Научная статья

УДК 351.355/359.07

doi: 10.34987/2712-9233.2024.63.59.004

Искусственный интеллект в борьбе с преступлениями коррупционной направленности

Андрей Александрович Архипов [1]
Евгений Вадимович Раков [1]
Ева Владиславовна Щербенко [2]

[1]*Министерство обороны Российской Федерации*
[2]*Сибирская пожарно-спасательная академия ГПС МЧС России*

Автор ответственный за переписку: Щербенко Ева Владиславовна, sherbenko.e@mail.ru

Аннотация. Представлены результаты анализа перспектив применения искусственного интеллекта (ИИ) для противодействия преступлениям коррупционной направленности. Показаны общие преимущества использования ИИ в сфере обеспечения безопасности государства. Отмечена возможность возникновения ситуаций, подпадающих под действие уголовно – правовой сферы и одновременное несовершенство соответствующей нормативно-правовой базы применения ИИ. Приведены примеры действий ИИ, противоречащих этике и нарушающих права людей. Акцентирована необходимость выработки мер противодействия негативным юридическим и этическим последствиям использования ИИ, в т.ч. международных стандартов его применения. Обобщены направления работы алгоритмов ИИ против коррупции, сделан вывод о современном состоянии легитимности применения технологии в рамках уголовного преследования, показан опыт КНР по реализации проекта Zero Trust, приведены цели и задачи ГИС «Посейдон» и её возможности для повышения эффективности государственного управления.

Ключевые слова: Противодействие коррупции, искусственный интеллект, преступления с использованием искусственного интеллекта, легитимность применения искусственного интеллекта

Для цитирования: Архипов А.А., Раков Е.В., Щербенко Е.В. Искусственный интеллект в борьбе с преступлениями коррупционной направленности // Актуальные проблемы безопасности в техносфере 2024. № 3 (15) С.24-30. URL:https://doi.org/ 10.34987/2712-9233.2024.63.59.004

Artificial intelligence in the fight against corruption-related crimes

Andrey A. Arkhipov [1]
Evgeny V. Rakov [1]
Eva V.Shcherbenko [2]

[1]*Ministry of Defense of the Russian Federation*
[2]*Siberian Fire and Rescue Academy EMERCOM of Russia*

Corresponding author: Eva V. Shcherbenko, sherbenko.e@mail.ru

Abstract. The results of the analysis of the prospects for the use of artificial intelligence (AI) to counter corruption-related crimes are presented. The general advantages of using AI in the field of state security are

shown. The possibility of situations falling within the scope of the criminal law sphere and the simultaneous imperfection of the relevant regulatory framework for the use of AI is noted. Examples of AI actions that contradict ethics and violate human rights are given. The need to develop measures to counteract the negative legal and ethical consequences of using AI, including international standards for its application, is emphasized. The directions of AI algorithms against corruption are summarized, a conclusion is made about the current state of the legitimacy of the use of technology in criminal prosecution, the experience of the People's Republic of China in implementing the Zero Trust project is shown, the goals and objectives of Poseidon GIS and its possibilities for improving the efficiency of public administration are presented.

Keywords: Anti-corruption, artificial intelligence, crimes using artificial intelligence, the legitimacy of the use of artificial intelligence

For citation: Arkhipov A.A., Rakov E.V., Shcherbenko E.V. The prospect of using artificial intelligence in the fight against corruption-related crimes // Actual problems of safety In the technosphere 2024. No. 3 (15). P. 24-30. URL:https://doi.org/ 10.34987/2712-9233.2024.63.59.004

Цифровая трансформация рассматривается как одно из ведущих направлений развития различных сфер современного общества. Внедрение сквозных технологий является приоритетной задачей ведущих мировых держав и тех стран мира, которые показывают высокие темпы развития. В Российской федерации вопросам цифровых технологий также уделяется особое внимание, приоритетно формируемое на самых верхних эшелонах власти.

Термин «сквозные» используется в силу того, что данные технологии носят глобальный характер применения, не ограничены каким-либо конкретным продуктом или областью деятельности, формируют возможности прорывного развития в различных отраслях и секторах экономики и определяют их перспективный облик в течение ближайших 10-15 лет.

В «Концепции технологического развития на период до 2030 года», утвержденной распоряжением Правительства Российской Федерации № 1315-р от 20 мая 2023 года [3] приведено следующее определение: сквозные технологии (технологические направления) – перспективные технологии межотраслевого назначения, обеспечивающие создание инновационных продуктов и сервисов и оказывающие существенное влияние на развитие экономики, радикально меняя существующие рынки и (или) способствуя формированию новых рынков.

