




DOI: 10.22363/2313-0660-2022-22-2-288-302

*Научная статья / Research article*

## Злонамеренное использование технологий искусственного интеллекта в странах Африки южнее Сахары: вызовы panaфриканской кибербезопасности

**К.А. Панцеров**  

Санкт-Петербургский государственный университет, Санкт-Петербург, Российская Федерация

 [pantserev@yandex.ru](mailto:pantserev@yandex.ru)

**Аннотация.** На протяжении двух десятилетий страны Африки южнее Сахары прилагали значительные усилия, направленные на быстрое развитие информационно-коммуникационных технологий. В настоящее время все ведущие мировые державы уделяют повышенное внимание созданию гибридных интеллектуальных систем, способных решать наиболее сложные задачи. Страны Африки южнее Сахары не остались в стороне от этого процесса. Их правительства убеждены, что передовые технологии являются наиболее эффективным инструментом, способным обеспечить устойчивый социально-экономический рост и решить наиболее насущные проблемы. Однако любые технологические новации, которые призваны упростить нашу жизнь, могут быть использованы и в злонамеренных целях. Настоящее исследование показывает возможные риски злонамеренного использования технологий искусственного интеллекта в странах Африки, расположенных южнее Сахары. Некоторые из этих рисков уже стали реальностью. Автор приходит к выводу, что проблема обеспечения информационно-психологической и кибербезопасности является общей для всех африканских стран. Именно она встает на пути обеспечения дальнейшего устойчивого социально-экономического роста государств рассматриваемого региона. На протяжении последнего десятилетия страны Африки южнее Сахары старались выработать совместное видение борьбы с киберпреступлениями и злонамеренным применением передовых технологий. Однако все их попытки создать действенные наднациональные институты, которые регулировали бы борьбу с кибератаками на panaфриканском уровне и учитывали бы интересы подавляющего большинства африканских стран, провалились. Данное обстоятельство демонстрирует наличие серьезных противоречий среди африканских государств, которые препятствуют установлению взаимовыгодного сотрудничества даже в такой важной сфере, какой является проблема обеспечения кибербезопасности. Тем не менее пока подобное сотрудничество не будет налажено, представляется маловероятным, что африканские страны хотя бы приблизятся к решению данной проблемы, что означает, что они и в дальнейшем будут подвергаться масштабным кибератакам, которые создают серьезную угрозу для личной, национальной и panaфриканской безопасности.

**Ключевые слова:** искусственный интеллект, стратегическая коммуникация, информационно-психологическое противоборство, информационная безопасность, кибербезопасность, страны Африки южнее Сахары

**Благодарности:** Статья выполнена при финансовой поддержке СПбГУ, проект № 93024916 «Искусственный интеллект и наука о данных: теория, технология, отраслевые и междисциплинарные исследования и приложения».

© Панцеров К.А., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.


<https://creativecommons.org/licenses/by/4.0/>

**Для цитирования:** Панцеров К. А. Злонамеренное использование технологий искусственного интеллекта в странах Африки южнее Сахары: вызовы панафриканской кибербезопасности // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 288—302. <https://doi.org/10.22363/2313-0660-2022-22-2-288-302>

## Malicious Use of Artificial Intelligence in Sub-Saharan Africa: Challenges for Pan-African Cybersecurity

Konstantin A. Pantserev  

St. Petersburg State University, Saint Petersburg, Russian Federation

 pantserev@yandex.ru

**Abstract.** For almost two decades, Sub-Saharan African countries have been making significant efforts to ensure the rapid development of industries related to information and communication technology (ICTs) in the region. At present, all leading nations are placing greater emphasis on the development of hybrid intelligent systems capable of solving extremely complicated tasks. This includes Sub-Saharan African countries, which consider the development of advanced technologies to be an effective instrument for ensuring sustainable social and economic growth and solving a great number of the continent's problems. It has become evident, however, that all technological novelties that should simplify our lives can be used for malicious purposes. The present study examines existing practices and risks of malicious use of artificial intelligence (MUAI) in Sub-Saharan African countries. At the end of the study, the author comes to the conclusion that the problem of ensuring information, psychological, and cybersecurity is common to all African countries, which creates a serious obstacle for their further sustainable social and economic development. Over the past decade, Sub-Saharan Africa has made significant efforts to elaborate a joint vision for counteracting cybercrimes and the malicious use of advanced technologies. But all the attempts to establish effective supranational instruments that would regulate the fight against cyberattacks at the Pan-African level and take into account the interests of the vast majority of African countries in this area have failed. This demonstrates the presence of serious contradictions among African countries, which, taken together, prevent the establishment of mutually beneficial cooperation even in such an important field as cybersecurity. However, until such cooperation is established, it seems unlikely that African countries will even come close to solving this problem, which means that their information space will continue to be subjected to large-scale cyber-attacks that pose a serious threat not only to the security of individuals, but also to national and Pan-African security.

**Key words:** artificial intelligence, strategic communication, psychological warfare, information security, cybersecurity, Sub-Saharan African countries

**Acknowledgements:** This research was supported by the St. Petersburg State University, project No. 93024916 “Artificial Intelligence and Data Science: Theory, Technology, Sectoral and Interdisciplinary Researches and Applications”.

**For citation:** Pantserev, K. A. (2022). Malicious use of artificial intelligence in Sub-Saharan Africa: Challenges for Pan-African cybersecurity. *Vestnik RUDN. International Relations*, 22(2), 288—302. <https://doi.org/10.22363/2313-0660-2022-22-2-288-302>

### Введение

Страны Африки южнее Сахары, несмотря на свое отставание в социально-экономическом развитии по сравнению с другими регионами, уделяют повышенное внимание технологическому развитию (Haula & Agbozo, 2020). При этом сегодня все ведущие страны делают особый акцент на исследования, направленные на создание гибридных интеллектуальных систем, способных решать

сложные прикладные задачи. Государства Африки южнее Сахары не являются исключением. Они убеждены, что развитие передовых технологий является эффективным инструментом, способным обеспечить устойчивый социально-экономический рост и решить многие типичные для региона проблемы. Однако и так очевидно, что все технологические новации, которые призваны упростить повседневную жизнь людей, могут быть использованы и со злым умыслом.

Технологии искусственного интеллекта (ИИ) открывают перед злоумышленниками широкий спектр возможностей и позволяют им пройти практически через любую киберзащиту. Благодаря передовым технологиям злоумышленники могут:

- скрывать вредоносные коды в официальных, безопасных приложениях;
- оказывать влияние на голосовую или визуальную аутентификацию;
- поставить устройства под свой контроль с помощью закрытых ключей;
- организовывать интеллектуальные атаки на системы или сети;
- имитировать надежные компоненты системы.

Принимая во внимание данное обстоятельство, автором предложена следующая гипотеза: технологии ИИ могут использоваться как с пользой, так и злонамеренно, и это всего лишь вопрос времени, когда злоумышленники начнут применять их в своих корыстных целях. В то время как государства должны поддерживать развитие передовых технологий, они также должны содействовать тому, чтобы правительственные органы, общество и отдельные лица не пострадали от неправильного использования таких технологий.

