DOI: 10.31696/S086919080032578-2

ЗЛОНАМЕРЕННОЕ ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И УГРОЗЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В ОБЪЕДИНЁННЫХ АРАБСКИХ ЭМИРАТАХ[1]

Е.Н. ПАШЕНЦЕВ [a, b], В.А. ЧЕБЫКИНА [a, c]

[a] – Санкт-Петербургский государственный университет, Санкт-Петербург, Россия
[b] – Дипломатическая академия МИД России, Москва, Россия
ORCID: 0000-0001-5487-4457; icspsc@mail.ru
[c] – Международный центр социально-политических исследований и консалтинга, Москва, Россия
ORCID: 0009-0003-5031-3339; sj.vvladilena@gmail.com

Резюме: *Статья посвящена анализу рисков, связанных со стремительным развитием технологий искусственного интеллекта (ИИ) в Объединённых Арабских Эмиратах (ОАЭ) и их влиянием на информационно-психологическую безопасность. С момента своего основания ОАЭ превратились в значимого игрока на международной арене благодаря стремительному развитию экономики, торговли и инноваций. Тем не менее, наряду с положительными аспектами внедрения ИИ, возникают и значительные риски, связанные с его злонамеренным использованием (ЗИИИ). Угрозы ЗИИИ рассматриваются авторами через призму трёхуровневой классификации: от распространения ложных представлений об ИИ и последствиях его развития, угроз критической инфраструктуре, до целенаправленных атак, нацеленных на подрыв информационно-психологической стабильности в государстве. Авторы подчёркивают, что ОАЭ, находясь в геополитически нестабильном регионе, сталкиваются с увеличением числа злонамеренных акторов, что делает страну уязвимой для операций по социальной дестабилизации. Проблема ЗИИИ при этом имеет тенденцию к обострению и охватывает все три уровня угроз. Первый уровень связан с манипуляциями на тему роста уровня безработицы и угроз личной безопасности, которые могут быть вызваны внедрением ИИ. На втором уровне наибольшие риски представляют виртуальное мошенничество, в том числе через использование чат-ботов, а также хакерские атаки на объекты критической инфраструктуры государства. Анализ третьего уровня угроз показал, что в обществе возросло беспокойство по поводу способности посредством ИИ создавать фейковую информацию и активно продвигать её в виртуальном пространстве. Часто граждане сами становятся жертвами использования таких технологий из-за излишней доверчивости и недостаточной осведомлённости о рисках в Интернете. В статье акцентируется внимание на необходимости усиления мер по обеспечению кибербезопасности и разработке комплексных стратегий по противодействию ЗИИИ с целью обеспечения положительной динамики в противостоянии угрозам, связанным со злонамеренным использованием ИИ в ОАЭ.*

Ключевые слова: искусственный интеллект, информационно-психологическая безопасность, Объединённые Арабские Эмираты, злонамеренное использование искусственного интеллекта, кибербезопасность, дипфейки

[1] Работа Е.Н. Пашенцева выполнена при поддержке СПбГУ, шифр проекта 116471555.

Для цитирования: Пашенцев Е.Н., Чебыкина В.А. Злонамеренное использование искусственного интеллекта и угрозы информационно-психологической безопасности в Объединённых Арабских Эмиратах. *Восток (Oriens).* 2024. № 6. С. 107–117. DOI: 10.31696/S086919080032578-2

MALICIOUS USE OF ARTIFICIAL INTELLIGENCE AND THREATS TO INFORMATION AND PSYCHOLOGICAL SECURITY IN THE UNITED ARAB EMIRATES[2]

© 2024 Evgeny N. PASHENTSEV [a, b], Vladilena A. CHEBYKINA [a, c]

[a] – Saint Petersburg State University, Saint Petersburg, Russia
[b] – Diplomatic Academy of the MFA of the Russian Federation, Moscow, Russia
ORCID: 0000-0001-5487-4457; icspsc@mail.ru
[c] – International Centre for Social and Political Studies and Consulting, Moscow, Russia
ORCID: 0009-0003-5031-3339; sj.vvladilena@gmail.com

Abstract: *The article analyzes the risks associated with the rapid development of artificial intelligence (AI) technologies in the United Arab Emirates (UAE) and their impact on psychological security. Along with the positive aspects of AI adoption, there are also significant risks associated with its malicious use (MUAI) in an advanced country. The authors consider the threats of malicious use of AI through the prism of a three-level classification: from the spread of misconceptions about AI and the consequences of its development, to targeted attacks aimed at undermining psychological stability in the state. The authors emphasize that the challenges for the country become pressing and encompass all three threat levels. The first level is related to the manipulation of rising unemployment rates and threats to personal security that can be caused by the introduction of AI. At the second level, the greatest risks are virtual fraud, including through the use of chatbots, as well as hacker attacks on critical infrastructure of the state. Analysis of the third level of threats has shown that there is growing public concern about the ability of AI to create fake information and actively promote it in virtual space. Citizens often fall victim to the use of such technologies themselves due to their excessive gullibility and insufficient awareness of online risks. The article emphasizes the need to strengthen cybersecurity measures and develop strategies to counter MUAI in order to ensure a positive trend against the threats posed by the malicious use of AI in the UAE.*

