 342.7

Д. М. Никеров,
К. Г. Карих,
П. Д. Сороковиков

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ И РИСКИ В ОБЛАСТИ ЗАЩИТЫ ТАЙНЫ ЧАСТНОЙ ЖИЗНИ

В статье анализируются масштабирование угроз национальной безопасности из-за стремительного развития инновационных технологий. Исследуются сферы жизни общества и государства, которые наиболее подвержены дестабилизации. В основе работы заложен понятийный аппарат искусственного интеллекта, нейросетей, централизованной и децентрализованной информационных систем, наравне с биометрией данных и цифровым следом, подчеркивается необходимость изучения их природы. Проведен сравнительный анализ различных систем, на основе чего и сделаны выводы о повышении преступности из-за облегчения выполнения объективной стороны преступлений, относящихся к категории виновных деяний против собственности, а именно хищение в форме мошенничества, рассмотрена и возможность увеличения латентности таких посягательств.

Ключевые слова: искусственный интеллект; нейросети; цифровой след; биометрические данные; интернет; мошенничество; тайна частной жизни; латентность.

D. M. Nikerov,
K. G. Karikh,
P. D. Sorokovikov

NEW THREATS AND CHALLENGES TO NATIONAL SECURITY DUE TO ARTIFICIAL INTELLIGENCE AND NEURAL NETWORKS

The article analyzes the scale of the threat to national security due to the rapid development of innovative technologies. It excludes the framework of the life of society and the state, which are especially susceptible to destabilization. The work is based on the conceptual apparatus of artificial intelligence, neural networks, centralized and decentralized information systems, compared with data biometrics and digital footprint, their nature is carefully studied. A comparative analysis of various systems was carried out on the basis of which the crime was detected due to facilitating the commission of the objective side of the crime, the identification of the category of guilty acts against property, namely theft in the form of fraud, consideration and increase in the possibility of latency of such attacks.

Keywords: artificial intelligence; neural networks; digital footprint; biometric data; internet; fraud; privacy; latency.

Стратегия национальной безопасности призвана обеспечить стабильное развитие Российского государства во всех сферах жизни общества. Развитие передовых технологий: искусственного интеллекта (ИИ) и нейросетей, безусловно может оказать значительное влияние на состояние защищенности общества и государства.

Закон Российской Федерации «О безопасности» предопределяет такую дефиницию, как безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних так и внешних угроз [2]. В свою же очередь, национальная безопасность отражает состояние защищенности национальных интересов Российской Федерации от двух видов угроз от внутренних и внешних угроз.

ИИ и нейросети из-за их несоразмерного и скоротечного развития могут стать не только внутренней, но и внешней угрозой национальной безопасности.

Понятие ИИ также дано законодателем РФ. ИИ — комплекс технологических решений, позволяющий имитировать 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 [3]. По нашему мнению, данная дефиниция во всей необходимой мере раскрывает признаки ИИ и его потенциал. Стоит различать нейросеть и ИИ, последний решает принципиально иные задачи, находящиеся на несравненно более высоком организационном этапе от первого. Нейросеть — минимальное представление об ИИ.

Авторы предполагают, что в первую очередью влияние ИИ будет оказано на такие сферы, как: дорожное движение, экономика, частная жизнь человека и гражданина, сельское хозяйство.

Тайна частной жизни является одним из составляющих элементов национальной безопасности каждого индивида, человек сам определяет для себя какая информация о его бытие должна быть неизвестна иным лицам. Однако с помощью передовых технологий тайна частной жизни может быть нарушена [1, с. 221]. «Интернет помнит все» такая цитата в полной мере реализуют функцию цифрового следа. Информационный (цифровой) след — сведения, возникающие в результате взаимодействия с сетью «Интернет» лицом, при использовании и (или) посещения разнообразных веб-сайтов.

Информационный след также бывает активным и пассивным. Активный — человек распространяет свои данные с умыслом, например, в социальных сетях. Пассивный — скрытый процесс, информация собирается без ведома индивида.

Невозможно скрыть полностью цифровой след, его можно уменьшить отметим, что при использовании ИИ либо нейросетей лицо будет использовать чужие данные и (или) виртуальную частную сеть (VPN), то отслеживание цифрового следа становится невообразимым.

Благодаря цифровому следу можно скомпрометировать данные, получаемые при посещении сайтов, однако такое возможно и при посещении разнообразных приложений на различные устройства, именно поэтому необходимо изучать политику конфиденциальности веб-сайтов, ресурсов и приложений, стоит обратить внимание на пункты, свидетельствующие о передаче данных третьим лицам.

Представляется возможным доработка функций, как отслеживание действий пользователя с последующим анализом массива собранных данных с помощью ИИ и (или) нейросетей. По сути своей подобный анализ уже реализуется, но с помощью современных технологий это все возможно не только масштабировать, классифицировать и прогнозировать поведение пользователя. Благодаря длительному анализу, например, три месяца, можно предопределить какое количество человек страдают от того или иного заболевания, и если для кого-либо такой факт индивид относится к тайне частной жизни, то не исключается момент мошеннических действий либо оказание давления для выполнения каких-либо деяний.

Также уже используется централизованная информационная система (далее — ЦИС) — одна из основных форм организации, обработки сведений (данных) и использования технических средств, которая базируется на сосредоточении вычислительных ресурсов информационных систем в едином центре (чаще всего это большие электронные вычислительные системы (ЭВМ) и вычислительные комплексы), которые обрабатывают в нем информацию, а затем передают результат пользователям.