В исследовании используются два основных метода: кейс-стади уровня развития передовых технологий в различных странах Африки к югу от Сахары и критический дискурс-анализ национальных стратегий, дорожных карт, посвященных дальнейшему развитию и внедрению технологий искусственного интеллекта в Африке и обеспечению кибербезопасности в африканских странах. Этот метод был выбран потому, что критический дискурс-анализ демонстрирует, каким образом язык работает в социокультурном и политическом контекстах, фокусируясь на отношениях власти и идеологических перспективах, отраженных в дискурсивных текстах, и их более широком значении для общества (Chiluwa, 2019b). Таким образом, он помогает определить социальные проблемы, выраженные или отраженные в текстах, такие как злоупотребление политической властью, расовая дискриминация, ксенофобия или террористические угрозы, и проанализировать

возможные способы их решения (Chiluwa, 2019b).

Цель исследования состоит в том, чтобы, используя анализ существующих практик применения технологий искусственного интеллекта в странах Африки южнее Сахары, определить наиболее очевидные потенциальные угрозы, исходящие от этих технологий, а также предложить меры по укреплению информационной и психологической безопасности стран рассматриваемого региона.

В статье были поставлены следующие исследовательские вопросы:

1. Каков текущий уровень развития технологий искусственного интеллекта в Африке?
2. Имели ли место случаи злонамеренного применения технологий ИИ в Африке?
3. Какие меры должны принять страны Африки южнее Сахары, чтобы остановить дальнейшее злонамеренное использование передовых технологий?

## Обзор литературы

Современный научный дискурс включает в себя широкий корпус работ, направленных на изучение различных аспектов, связанных с технологиями ИИ<sup>1</sup>, часть из которых всецело посвящена вопросам злонамеренного применения таких технологий (Brundage et al., 2018; Chesney & Citron, 2018; Antinori, 2019; Bazarkina & Pashentsev, 2019; Dack, 2019). Отдельная группа работ посвящена информационно-психологическому противоборству в целом и проблеме манипулирования информацией в частности (Jeangène Vilmer et al., 2018; Pashentsev, 2019; Bazarkina, Pashentsev & Simons, 2020). При этом практически отсутствуют исследования, посвященные развитию

<sup>1</sup> См.: Chandler S. Deepfakes 2.0: The Terrifying Future of AI and Fake News // Daily Dot. October 5, 2018. URL: <https://www.dailydot.com/debug/deepfakes-ai-clones-fake-news> (accessed: 04.07.2021); Chesney R., Citron D. Deepfakes and the New Disinformation War: The Coming Age of Post Truth Geopolitics // Foreign Affairs. January/February 2019. URL: <https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war> (accessed: 04.07.2021); Fillion R. M. Fighting the Reality of Deepfakes // Nieman Lab. 2019. URL: <https://www.niemanlab.org/2018/12/fighting-the-reality-of-deepfakes> (accessed: 30.07.2021).

технологий ИИ в странах Африки южнее Сахары, в том числе тому, в какой степени страны рассматриваемого региона защищены от потенциального и фактического злонамеренного применения таких технологий. Настоящая статья призвана восполнить этот пробел.

### **Передовые технологии в странах Африки южнее Сахары: миф или реальность?**

Необходимость развития передовых технологий рассматривается как важнейшее условие обеспечения мирового лидерства в современном мире. В существующих реалиях может показаться, что африканские страны сталкиваются с большим количеством типичных для континента проблем, не связанных с развитием технологий, таких как гражданские беспорядки, коррупция в государственных структурах, низкий уровень образования, плохое медицинское обслуживание, цифровой разрыв, равно как отсутствие инфраструктуры для удовлетворения социально-экономических потребностей (Haula & Agbozo, 2020). На первый взгляд очевидно, что в сложившихся условиях необходимость развития технологий ИИ неизбежно должна отойти на второй план; однако это не совсем так. Дело в том, что за последнее десятилетие в Африке произошли существенные сдвиги в осознании роли технологий и инноваций в содействии решению всех наиболее значимых проблем региона (Haula & Agbozo, 2020).

Объясняется данное обстоятельство тем, что африканские страны рассматривают развитие прорывных технологий как определенную гарантию своего технологического суверенитета и убеждены, что технологии искусственного интеллекта могут, среди прочего, решить многие традиционные проблемы континента (*Artificial Intelligence for Africa...*, 2018). Так, например, в сельском хозяйстве технологии ИИ могут быть использованы для повышения производительности и эффективности сельскохозяйственных работ. Использование беспилотных летательных аппаратов, оснащенных гибридными интеллектуальными системами, могло бы найти широкое применение в Африке. Эти беспилотники было бы целесообразно не только

использовать для удобрения сельскохозяйственных плантаций, но и оснащать аппараты точными датчиками, которые помогли бы при осуществлении мониторинга сельскохозяйственных плантаций обнаруживать признаки вредителей и болезней сельскохозяйственных культур, а также оценивать степень засушливости почвы. Изображения, сделанные с помощью беспилотных летательных аппаратов, затем могут автоматически проверяться и анализироваться, а полученные данные предоставят фермерам ценную информацию о состоянии их посевов без необходимости дополнительных лабораторных исследований<sup>2</sup>.

Технологии ИИ также могли бы оказать значительную помощь в модернизации систем здравоохранения африканских стран, сделав медицину в регионе более высокотехнологичной. Одной из главных проблем африканских медицинских учреждений является нехватка квалифицированного медицинского персонала, и технологии искусственного интеллекта могли бы частично решить эту проблему, обеспечивая первичную медицинскую диагностику, а также сбор и обработку данных о пациентах и их истории болезни. Тогда врач сможет принимать больше пациентов за одну смену. Передовые технологии также могли бы повысить уровень медицинской диагностики и выявлять опасные заболевания на более ранней стадии, что увеличивает шансы на полное выздоровление. ИИ также был бы полезен для обеспечения удаленной диагностики в сельских районах с помощью чат-ботов и компьютерного зрения, обеспечивая тем самым доступ к медицинской помощи миллионам африканцев, которые в противном случае не смогли бы ее получить. Таким образом, чат-боты, например, могли бы свести к минимуму посещения больниц, помогали проводить первичные консультации, давать рекомендации по лечению и записывать на прием к профильному специалисту. Наконец, специально разработанные мобильные приложения, работающие на основе искусственного интеллекта, могли бы помочь в диагностике асфиксии при

<sup>2</sup> Oduma E. How AI Can Transform Kenyan Industries // Ai Kenya. January 21, 2019. URL: <https://kenya.ai/how-ai-can-transform-kenyan-industries> (accessed: 28.07.2021).

рождении и малярии в сельских районах Африки, где ощущается нехватка квалифицированных медицинских работников и медицинского оборудования (Owoyemi et al., 2020).

ИИ также может широко использоваться правительствами африканских стран и значительно сократить бумажную волокиту, повысить эффективность государственного сектора и увеличив скорость предоставления государственных услуг. Это позволило бы руководителям государственных органов решить проблему распределения ресурсов путем перенаправления сотрудников туда, где они были бы наиболее востребованы. Прогностические возможности ИИ могут иметь особое значение, поскольку позволят государственным чиновникам и политикам быстрее реагировать на потребности общества: от профилактического вмешательства социальных служб для помощи детям и другим социально уязвимым слоям населения в трудных жизненных ситуациях до предупреждения преступности и быстрого реагирования в чрезвычайных ситуациях. Наконец, алгоритмы на основе искусственного интеллекта могли бы также предоставить гражданам новые платформы для оценки качества, адекватности и эффективности государственных услуг, что обеспечило бы более эффективную обратную связь с населением.

