

DOI: 10.31696/S086919080036995-1

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ: ВЫЗОВЫ ДЛЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ЕГИПТА¹

© 2026

Е.Н. ПАШЕНЦЕВ ^a

^a – Санкт-Петербургский государственный университет,
Санкт-Петербург, Россия
ORCID: 0000-0001-5487-4457, icspsc@mail.ru

Резюме: Технологии искусственного интеллекта (ИИ) в руках злонамеренных акторов становятся опасным средством информационно-психологической и социально-политической дестабилизации. Высокие темпы индустриального и научно-технического развития Египта в сочетании с острыми социально-экономическими противоречиями, политическими вызовами, а также геополитическими рисками на Ближнем Востоке формируют благоприятные условия для роста угроз злонамеренного использования ИИ (ЗИИИ) в этой стране. Для оценки угроз, связанных с ЗИИИ и его влиянием на информационно-психологическую безопасность, в работе применяется трёхуровневый подход. Первый уровень угроз характеризуется распространением заведомо искажённой, ложной информации о сути и возможностях ИИ, что может формировать у населения недоверие к новым технологиям. Второй уровень связан с практикой ЗИИИ, когда атака на общественное сознание не является основной целью, но имеет негативные для него последствия в результате ущерба, наносимого критической инфраструктуре, жизни и здоровью людей и их имуществу. На третьем, самом высоком уровне угроз, ИИ применяется для манипулятивного воздействия на общественное сознание в целях социальной дезориентации и дестабилизации. Данный подход позволяет систематизировать угрозы ЗИИИ и оценить их влияние на устойчивость информационной среды. На первом уровне угроз основную опасность в Египте представляют манипуляции с тревожными нарративами о технологической безработице, прогнозами о рисках утраты контроля над ИИ; на втором уровне угроз – рост цифрового мошенничества со всё более активным использованием ИИ-технологий; на третьем – использование технологий дипфейков и генеративного ИИ для создания и распространения дезинформации. В статье подчёркивается необходимость разработки комплексных стратегий по противодействию ЗИИИ, включающих усиление нормативно-правового регулирования, повышение цифровой грамотности населения и развитие национальных механизмов кибербезопасности. Только системный подход позволит минимизировать угрозы, связанные с ЗИИИ, и обеспечить устойчивость Египта перед современными вызовами в информационно-психологической сфере.

Ключевые слова: искусственный интеллект, национальная безопасность, информационно-психологическая безопасность, Египет, злонамеренное использование искусственного интеллекта, кибербезопасность, дезинформация, дипфейки

¹ Исследование выполнено за счет гранта Российского научного фонда № 25-18-00699 <https://rscf.ru/project/25-18-00699/>.

Для цитирования: Пашенцев Е.Н. Искусственный интеллект как инструмент информационно-психологического воздействия: вызовы для национальной безопасности Египта. *Восток (Oriens)*. 2026. № 1. С. 127–139. DOI: 10.31696/S086919080036995-1

ARTIFICIAL INTELLIGENCE AS A TOOL OF PSYCHOLOGICAL INFLUENCE: CHALLENGES FOR THE NATIONAL SECURITY OF EGYPT²

© 2026

Evgeny N. PASHENTSEV ^a

^a – Saint Petersburg State University, Saint Petersburg, Russia

ORCID: 0000-0001-5487-4457, icpspc@mail.ru

Abstract: Artificial intelligence (AI) technologies may become a dangerous means of psychological and socio-political destabilization in the hands of malicious actors. This article provides a comprehensive analysis of the key threats associated with the phenomenon of malicious use of AI (MUAI). The high pace of Egypt's industrial, scientific and technological development, combined with acute economic, social contradictions, political challenges, create favorable conditions for the growth of MUAI threats in this country. A three-level approach is used to assess the MUAI threats and their impact on psychological security. The first level of threats is characterized by the spread of deliberately distorted information about the nature and capabilities of AI. The second level pertains to cases of MUAI where public consciousness is not the direct target, but negative consequences occur nonetheless—due to harm inflicted on critical infrastructure, public health systems, energy and transport security, as well as individuals' lives, health, and property. At the third and highest level of threat, AI is employed as a tool for manipulative influence on public consciousness with the explicit aim of social destabilization. Among the main MUAI threats in Egypt are: manipulation of alarming narratives about technological unemployment (the first level), growth of digital fraud with the increasing use of AI technologies (the second level), use of deepfake technologies and generative AI to create and spread disinformation (the third level). The article emphasizes the need to develop comprehensive strategies to counter MUAI, including strengthening regulatory frameworks, enhancing digital literacy, and advancing national cybersecurity mechanisms.

Keywords: artificial intelligence, national security, psychological security, Egypt, malicious use of artificial intelligence, cybersecurity, disinformation, deepfakes

For citation: Pashentsev E.N. Artificial Intelligence as a Tool of Psychological Influence: Challenges for the National Security of Egypt. *Vostok (Oriens)*. 2026. No. 1. Pp. 127–139. DOI: 10.31696/S086919080036995-1

ВВЕДЕНИЕ

Египет добился заметного прогресса в развитии искусственного интеллекта (ИИ), особенно в области законодательства, институционального развития и цифровой инфраструктуры. В 2019 г. правительство Египта учредило Национальный совет по искусственному интеллекту (NCAI). Год спустя NCAI подготовил и принял первую редакцию Национальной стратегии Египта в области ИИ (NAIS) [UNESCO, 2025, р. 10]. В 2023 г. была принята Египетская хартия ответственного ИИ, представляющая собой интерпретацию страной

² The research was supported by the Russian Science Foundation Grant No. 25-18-00699.