ЦИС необходимо отличаться от частично или полностью децентрализованной информационной системы (ДИС). ДИС более тривиальная программа сточки зрения реализации, ее составляющих могут находится совершенно в дифференцированных юрисдикциях, что делает невозможным расследование различных преступлений так, как используются несколько серверов и она является более безопасной. Деятельность ЦИС сосредоточена на одном четко определенном сервере и уровень безопасности ниже. Как правило в ЦИС, имеет место монолитная организация с централизованным автократическом подходом к управлению. Монолитная архитектура означает, что все составляющие этой системе являются элементами единой программы.

Наиболее распространенным примером ЦИС является Интернет, а ДИС — Blockchain [4, с. 48].

Последствия взлома ЦИС и (или) ДИС или потеря контроля над ними носят критический характер, несут угрозу не только физическим или юридическим лицам, но и государству в целом. Можно констатировать, что на современном этапе централизация систем и их возможностей шагает в разы быстрее нежели чем развивается обеспечение их защиты, что несравнимо с ценностью хранящихся данных.

Угроза национальной безопасности в разы повышается, если в ЦИС и (или) ДИС используется биометрические данные.

Биометрия данных (они же биометрические данные) — особая идентификация личности, которая строится на своеобразных физиологических и поведенческих характеристик [5, с. 16]. С помощью таких данных удаленно можно получить доступ к изображению лица любого человека, кто ей подвергся вплоть до ДНК, а равно подпись, интонация голоса и прочие.

Взлом систем с биометрией влечет масштабирование последствий. С помощью таких данных можно получить доступ к устройствам с функцией FaceID, доступ к банковским счетам, (например, СберБанк собирает со своих пользователей биометрию, и их система является централизованной). Таким образом, нарушение тайны частной жизни с помощью ИИ либо нейросетей упрощает выполнение объективной стороны преступлений, предусмотренных ст. 159, 159.1, 159.3, 159.6 УК [6].

Представляется возможным и введение новых форм совершения преступных виновных деяний, на настоящий момент нам не известные и критически усложняет возможность раскрытия данных преступлений и привлечение к уголовной ответственности виновных лиц. Общественно виновные опасные посягательства носят латентный характер, обладая негоменной природой. Невозможность расследование преступлений при сливе данных, при отсутствии реальной возможности отслеживания цифрового следа. Таким образом, возрастут и латентные преступления, что несомненно окажет еще большее влияние на национальную безопасность Российской Федерации, хотя уже установлена методика расследования таких преступлений, однако в рамках современного прогресса данная методология будет неработоспобна.

Считается необходимым полное изучение природы приведенных понятий (ИИ, нейросетей, централизованной цифровой системы, биометрии данных) с точки зрения информационного составляющего для последующего четкого урегулирования деятельности умных систем. Безусловно надо определить четкие рамки их взаимодействия и сложных систем безопасности таких технологий.

Список использованной литературы

1. Данилина А. С. Конституционные основы гражданско-правового регулирования искусственного интеллекта в Российской Федерации / А. С. Данилина, Е. М. Якимова // Право и государство: теория и практика. — 2023. — № 6 (222). — С. 221–223.

2. О безопасности : федер. закон от 28 дек. 2010 г. № 390-ФЗ // СПС «КонсультантПлюс».

3. 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 статьи 6 и 10 Федерального закона «О персональных данных» : федер. закон от 24 апр. 2020 г. № 123-ФЗ // Собрание законодательства Российской Федерации. — 2020. — № 17. — Ст. 2701.

4. Передерий В. А. Децентрализованная информационная система сертификации специалистов на основе технологии Blockchain / В. А. Передерий, М. Л. Рысин // Международный журнал гуманитарных и естественных наук. — 2022. — № 5-2 (68). — С. 47–55.

5. Степенко В. Е. Биометрические персональные данные / В. Е. Степенко, А. Д. Богдановская // Евразийский Союз Ученых. — 2020. — № 4 (73). — С. 15–19.

6. Якимова Е. М. Концепция свободы предпринимательской деятельности через призму уголовно-правовой характеристики мошенничества / Е. М. Якимова // Всероссийский криминологический журнал. — 2019. — Т. 13, № 2. — С. 291–299.

Информация об авторах

Никеров Дмитрий Михайлович — доцент кафедры государственного права и национальной безопасности, Байкальский государственный университет, 664003, ул. Ленина, 11, г. Иркутск, Российская Федерация, e-mail: 009501@bgu.ru.

Карих Ксения Георгиевна — студент, Институт государственного права и национальной безопасности, Байкальский государственный университет, 664003, ул. Ленина, 11, г. Иркутск, Российская Федерация, e-mail: karihmwakeup@gmail.com.

Сороковиков Павел Дмитриевич — магистрант, кафедра математики и информационных систем, Байкальский государственный университет, 664003, ул. Ленина, 11, г. Иркутск, Российская Федерация, e-mail: gfifgfif31@gmail.com.

Authors

Nikerov Dmitry Mikhailovich — Associate Professor, the Department of Legal Support of National Security, Baikal State University, 664003, Lenin st., 11, Irkutsk, the Russian Federation, e-mail: 009501@bgu.ru.

Karikh Ksenia Georgievna — Student, Institute of State Law and National Security, Baikal State University, 664003, Lenin st., 11, Irkutsk, the Russian Federation, e-mail: karihmwakeup@gmail.com.

Sorokovikov Pavel Dmitrievich — Undergraduate student, Department of Mathematics and Information Systems, Baikal State University, 664003, Lenin st., 11, Irkutsk, the Russian Federation, e-mail: gfifgfif31@gmail.com.