Гибридные интеллектуальные системы также можно было бы использовать в сфере образования для автоматизации оценки знаний учащихся, что позволило бы преподавателям высвободить время для решения других важных задач, включая дополнительное консультирование учащихся по изучаемым предметам, подготовку к занятиям или повышение собственной квалификации. ИИ также может оказать дополнительную помощь учащимся в виде голосовых помощников, автоматизированных преподавателей и кураторов с целью создания индивидуальной траектории обучения, основанной на способностях каждого отдельного учащегося. Кроме того, искусственный интеллект может использоваться для мониторинга успеваемости учащихся и оповещения преподавателей о возможных проблемах с успеваемостью, обеспечивая полезную обратную связь об эффективности курса.

Таким образом, на основе вышеизложенного можно сделать вывод, что искусственный интеллект является мощным потенциальным инструментом, способным оказать помощь африканским странам в решении наиболее значимых проблем континента и обеспечить устойчивое социально-экономическое развитие и переход к инновационной экономике. Сами африканские страны стремятся проводить собственные научные исследования в этой области. Так, в Африке уже сегодня реализуется ряд стартапов, широко применяющих технологии искусственного интеллекта.

Например, 1 июня 2012 г. в ЮАР была запущена специальная служба управления данными под названием *MySmartFarm*, которая существенно упрощает сбор информации для фермеров. Данный сервис автоматически собирает широкий корпус данных для того, чтобы представить фермерам различную полезную информацию, а также дать некоторые рекомендации и прогнозы<sup>3</sup>. Этот стартап стал быстро пользоваться большим спросом среди южноафриканцев и в 2013 г. получил награду *IBM South Africa SmartCamp Award*, которая предполагала поддержку и наставничество со стороны американской корпорации IBM<sup>4</sup>.

Другой стартап, *DroneClouds*, был запущен в ЮАР в 2015 г. Его цель — помочь фермерам повысить урожайность, предоставляя им оперативную информацию о растениеводстве, полученную с помощью дронов, спутников, мобильных устройств, облачных технологий и агроэкспертов<sup>5</sup>.

В Гане стартап *SyeComp* также фокусируется на развитии сельского хозяйства при помощи передовых технологий. Он специализируется на сборе, обработке и анализе данных, полученных со спутников и беспилотных

<sup>3</sup> MySmartFarm // Solar Impulse Foundation. URL: <https://solarimpulse.com/companies/mysmartfarm> (accessed: 18.08.2021).

<sup>4</sup> Sanchez D. MySmartFarm Ag Solution Wins IBM SmartCamp Award // The Moguldom Nation. October 11, 2013. URL: <https://moguldom.com/24914/mysmartfarm-app-wins-ibm-south-africa-award> (accessed: 01.02.2022).

<sup>5</sup> Lourie G. 7 South African Drone Firms to Keep an Eye on // TFS Media. September 12, 2017. URL: <https://www.techfinancials.co.za/2017/09/12/httpstalkiot-co-za201709117-south-african-drone-firms-to-keep-an-eye-on> (accessed: 01.02.2022).

летательных аппаратов (Artificial Intelligence for Africa..., 2018, p. 19).

В Кении также начата реализация двух стартапов, основанных на алгоритмах искусственного интеллекта. Один из них, именуемый *FarmDrive*, представляет собой технологическую платформу, которая предоставляет финансовым учреждениям модель, основанную на большом объеме данных, относящихся к сельскохозяйственной отрасли, и необходимую для оценки рисков при выдаче кредитов и разработки целевых кредитных продуктов, которые отвечали бы потребностям мелких фермеров<sup>6</sup>. Другой стартап предполагает интеграцию в социальные сети и мессенджеры специализированного чат-бота по имени *Sophie*<sup>7</sup>. Этот бесплатный чат-бот, оснащенный удобным голосовым интерфейсом, представляет собой платформу, на которой любой пользователь может задать вопросы в интимной сфере, в том числе в области репродуктивной медицины, и получить исчерпывающий ответ. Эта услуга доступна на нескольких популярных платформах социальных сетей, таких как Messenger и Twitter.

Нигерия также активно внедряет технологии искусственного интеллекта в повседневную жизнь людей. Наиболее успешным примером является технологическая платформа *Kudi.ai* (слово *kudi* означает «деньги» на языке хауса). Она была запущена в 2017 г. как чат-бот, работающий на алгоритмах искусственного интеллекта; его основной задачей является оказание помощи в финансовой сфере, включая перевод денег и оплату счетов. Кроме того, как и в случае с *Sophie*, *Kudi* интегрирован в большинство популярных приложений для обмена сообщениями и социальных сетей<sup>8</sup>, в частности Facebook (21.03.2022 г. Тверской районный суд г. Москвы удовлетворил иск Генпрокуратуры РФ и признал деятельность соцсети Facebook,

принадлежащей Meta, экстремистской, запретив их работу в России. — *Прим. ред.*). Другой чат-бот под названием *Lara*, запущенный 5 марта 2017 г., представляет собой интеллектуальную систему, которая помогает пользователям добираться из одной точки в другую посредством подробной текстовой пошаговой инструкции и заблаговременно сообщает точную стоимость проезда<sup>9</sup>.

Банковский сектор Нигерии также начинает использовать технологии искусственного интеллекта. Так, расположенный в Нигерии *Zenith Bank* запустил несколько новых технологических решений, которые обеспечивают клиентов более удобными, безопасными и быстрыми транзакциями. Среди таких решений банковское приложение *Scan to Pay*, которое клиенты банка могут использовать для совершения онлайн-платежей и покупок в магазинах за считанные секунды с помощью сканирования кода на любом телефоне, имеющем подключение к Интернету. Мобильное приложение банка также предлагает расширенные функциональные возможности, такие как мгновенное открытие счета для новых клиентов (Artificial Intelligence for Africa..., 2018, p. 14).

В мае 2017 г. другой нигерийский банк — *Wema Bank* — запустил первый африканский полностью цифровой банк под названием *ALAT*. Он дает возможность клиентам открыть счет с помощью мобильного телефона или Интернета менее чем за пять минут, а дебетовые карты доставляются в любую точку Нигерии в течение двух-трех дней бесплатно (Artificial Intelligence for Africa..., 2018, p. 14).

В Уганде была запущена *Awamo* — цифровая банковская платформа и кредитное бюро, использующее технологии искусственного интеллекта для борьбы с мошенничеством при регистрации клиентов и предприятий на своей платформе. Платформа помогает оцифровывать бизнес-процессы, обмениваться кредитной информацией и предоставляет много других услуг с использованием

<sup>6</sup> FarmDrive. URL: <https://farmdrive.co.ke> (accessed: 18.08.2021).

<sup>7</sup> SophieBot. URL: <https://web.archive.org/web/20161104205907/http://www.sophiebot.tk/> (accessed: 18.08.2021)

<sup>8</sup> Akinwamide N. Kudi AI is Putting a Human Feel to Online Payments in Nigeria // Techpoint Africa. February 8, 2017. URL: <https://techpoint.africa/2017/02/08/kudi-ai-online-payments-nigeria> (accessed: 29.07.2021).

<sup>9</sup> Ndiomewese I. Startup Profile: Lara — Get Step-By-Step Public Transportation Directions to Any Destination // Techpoint Africa. April 17, 2017. URL: <https://techpoint.africa/2017/04/17/lara-profile> (accessed: 29.07.2021).

мобильных устройств (Butcher, Wilson-Strydom & Baijnath, 2021, p. 48).