различных международных руководящих принципов, адаптированную к местным условиям [Just AI, 2024]. Эта хартия направлена на обеспечение ответственной разработки, развертывания и использования систем ИИ на основе прозрачности алгоритмов и человекоцентричного подхода.

В январе 2025 г. в ответ на появление больших языковых моделей и технологий генеративного ИИ, с учетом новых возможностей и рисков, президент Египта Абдель Фаттах ас-Сиси представил обновлённую Национальную стратегию в области ИИ на период 2025–2030 гг. Согласно этому документу, планируется, что 26% рабочей силы Египта получит выгоду от инструментов и приложений ИИ, а 36% населения в целом будут иметь доступ к ИИ и продуктам на его основе в своей повседневной жизни. В стране будет обеспечено создание и поддержка более 250 успешных компаний в области ИИ. Технологии ИИ помогут ускорить процесс научных исследований, вдвое увеличится число публикаций по ИИ, достигнув 6000 в год. Эти и другие намечаемые показатели позволят Египту стать важным региональным центром сотрудничества в области ИИ [*Egypt National AI Strategy*, 2025, p. 7; Just AI, 2024].

Вместе с тем Египет заметно уступает по притоку инвестиций лидерам гонки по внедрению ИИ на Ближнем Востоке. Так, PwC в статье «Потенциальное влияние искусственного интеллекта на Ближнем Востоке» полагает, что к 2030 г. доля ИИ в ВВП Египта составит около 7,7% [Africazine, 2025]. В ОАЭ, как ожидается, эта доля составит 13,6%, а в Саудовской Аравии – 12,4% [Jain, 2018]. Количество центров обработки данных в стране является другим важным показателем прогресса в развитии инфраструктуры ИИ. Согласно последним данным Международного института стратегических исследований (IISS), Израиль занимает первое место в регионе с 55 центрами обработки данных. За ним следуют Саудовская Аравия с 36 центрами, ОАЭ – 34, Иран – 20, Оман – 15, и Египет – 13 [Ragab, 2025]. Несмотря на общее отставание Египта от ведущих стран Ближнего Востока по темпам развития ИИ, не следует преувеличивать это отставание. Учитывая общий экономический потенциал, численность населения, быстрый рост профильных кадров, Египет имеет хорошие шансы занять одно из лидирующих мест в регионе по уровню развития и внедрения ИИ.

В Египте действуют законы и нормативные акты, регулирующие некоторые аспекты разработки и применения ИИ: закон о защите данных (принят в 2020 г.), нормативная база для центров обработки данных (2021 г.); закон о борьбе с киберпреступлениями и преступлениями в области информационных технологий (2018 г.); закон о защите прав потребителей (2018 г.) [*Egypt National AI Strategy*, 2025, n. d., p. 17]. Принятые меры дают широкий спектр возможностей регулирования ИИ в рамках действующего законодательства.

Подтверждением успехов в развитии ИИ в Египте является и улучшение его позиций в международных рейтингах. Согласно глобальному индексу ИИ Tortoise Media, в 2024 г. Египет занимал 52-е место по сравнению с 58-м в 2019 г. В рейтинге Oxford Insights «Индекс готовности правительства к ИИ» за 2024 г. Египет занял 65-е место из 188 стран по сравнению со 111-м в 2019 г. В том же рейтинге Египет занял 1-е место в Африке и 7-е место в регионе Ближнего Востока [UNESCO, 2025, p. 8].

Настоящая статья представляет собой качественное развитие крайне небольшой по объёму главы по Египту [Пашенцев, Чебыкина, Шеметова, 2024] в информационно-аналитическом докладе по проблематике ЗИИИ и угроз информационно-психологической безопасности (ИПБ) в странах БРИКС. Ограниченность источников, характер и объём работы не позволили тогда авторам выйти на уровень системного исследования, попытка которого предпринята в настоящей статье впервые с использованием самых последних материалов. Угрозы ЗИИИ рассматриваются в статье в контексте социально-политических

реалий современного Египта при опоре на широкий круг научной литературы, посвящённой социально-экономическому и политическому развитию Египта. Среди использованных трудов – комплексный анализ стратегии управления кризисами и реформами в Египте [Mohieldin et al., 2024], исследования региональных интересов страны в условиях внутренних политических и экономических противоречий [Bahi, 2016; Kamal, 2018], а также аналитические обзоры актуального положения страны в глобальном и региональном контексте [Hokayem, Momtaz, 2024; McBride, 2024].

Проблематика внедрения ИИ в странах Ближнего Востока и, в частности, в Египте, исследуется в контексте региональной безопасности [Sarkin, Sotoudehfar, 2024]. В статье учтены результаты исследования роли ИИ в области ИПБ [Hashmi et al., 2024; Kertysova, 2019; Pashentsev, 2023]. Особое внимание уделяется изучению дезинформации, пропаганды и роли ИИ в возрастании информационных угроз. В данном контексте использованы исследования, посвящённые влиянию ИИ на производство и распространение дезинформации [Bontridder, Pouillet, 2021; Shin, 2024], в частности – злонамеренному использованию дипфейков [AbuJarour et al., 2024; Sandoval et al., 2024]. В статье также использованы публикации, посвящённые использованию генеративных моделей ИИ для манипулирования общественным сознанием [Bi et al., 2024; Goldstein et al., 2024]. Несмотря на наличие значительного числа публикаций в области киберугроз и дезинформации, системный анализ ЗИИИ остаётся недостаточно разработанным, что подчёркивает актуальность настоящей работы.