Keywords: artificial intelligence, psychological security, United Arab Emirates, malicious use of artificial intelligence, cybersecurity, deepfakes

For citation: Pashentsev E.N., Chebykina V.A. Malicious Use of Artificial Intelligence and Threats to Information and Psychological Security in the United Arab Emirates. *Vostok (Oriens).* 2024. No. 6. Pp. 107–117. DOI: 10.31696/S086919080032578-2

ВВЕДЕНИЕ

Бурное развитие торговли, туризма, промышленности превратило ОАЭ в глобальный центр бизнеса, инноваций и культурного обмена [Burt, 2024]. ОАЭ стали первой страной

[2] E.N. Pashentsev acknowledges Saint-Petersburg State University for a research project 116471555.

на Ближнем Востоке, где в 2017 г. было создано Министерство искусственного интеллекта. Это событие ознаменовало запуск Национальной стратегии по искусственному интеллекту до 2031 г. Практически все банки страны уже внедрили системы на основе ИИ – чат-боты, виртуальные помощники [Mehta, Bhavani, 2017]. В 2019 г. мир стал свидетелем открытия в Дубае первого в мире Университета искусственного интеллекта [*Khaleej Times*, 16.10.2019]. Это учреждение было создано для развития необходимой экосистемы ИИ на всех уровнях – от образования и науки до бизнеса и государственного управления. На Всемирном правительственном саммите в Дубае в феврале 2024 г. министр ОАЭ по вопросам ИИ Омар аль-Олама подчеркнул, что к сентябрю 2023 г. количество людей, занятых в сфере ИИ или смежных с ним отраслях, возросло до 120 000 человек по сравнению с 30 000 двумя годами ранее [Al Olama, 2024].

Однако вместе с развитием ИИ появляются и проблемы, связанные с его злонамеренным использованием (ЗИИИ). Они всё более актуальны в стране, которая, несмотря на высокий уровень социально-политической стабильности, находится в регионе с высоким уровнем конфликтности.

В процессе работы над статьей были использованы документы органов государственной власти ОАЭ, отражающие различные аспекты регулирования ИИ-отрасли, а также экспертные доклады по различным аспектам кибербезопасности, рисков ИИ, ЗИИИ. Данная работа подготовлена с использованием широкого пласта академических исследований в области социальных аспектов применения искусственного интеллекта в ОАЭ [Chenguel, 2023; Faraz et al., 2022; Keding, 2021; Mehta, Bhavani, 2017; Halabi, Hill, 2024; Khansaheb, 2024; Sajwani, 2024; AlGhanem, Abdallah, 2024], правового регулирования ИИ [Nakkach, 2021; Safar-Aly, 2024], использования ИИ как преступниками, так и правоохранительными органами [Othman, Al Hammadi, 2022; Sukhodolov et al., 2020, Keding, 2021; Alshamsi, Al-Kumaim, 2021], а также общих работ по проблемам социально-политического развития ОАЭ и других стран Ближнего Востока с целью определения общего контекста ЗИИИ и его последствий [Burt, 2024; Salameh, Benkohila, 2024; Smith, Zeigler, 2017; Matheson, 2020].

Для анализа угроз информационно-психологической безопасности с использованием ЗИИИ применяется трехуровневая классификация. На *первом уровне* происходит распространение ложного образа ИИ, последствий его развития и применения. *Второй уровень угроз* связан с практикой ЗИИИ, когда атака на общественное сознание не является основной целью, но имеет негативные для него последствия. ЗИИИ, направленное в первую очередь на нанесение ущерба в информационно-психологической сфере, можно выделить как *третий и высший уровень угроз* (см. подр.: [Pashentsev, 2023]).

Угрозы, продуцируемые ЗИИИ, становятся всё более актуальными во всём мире на всех трех уровнях по мере роста политического соперничества, активности различных государственных и негосударственных антисоциальных акторов, а также развития и растущей доступности технологий ИИ, что делает возможным их широкое злонамеренное применение.

ПЕРВЫЙ УРОВЕНЬ УГРОЗ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПОСРЕДСТВОМ ЗЛОНАМЕРЕННОГО ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

С широким распространением технологий ИИ и интеграцией автоматизированных систем в повседневную жизнь общества ОАЭ на первый план среди угроз первого уровня выходят целенаправленные спекуляции на фоне растущих опасений относительно потенциальной потери миллионов рабочих мест. В ближайшие 15 лет ИИ создаст в ОАЭ более 2,5 млн рабочих мест. Министерство человеческих ресурсов и эмиратизации (MOHRE) –

регулирующий орган по вопросам труда и занятости в ОАЭ, опубликовало список, согласно которому большинство вакансий в ОАЭ в ближайшее десятилетие будут связаны с ИИ, машинным обучением и автоматизацией [Tabrez, 2022].