На основании всех этих примеров можно сделать вывод, что африканские страны начинают использовать технологии искусственного интеллекта при создании различных сервисов, направленных на удовлетворение потребностей своих граждан. В то же время необходимо иметь в виду, что все эти технологии могут быть использованы и со злым умыслом. Именно поэтому представляется чрезвычайно важным изучить существующие практики и риски злонамеренного использования искусственного интеллекта в Африке.

### **Риски злонамеренного использования технологий искусственного интеллекта в странах Африки южнее Сахары**

Страны Африки южнее Сахары постоянно подвергаются различным кибератакам, таким как фишинг, DDoS-атаки и кража данных (Online African Organized Crime..., 2020). Данное обстоятельство дает нам возможность заключить, что при развитии информационного сектора в каждой отдельно взятой стране необходимо уделять повышенное внимание вопросам обеспечения информационной безопасности как государства в целом, так и его граждан.

Согласно официальным данным, в 2017 г. общий ущерб от киберпреступности по всей Африке составил 3,5 млрд долл. США. Наибольший ущерб — 649 млн долл. США — был причинен Нигерии, на втором месте находится Кения с 210 млн долл. США, а замыкает тройку лидеров ЮАР с общим ущербом в 157 млн долл. США<sup>10</sup>. Несомненно, эти впечатляющие цифры свидетельствуют о том, что правительства африканских стран должны предпринять определенные усилия для укрепления информационной безопасности в своих странах. Дальнейший анализ статистики показывает, что африканские банки наиболее часто подвергаются кибератакам — на их долю приходится 23 % атак, за ними следуют государственные органы различного уровня

<sup>10</sup> Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line // Serianu. 2017. URL: <https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf> (accessed: 05.07.2021).

(19 %), электронная коммерция (16 %), мобильные транзакции (13 %) и телекоммуникационный сектор (11 %) <sup>11</sup>.

Проблема осложняется тем обстоятельством, что страны Африки в целом уделяют крайне незначительное внимание вопросам, связанным с обеспечением своей информационной безопасности. Согласно официальным данным, сегодня свыше 60 % африканских предприятий не обучили свой персонал основам кибербезопасности. Более 90 % крупных африканских компаний тратят менее 10 тыс. долл. США на различные вопросы, связанные с обеспечением своей кибербезопасности<sup>12</sup>. Таким образом, африканские страны являются крайне привлекательными для киберпреступников. В отчете 2013 г., посвященном вопросам кибербезопасности, выделяются два ключевых обстоятельства, способствующих росту киберпреступности в Африке: массовый доступ к оптоволоконной широкополосной системе связи, что способствует быстрому увеличению числа пользователей Интернета, и отсутствие развитого законодательства, направленного на борьбу с киберпреступностью (Kharouni, 2013). Примечательно, что за все это время, несмотря на то, что многие африканские страны приняли ряд законов, направленных на защиту персональных данных и борьбу с киберпреступностью, позитивных изменений в этой области не произошло, а резкое увеличение числа киберпреступлений в Африке представляет серьезную угрозу личной, национальной и даже международной информационной безопасности.

В настоящее время высокий уровень коррупции в государственных учреждениях и слабая инфраструктура обработки данных, подверженная их утечкам, представляют угрозу конфиденциальности данных и успешному внедрению технологий ИИ (Butcher, Wilson-Strydom & Baijnath, 2021, p. 62).

Подавляющее большинство киберпреступлений, происходящих в Африке, носят финансовый характер и направлены на кражу

<sup>11</sup> Isiauwe D. Cybersecurity Threat Evolution: Perspectives from Africa // The Information Security Society of Africa — Nigeria. February 15, 2020. URL: <https://www.issan.org.ng/download/cyber-security-threat-evolution> (accessed: 05.07.2021).

<sup>12</sup> Ibid.



денег у частных лиц. Согласно отчету Интерпола об оценке киберугроз в Африке, наиболее распространенными киберугрозами в Африке являются онлайн-мошенничество, цифровое вымогательство, компрометация деловой электронной почты, ботнеты и программы-вымогатели<sup>13</sup>. Ситуация упрощается тем фактом, что массовая цифровизация породила значительный массив различных баз данных, которые содержат персональные данные огромного количества обычных людей. В Африке такие базы данных имеют очень слабую киберзащиту и довольно часто попадают в руки злоумышленников, которые используют эту информацию, чтобы получить что-то ценное от своих жертв.

Одной из крупнейших кибератак в Африке является утечка персональных данных жителей ЮАР, произошедшая в 2017 г.<sup>14</sup> Файлы, содержащие личную информацию миллионов как живых, так и умерших южноафриканцев, оказались в свободном доступе в Интернете, среди прочего файлы содержали национальные идентификационные номера, информацию о семейном положении, доходах, месте работы и имуществе. Примечательно, что эту утечку данных нельзя назвать хакерской атакой в полном смысле этого слова, поскольку вся эта информация о пользователях была размещена на веб-сайте компании по обработке данных *Dracore Data Sciences* без какой-либо дополнительной защиты<sup>15</sup>. Совершенно очевидно, что это был лишь вопрос времени, когда эта информация попадет в руки хакеров, которые могут распоряжаться ею по своему усмотрению.

<sup>13</sup> Cyberthreat Assessment Report: Interpol's Key Insight into Cybercrime in Africa // Interpol. October 21, 2021. URL: <https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa> (accessed: 11.07.2021).

<sup>14</sup> Mohapi T. What We Know So Far about South Africa's Largest Ever Data Breach // iAfrikan. October 18, 2017. URL: <https://web.archive.org/web/20210122034431/https://iafrikan.com/2017/10/17/south-africas-govault-hacked-over-30-million-personal-records-leaked/> (accessed: 11.07.2021).

<sup>15</sup> Mohapi T. Is Dracore Data Sciences Responsible for South Africa's Largest Ever Data Leak? // iAfrikan. October 18, 2017. URL: <https://web.archive.org/web/20210404225144/https://www.iafrikan.com/2017/10/18/dracore-data-sciences/> (accessed: 11.07.2021).

Помимо подобных случаев, имеющих все признаки преступной халатности, африканские страны регулярно сталкиваются с массированными кибератаками, часть из которых активно использует возможности искусственного интеллекта и атакует критическую инфраструктуру в Африке. Так, например, *Life Healthcare*, второй по величине оператор частных больниц в Южной Африке, отвечающий за предоставление цифровых услуг в больницах ЮАР, в июне 2020 г. столкнулся с крупномасштабной кибератакой, которая вывела из строя его базы данных и серверы электронной почты. Это привело к месячному простоем медицинских учреждений и, таким образом, к фатальным последствиям в разгар пандемии коронавируса.

В октябре 2020 г. в ЮАР произошли две другие кибератаки, в результате которых в Йоханнесбурге были выведены из строя ключевые социальные службы и службы экстренной помощи. Целью атак было принуждение властей ЮАР к выплате выкупа в криптовалюте<sup>16</sup>. В июле 2021 г. государственная южноафриканская компания *Transnet* столкнулась с беспрецедентной кибератакой, в результате которой были нарушены контейнерные операции в двух наиболее крупных южноафриканских портах (Кейптаун и Дурбан). 22 июля 2021 г. официальный веб-сайт *Transnet* вышел из строя и показывал лишь сообщение об ошибке. Компания, которая управляет не только крупнейшими портами ЮАР, но и огромной железнодорожной сетью, перевозящей полезные ископаемые и другие идущие на экспорт товары, официально подтвердила, что в ее компьютерной системе произошли сбои. Институт исследований безопасности (Institute for Security Studies, ISS) в этой связи отметил, что впервые целостность важнейшей морской инфраструктуры Южной Африки была серьезно нарушена в результате масштабной кибератаки, способной полностью парализовать

<sup>16</sup> Cyberthreat Assessment Report: Interpol's Key Insight into Cybercrime in Africa // Interpol. October 21, 2021. URL: <https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa> (accessed: 11.07.2021).