Для оценки угроз, связанных с ЗИИИ и его влиянием на информационно-психологическую безопасность, в работе применяется трёхуровневый подход, предложенный автором настоящей статьи в своих предшествующих публикациях. *Первый уровень угроз* характеризуется распространением заведомо искажённой, ложной информации о сути и возможностях ИИ, а также о последствиях его развития и применения. *Второй уровень* связан с практикой ЗИИИ, когда атака на общественное сознание не является основной целью, но имеет негативные для него последствия – в результате ущерба, наносимого критической инфраструктуре, жизни и здоровью людей и их имуществу. На *третьем*, самом высоком *уровне угроз*, ИИ применяется для манипулятивного воздействия на общественное сознание в целях социальной дезориентации и дестабилизации [Pashentsev, 2023]. Данный подход позволяет систематизировать угрозы ЗИИИ и оценить их влияние на устойчивость информационной среды Египта.

ПЕРВЫЙ УРОВЕНЬ УГРОЗ

В Египте существуют объективные предпосылки для формирования угроз ИПБ посредством ЗИИИ. В целом они схожи с такими предпосылками, существующими в других странах. На первом месте здесь риски массовой безработицы из-за быстрого внедрения технологий ИИ и роботизации в различные виды трудовой деятельности. С одной стороны, это порождает беспокойство по поводу возможной потери рабочих мест, а с другой, дает основания для признания преимуществ ИИ в повышении эффективности и появлении новых возможностей, связанных с освоением новых навыков. Так, согласно опросу АО «Лаборатория Касперского», в начале 2023 г. около половины (44%) сотрудников компаний в Египте боялись потерять работу из-за роботов и каждый четвертый сотрудник (25%) сообщил, что слышал об инцидентах с кибербезопасностью, связанных с роботами или автоматизированными системами в их компании [Daily News Egypt, 2023 (1)].

Другой опрос, проведенный «Лабораторией Касперского» в 2023 г., показал, что преобладающая часть руководителей отделов компаний и топ-менеджеров считает, что в

ближайшие пять лет они потеряют работу из-за отсутствия навыков работы с цифровыми технологиями [*Daily News Egypt*, 2023 (2)]. Данные обстоятельства усложняют внедрение ИИ-решений и требуют дополнительных усилий со стороны правительства по формированию позитивного имиджа технологий среди населения.

Египетский центр экономических исследований разработал систему мониторинга рынка труда на базе ИИ в режиме реального времени – проект, в рамках которого систематически анализируется более 350 000 уникальных онлайн-объявлений о вакансиях. Работа исследователей дает основания полагать, что рынок труда Египта страдает не от какого-то одного недуга, а от целого ряда глубоко укоренившихся структурных перекосов. Географическая централизация возможностей в Каире, «ловушка опыта» (нет опыта – нет квалифицированной работы), которая часто закрывает новичкам дорогу к карьерному росту, и другие проблемы складывались здесь на протяжении десятилетий. Появление ИИ действует как мощный ускоритель, подливая «технологическое топливо» в уже существующие очаги «возгорания» проблем на рынке труда. Как показывает анализ, ИИ расширит возможности опытных профессионалов, например, опытных инженеров-программистов. Одновременно, автоматизируя те самые базовые задачи, которые когда-то служили отправной точкой для молодых специалистов, технология угрожает превратить «ловушку опыта» в почти непреодолимый барьер [Dawoud, Nabashy, 2025].

Рост безработицы или снижение уровня заработной платы вследствие внедрения технологий ИИ могут быть использованы внутренними и внешними антисоциальными акторами в деструктивных целях, включая дестабилизацию политической обстановки в собственных интересах. В этом контексте проблемы занятости, обусловленные внедрением ИИ, требуют особого внимания, поскольку их масштабное распространение и усугубление представляются весьма вероятными в недалёком будущем.

В Египте, аналогично ряду других государств, начинают звучать крайне пессимистичные прогнозы относительно перспектив взаимодействия человека и ИИ. Так, Мохаммед Гавдат, вице-президент Google по развивающимся рынкам, выразил обеспокоенность тем, что машины, оснащённые ИИ, могут однажды начать рассматривать людей как «отбросов общества» и создавать «машины для убийств», подобные тем, что изображены в научно-фантастическом фильме «Я, робот» с Уиллом Смитом в главной роли [Zilber, 2023]. М. Гавдат опасается будущего сценария, при котором ИИ решит, что ему необходимо уничтожить человеческую расу, хотя до этого дня еще «немного далеко». Основная проблема связана с тем, что языковые модели учатся на данных, представленных в открытом пространстве, где преобладает большое количество негатива, и действительно, ИИ отражает предвзятости данных, на которых он обучается. Однако на практике компании, разрабатывающие ИИ, уже используют фильтры и алгоритмы для минимизации таких эффектов, хотя полностью избежать их сложно.

Подобные заявления, несмотря на их кажущуюся фантастичность, отражают не только опасения отдельных экспертов, но и более широкий социальный контекст, в котором происходит освоение ИИ-технологий. Подобные нарративы могут быть использованы в информационной войне или просто стать триггером для массового страха перед технологиями. История знает примеры, когда большинство инноваций изначально воспринимались как угроза установленному порядку (первые автомобили, Интернет, ядерная энергия и т. д.). Со временем общество к ним адаптировалось, а государства выработали соответствующие нормативные и институциональные ответы. Однако впервые получает стремительное развитие набор технологий, который в растущей мере заменяет интеллектуальные возможности человека, и аналогии с прошлым опытом человечества здесь далеко не всегда уместны. Особенно принимая во внимание развитие интеллектуальных робототехнических

систем, которые берут на себя широкий спектр трудовых функций, до этого выполняемых человеком. И делают это они не только в виртуальном пространстве, а в качестве всё более эффективных акторов физического мира.