Сквозные технологии играют важную роль в цифровизации, формируя основу создания гибкой и адаптивной инфраструктуры на основе цифровых инноваций. Их использование выступает наиболее продуктивным и важным способом цифровой трансформации, который предполагает слияние различных технологий и процессов внутри субъекта цифровизации в целях улучшения управления бизнес-процессами и обработки данных, встраивая его в современные экосистемные форматы деятельности.

Одной из основных сквозных технологий, активно расширяющей сферы своего применения, выступает искусственный интеллект [6]. В «Национальной стратегии развития искусственного интеллекта на период до 2030 года» [1] закреплено следующее определение: … «искусственный интеллект (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». Элементами такого комплекса выступает информационно-коммуникационная инфраструктура, программное обеспечение (в т.ч. с использованием машинного обучения), а также процессы и сервисы по обработке данных и поиску решений.

В настоящее время ИИ применяется практически во всех сферах деятельности человека, формируя новые векторы и перспективы их развития. В частности, в сфере безопасности государства ИИ может значительно улучшить возможности предотвращения угроз и эффективность обеспечения общественной безопасности. Общими преимуществами использования ИИ являются:

- улучшение производительности и эффективности работы;
- автоматизация рутинных задач;
- повышение точности и качества принимаемых решений;
- повышение скорости обработки и анализа больших объемов данных;
- улучшение опыта пользователей за счет персонализированных рекомендаций;

- автоматическое обнаружение и предотвращение кибератак;
- улучшение прогнозирования и планирования;
- снижение затрат на операции и обслуживание;
- создание новых возможностей для инноваций и развития бизнеса;
- улучшение безопасности и надежности систем.

Однако, ряд специалистов отмечает [4,10], что применение ИИ порождает возможность возникновения ситуаций, подпадающих под действие уголовно – правовой сферы, в том числе:

- совершение ИИ такой ошибки, которая впоследствии приведет к совершению преступления;
- создание и запуск ИИ субъектами противоправных действий в целях совершения преступлений;
- принятие ИИ решений, которые могут квалифицироваться как преступление.

В связи с этим, в случае нарушения при применении ИИ действующего законодательства, возникает немаловажный вопрос – кто несет ответственность за данные правонарушения: разработчик ИИ, эксплуатант ИИ или оператор? [5]

Следует отметить, что в настоящее время этот аспект находится за рамками правового поля, в т.ч. и российского законодателя [4,7]. В одной плоскости таких негативных эффектов находится этическая и социальная ответственность за отсутствие неблагоприятного воздействия на граждан и общество. Зафиксированных примеров действий ИИ, противоречащих этике и нарушающих права людей немало:

- в 2017 году в США был создан ИИ-сервис, который с вероятностью 81 % для мужчин и 74 % для женщин распознает по лицу людей с нетрадиционной сексуальной ориентацией [11]. В открытом доступе такая технология может повлечь непредсказуемые последствия, особенно в странах, основной религией которых является ислам.

- ИИ-сервис DeepGestalt по фотографии лица с высокой долей вероятности определяет редкие генетические заболевания [12]. Данный сервис создан для использования в медицинских целях, но при применении его, например работодателем, в отношении соискателя может быть принято решение об отказе в трудоустройстве.

- нейросеть GPT-4 для решения теста, предназначенного для защиты от роботов, самостоятельно «наняла» фрилансера на сайте вакансий, который решил данный тест [14]. Для этого нейросеть ввела в заблуждение человека, попросив помочь решить поставленную задачу, объяснив просьбу о помощи проблемами со зрением. Таким образом, для достижения цели ИИ использовал возможности человека в своих интересах.

Для выработки возможных корректирующих направлений развития технологии, такие негативные проявления в применении ИИ становятся сферой специальных исследований. Так, сотрудники журнала Crime Science [13] определили рейтинг возможных преступлений с использованием ИИ:

1. Подделка фотографий и видео. Например, с помощью нейросети Deepfake генерируются высококачественные видео, которые практически не отличаются по качеству от реального видеоконтента.
2. Использование беспилотных автомобилей в качестве оружия.
3. Создание продвинутых фишинговых сообщений. Целью таких сообщений является получение паролей или данных банковских карт пользователей.
4. Нарушение систем под управлением других ИИ.
5. Массовый несанкционированный сбор личной информации о пользователях.
6. Фейковые новости, созданные ИИ.
7. Крупномасштабный шантаж.
8. Неправильное использование беспилотной военной техники.
9. Манипулирование финансовыми рынками.
10. Преследования с помощью ИИ.