работу двух наиболее крупных и значимых южноафриканских портов<sup>17</sup>. Так, например, такие горнодобывающие компании, как Glencore и Barrick Gold, разрабатывающие крупные месторождения меди и кобальта в Демократической Республике Конго и Замбии, используют Дурбан для отправки грузов из Африки<sup>18</sup>.

Этот последний пример наглядно демонстрирует, как передовые технологии могут быть злонамеренно использованы с целью отключения критически важной инфраструктуры в африканских странах. Истинная причина кибератаки на компьютерные системы Transnet не была установлена, но есть некоторые опасения, что это может быть связано с беспорядками и насилием, которые прокатились по некоторым районам страны ранее в том же году.

Время от времени Эфиопия также сталкивалась с крупномасштабными кибератаками на свою критически важную инфраструктуру. Особого внимания в этой связи заслуживают события, развернувшиеся вокруг строительства эфиопской плотины на р. Нил, которая, как известно, является источником напряженности в отношениях между Эфиопией и Египтом. Так, в июне 2020 г. египетская группа *Cyber\_Horus* предприняла попытку крупной кибератаки с целью создания значительного экономического, психологического и политического давления на Эфиопию<sup>19</sup>. Этой группе удалось взломать ряд правительственных веб-сайтов и распространить сообщения с угрозами войны, если Эфиопия введет в строй данную плотину.

Последний пример иллюстрирует, что передовые технологии используются в Африке не только с целью получения некоторой

выгоды в материальной сфере, но и для манипулирования общественным мнением и усиления социальной напряженности. Наиболее подходящим техническим решением для этого является технология создания поддельных видео и аудио. Сама по себе эта технология, также называемая дипфейки, представляет собой метод синтеза изображений с использованием соответствующих алгоритмов искусственного интеллекта, в результате чего получается виртуальный двойник реального человека, который двигается и говорит точно так же, как и его прообраз. Эта технология открывает широкий спектр возможностей для злонамеренного использования и представляет серьезную угрозу личной, национальной и международной безопасности, поскольку позволяет злоумышленнику или потенциальному террористу заставить любого политика или просто известного человека сказать или сделать все, что захочет злоумышленник. В дальнейшем это поддельное видео может быть опубликовано на поддельном аккаунте того или иного человека в социальных сетях или на поддельном сайте известного СМИ. За короткое время видео может набрать значительное количество просмотров и быстро распространиться по всему Интернету и, в конце концов, положить конец политической карьере выбранного человека или даже спровоцировать глубокий политический кризис между странами.

Примечательно, что сегодня дипфейки могут быть созданы практически любым человеком, имеющим необходимое программное обеспечение и готовым потратить на это несколько часов своего времени. Результаты же этой деятельности могут нанести серьезный ущерб не только репутации отдельных людей, но, что еще более страшно, могут быть использованы для манипулирования массовым сознанием<sup>20</sup>.

Одним из наиболее показательных примеров использования передовых технологий для разжигания массового недовольства и

<sup>17</sup> Cyberthreat Assessment Report: Interpol's Key Insight into Cybercrime in Africa // Interpol. October 21, 2021. URL: <https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa> (accessed: 11.07.2021).

<sup>18</sup> Shabalala Z., Heiberg T. Cyber Attack Disrupts Major South African Port Operations // Reuters. July 22, 2021. URL: <https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/> (accessed: 29.09.2021).

<sup>19</sup> Allen N. Africa's Evolving Cyber Threats // Africa Center for Strategic Studies. January 19, 2021. URL: <https://africacenter.org/spotlight/Africa-evolving-cyber-threats> (accessed: 29.09.2021).

<sup>20</sup> Neille D. Manipulating Reality: The Rise of Deepfakes and How to Spot Them // Daily Maverick. May 05, 2021. URL: <https://www.dailymaverick.co.za/article/2021-05-05-manipulating-reality-the-rise-of-deepfakes-and-how-to-spot-them> (accessed: 18.09.2021).

напряженности в отношениях между различными африканскими странами является активное применение дипфейков во время волны беспорядков и насилия, которая прокатилась в ЮАР в 2019 г. на почве ксенофобских настроений после того, как водители грузовиков устроили забастовку в знак протеста против трудоустройства иностранцев. Во время массовых погромов предприятий, принадлежащих иностранным компаниям, в Йоханнесбурге в начале сентября 2019 г. погибли 12 человек. Хотя на самом деле никто из граждан Нигерии не пострадал (среди убитых десять были гражданами ЮАР, а двое — Зимбабве), в социальных сетях быстро появилось множество поддельных видеороликов и изображений, на которых якобы изображены нападения и убийства нигерийцев или их массовая депортация<sup>21</sup>. Чтобы еще больше разжечь массовое недовольство, в Интернете также появилось вырванное из контекста видео, в котором утверждается, что на нем изображено горящее здание в ЮАР, хотя на самом деле пожар произошел в Индии в штате Гуджарат и никакого отношения к событиям в ЮАР не имел<sup>22</sup>.

В результате распространения этих поддельных видеороликов Нигерия отозвала делегацию с большой международной конференции, проходившей в ЮАР, и объявила об эвакуации своих граждан из этой страны. Данное событие вынудило правительство ЮАР принести официальные извинения Нигерии за нападения на почве ксенофобии, которые вызвали всплеск напряженности между двумя странами, и заверить своих нигерийских партнеров, что все случаи массовых погромов принадлежащих нигерийцам предприятий будут тщательно расследованы<sup>23</sup>. По-

<sup>21</sup> Faife C. In Africa, Fear of State Violence Informs Deepfake Threat // WITNESS. December 9, 2019. URL: <https://blog.witness.org/2019/12/africa-fear-state-violence-informs-deepfake-threat> (accessed: 18.07.2021).

<sup>22</sup> Burning Building Video from India, Not from Xenophobic Violence in South Africa // Africa Check. September 19, 2019. URL: <https://africacheck.org/fact-checks/fbchecks/burning-building-video-india-not-xenophobic-violence-south-africa> (accessed: 18.07.2021).

<sup>23</sup> South Africa Offers 'Profuse' Apologies to Nigeria After Attacks // Al Jazeera. September 16, 2019. URL: [https://www.aljazeera.com/news/2019/9/16/south-africa-](https://www.aljazeera.com/news/2019/9/16/south-africa-offers-profuse-apologies-to-nigeria-after-attacks)

добное злонамеренное использование передовых технологий с целью разжигания конфликта между двумя странами в регионе, в котором у многих стран есть нерешенные споры и претензии друг к другу, представляет очень серьезную угрозу международной информационной и психологической безопасности, поскольку любое такое столкновение может перерасти в еще один полномасштабный вооруженный конфликт на континенте.