Следовательно, представляется обоснованным утверждение, что угрозы ЗИИИ первого уровня актуальны и носят не теоретический, а вполне прикладной характер. Эти угрозы связаны с возможностью целевой трансформации восприятия и реакции египтян в интересах злонамеренных акторов на реально существующие серьёзные проблемы развития и использования ИИ. Подобная ситуация предполагает упреждающий анализ междисциплинарного экспертного сообщества Египта, занимающегося исследованиями ИИ, результаты которого предстоит внедрить в соответствующие механизмы контроля, регулирования и стратегического использования ИИ в интересах общества.

ВТОРОЙ УРОВЕНЬ УГРОЗ

Многие угрозы второго уровня связаны с ещё существующими недостатками регулирования ИИ в Египте. Акторы ЗИИИ могут использовать и используют правовые бреши в своих целях. Так, несмотря на то что прошло свыше пяти лет после принятия закона о защите данных, правительство Египта до сих пор не издало соответствующих подзаконных актов. Учитывая, что закон делегирует регулирование значительной части своих правил и этим актам, сохраняется множество возможностей для его нарушения, в том числе и с использованием технологий ИИ. Другой проблемой является отсутствие должного надзора за использованием цифровых сервисов, что также оставляет серые зоны неконтролируемого применения ИИ, включая его злонамеренное использование [Masaar, 2025].

Решение этих и других проблем видится по двум направлениям: совершенствование действующего законодательства и разработка закона об ИИ, которая интенсивно идёт в настоящее время. Закон, как ожидается, гарантирует, что использование систем ИИ не нарушит принципов защиты данных, поставив ещё более надежный заслон для совершения преступлений с использованием технологий ИИ.

Проблемы регулирования ИИ серьёзно осложнены ролью крупнейших технологических компаний – Big Tech – из США, доминирующих в Египте. По данным правительства, в стране на май 2025 г. работало более 1800 американских компаний, а общий объем инвестиций США за последние два десятилетия превысил 47 млрд долл. [Daily News Egypt, 2025]. Американская торговая палата в Египте признает большие перспективы роста американских инвестиций в области информационных технологий [American Chamber of Commerce in Egypt, n. d.].

Ключевые компании, такие как Amazon, IBM и Microsoft, расширяют свое присутствие в Каире, создавая новые возможности в области ИИ, кибербезопасности и разработки программного обеспечения [Fourrage, 2025]. Однако цифровые платформы, возможности киберразведки, поддерживаемые Big Tech, часто являются источником ЗИИИ на всех трёх уровнях, включая распространение клеветы и дезинформации о стране. Аналогичная проблема стоит во многих странах. Видимо, только дальнейшая диверсификация внешнеэкономических связей Египта и, не в последнюю очередь, дальнейшее развитие сотрудничества в области технологий ИИ со странами БРИКС, должным образом укрепит ИПБ страны.

Помимо пробелов в регулировании, серьёзной проблемой является уровень подготовки сотрудников в области кибербезопасности с учетом текущих и перспективных рисков ЗИИИ. Исследование АО «Лаборатория Касперского», озаглавленное «Кибербезопасность на рабочем месте: знания и поведение сотрудников», показало, что 87,5% специалистов, опрошенных в Египте, говорят, что используют инструменты ИИ для решения рабочих

задач. Однако только 46,5% прошли обучение по аспектам кибербезопасности, связанным с использованием нейронных сетей, которые являются одним из важнейших элементов защиты от рисков, связанных с ИИ, начиная от утечки данных и заканчивая сложными схемами ЗИИИ [Bosman, 2025]. Между тем быстрое развитие цифровой среды, постоянно растущее число пользователей Интернета и геополитическое положение Египта сделали его привлекательной мишенью для киберпреступников. В 2024 г. на Египет пришлось примерно 13% всех кибератак на континенте, и он занял второе место после Южной Африки [Interpol, 2025, p. 22]. Большинство кибератак в Египте в 2024 г. были направлены против компьютерных систем, мобильных устройств и отдельных лиц с помощью социальной инженерии [Lukash, 2025; IPST, 2025].

Подразделение Microsoft по цифровым преступлениям (DCU) в конце 2024 г. изъяло 240 мошеннических веб-сайтов, связанных с египетским посредником в киберпреступности. Абануб Нади (известный в Интернете как «MRxC0DER»), разработал и продавал фиш-киты³ «сделай сам», обманным путем используя торговую марку «ONNX» для продажи этих услуг. Многочисленные киберпреступники приобрели эти наборы и использовали их в широко распространенных фишинговых кампаниях, чтобы обойти дополнительные меры безопасности и взломать учетные записи клиентов Microsoft [Microsoft Threat Intelligence, 2024; Greig, 2024]. Все большую роль в фишинговых атаках, включая Египет, играет ИИ.

В ноябре 2025 г. АО «Лаборатория Касперского» предупредило пользователей по всему Ближнему Востоку о волне поддельных инвестиционных платформ, которые используют популярность онлайн-трейдинга и цифровых инвестиционных сервисов. С 2024 г. решения Касперского позволили заблокировать более 100 тыс. фишинговых рассылок, имитирующих инвестиционные платформы, в ОАЭ, Саудовской Аравии, Катаре и Египте. В случае успеха такие атаки предоставляют киберпреступникам доступ к реквизитам кредитных карт и другой конфиденциальной информации, что делает персональные данные уязвимыми для преступного использования [Kaspersky, 2025].

В ходе фишинговых атак, основанных на ИИ, используются следующие методы:

- Алгоритмы, созданные с помощью ИИ, имитируют стиль письма, чтобы генерировать электронные письма, предположительно отправляемые человеком или доменом, которым доверяет жертва.

- Анализ настроений использует эмоциональные уязвимости жертв. Например, пишутся электронные письма, в которых применяется тактика запугивания или предлагается помощь кому-либо, попавшему в беду.