Таким образом, обществу необходимо учитывать и противодействовать такого рода проявлениям, вырабатывать противодействия негативным юридическим и этическим последствиям использования возможностей технологии ИИ. Справедливо полагать, что данный аспект имеет политическое измерение, связанное с возможными негативами её распространения (в т.ч. это проблемы обеспечения конфиденциальности и безопасности данных, кибермошенничество, киберпреступность, преступления в отношении интеллектуальной собственности и т. д.). Формирование безопасной среды повсеместного

использования ИИ требует выработки некоторых международных стандартов его функционирования, сотрудничества государств, компаний и ученых.

В тоже время, использование возможностей ИИ соответствует условиям непредвзятости и беспристрастности, в отличие от действий человека. Невозможность влияния на процессы, проводимые ИИ, обеспечивает объективную оценку действий лиц, склонных к совершению преступлений, а также непосредственное предупреждение противоправных действий. Так повсеместное распространение ИИ привело к использованию интеллектуальных систем в криминологии, ИИ всё чаще используется на различных стадиях уголовного процесса. [9] Противодействие преступлениям коррупционной направленности не стало исключением.

Одним из самых главных условий борьбы с коррупцией является неотвратимость наказания для субъектов противоправных действий. В настоящее время ИИ применяется для прогнозирования возможных преступлений, предсказания результатов уголовного процесса, повышения эффективности управления уголовным процессом. Электронная почта, социальные сети, зашифрованные чаты и сообщения в WhatsApp стали основными источниками ключевых доказательств при расследовании тяжких преступлений и выявлении их исполнителей. [9]

Исследования проблем применения ИИ в сфере противодействия коррупции, важным вопросом выявляют легитимность его применения. В настоящее время законодательная база, регулирующая данный процесс практически отсутствует и проявляется это как на национальном, так и на международном уровне [4,7]. ИИ в рамках уголовного преследования можно использовать только как источник дополнительной информации, которую необходимо преобразовывать в доказательную базу. Данный факт объясняет особо активное развитие применения ИИ непосредственно в профилактике коррупционных действий.

Исследование [4,8,9] позволяет обобщить, что работа алгоритмов ИИ против коррупции формируется по ряду основных направлений:

1. Анализ данных. ИИ может проводить анализ больших объемов данных для обнаружения потенциальных случаев коррупции и неэффективного управления. Алгоритмы машинного обучения могут обнаруживать аномалии и необычные изменения в финансовых транзакциях или бизнес-процессах, что может указывать на возможные случаи коррупции.

2. Мониторинг государственных закупок. ИИ может использоваться для автоматического анализа процедур государственных закупок и обнаружения признаков коррупции или нечестных практик, таких как завышенные цены или отсутствие конкуренции.

3. Разработка алгоритмов прозрачности и открытости. ИИ может использоваться для создания алгоритмов, обеспечивающих прозрачность и открытость процессов. Например, ИИ может помочь определить оптимальные методы распределения ресурсов, а также контроля за выполнением контрактов и процедур.

4. Автоматизация сбора и анализа жалоб и обращений. Системы искусственного интеллекта могут быть использованы для автоматизации сбора и анализа обращений граждан и работников на предмет выявления возможных случаев коррупции в государственных органах и компаниях.

Перспективность и эффективность применения ИИ для борьбы с коррупцией доказывает опыт иностранных государств. В КНР в 2012 году запущен проект Zero Trust («Нулевое доверие») [8,10]. Это концепция безопасности информации, которая подразумевает, что ни один узел или пользователь в сети не должен быть автоматически достоверным. Каждый запрос на доступ к ресурсам должен быть проверен и авторизован независимо от источника запроса. Все пользователи системы, даже внутренние, должны проходить аутентификацию и авторизацию, в той усиленной мере, как если бы они были внешними угрозами.

С помощью алгоритмов Zero Trust был проведен анализ закрытых баз данных результатов работы чиновников, который основывался на сопоставлении деятельности отдельно взятого чиновника с деятельностью других должностных лиц на предмет определения возможных случаев коррупции, растрат и конфликта интересов. Алгоритмы позволяли вычислять незаконную передачу имущества, подозрительные приобретения земли и недвижимости. При этом информация использовалась из 150 различных баз данных, что позволяло находить несоответствия в данных, представляемых чиновниками. Также ИИ имел доступ к фотографиям со спутников в режиме реального времени в целях подтверждения строительства объектов, на которые выделяется государственное финансирование. Система также