Правительство ОАЭ финансирует образовательные инициативы, направленные на создание кадрового резерва в области инноваций, включая бесплатные курсы для людей, желающих повысить свои навыки в области информационных технологий [Alrahmah, Ahmed, 2024]. Однако этого часто оказывается недостаточно для того, чтобы люди перестали опасаться за свою конкурентоспособность на рынке труда. В опросе, который был проведен в ОАЭ, респондентам задавали вопрос, как они считают, повлияет ли ИИ на их жизнь. 55% опрошенных выразили беспокойство по поводу того, что к 2033 г. их рабочие обязанности будут выполнять ИИ или роботы. Примечательно, что 66% молодых людей в возрасте до 25 лет считают, что автоматизация затронет их специальность в следующем десятилетии [Webster, 2023(1)]. Таким образом, данные свидетельствуют о значительном уровне тревоги, особенно среди молодежи, которая только начинает свою профессиональную карьеру.

Эксперты активно участвуют в обсуждении этих рисков. По словам Шалини Вермы, генерального директора компании Pivot Technologies, «люди, которые выйдут на рынок труда, начнут с гораздо более высокого уровня, чем ожидается – от стажеров и младших руководителей сегодня… Если вы не являетесь уникальным (исключительным) специалистом, вы рискуете быть заменённым ботом. Если же вы эксперт, то, вероятно, будете выполнять свою работу по-другому, поскольку основной объем задач возьмёт на себя ИИ» [Abbas, 2023]. Сама формулировка «исключительный» заставляет большинство не «исключительных» специалистов со всё большей тревогой смотреть в будущее.

Есть опасения среди населения и специалистов в области ИИ в ОАЭ по поводу конфиденциальности данных, предвзятости рекомендаций и других этических аспектов функционирования интеллектуальных систем, что подчеркивает необходимость совершенствования директивными органами нормативно-правовой базы для преодоления разрыва между технологическими достижениями и соблюдением требований законодательства [Ghandour, Woodford, 2019; Shwedeh et al., 2024].

Использование ИИ на национальном уровне в ОАЭ, существующие опасения на этот счет могут стать поводом для манипулирования сознанием широких слоев населения, особенно молодежи, что способно привести к негативным последствиям. Это может произойти в ОАЭ даже раньше, чем в других странах, именно в силу общественно-необходимого, но и имеющего свои риски быстрого развития и внедрения технологий ИИ. Руководство ОАЭ осознаёт всю сложность ситуации. Омар аль-Олама, выступая на Дубайской ассамблее по вопросам генеративного ИИ в октябре 2023 г., призвал граждан не бояться потери работы [Awienat, 2023].

Несмотря на значительные угрозы первого уровня, связанные с внедрением ИИ, для успешной реализации вышеупомянутых инициатив, ОАЭ акцентируют внимание на создании гибких образовательных программ и курсов, которые будут соответствовать требованиям будущего рынка труда. Эти меры, а также международное сотрудничество, поддержка стартапов и инновационных компаний призваны обеспечить гармоничное и безопасное внедрение ИИ для экономического и социального развития страны.

ВТОРОЙ УРОВЕНЬ УГРОЗ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПОСРЕДСТВОМ ЗЛОНАМЕРЕННОГО ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Среди угроз второго уровня можно выделить риски, связанные с применением технологий ИИ, которые могут быть направлены на объекты критической инфраструктуры

и физическую безопасность граждан, а также могут наносить ущерб их имуществу и благосостоянию. В конечном итоге это также представляет угрозу информационно-психологической безопасности. За первые три квартала 2023 г. в ОАЭ было предотвращено более 71 млн попыток совершения кибератак [Shouk, 2023], за один первый квартал 2024 г. было отражено такое же количество атак – 71 млн [Al Amir, 2024]. Использование ИИ злоумышленниками представляет собой серьёзную угрозу, так как они могут применять технологии ИИ для создания сложных мошеннических схем, взлома систем онлайн-банкинга или кражи личных данных граждан.

ОАЭ – одна из первых стран в мире, которая внедрила ИИ в работу полиции для отслеживания и предотвращения преступлений. Появилась так называемая концепция предиктивной полиции и систем машинного обучения для прогнозирования будущих преступлений [Othman, Al Hammadi, 2022]. ИИ используется для обнаружения и обезвреживания бомб, наблюдения, прогнозирования, анализа социальных сетей и опросов подозреваемых. В настоящее время службы безопасности по всему миру работают над тем, чтобы использовать больше подходов, основанных на ИИ и анализе данных, для раскрытия преступлений [Sukhodolov et al., 2020; Keding, 2021]. Генерал-лейтенант Д.Х. Тамим, заместитель начальника полиции и службы общей безопасности в Дубае, считает необходимым внесение поправок в законодательство для борьбы с быстрым развитием нетрадиционных электронных преступлений, особенно тех, в которых используются технологии ИИ и, в частности, дипфейки. Он рассказал о том, как преступники используют ИИ для кражи данных, атак на критически важные объекты инфраструктуры и кибершпионажа, выходя за пределы физических и географических границ [Al Amir, 2024]. Этот феномен кардинально меняет характер преступности и ставит перед правоохранительными органами новые вызовы: преступники могут действовать из любой точки мира, не оставляя следов в физическом пространстве.