- Обработка естественного языка (NLP) обеспечивает грамматическую точность электронных писем [Drolet, 2025]. Таким образом, технологии ИИ существенно (а во многих случаях – решающим образом) повышают эффективность фишинговых атак, поскольку обеспечивают высокую достоверность сообщений. Данные по Египту отражают глобальную тенденцию к росту фишинговых атак и технологий социальной инженерии на основе ИИ.

Фишинговые атаки помимо прямого финансового ущерба как частному сектору, так и индивидуальным пользователям (проведенный АО «Лаборатория Касперского» опрос об электронных платежах показал, что 57% пользователей в Египте сталкивались с попытками фишинга при использовании услуг онлайн-банкинга или цифровых кошельков [Egypt Independent, 2022]), создают чувство неуверенности в деловой коммуникации. Проверять всё – невозможно, встанут дела, мания всеобщей подозрительности и социально опасна, раз-

³ Фиш-киты – наборы готовых шаблонов и скриптов, с помощью которых можно быстро и массово создавать фишинговые страницы.

лагаю общество не в меньшей степени, чем необоснованная беспечность. Психологические эффекты уже оказывают негативное влияние на общество, сея недоверие к ИИ.

Ещё одной формой угроз на втором уровне, получивших развитие в Египте, стало использование дипфейков. Следует учитывать, что сегодня качественные дипфейки могут обмануть большинство людей. В то время большинство людей убеждены в своей способности распознавать дипфейки. В начале 2025 г. iProov, одна из ведущих в мире компаний в области биометрической идентификации, попросила 2000 жителей Великобритании и США выявить дипфейки. В результате опроса лишь небольшая часть людей – 0,1% – смогли точно отличить реальный контент от поддельного, например, изображения и видео. Несмотря на эти плачевные результаты, около 60% респондентов заявили, что уверены в своих навыках распознавания подделок [Borak, 2025]. Необходимо также учитывать, что и дипфейки низкого качества могут ввести в заблуждение, например, если человек находится в кризисной ситуации, крайнего волнения и нужны быстрая оценка и решение.

По данным Tadween for Gender Studies, египетская пресса зафиксировала 169 случаев сексуального принуждения и вымогательства в Интернете в период с 2019 по 2022 г., причем 50,3% из этих инцидентов были зарегистрированы только в 2022 г. Хотя данные о жертвах были неполными, женщины составляли большинство случаев – 82,9% [Salah, 2024]. Согласно данным ООН на ноябрь 2025 г., развитие ИИ значительно усилило цифровое насилие, сделав его более быстрым, целенаправленным и трудно обнаруживаемым. 38% женщин сталкивались с насилием в Интернете, а 85% были его свидетелями [Carno, 2025]. Применение дипфейков с целью сексуального принуждения и вымогательства может получить ещё большее развитие в самом ближайшем будущем с дальнейшим прогрессом этой технологии.

Таким образом, в Египте проблема киберпреступности становится всё более актуальной на фоне активного внедрения и использования ИИ-технологий. Эти изменения свидетельствуют о том, что Египет стоит перед необходимостью усиления мер по защите как государственного, так и частного секторов от киберугроз, связанных с развитием интеллектуальных технологий.

ТРЕТИЙ УРОВЕНЬ УГРОЗ

На третьем уровне угроз информационно-психологической безопасности посредством ЗИИИ в Египте стоит назвать злонамеренное использование дипфейков и чат-ботов на основе ИИ. Один из самых актуальных случаев произошел в феврале 2025 г., когда Армия обороны Израиля (ЦАХАЛ) изучала вопрос о том, не причастны ли «иностранные элементы» к подрыву отношений с Египтом. Израиль получил протест от высокопоставленных египетских чиновников после распространения в социальных сетях нескольких видеороликов, на которых предполагаемый представитель ЦАХАЛа благодарит президента Египта Абдель Фаттах ас-Сиси на арабском языке за помощь, оказываемую Израилю в войне в Газе и Ливане (в Египте это вызвало массовые протесты). Египетские власти обратились к официальным каналам за разъяснениями. ЦАХАЛ пояснила, что это фейковые видео, созданные с использованием технологий ИИ, и даже выступила с официальным опровержением. Затем было распространено ещё больше фейковых видео. Некоторые из них показывают военные учения египетской армии, проводившиеся в 2017 и 2020 г., которые были представлены так, как будто они происходят в 2025 г., а также фотографии, якобы сделанные на Синае [Yehoshua, 2025]. Подобный опыт свидетельствует о возросшем качестве продуктов, созданных с помощью технологии дипфейков, что может в будущем повлечь новые политические провокации.

В ходе Арабского медиафорума, состоявшегося в Дубае в сентябре 2023 г., египетский журналист и предприниматель И.Э. Адиб подчеркнул, что перспективы медиаиндустрии остаются неопределёнными. Он отметил, что информационное пространство уже вступило в фазу, характеризующуюся стремительным распространением недостоверных сведений, что создаёт дополнительные угрозы для общественного восприятия реальности. В качестве примера И.Э. Адиб рассказал о случае из личного опыта: его знакомые отправили ему видео, на котором американский президент Д. Трамп якобы перенёс операцию по пересадке сердца, ранее принадлежавшего мусульманину, после чего принял ислам [Al-Faour, 2023]. Этот случай иллюстрирует ключевую проблему – склонность людей доверять визуальной информации, даже если она не имеет под собой реальных оснований.