производила мониторинг банковских счетов не только самого чиновника, но и членов семей и близких лиц, на предмет необычных изменений. При наличии нелогичных изменений система высчитывала процент вероятности коррумпированной активности. Если данный процент превышал установленные пределы, ИИ сообщал об этом заинтересованным лицам. За первые пять лет работы алгоритмы Zero Trust помогли поймать 8721 коррупционеров. Однако, в настоящее время большинство провинций КНР отказались от использования проекта Zero Trust по различным причинам [8,15]. Данный пример отчетливо показывает конфликт интересов лиц, заинтересованных в проведении антикоррупционной деятельности, и лиц, являющихся объектами контроля (чиновники), которые против нахождения под постоянным наблюдением и обладают значимым административным ресурсом для препятствования проведению антикоррупционной политики и ее мероприятиям. Таким образом, одним из главных элементов успешной реализации технологий в борьбе с коррупцией является политическая воля руководства страны.

В 2022 г. указом Президента РФ Владимира Путина в России запущен в работу аналог китайского проекта Zero Trust – государственная информационная система Посейдон (Указ от 25 апреля 2022 года № 232 «О государственной информационной системе в области противодействия коррупции «Посейдон» и внесении изменений в некоторые акты Президента Российской Федерации») [2].

Основная цель ГИС "Посейдон" заключается в создании прозрачной и контролируемой среды для государственных служащих в целях выявления коррупционных действий. Система нацелена на то, чтобы сделать коррупцию невыгодной и рискованной, тем самым стимулируя чиновников к соблюдению законодательства и этических норм [4]. Основными задачами ГИС «Посейдон» являются [2]:

- автоматизация включения в систему "Посейдон" информации, предоставляемой поставщиками информации, ее сбора, учета, хранения и анализа, а также предоставления информации, содержащейся в системе "Посейдон" (получения доступа к ней);

- информационно-аналитическое обеспечение деятельности внутренних и внешних пользователей системы "Посейдон" по проведению анализа и проверок соблюдения ограничений, запретов и требований, установленных в целях противодействия коррупции, лицами, на которых распространены такие ограничения, запреты и требования;

- формирование на основании запросов внутренних и внешних пользователей системы "Посейдон" статистических и информационно-аналитических материалов по вопросам противодействия коррупции;

- информационное взаимодействие системы "Посейдон" с другими информационными системами, содержащими информацию, которая может быть использована в целях противодействия коррупции.

ГИС "Посейдон" обладает широкими возможностями доступа к разнообразным источникам данных, таким как официальные базы данных, социальные сети и служебные документы. Система проводит анализ этих данных для выявления ситуаций, когда государственные служащие маскируют свою собственность, передавая права на нее третьим лицам, например, родственникам или друзьям [9]. Кроме того, "Посейдон" следит за финансовыми расходами, что позволяет оценить соответствие между доходами и тратами лиц, на которых распространяются коррупционные ограничения.

Согласно замыслу авторов системы, обычный государственный служащий, осознавая постоянный надзор со стороны системы, должен избегать коррупционных действий. Это позволит сделать коррупционные схемы менее эффективными и увеличить прозрачность работы государственной системы.

К сожалению, в настоящее время в открытых источниках пока не накоплена информация, системно обобщающая эффективность работы ГИС «Посейдон».

Задачей исследования был поставлен анализ проблем и рисков, вызванных внедрением ИИ в процессы борьбы с коррупцией и тех аспектов, которые способны существенно повлиять на них. Исследование осуществлялось посредством контент-анализа публикаций в области изучаемой тематики.

Описанные в статье процессы, их качественные и количественные аспекты важны для дальнейшего изучения, поскольку рассматриваемая технология стремительно развивается. Соответственно, требует дальнейшей оценки и детализации риски и ограничения её применения. Применение ИИ в борьбе с коррупцией представляет собой эффективное направление, которое может кардинально изменить подходы к противодействию этому глобальному явлению.

Этот инструмент повышает эффективность расследований, снижает зависимость от человеческого фактора и выявляет потенциальные конфликты интересов. Однако, внедрение ИИ в антикоррупционные стратегии требует тщательной регуляции и защиты данных, чтобы избежать злоупотреблений и нарушений прав человека. Результаты исследований приводят к выводу, что ИИ не может полностью заменить человеческий опыт, интуицию и должен использоваться как дополнение к существующим методам. Использование искусственного интеллекта в борьбе с коррупцией открывает новые возможности для прозрачности, подотчетности и эффективности государственного управления и требует сбалансированного подхода, который сочетает в себе технологические инновации с сохранением основных демократических ценностей и прав граждан.

Список использованных источников:

1. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (утверждает Национальную стратегию развития искусственного интеллекта на период до 2030 года) //Гарант: справочно-правовая система [Офиц. сайт]. URL: http://www. base.garant.ru/ (дата обращения 06.06.2024).