Остается только вопросом времени, когда подобные технологии начнут использоваться действующие в Африке террористические группировки, такие как Бoko Харам в Нигерии, Ансар ад-Дин в Мали, Движение за единство и джихад в Западной Африке и «Аш-Шабаб» в Сомали. Эти группировки могли бы применять передовые технологии с целью улучшения коммуникации между боевиками, распространения пропаганды своих взглядов по всей Африке и вербовки новых сторонников. Поскольку Интернет сочетает в себе такие преимущества, как скорость, дешевизна, доступность и анонимность, он предлагает террористам множество вариантов для пропаганды своей экстремистской идеологии и вербовки новых сторонников (Chiluwa, 2019c, p. 208). Таким образом, Интернет в целом — и социальные сети в частности — следует рассматривать как очень удобный инструмент для террористической пропаганды и вербовки (Chiluwa, 2019a, p. 522). Важность Интернет-коммуникаций в современной общественной жизни и применение Интернета и информационных технологий террористами породили концепцию «Терроризма 2.0», когда террористические группировки широко используют Интернет и передовые технологии в своей повседневной деятельности (Ishengoma, 2013).

Не исключено также, что скоро террористы достаточно хорошо познакомятся с искусственным интеллектом и начнут использовать его возможности для организации высокотехнологичных террористических атак. Бoko Харам, например, активно эксплуатирует для ведения наблюдения беспилотные

[offers-profuse-apologies-to-nigeria-after-attacks](https://www.aljazeera.com/news/2019/9/16/south-africa-offers-profuse-apologies-to-nigeria-after-attacks) (accessed: 18.07.2021).

летательные аппараты, которые, как сообщается, являются более современными, чем те, которые имеются в распоряжении правительства<sup>24</sup>. «Аш-Шабаб» уже обвиняли в «твиттер-терроризме» и разжигании ненависти, что привело к закрытию ряда их аккаунтов в Twitter (Chiluwa, Chimuanya & Ajiboeye, 2020). Проблема заключается в том, что вместо заблокированного аккаунта тут же создается десяток новых. Поэтому африканские страны должны приложить все усилия для укрепления своей информационно-психологической и кибербезопасности и предотвращения дальнейшего злонамеренного использования технологий на основе искусственного интеллекта.

### **Обеспечение информационно-психологической безопасности в странах Африки южнее Сахары: проблемы и перспективы**

Проблема обеспечения информационно-психологической и кибербезопасности продолжает оставаться ключевым фактором, препятствующим дальнейшему устойчивому социально-экономическому развитию стран Африки южнее Сахары. Сегодня на континенте наблюдается дефицит сертифицированных специалистов по кибербезопасности, составляющий 100 тыс. человек<sup>25</sup>. Многим организациям и предприятиям не удается внедрить элементарные меры, направленные на повышение уровня своей кибербезопасности. Правительства часто не отслеживают киберугрозы и не преследуют киберпреступников. 96 % киберпреступлений остаются незарегистрированными или нераскрытыми, а это означает, что реальное количество киберпреступлений в Африке, по всей видимости, существенно превышает официальные данные<sup>26</sup>. Тем не менее целый ряд африканских

стран усердно работают над этим вопросом и приступили к существенной модернизации своего национального законодательства, поскольку для государств с более слабым потенциалом в области кибербезопасности сильная нормативно-правовая база является важным элементом, обеспечивающим защиту от иностранного вмешательства и киберугроз<sup>27</sup>. Согласно данным, предоставленным Международным союзом электросвязи (МСЭ), около 40 африканских стран имеют законы, направленные на борьбу с киберпреступностью. Кроме того, 11 стран (ЮАР, Ботсвана, Уганда, Замбия, Буркина-Фасо, Танзания, Камерун, Нигерия, Бенин, Гана и Кот-д'Ивуар) участвуют в совместных программах и инициативах в области кибербезопасности<sup>28</sup>.

В частности, Руанда, Кения и Уганда приняли ряд мер по противодействию киберугрозам и защите данных в киберпространстве. Эти меры следует признать эффективными, но их недостаточно для комплексного решения проблемы. Руанда, например, разработала Национальную политику в области кибербезопасности, в рамках которой была выдвинута инициатива создания Национального центра компьютерной безопасности и реагирования, ориентированного на выявление и предотвращение киберугроз. Также был разработан Национальный план действий в чрезвычайных ситуациях в киберпространстве для противодействия киберкризисам. Наконец, в 2016 г. в Руанде был принят закон, направленный на регулирование всего информационно-телекоммуникационного сектора, содержащий ряд статей, посвященных злонамеренному использованию информационных технологий с целью совершения преступлений, и предусматривающий уголовную ответственность за несанкционированный доступ к данным<sup>29</sup>.

<sup>24</sup> Allen N. Africa's Evolving Cyber Threats // Africa Center for Strategic Studies. January 19, 2021. URL: <https://africacenter.org/spotlight/Africa-evolving-cyber-threats> (accessed: 29.09.2021).

<sup>25</sup> Ibid.

<sup>26</sup> Van der Waag-Cowling N. Living Below the Cyber Poverty Line: Strategic Challenges for Africa // Humanitarian Law and Policy. June 11, 2020. URL: <https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa> (accessed: 18.08.2021).

<sup>27</sup> Ibid.

<sup>28</sup> Digital Trends in Africa: Information and Communication Technology Trends and Developments in the Africa Region, 2017—2020 // International Telecommunication Union, 2021. URL: [https://www.itu.int/dms\\_pub/itu-d/opb/ind/D-IND-DIG\\_TRENDS\\_AFR.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AFR.01-2021-PDF-E.pdf) (accessed: 18.08.2021).

<sup>29</sup> Rwanda: 2016 Law Governing Information and Communication Technologies // ARTICLE 19. May 2018. URL: <https://www.article19.org/wp-content/uploads/2018/>

Кения разработала свою собственную Национальную стратегию кибербезопасности в 2014 г.<sup>30</sup> В соответствии с этой стратегией были приняты поправки к закону об информационных технологиях, направленные на криминализацию незаконного доступа к информации. Также была создана Национальная Кенийская группа реагирования на компьютерные инциденты — Координационный центр (National KE-CIRT/CC), которая получила поддержку МСЭ и осуществляет координацию мер реагирования на киберугрозы на национальном уровне<sup>31</sup>.

Уганда также имеет более или менее хорошо развитую законодательную базу для обеспечения кибербезопасности. В стране принят специальный закон о злонамеренном использовании компьютерных технологий, который обеспечивает защиту банковских транзакций и позволяет отслеживать и перехватывать подозрительные сообщения. Также были созданы специальная Национальная группа реагирования на чрезвычайные ситуации в киберпространстве и специализированный Национальный информационно-консультативный и технологический орган, в задачи которых входит оказание технической поддержки и обучение в области кибербезопасности.

Однако очевидно, что невозможно решить все проблемы, с которыми сталкиваются африканские страны в этой области, только путем введения различных запретительных мер на национальном уровне. Проблема обеспечения кибер- и информационно-психологической безопасности представляется крайне сложной, и ее комплексное решение возможно только при участии всех заинтересованных

сторон, к которым относятся представители различных государственных органов, топ-менеджеры крупных компаний, представители финансового сектора и гражданского общества. В то же время особое внимание следует уделить необходимости активизации сотрудничества в этой области между всеми африканскими странами.