Не вполне очевидная сегодня, но острая угроза может возникнуть в будущем, в том числе и в Египте, если исследователи и представители творческих профессий будут злоупотреблять чат-ботами на основе ИИ для решения научных и творческих задач соответственно. Чрезмерное применение таких инструментов, как ChatGPT, для генерации контента для статей, сценариев, репортажей и т. п. может привести к резкому падению качества медиапродукции. Еще более непоправимый вред недобросовестное применение сгенерированного текста может принести в науке. Вместе с тем исследование опыта студентов Александрийского института СМИ в Египте в 2024 г. внушает оптимизм, так как молодежь в целом довольно критически относится к применению ChatGPT в профессиональной сфере.

Анализ полученных данных выявил широкий спектр проблем и ограничений, с которыми сталкиваются студенты-медиаспециалисты при использовании ChatGPT для решения конкретных задач. В уже упомянутом исследовании в Александрийском институте СМИ студенты отмечали трудности с созданием контента, отвечающего их ожиданиям, поскольку он был неточным, а иногда и слишком общим. Респонденты обнаружили пробелы в знаниях в ответах ChatGPT по различным темам, включая искусство, музыку, литературу и культурные отсылки. Некоторые ответы вызывали опасения по поводу этических вопросов, достоверности и качества контента, генерируемого ChatGPT. Результаты выявили несколько тем, охватывающих разнообразный опыт и восприятие участников. К ним относятся «риск плагиата», «снижение качества», «отсутствие оригинальности» и опасения некоторых участников по поводу компромисса между креативностью и качеством при использовании ChatGPT [Assad, 2024]. Подобные исследования показывают, что качество контента, производимого с помощью чат-ботов общего назначения, пока ещё ниже, чем качество текстов, создаваемых человеком. Вместе с тем контент, созданный специализированными чат-ботами, уже очень трудно отличить от «человеческого», и, если количество недобросовестных исследователей или представителей творческих профессий, неправомерно размещающих в своих работах сгенерированный контент, будет расти, это крайне негативно отразится на развитии науки и творчества, а, следовательно, и на ИПБ граждан.

В Египте уделяют активное внимание угрозам третьего уровня, в том числе такой «чувствительной» сфере, как религиозная (особенно актуальной стала проблема использования религиозных чат-ботов). В августе 2025 г. доктор Омар Хабтур Аль-Дарей, председатель Главного управления по делам ислама, вакуфов и закята ОАЭ, встретился с доктором Назиром Мухаммедом Айядом, верховным муфтием Египта, чтобы обсудить вопросы укрепления сотрудничества, интеграции и обмена опытом в области фетв. В ходе переговоров основное внимание уделялось использованию цифровых технологий и ИИ для предоставления точных и своевременных фетв сообществам, решения современных проблем и сложных вопросов, с которыми сталкиваются различные слои общества [Shahzaib, 2025].

Таким образом, социальные проблемы, которые становятся основным фактором ЗИИИ, в Египте всё чаще выносятся в повестку дня.

ЗАКЛЮЧЕНИЕ

Египет является одним из лидеров в регионе Ближнего Востока и Северной Африки по темпам развития ИИ и продолжает активно инвестировать в данную сферу. На основании проведённого исследования можно сделать вывод о том, что проблема ЗИИИ в стране охватывает все три уровня угроз ИПБ, что требует комплексного и многоуровневого подхода к их нейтрализации. На первом уровне угроз основное внимание следует уделять манипуляциям общественным мнением, связанным с распространением тревожных нарративов о технологической безработице, пессимистических прогнозов относительно будущего взаимодействия между человеком и машиной, а также рисков утраты контроля над ИИ. Второй уровень угроз характеризуется ростом фишинга, дипфейков на основе всё более совершенных технологий ИИ, что создаёт дополнительные вызовы для государственной и корпоративной кибербезопасности и негативно влияет на ИПБ на личном, групповом и национальном уровнях воздействия. Анализ третьего уровня показал, что наибольшую опасность представляют технологии дипфейков и генеративного ИИ, применяемые для создания и распространения дезинформации, подрыва доверия к государственным институтам и СМИ, а также провоцирования социальных потрясений.

Острые экономические и социальные проблемы, внутривластные противоречия в сочетании с внешним давлением порождают благоприятные условия для ЗИИИ. Дальнейшее быстрое развитие и внедрение технологий ИИ без устранения негативных внутренних и внешних факторов однозначно повысит риски ИПБ посредством ЗИИИ для Египта уже в недалеком будущем. Социально-ориентированное и, вместе с тем, инновационное развитие – залог использования ИИ в национальных интересах, для мира и безопасности страны.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Пашенцев Е.Н., Чебыкина В.А., Шеметова Ю.Н. Злонамеренное использование искусственного интеллекта: вызовы информационно-психологической безопасности в Арабской Республике Египет. *Злонамеренное использование искусственного интеллекта и вызовы информационно-психологической безопасности в странах БРИКС*. М.: САМ Полиграфист, 2024. С. 36–43 [Pashentsev E.N., Chebykina V.A., Shemetova J.N. Malicious Use of Artificial Intelligence and Challenges to Psychological Security in the Arab Republic of Egypt. *Malicious Use of Artificial Intelligence and the Challenges of Information and Psychological Security in the BRICS Countries*. Moscow: SAM Poligrafist, 2024. Pp. 36–43 (in Russian)].

33% of employees in Egypt feel the lack of digital competencies. *Daily News Egypt*. 19.09.2023 (2). <https://www.dailynewsegypt.com/2023/09/19/33-of-employees-in-egypt-feel-the-lack-of-digital-competencies/> (accessed: 30.11.2025).

44% of employees in Egypt fear losing their jobs to AI. *Daily News Egypt*. 20.02.2023 (1). <https://www.dailynewsegypt.com/2023/02/20/44-of-employees-in-egypt-fear-losing-their-jobs-to-ai/> (accessed: 30.11.2025).