М. Х. аль-Кувейти, глава Совета по кибербезопасности ОАЭ, подчеркнул важность использования опыта образовательных учреждений ОАЭ, специализирующихся на ИИ [Al Amir, 2024]. В стране существует уголовная ответственность за такие киберпреступления, как подделка электронных писем, веб-сайтов и фейковые страницы в социальных сетях, которые регулируются статьей *Федерального закона № 34 от 2021 г. о борьбе со слухами и киберпреступлениями* [*Federal Decree-Law No. 34,* 2021].

В настоящее время Совет по кибербезопасности ОАЭ разрабатывает новую политику, которая включает в себя три основных направления: облачные вычисления и безопасность данных, безопасность Интернета вещей и операционные центры кибербезопасности [*Khaleej Times*, 24.07.2024]. Ожидается, что эти документы будут опубликованы уже к концу 2024 г.

В последнее время ОАЭ активно совершенствуют свою деятельность по борьбе с отмыванием денег и финансированием терроризма, особенно в отношении виртуальных активов. После исключения из «серого» списка Международной организации по противодействию отмыванию преступных доходов (FATF) Исполнительное управление по борьбе с отмыванием денег и финансированием терроризма приступило к выполнению более 100 рекомендаций по результатам Национальной оценки рисков 10 июля 2024 г. Эти усилия, курируемые шейхом А. бен Заидом аль-Нахайяном, направлены на снижение рисков в секторах с высокой степенью угрозы, повышение прозрачности юридических лиц и поддержку инициатив в секторе виртуальных активов. ОАЭ создали первый в мире специальный регулятор виртуальных активов в Дубае – Ведомство Дубая по Виртуальным Активам. Кроме того, в период с 2024 по 2026 г. планируется провести комплексную программу более чем из 50 семинаров по обучению заинтересованных сторон рискам отмывания денег и финан-

сирования терроризма [Malak, 2024]. Правительство ОАЭ стремится создать безопасную и прозрачную экосистему для операций с виртуальными активами, принимая во внимание потенциал и вызовы, связанные с ИИ.

В сентябре 2023 г. «Смишинговая триада» значительно расширила свою целевую аудиторию на территории ОАЭ. Группа была замечена в использовании доменных имен, похожих на те, что применялись в предыдущих кампаниях, и внедрила геофильтрацию, чтобы специально нацеливаться на граждан ОАЭ с помощью смишинговых страниц. Выдавая себя за авторитетные организации, такие как Emirates Post (официальная служба доставки ОАЭ), группа рассылает текстовые сообщения для сбора личной и финансовой информации. Затем эти данные используются для мошеннических действий в отношении частных лиц и предприятий. «Смишинг-триада» получает базы данных персональной идентифицируемой информации (PII) с учетом географических особенностей от брокеров Dark Web, чтобы выявлять потенциальных жертв [Resecurity, 2023]. Раньше фишинговые письма можно было распознать по языковым ошибкам и их безличному характеру. Однако с появлением ChatGPT злоумышленники теперь могут создавать персонализированные фишинговые сообщения, основанные на предыдущих «успешных» сообщениях или содержащие конкретные детали, чтобы сделать их более правдоподобными. Распознать такие аферы с первого взгляда становится всё труднее.

Благодаря современным технологиям хакеры теперь могут без труда распространять ложную информацию. Достижения в области ИИ уже оказали значительное влияние на системы блокчейна и криптовалют, которые получили распространение после финансового кризиса 2008 г. [Chenguel, 2023]. Продвигая определённые акции или криптовалюты как представляющие ценность, с помощью ложной информации, хакеры могут спровоцировать ажиотаж среди инвесторов. Как следствие, компании и частные лица могут вкладывать деньги в эти акции, искусственно завышая их стоимость. Это создает выгодную схему для преступников, которые уже заранее приобрели часть акций или криптовалюту.

Таким образом, влияние угроз второго уровня выходит за рамки физических и кибернетических аспектов, затрагивая и психологические последствия – как непосредственные, так и долгосрочные. Эти последствия могут оказывать как контролируемое, так и неконтролируемое негативное воздействие на психическое состояние людей. Необходимо также понимать, что технологии ИИ развиваются быстрее, чем законодательная база – это создает риск использования ИИ без надлежащего контроля и соблюдения этических норм. Без четких регуляторных норм и международных соглашений существует опасность неконтролируемого распространения технологий и их использования в злонамеренных целях.

ТРЕТИЙ УРОВЕНЬ УГРОЗ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПОСРЕДСТВОМ ЗЛОНАМЕРЕННОГО ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Несмотря на наличие национальных законов, таких как Закон о киберпреступлениях, который запрещает кибербуллинг, создание дипфейков и публикацию фейковых новостей, ОАЭ, как и многие другие страны, сталкиваются с проблемой распространения дезинформации. Такие фальшивые материалы могут угрожать политической стабильности государства, нанося ущерб политическим институтам и разжигая общественное недовольство.