С этой целью в 2006 г. по итогам Международной конференции по компьютерной безопасности и киберпреступности в Африке была создана Африканская ассоциация и информационной безопасности<sup>32</sup>. Миссия этой организации заключается в развитии информационной безопасности в Африке, и любая заинтересованная сторона, стремящаяся к обеспечению информационной безопасности, включая частных лиц, организации и различные правительственные органы власти, может присоединиться к ассоциации. Согласно информации, представленной на ее веб-сайте, основная деятельность данной Ассоциации направлена на обмен передовым мировым опытом в области информационной, компьютерной и интернет-безопасности и организацию кампаний по борьбе с киберпреступностью в Африке, в первую очередь путем организации и проведения семинаров и конференций, публикации книг и журналов, ведения веб-сайтов и блогов, а также консультаций и разработки различных руководящих принципов по вопросам обеспечения кибербезопасности<sup>33</sup>. Ежегодный мониторинг уровня информационной безопасности в Африке является одним из наиболее важных направлений деятельности Ассоциации. Однако, несмотря на то, что данная Ассоциация существует более десяти лет, мы не смогли найти каких-либо существенных результатов ее деятельности, а содержание ее веб-сайта остается достаточно скудным.

Среди других важных инициатив, демонстрирующих попытку африканских стран выработать совместный подход к обеспечению информационной безопасности, следует отметить Конвенцию Африканского союза по кибербезопасности и защите персональных

05/Analysis-Rwanda-ICT-Law-April-2018.pdf (accessed: 18.08.2021).

<sup>30</sup> National Cybersecurity Strategy of Kenya // Ministry of Information Communications and Technology of Kenya. February 2014. URL: [https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National\\_Strategies\\_Repository/Kenya\\_2014\\_GOK-national-cybersecurity-strategy.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Kenya_2014_GOK-national-cybersecurity-strategy.pdf) (accessed: 18.08.2021).

<sup>31</sup> Digital Trends in Africa: Information and Communication Technology Trends and Developments in the Africa Region, 2017—2020 // International Telecommunication Union, 2021. URL: [https://www.itu.int/dms\\_pub/itu-d/opb/ind/D-IND-DIG\\_TRENDS\\_AFR.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AFR.01-2021-PDF-E.pdf) (accessed: 18.08.2021).

<sup>32</sup> African Information Security Association (AISA). URL: <https://web.archive.org/web/20120128191125/http://www.jidaw.com/aisa> (accessed: 18.08.2021).

<sup>33</sup> Ibid.

данных, которая была принята в 2014 г. в Малабо, Экваториальная Гвинея<sup>34</sup>. Появление этого документа следует считать важным шагом, который доказывает желание африканских стран разработать совместные механизмы для дальнейшей борьбы с киберпреступностью и обеспечить основу для кибербезопасности в Африке. В рамках этой задачи государствам — участникам Конвенции предлагается разработать национальную политику в области кибербезопасности, а также правовые, нормативные и институциональные рамки для ее обеспечения<sup>35</sup>. В то же время, однако, процесс подписания и последующей ратификации этого документа показывает наличие серьезных противоречий между различными африканскими странами в области кибербезопасности. На сегодняшний день Конвенцию подписали только 14 африканских стран, и только 13 (Ангола, Гана, Гвинея, Замбия, Кабо-Верде, Маврикий, Мозамбик, Намибия, Нигер, Республика Конго, Руанда, Сенегал и Того) ратифицировали ее<sup>36</sup>. Примечательно, что региональные лидеры в области информационных технологий, такие как Кения, Нигерия и ЮАР, не подписали этот документ.

Принимая во внимание то обстоятельство, что Конвенция так и не вступила в силу, поскольку ее должны ратифицировать по меньшей мере 15 стран, ее подписавших<sup>37</sup>, ее можно

<sup>34</sup> African Union Convention on Cyber Security and Personal Data Protection // The Institute for Security Studies. June 27, 2014. URL: <https://issafrica.org/ctafrika/uploads/AU%20Convention%20on%20Cyber%20Security%20and%20Personal%20Data%20Protection.pdf> (accessed: 21.07.2021).

<sup>35</sup> Jili B. The Spread of Surveillance Technology in Africa Stirs Security Concerns // Africa Center for Strategic Studies. December 11, 2020. URL: <https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns> (accessed: 05.09.2021).

<sup>36</sup> List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection // African Union. March 25, 2022. URL: [https://au.int/sites/default/files/treaties/29560-sl-AFRICAN\\_UNION\\_CONVENTION\\_ON\\_CYBER\\_SECURITY\\_AND\\_PERSONAL\\_DATA\\_PROTECTION.pdf](https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf) (accessed: 01.04.2022).

<sup>37</sup> African Union Convention on Cyber Security and Personal Data Protection // African Union. June 27, 2014. URL: [https://au.int/sites/default/files/treaties/29560-treaty-0048\\_-\\_african\\_union\\_convention\\_on\\_cyber\\_security\\_and\\_personal\\_data\\_protection\\_e.pdf](https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf) (accessed: 05.09.2021).

рассматривать только как еще один программный документ, пытающийся регулировать вопросы обеспечения кибербезопасности. Однако даже с учетом трудностей, связанных с ратификацией Конвенции, само появление этого документа свидетельствует о глубокой озабоченности стран Африки вопросами, связанными с обеспечением своей кибербезопасности<sup>38</sup>. При этом Конвенция в очередной раз показала, что наднациональные институты и инструменты работают крайне плохо в африканских условиях, возможно, из-за многочисленных противоречий между африканскими странами, препятствующих разработке общих рабочих инструментов для решения наиболее значимых проблем континента, включая информационно-психологическую и кибербезопасность.

В этой связи только Нигерийской Ассоциации информационной безопасности (ISSAN) удалось добиться относительного успеха и стать реальной платформой для сотрудничества и обмена мнениями между всеми заинтересованными сторонами, включая банки, телекоммуникационные компании, государственные учреждения, государственные регулирующие органы, IT-компании, консультантов по информационной безопасности и юристов<sup>39</sup>. Следует особо подчеркнуть, что данная Ассоциация является некоммерческой организацией, направленной на обеспечение защиты нигерийского киберпространства, в первую очередь банковского и государственного секторов. Она решает эту задачу путем проведения комплекса мероприятий, направленных на знакомство всех заинтересованных сторон с передовым опытом в этой области.

## Заключение

На основе вышеизложенного можно сделать следующие выводы.

Страны Африки южнее Сахары уделяют повышенное внимание разработке различных

<sup>38</sup> Tomlin S. N. Cyberspace Security in Africa — Where Do We Stand? // African Academic Network on Internet Policy. February 12, 2020. URL: <https://aanoip.org/cyberspace-security-in-africa-where-do-we-stand> (accessed: 18.08.2021).

<sup>39</sup> Information Security Society of Africa — Nigeria (ISSAN). URL: <https://issan.org.ng> (accessed: 18.08.2021).

технологических решений, основанных на алгоритмах искусственного интеллекта. Использование беспилотных летательных аппаратов следует рассматривать как наиболее перспективную технологию с большим потенциалом в регионе. Применение беспилотников способно оказать существенную помощь не только в сфере сельского хозяйства, но также и в других областях, в том числе сфере безопасности (Haula & Agbozo, 2020). Например, дроны могут использоваться для мониторинга перемещений террористов и выявления целей / угроз, эффективного управления земельными ресурсами и проведения кадастровой разведки, обработки сельскохозяйственных угодий удобрениями и орошения, а также повышения урожайности сельскохозяйственных культур.

Вместе с тем очевидно, что любые технологические новации могут быть использованы и со злым умыслом. Страны Африки к югу от Сахары продолжают страдать от всевозможных киберпреступлений, которые в эпоху стремительного развития технологий, основанных на искусственном интеллекте, становятся все более высокотехнологичными. Проблема обеспечения информационно-психологической и кибербезопасности является общей для всех африканских стран, что создает серьезное препятствие для их дальнейшего устойчивого социально-экономического развития. Так, дроны, например, могут использоваться для блокирования других дронов или GPS-

сигналов. Такие угрозы должны быть тщательно изучены, прежде чем использование беспилотных летательных аппаратов станет широко распространенным в регионе (Vattapparamban et al., 2016).