AbuJarour S., Qarariah A., Saadeh N., Salem M. AI, Misinformation, and Fake News: A Literature Review of Ethical and Technical Approaches. *Finance and Law in the Metaverse World. Contributions to Finance and Accounting*. N. Mansour, L.M. Bujosa Vadell (eds.) Cham: Springer, 2024. Pp. 641–652.

AI regulation in Egypt. *Just AI*. 23.05.2024. <https://justai.in/ai-regulations-in-egypt/> (accessed: 26.11.2025).

Assad A. Exploring the use of ChatGPT among media students in Egypt: Opportunities and challenges. *Online Journal of Communication and Media Technologies*. 2024. Vol. 14(2). Article e202424. <https://doi.org/10.30935/ojcm/14416>. (accessed: 30.11.2025).

Bahi R. Egypt as a Leading Nation: Regional Imperatives and Domestic Constraints. *Diplomatic Strategies of Nations in the Global South*. J. Braveboy-Wagner (ed.) Cham: Palgrave Macmillan, 2016. Pp. 155–179.

Bi X., Su X., Liu X. An Ellulian Analysis of Propaganda in the Context of Generative AI. *Ethics and Information Technology*. 2024. Vol. 26. Pp. 1–11.

Bontridder N., Poulet Y. The Role of Artificial Intelligence in Disinformation. *Data & Policy*. 2021. <https://doi.org/10.1017/DAP.2021.20>. (accessed: 30.11.2025).

Borak M. Only 0.1% of people can tell a deepfake, says iProov. *Biometric Update*. 12.02.2025. <https://www.biometricupdate.com/202502/only-0-1-of-people-can-tell-a-deepfake-says-iproov> (accessed: 30.11.2025).

Bosman A. Shadow AI vs Managed AI: Kaspersky reviews the use of neural networks for work in Egypt. *TECHZ Magazine*. 22.10.2025. <https://techznw.com/shadow-ai-vs-managed-ai-kaspersky-reviews-the-use-of-neural-networks-for-work-in-egypt/> (accessed: 30.11.2025).

Carno A. AI and anonymity fuel surge in digital violence against women. *UN News*. 20.11.2025. <https://news.un.org/en/story/2025/11/1166411> (accessed: 30.11.2025).

Dawoud A., Habashy A. W. A. An AI Blueprint for the Future of Work: Lessons from Egypt's Labour Market. *ORF Middle East*. 23.06.2025. <https://orfme.org/expert-speak/an-ai-blueprint-for-the-future-of-work-lessons-from-egypts-labour-market/> (accessed: 30.11.2025).

Drolet M. AI Is Amping Up Phishing, Smishing and Vishing Attacks. *Forbes*. 02.05.2025. <https://www.forbes.com/councils/forbestechcouncil/2025/05/02/ai-is-amping-up-phishing-smishing-and-vishing-attacks/> (accessed: 30.11.2025).

Egypt's AI Revolution: Driving Toward a 7.7% GDP Boost by 2030 with Cybersecurity Empowerment! *Africazine*. 25.11.2025. <https://africazine.com/2025/11/egypts-ai-revolution-driving-toward-a-7-7-gdp-boost-by-2030-with-cybersecurity-empowerment/> (accessed: 19.01.2026).

Egypt National AI Strategy. Second Edition (2025–2030). *The National Council for Artificial Intelligence*. https://www.asu.edu.eg/141090/_mediacenter/2025/pdf/c126e0d5c610f9e67ddb37b06d388bcf.pdf (accessed: 28.01.2025).

Egypt Artificial Intelligence Readiness Assessment Report 2025. *UNESCO*. <https://unesdoc.unesco.org/ark:/48223/pf0000395173> (accessed: 26.11.2025).

Al-Faour N. Egyptian Journalist Warns of Threat Posed by AI to Media Sector. *Arab News*. 27.09.2023.

Fourrage L. Top 10 Tech Companies to Work for in Egypt in 2025. *Nucamp*. 20.02.2025. <https://www.nucamp.co/blog/coding-bootcamp-egypt-egy-top-10-tech-companies-to-work-for-in-egypt-in-2025> (accessed: 30.11.2025).

Goldstein J.A., Chao J., Grossman S., Stamos A., Tomz M. How Persuasive is AI-Generated Propaganda? *PNAS Nexus*. 2024. <https://doi.org/10.1093/pnasnexus/pgae034>. (accessed: 30.11.2025).

Greig J. Microsoft seizes 240 websites used by Egyptian phishing-as-a-service operation 'ONNX'. *The Record*. 22.11.2024. <https://therecord.media/microsoft-seizes-websites-onnx-phishing> (accessed: 30.11.2025).

Harnessing Digital Egypt. *American Chamber of Commerce in Egypt*. <https://www.amcham.org.eg/publications/industry-insight/issue/41/harnessing-digital-egypt> (accessed: 30.11.2025).

Hashmi E., Yamin M.M., Yayilgan S.Y. Securing Tomorrow: a Comprehensive Survey on the Synergy of Artificial Intelligence and Information Security. *AI Ethics*. Cham: Springer, 2024. <https://doi.org/10.1007/s43681-024-00529-z>. (accessed: 30.11.2025).

Hokayem E., Momtaz R. Chapter Ten. Egypt: Regional Ambitions and Domestic Weakness. *Strategic Dossiers*. 2024. Vol. 2(1). Pp. 192–203.

Interpol Africa Cyberthreat Assessment Report 2025. 4th Edition. May 2025. *Interpol*. https://www.interpol.int/content/download/23094/file/Cybercrime_Africa%20Cyberthreat%20Assessment%20Report_Design_FINAL.pdf (accessed: 30.11.2025).