Рост объемов созданных дипфейков и их распространение представляют собой серьёзную угрозу для различных аспектов безопасности, как личной, так и государственной. Инструменты для создания дипфейков предоставляют рынки даркнета – анонимные площадки, на которых торгуют запрещёнными товарами и услугами. Согласно результатам

исследования Kaspersky Business Digitization, около 51% сотрудников в регионе Ближнего Востока и Северной Африки считают, что могут отличить подделку от реального изображения. Однако при проведении тестирования только 25% смогли отличить подлинное изображение от созданного ИИ [Kaspersky, 2024]. Это говорит о том, что организации уязвимы для потенциальных мошенников, поскольку киберпреступники используют созданные ИИ изображения в незаконных целях. Например, киберпреступники могут создать поддельное видео, на котором генеральный директор санкционирует денежный перевод или утверждает платеж, что приведет к краже корпоративных средств.

В ОАЭ существуют примеры, которые подтверждают сложившуюся ситуацию. Так, в ноябре 2023 г. власти ОАЭ задержали 43 человека, подозреваемых в участии в международной преступной группе, которая использовала дипфейк-технологию для кражи 36 млн долл. (131,4 млн дирхамов) у двух азиатских фирм. Предположительно, группа нацеливалась на крупные предприятия, взламывая электронную переписку между руководителями компаний и местными менеджерами, убеждая сотрудников перевести значительные суммы денег на их банковские счета в Дубае. В ходе расследования выяснилось, что группа получила несанкционированный доступ к системам электронной почты компании, перехватывая сообщения между генеральным директором и филиалами. Используя дипфейк-технологию, члены группировки выдавали себя за директоров компании и копировали их голоса, чтобы поручить менеджерам филиалов перевести 19 млн долл. на счет в Дубае для проведения конфиденциальной деловой сделки. Преступники использовали сложные методы перевода денег, перемещая похищенные средства по нескольким счетам, а затем снимая их и направляя в специализированные предприятия, занимающиеся хранением и переводом денег [Salim, 2023]. Этот случай стал одним из крупнейших за последние годы, продемонстрировав, насколько уязвимы даже крупные компании перед лицом кибермошенников, использующих передовые технологии для осуществления своих преступных замыслов.

Мошенничество с использованием ИИ распространено не только среди известных компаний, но также может быть нацелено на частных лиц. В 2023 г. в ОАЭ произошёл ещё один резонансный случай, связанный с телефонным мошенничеством. Злоумышленник из Индии использовал сфальсифицированные аудио- и видеозвонки, чтобы заполучить тысячи дирхамов, представившись другом, попавшим в трудное финансовое положение из-за проблем со здоровьем. Пострадавшим оказался 73-летний мужчина, который не заподозрил обмана, поскольку мошенник применил тактику раскрытия подробностей из личной жизни жертвы, что способствовало созданию доверительных отношений и затруднило выявление фальсификации [Sankar, 2023]. Этот случай подчёркивает, что преступники продолжают использовать и усовершенствовать свои методы для оказания информационно-психологического воздействия на свою жертву, будь то компания или частные лица.

Доступ к онлайн-играм, появление генеративного ИИ подвергают детей многогранным угрозам, таким как киберзапугивание, груминг и секстинг [Faraz et al. 2022]. По данным исследований компании WeProtect, которая занимается защитой детей от сексуального насилия, число сообщений о груминге с целью финансового мошенничества возросло со 139 в 2021 г. до более чем 10 000 в 2022 г. [Webster, 2023(2)]. Этот рост эксперты связывают с популярностью социальных сетей и развитием технологий ИИ. Наибольшую опасность представляют случаи, когда злоумышленники, представляясь молодыми девушками, рассылают фейковые непристойные фото- и видеозаписи. Эти действия направлены на то, чтобы манипулировать подростками, которые в ответ отправляют реальные материалы. После этого преступники шантажируют жертв, требуя деньги за молчание и угрожая разоблачением перед родителями. Эти факты подчёркивают необходимость принятия более строгих мер регулирования контента и повышения осведомлённости подростков и их родителей

о потенциальных угрозах. IT-компаниям также необходимо принимать более активное участие в борьбе с подобными преступлениями, включая разработку и внедрение инструментов для обнаружения и предотвращения груминга и распространения непристойного контента. В совокупности эти усилия смогут помочь снизить риск для детей и подростков, а также сделать цифровое пространство более безопасным.

Учитывая угрозы, которые представляют собой дипфейки, их использование для распространения фальшивых медиа и дезинформации, подрыва репутации (частных лиц, организаций или государств), а также клеветы вызывает серьёзные опасения. Правовые меры в ОАЭ в значительной степени зависят от характера и последствий использования дипфейков. Если дипфейки приводят к диффамации, то согласно *Федеральному закону № 31 от 2021 г.* [*Federal Decree-Law No. 31,* 2021] это может быть наказуемо по *статьям 425 или 426*, что может включать тюремное заключение или наложение штрафа. Для осуществления диффамации при использовании цифровых средств, *статья 44 Закона ОАЭ о киберпреступлениях* увеличивает наказание до одного года тюрьмы и/или штрафа от 250 тыс. до 500 тыс. дирхамов за каждое нарушение. Также, если действия, связанные с дипфейками, представляют собой акт мошенничества, то *статья 451 Уголовного кодекса ОАЭ* [*UAE Penal Code*, 2024] предполагает наказание в виде лишения свободы или штрафа. При этом, согласно Закону о киберпреступлениях, такое мошенничество может повлечь за собой тюремный срок минимум на год и штраф от 250 тыс. до 1 млн дирхамов. Аналогично, законы предусматривают ответственность за нарушение личной неприкосновенности [Safar-Aly, 2024]. Таким образом, использование дипфейков в ОАЭ сопряжено с серьёзными правовыми рисками и может повлечь за собой суровые наказания, включая тюремное заключение. Законы, направленные на защиту частной жизни граждан, репутации и национальной безопасности, отражают решимость государства бороться с угрозами, исходящими от цифровых технологий, используемых в злонамеренных целях.