В течение последнего десятилетия страны Африки южнее Сахары предприняли значительные усилия по разработке совместного видения противодействия киберпреступлениям и злонамеренному использованию передовых технологий. Все их попытки создать эффективные наднациональные инструменты, которые регулировали бы борьбу с кибератаками на panaфриканском уровне и учитывали интересы подавляющего большинства африканских стран в этой области, провалились. Это свидетельствует о наличии между африканскими странами серьезных противоречий, которые в своей совокупности препятствуют налаживанию взаимовыгодного сотрудничества даже в такой важной области, как кибербезопасность.

Однако до тех пор, пока такое сотрудничество не появится, представляется маловероятным, что африканские страны хотя бы приблизятся к решению этой проблемы, а это означает, что их информационное пространство будет продолжать подвергаться крупномасштабным кибератакам, которые представляют серьезную угрозу не только для безопасности отдельных лиц, но и для национальной и panaфриканской безопасности.

Поступила в редакцию / Received: 10.03.2022

Доработана после рецензирования / Revised: 03.04.2022

Принята к публикации / Accepted: 18.04.2022

### Библиографический список

- Antinori A.* Terrorism and Deepfakes: From Hybrid Warfare to Post-Truth Warfare in a Hybrid World // Proceedings of the European Conference on the Impact of Artificial Intelligence and Robotics / ed. by P. Griffiths, M. Nowshade. Reading, South Oxfordshire, England : Academic Conferences and publishing limited, 2019. P. 23—20.
- Artificial Intelligence for Africa: An Opportunity for Growth, Development, and Democratisation* // Access Partnership. 2018. URL: [https://www.up.ac.za/media/shared/7/ZP\\_Files/ai-for-africa.zp165664.pdf](https://www.up.ac.za/media/shared/7/ZP_Files/ai-for-africa.zp165664.pdf) (accessed: 12.02.2022).
- Bazarkina D. Y., Pashentsev E. N.* Artificial Intelligence and New Threats to International Psychological Security // *Russia in Global Affairs*. 2019. Vol. 17, no. 1. P. 147—170. <https://doi.org/10.31278/1810-6374-2019-17-1-147-170>
- Bazarkina D. Y., Pashentsev E. N., Simons G.* Terrorism and Advanced Technologies in Psychological Warfare: New Risks, New Opportunities to Counter the Terrorist Threat. New York : Nova Science Publishers, 2020.

- Brundage M., Avin S., Clark J., Toner H., Eckersley P. et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAI, 2018. P. 1—100. URL: <https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf> (accessed: 12.02.2022).
- Butcher N., Wilson-Strydom M., Baijnath M. Artificial Intelligence Capacity in Sub-Saharan Africa // Compendium Report. International Development Research Centre. 2021. URL: <https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/59999/27ea1089-760f-4136-b637-16367161edcc.pdf?sequence=1> (accessed: 12.02.2022).
- Chesney R., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // California Law Review. 2018. Vol.107, no. 1753. P. 1753—1820. <https://doi.org/10.15779/Z38RV0D15J>
- Chiluwa I. E. (2019a). Deception in Online Terrorist Propaganda: A Study of ISIS and Boko Haram // Handbook of Research on Deception, Fake News, and Misinformation Online / ed. by I. E. Chiluwa, S. A. Samoilenko. Hershey, PA : Information Science Reference, 2019a. P. 520—537. <https://doi.org/10.4018/978-1-5225-8535-0.ch028>
- Chiluwa I. E. Discourse Analysis and Conflict Studies // SAGE Research Methods Cases. London : SAGE Publications, 2019b. <https://dx.doi.org/10.4135/9781526468208>
- Chiluwa I. E. Online Activism in Mali: A Study of Digital Discourses of the Movement for the Liberation of Azawad // Activism, Campaigning and Political Discourse on Twitter / ed. by I. E. Chiluwa, G. Bourvier. New York : Nova Science Publishers, 2019c. P. 207—234.
- Chiluwa I. E., Chimuanya L., Ajiboye E. Communicating Religious Extremism in West Africa // Themes in Religion and Human Security in Africa / ed. by J. Tarusarira, E. Chitando. London : Routledge, 2020. P. 166—179. <https://doi.org/10.4324/9781003017080-12>
- Dack S. Deep Fakes, Fake News, and What Comes Next. The Henry M. Jackson School of International Studies, University of Washington, 2019. URL: <https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next> (accessed: 12.02.2022).
- Haula K., Agbozo E. A Systematic Review on Unmanned Aerial Vehicles in Sub-Saharan Africa: A Socio-Technical Perspective // Technology in Society. 2020. Vol. 63. P. 1—7. <https://doi.org/10.1016/j.techsoc.2020.101357>
- Ishengoma F. R. Online Social Networks and Terrorism 2.0 in Developing Countries // International Journal of Computer Science and Network Solutions. 2013. Vol. 1, no. 4. P. 1—12. <https://doi.org/10.48550/arXiv.1410.0531>
- Jeaugène Vilmer J.-B., Escorcía A., Guillaume M., Herrera J. Les manipulations de l'information: un défi pour nos démocraties // Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées. 2018. P. 1—214. URL: [https://www.diplomatie.gouv.fr/IMG/pdf/les\\_manipulations\\_de\\_l\\_information\\_2\\_cle04b2b6.pdf](https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2_cle04b2b6.pdf) (accessed: 12.02.2022).
- Kharouni L. Africa: A New Safe Harbor for Cybercriminals? // Trend Micro Incorporated Research Paper. 2013. P. 1—31. URL: <https://web.archive.org/web/20220403192613/https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf> (accessed: 12.02.2022).
- Online African Organized Crime from Surface and Dark Web // Interpol Analytical Report. 2020. URL: <https://www.euneighbours.eu/sites/default/files/publications/2020-08/INTERPOL%20report.pdf> (accessed: 12.02.2022).
- Owoyemi A., Owoyemi J., Osiyemi A., Boyd A. Artificial Intelligence for Healthcare in Africa // Frontiers in Digital Health. 2020. Vol. 2. P. 1—5. <https://doi.org/10.3389/fgth.2020.00006>
- Pashentsev E. Destabilization of Unstable Dynamic Social Equilibriums through High-Tech Strategic Psychological Warfare // Proceedings of the 14th International Conference on Cyber Warfare and Security / ed. by N. van der Waag-Cowling, L. Leenen. Reading, South Oxfordshire, England : Academic Conferences and publishing limited, 2019. P. 322—328.
- Vattapparamban E., Güvenç İ., Yurekli A., Akkaya K., Uluagaç S. Drones for Smart Cities: Issues in Cybersecurity, Privacy, and Public Safety // 2016 International Wireless Communications and Mobile Computing Conference (IWCMC). New York : Institute of Electrical and Electronics Engineers, 2016. P. 216—221. <https://doi.org/10.1109/IWCMC.2016.7577060>

**Сведения об авторе:** Панцеров Константин Арсеньевич — доктор политических наук, профессор кафедры теории и истории международных отношений факультета международных отношений Санкт-Петербургского государственного университета; ORCID: 0000-0002-2164-9525; e-mail: pantserev@yandex.ru