Jain S. US\$320 billion by 2030? The potential impact of Artificial Intelligence in the Middle East. *PWC*. 2018. <https://www.pwc.com/m1/en/publications/potential-impact-artificial-intelligence-middle-east.html> (accessed: 26.11.2025).

Kamal M. The Middle East According to Egypt. *Cairo Review*. 2018. Pp. 70–77. <https://www.thecairor-view.com/wp-content/uploads/2018/05/cr29-kamal.pdf> (accessed: 04.02.2025).

Kaspersky Urges Users to Stay Alert Amid Wave of Fake Investment Platforms. *Kaspersky*. 19.11.2025. <https://me-en.kaspersky.com/about/press-releases/kaspersky-urges-users-to-stay-alert-amid-wave-of-fake-investment-platforms> (accessed: 30.11.2025).

Kertysova K. Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered. *Security and Human Rights*. Vol. 29(1). 2019. Pp. 55–81.

Lukash A. Cyberattacks on Egypt's infrastructure in 2024. *Positive Technologies*. 26.02.2025. <https://global.ptsecurity.com/en/research/analytics/cyberattacks-on-egypt-s-infrastructure-in-2024/> (accessed: 30.11.2025).

Regulating Artificial Intelligence in Egypt: Proposed Standards and Principles. *Masaar*. 25.05.2025. <https://masaar.net/en/regulating-artificial-intelligence-in-egypt-proposed-standards-and-principles/> (accessed: 30.11.2025).

McBride J. Egypt's Growing Military Capabilities and Regional Implications Going Forward. *Manara Magazine*. 09.12.2024. <https://manaramagazine.org/2024/12/egypts-growing-military-capabilities-and-regional-implications-going-forward/> (accessed: 12.01.2025).

Mohieldin M., Amin-Salem H., El-Shal A., Moustafa E. *The Political Economy of Crisis Management and Reform in Egypt*. Cham: Palgrave Macmillan. 2024. <https://doi.org/10.1007/978-3-031-19482-5>. (accessed: 30.11.2025).

Over 1,800 US companies operate in Egypt with \$47bn invested over two decades: Madbouly. *Daily News Egypt*. 25.05.2025. <https://www.dailynewsegypt.com/2025/05/25/over-1800-us-companies-operate-in-egypt-with-47bn-invested-over-two-decades-madbouly/> (accessed: 30.11.2025).

Over 50% of users in Egypt encountered phishing attempts during electronic payments: report. *Egypt Independent*. 31.07.2022. <https://www.egyptindependent.com/over-50-of-users-in-egypt-encountered-phishing-attempts-during-electronic-payments-report/> (accessed: 30.11.2025).

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.

Ragab E. Regional competition for AI. *Ahram Online*. 24.10.2025. <https://english.ahram.org.eg/NewsContent/4/1204/555312/Opinion/Opinion/Regional-competition-for-AI.aspx> (accessed: 26.11.2025).

Rise in Cybercrimes in Egypt: Artificial Intelligence Between Innovation and Exploitation. *IPST*. 13.03.2025. <https://ipst.education/rise-in-cybercrimes-in-egypt-artificial-intelligence-between-innovation-and-exploitation/> (accessed: 30.11.2025).

Salah A. The Dark Side of AI: Perpetuating Digital Violence Against Women. *Women of Egypt Network*. 27.11.2024. <https://womenofegyptmag.com/2024/11/27/the-dark-side-of-ai-perpetuating-digital-violence-against-women/> (accessed: 30.11.2025).

Sandoval M.P., de Almeida Vau M, Solaas J. et al. Threat of Deepfakes to the Criminal Justice System: a Systematic Review. *Crime Science*. 2024. Vol. 13(41). <https://doi.org/10.1186/s40163-024-00239-1>. (accessed: 30.11.2025).

Sarkin J. J., Sotoudehfar S. Artificial Intelligence and Arms Races in the Middle East: The Evolution of Technology and Its Implications for Regional and International Security. *Defense & Security Analysis*. 2024. Vol. 40(1). Pp. 97–119.

Shahzaib. UAE, Egypt Explore Fatwa Cooperation and Digital Innovation in Religious Guidance. *MEA Tech Watch*. 14.08.2025. <https://meatechwatch.com/2025/08/14/uae-egypt-explore-fatwa-cooperation-and-digital-innovation-in-religious-guidance/> (accessed: 30.11.2025).

Shin D. Conclusion: Misinformation and AI – How Algorithms Generate and Manipulate Misinformation. *Artificial Misinformation. Exploring Human-Algorithm Interaction Online*. Cham: Palgrave Macmillan, 2024. Pp. 259–277.

Targeting the cybercrime supply chain. *Microsoft*. 22.11.2024. <https://www.microsoft.com/en-us/security/security-insider/risk-management/egypt-based-cybercriminal-suppliers-websites-seized> (accessed: 30.11.2025).

Yehoshua Y. IDF examining whether ‘foreign elements’ working to sabotage relations with Egypt. *Ynet Global*. 19.02.2025. <https://www.ynetnews.com/article/s11rnwm9je> (accessed: 30.11.2025).

Zilber A. Ex-Google Exec Mo Gawdat Warns AI Will View Humans as ‘Scum’, Could Create ‘Killing Machines’. *New York Post*. 18.05.2023. <https://nypost.com/2023/05/18/ex-google-exec-warns-ai-will-view-humans-as-scum/> (accessed: 30.04.2025).

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

ПАШЕНЦЕВ Евгений Николаевич –
доктор исторических наук, профессор,
главный научный сотрудник факультета
международных отношений Санкт-
Петербургского государственного
университета, СПб., Россия.

Evgeny N. PASHENTSEV, DSc (History),
Professor, Chief Research Fellow, Faculty of
International Relations, Saint Petersburg State
University, Saint Petersburg, Russia.