Развитие ИИ также привело к созданию и распространению религиозных чат-ботов. ОАЭ стали одной из 10 стран, где пользователи используют чат-бот QuranGPT [Prabhakar, 2023]. Однако этот тренд сопряжён с двумя основными проблемами: предвзятостью ИИ и получением доступа к религиозному чат-боту злоумышленниками. Создатели стремятся предоставить достоверное представление о своей религии и помочь пользователям лучше понять её учение. Тем не менее виртуальный мир продолжает оставаться подверженным предвзятости, как это показал случай с GPT-3, который был обвинён в исламофобии в 2021 г. [Samuel, 2021]. Такие проблемы могут возникать из-за неправильной интерпретации запросов пользователей ИИ, что может привести как к распространению дезинформации, так и к потенциальным конфликтам в обществе.

ЗАКЛЮЧЕНИЕ

Анализ угроз, связанных с технологиями ИИ в ОАЭ, подчёркивает многоуровневый характер этих рисков. На первом уровне внимание привлекают риски намеренно искаженного толкования восприятия ИИ со стороны антисоциальных групп, что может спровоцировать социально-экономические конфликты в регионе. Хотя данный феномен пока не играет существенной роли в общественной жизни ОАЭ, стоит ожидать, что злонамеренные акторы попытаются использовать негативные последствия и достижения в развитии отрасли в своих целях. Особенно это актуально в условиях крайне напряжённой и опасной ситуации на Ближнем Востоке и во всём мире в целом. Второй уровень угроз представлен возможностью проведения кибератак на критически важные объекты инфраструктуры, что может повлечь за собой значительные потери и негативные последствия для населения.

Количество подобных атак неуклонно растет, а роль ИИ в их реализации становится всё более значимой. Наконец, третий уровень угроз заключает в себе опасность манипуляции общественным мнением с помощью деструктивных методов информационно-психологического воздействия, включая дипфейки и чат-боты. Данные многообразные риски требуют комплексного подхода и незамедлительных действий со стороны государственных структур и общества, чтобы гарантировать информационно-психологическую безопасность и защиту интересов граждан в условиях быстро меняющегося технологического ландшафта. Одним из практических решений на этом направлении может стать, не эпизодическое, а комплексное предсказание рисков использования технологий ИИ (включая злонамеренное) по открытым базам данных и научных исследований с использованием как существующих моделей генеративного ИИ, так и перспективных возможностей нейроморфного и квантового ИИ.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Abbas W. Jobs in UAE: Entry Level Roles Set to Be Wiped Out by AI, Automation and ChatGPT. *Khaleej Times.* 30.03.2023. https://www.khaleejtimes.com/jobs/jobs-in-uae-entry-level-roles-set-to-be-wiped-out-by-ai-automation-and-chatgpt (accessed: 24.07.2024).

Al Amir S. UAE Officials Call for Stricter Penalties to Combat Cybercrime Threat. *The National.* 04.07.2024. https://www.thenationalnews.com/news/uae/2024/07/04/uae-officials-call-for-stricter-penalties-to-combat-cybercrime-surge/ (accessed: 16.07.2024).

Awienat D. Generative AI Should Not Be Feared Despite Risks, Says UAE Minister of Artificial Intelligence. *Arab News.* 13.10.2023. https://arab.news/ptrum (accessed: 24.07.2024).

Beware of Deepfakes in the AI Age, Warns Kaspersky. *Kaspersky*. 05.04.2024. https://www.kaspersky.co.za/about/press-releases/2024_beware-of-deepfakes-in-the-ai-age-warns-kaspersky?ysclid=lyowio7494275241691 (accessed: 08.07.2024).

Burt J.A. A Natural History of the Emirates: An Introduction. *A Natural History of the Emirates.* J.A. Burt (ed.) Cham: Springer, 2024. Pp. 1–9.

Chenguel M.B. Is Artificial Intelligence the Ideal Partner for Blockchain. And Crypto Currencies? *From the Internet of Things to the Internet of Ideas: The Role of Artificial Intelligence. EAMMIS 2022. Lecture Notes in Networks and Systems*. Vol. 557. A.M.A. Musleh Al-Sartawi, A. Razzaque, M.M. Kamal (eds.) Cham: Springer, 2022. Pp. 329–342.

Faraz A., Mounsef J., Raza A., Willis S. Child Safety and Protection in the Online Gaming Ecosystem. *IEEE Access.* 2022. Vol. 10. Pp. 115895–115913.

Federal Decree-Law No. 31 of 2021 on Promulgating the Crimes and Penalties Law. *Official portal of UAE Government.* 20.09.2021. https://uaelegislation.gov.ae/en/legislations/1529 (accessed: 15.07.2024).