2. Указ Президента РФ от 25 апреля 2022 г. № 232 «О государственной информационной системе в области противодействия коррупции «Посейдон» и внесении изменений в некоторые акты Президента Российской Федерации» (ред. 26 октября 2023 г.) //Гарант: справочно-правовая система [Офиц. сайт]. URL: http://www. base.garant.ru/ (дата обращения 06.06.2024).

3. Распоряжение Правительства РФ от 20 мая 2023 г. № 1315-р «Об утверждении Концепции технологического развития на период до 2030 г.» //Гарант: справочно-правовая система [Офиц. сайт]. URL: http://www. base.garant.ru/ (дата обращения 06.06.2024).

4. Корякин В.М. Внедрение цифровых технологий в деятельность по профилактике коррупционных правонарушений / В. М. Корякин // Вестник Юридического института МИИТ. – 2022. – № 2(38). – С. 14-24. – EDN PNPGLA.

5. Некрасов В.Н. Уголовно-правовая охрана общественных отношений в сфере инновационной деятельности: дис. доктора юридических наук: 5.1.4. / Некрасов Василий Николаевич; [Электронный ресурс]. – Режим доступа: URL: https://search.rsl.ru/ru/record/01011577165 (дата обращения 06.06.2024).

6. Подшивалова Т. П. Право цифровой среды / Т. П. Подшивалова, Е. В. Титова, Е. А. Громова. – Москва : Проспект, 2022. – 896 с.

7. Чукин Д. С. Посейдон: как Бог морей поможет бороться с коррупцией / Д. С. Чукин, И. Р. Маллаалиев // Известия Саратовского военного института войск национальной гвардии. – 2022. – № 3(8). – С. 116-121. – EDN UHAYDX.

8. Избавит ли искусственный интеллект человечество от коррупции [Электронный ресурс]. – Режим доступа: URL: https://www.techinsider.ru/science/731753-izbavit-li-iskusstvennyy-intellekt-chelovechestvo-ot-korrupcii (дата обращения 06.06.2024).

9. Сикач А. С. Роль искусственного интеллекта в противодействии коррупции / А. С. Сикач // Аллея науки. – 2022. – Т. 1, № 7(70). – С. 327-338. – EDN FFDHWQ.

10. Высокотехнологичное право: современные вызовы: материалы IV Международной межвузовской научно-практической конференции (17-20 февраля 2023 года, Москва – Красноярск) / Национальный исследовательский университет «Московский институт электронной техники»; Красноярский государственный аграрный университет. Часть 1. – Красноярск, 2023. – 336 с.

11. Искусственный интеллект научили по лицу определять политические убеждения [Электронный ресурс]. – Режим доступа: URL: https://www. rg.ru/2021/01/19/iskusstvennyj-intellekt-nauchili-po-licu-opredeliat-politicheskie-ubezhdeniia.html (дата обращения 06.06.2024).

12. Искусственный интеллект может диагностировать редкие генетические нарушения по фотографии лица [Электронный ресурс]. – Режим доступа: URL: https://www. https://scientificrussia.ru/articles/iskusstvennyj-intellekt-mozhet-diagnostirovat-redkie-geneticheskie-narusheniya-po-fotografii-litsa (дата обращения 06.06.2024).

13. AI-enabled future crime (преступления будущего с помощью искусственного интеллекта) [Электронный ресурс]. – Режим доступа: URL:

https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8 (дата обращения 06.06.2024).

14. ChatGPT-4 обошел капчу, наняв фрилансера и притворившись слепым человеком [Электронный ресурс]. – Режим доступа: URL: https://rb.ru/news/chatgpt-4-captcha (дата обращения 16.07.2024)

15. Is China’s corruption-busting AI system being turned off for being too efficient? (Неужели китайскую систему искусственного интеллекта, борющуюся с коррупцией, отключают из-за того, что она слишком эффективна?) [Электронный ресурс]. – Режим доступа: URL: https://www.techinasia.com/chinas-corruptionbusting-ai-system-trust-turned-efficient (дата обращения 06.06.2024)

Информация об авторах

Е.В. Щербенко – доктор экономических наук, доцент

Information about the author

E.V. Shcherbenko - Holder of an Advanced Doctorate (Doctor of Science) in Economic Sciences, Docent

Статья поступила в редакцию 29.07.2024, одобрена после рецензирования 27.08.2024, принята к публикации 25.09.2024.

The article was submitted 29.07.2024, approved after reviewing 27.08.2024, accepted for publication 25.09.2024