Federal Decree-Law No. 34 of 2021 on Combatting Rumors and Cybercrimes. *Official portal of UAE Government.* 20.09.2021. https://uaelegislation.gov.ae/en/legislations/1526 (accessed: 15.07.2024).

Ghandour A., Woodford B.J. Ethical Issues in Artificial Intelligence in UAE. *2019 International Arab Conference on Information Technology (ACIT)*, Al Ain, United Arab Emirates. 2019. Pp. 262–266.

AlGhanem H., Abdallah S. The Future of the Internet of Vehicles (IoV). *BUiD Doctoral Research Conference 2023. Lecture Notes in Civil Engineering*. Vol. 473. K. Al Marri, F.A. Mir, S.A. David, M. Al-Emran (eds.) Cham: Springer, 2024. Pp. 301–309.

Halabi L., Hill C. The Emerging Nature of ICT Policies in Education: A Comparative Analysis of School ICT Policies. *BUiD Doctoral Research Conference 2023. Lecture Notes in Civil Engineering.* Vol. 473. K. Al Marri, F.A. Mir, S.A. David, M. Al-Emran (eds.) Cham: Springer, 2024. Pp. 141–148. https://doi.org/10.1007/978-3-031-56121-4_14

Keding C. Understanding the Interplay of Artificial Intelligence and Strategic Management: Four Decades of Research in Review. *Management Review Quarterly*. 2021. Vol. 71. Pp. 91–134.

Khansaheb K.S.H.A. The Role of Artificial Intelligence in Enhancing Sustainability: The Case of UAE Smart Cities. *BUiD Doctoral Research Conference 2023. Lecture Notes in Civil Engineering.* Vol. 473. K. Al Marri, F.A. Mir, S.A. David, M. Al-Emran (eds.) Cham: Springer, 2024. Pp. 235–242.

Malak L.A. Virtual Assets Are Considered in UAE's 100 New AML/CTF Recommendations. *Cryptopolitan*. 18.07.2024. https://www.cryptopolitan.com/virtual-assets-uaes-aml-ctf-recommendations/?ysclid=lytxukrz9i123605259 (accessed: 18.07.2024).

Matheson E. *UAE Adoption of Digital Authoritarianism Weakens US Security and Portends Soft Power Shift.* Center for Anticipatory Intelligence, Utah State University, April 2020.

Mehta A., Bhavani G. What Determines Banks' Profitability? Evidence from Emerging Markets – The Case of the UAE Banking Sector. *Accounting and Finance Research*. 2017. Vol. 6(1). Pp. 77–88.

Al Olama O. UAE Backs Sam Altman Idea to Turn Itself into AI Testing Ground. *Bloomberg Law.* 15.02.2024. https://clck.ru/3Eq26B (accessed: 10.08.2024).

Othman M.M.Y., Al Hammadi M.M.H. The Use of Artificial Intelligence in Combating Crimes in the UAE: Critical Review. *From the Internet of Things to the Internet of Ideas: The Role of Artificial Intelligence. EAMMIS 2022. Lecture Notes in Networks and Systems*. Vol. 557. A.M.A. Musleh Al-Sartawi, A. Razzaque, M.M. Kamal (eds.) Cham: Springer, 2022. Pp. 357–366.

Pashentsev E. General Content and Possible Threat Classifications of the Malicious Use of Artificial Intelligence to Psychological Security. *The Palgrave Handbook of Malicious Use of AI and Psychological Security.* E. Pashentsev (ed.) Cham: Palgrave Macmillan, 2023. Pp. 23–46.

Prabhakar A. Religious GPT: The Chatbots and Developers Fighting Bias with AI. *The National.* 28.07.2023. https://www.thenationalnews.com/weekend/2023/07/28/religious-gpt-the-chatbots-and-developers-fighting-bias-with-ai/ (accessed: 27.07.2024).

Alrahmah B., Ahmed M.A. The UAE's Harnessing of AI at the National Level Can Benefit Everyone. *The National.* 16.01.2024. https://www.thenationalnews.com/opinion/comment/2024/01/16/the-uaes-harnessing-of-ai-at-the-national-level-can-benefit-everyone/ (accessed: 24.07.2024).

Sajwani R.A. Artificial Intelligence for Sustainability Development in Healthcare. *BUiD Doctoral Research Conference 2023. Lecture Notes in Civil Engineering*. Vol. 473. K. Al Marri, F.A. Mir, S.A. David, M. Al-Emran (eds.) Cham: Springer, 2024. Pp. 264–272.

Salameh N., Benkohila N. The Impact of Job Satisfaction on Teachers' Performance in the UAE. *BUiD Doctoral Research Conference 2023. Lecture Notes in Civil Engineering.* Vol. 473. K. Al Marri, F.A. Mir, S.A. David, M. Al-Emran (eds.) Cham: Springer, 2024. Pp. 9–30.

Salim S. Dubai Police Arrest 43 Suspects over $36-Million Scam; Bust International Network of Cybercriminals. *Khaleej Times.* 09.11.2023. https://www.khaleejtimes.com/uae/dubai-police-arrest-43-suspects-over-36-million-scam-bust-international-network-of-cybercriminals (accessed: 16.07.2024).

Samuel S. AI's Islamophobia Problem. *Vox*. 18.09.2021. https://www.vox.com/future-perfect/22672414/ai-artificial-intelligence-gpt-3-bias-muslim (accessed: 27.07.2024).

Sankar A. Deepfake Video Call Said to Be from Dubai Used to Swindle Kerala Man Out of Thousands. *The National.* 19.07.2023. https://www.thenationalnews.com/uae/2023/07/19/deepfake-video-call-pretending-to-be-dubai-friend-used-to-swindle-man-out-of-thousands/ (accessed: 27.07.2024).

Alshamsi S.K.H.K., Al-Kumaim N.H.S. A Conceptual Model for Prevention of E-Financial Crimes in UAE: A Review Paper. *Academy of Strategic Management Journal*. 2021. Vol. 20. Special Issue 6. Pp. 1–10.

Shouk A. A. UAE Has Thwarted 71 Million Cyber Attacks This Year, Authorities Say. *The National.* 03.11.2023. https://www.thenationalnews.com/uae/2023/11/03/uae-has-thwarted-71-million-cyber-attacks-this-year-authorities-say/ (accessed: 13.08.2024).

Shwedeh F., Salloum S.A., Aburayya A., Fatin B., Elbadawi M. A., Al Ghurabli Z., Al Dabbagh T. AI Adoption and Educational Sustainability in Higher Education in the UAE. *Artificial Intelligence in*

Education: The Power and Dangers of ChatGPT in the Classroom. Studies in Big Data. Vol. 144. A. Al-Marzouqi, S.A. Salloum, M. Al-Saidat, A. Aburayya, B. Gupta (eds.) Cham: Springer, 2024.

Smishing Triad Impersonates Emirates Post To Target UAE Citizens. *Resecurity*. 25.09.2023. https://www.resecurity.com/blog/article/Smishing-Triad-Impersonates-Emirates-Post-Target-UAE-Citizens?ref=news.risky.biz (accessed: 17.07.2024).

Smith M., Zeigler S. M. Terrorism before and after 9/11 – A More Dangerous World? *Research & Politics*. 2017. Vol. 4(4). Pp. 1–8.

Sukhodolov A.P., Bychkov A.V., Bychkova A.M. Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects. *Journal of Siberian Federal University. Humanities & Social Sciences.* 2020. Vol. 13(1). Pp. 116–122.

Tabrez H. What UAE Jobs Will Be in Demand for the Next 10 Years? Find Out. *Gulf News.* 18.01.2022. https://gulfnews.com/living-in-uae/ask-us/what-uae-jobs-will-be-in-demand-for-the-next-10-years-find-out-1.1642432873987 (accessed: 15.07.2024).

UAE Penal Code. https://cdn.expatwoman.com/s3fs-public/UAE%20Penal%20Code.pdf (accessed: 15.07.2024).

UAE to Issue 3 New Policies to Boost Cybersecurity by End of 2024. *Khaleej Times.* 27.07.2024. https://www.khaleejtimes.com/uae/uae-to-issue-3-new-policies-to-boost-cybersecurity-by-end-of-2024?_refresh=true (accessed: 08.08.2024).

Webster N. Rise of AI Creates Job Worries, UAE Survey Finds. *The National News*. 19.01.2023(1). https://www.thenationalnews.com/uae/ 2023/01/19/rise-of-ai-creates-job-worries-uae-survey-finds/ (accessed: 24.07.2024).

Webster N. Online Gaming Poses Alarming Threat to Children's Safety, Report Finds. *The National News.* 19.10.2023(2). https://www.thenationalnews.com/uae/2023/10/19/online-gaming-poses-alarming-threat-to-childrens-safety-report-finds/ (accessed: 24.07.2024).

World's First Artificial Intelligence Varsity in Abu Dhabi. *Khaleej Times.* 16.10.2019. https://www.khaleejtimes.com/uae/worlds-first-artificial-intelligence-varsity-in-abu-dhabi (accessed: 10.07.2024).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

ПАШЕНЦЕВ Евгений Николаевич – доктор исторических наук, профессор факультета международных отношений Санкт-Петербургского государственного университета, Санкт-Петербург, Россия; главный научный сотрудник Института актуальных международных проблем Дипломатической академии МИД России, Москва, Россия.

Evgeny N. PASHENTSEV, DSc (History), Professor, Faculty of International Relations, Saint Petersburg State University, Saint Petersburg, Russia; Chief Research Fellow, Institute of Current International Problems, Diplomatic Academy of the MFA of the Russian Federation, Moscow, Russia.

ЧЕБЫКИНА Владилена Александровна – магистрант 2 курса факультета международных отношений Санкт-Петербургского государственного университета, Санкт-Петербург, Россия; стажер-исследователь Международного центра социально-политических исследований и консалтинга, Москва, Россия.

Vladilena A. CHEBYKINA, 2nd year Master's student, Faculty of International Relations, Saint Petersburg State University, Saint Petersburg, Russia; Research Intern, International Centre for Social and Political Studies and Consulting, Moscow, Russia.