DOI: 10.31857/S032150750016841-7 *Оригинальная статья / Original article*

Существующие практики и риски злонамеренного использования искусственного интеллекта в странах Африки к югу от Сахары

© Панцерев К.А.[a], 2021

[a] Санкт-Петербургский государственный университет. Санкт-Петербург, Россия
ORCID ID: 0000-0002-2164-9525; pantserev@yandex.ru

Резюме. В современном мире непременным условием обеспечения лидирующих позиций на мировой арене для любого государства является развитие прорывных технологий. Однако и так очевидно, что любые технологические новации создают риск их злонамеренного использования в будущем. Страны Африки в этом отношении не являются исключением. Они регулярно становятся жертвами кибератак, которые с каждым годом, по мере развития информационных технологий, становятся все более высокотехнологизированными.

В статье предпринят анализ существующей практики и рисков злонамеренного применения передовых технологий в странах Африки, расположенных южнее Сахары. Автор отмечает, что сегодня кибератакам в наибольшей степени подвергается банковский сектор. Однако передовые технологии постепенно начинают применяться также с целью манипулирования массовым сознанием и создания необходимого злоумышленникам общественного мнения, направленного на рост социальной напряженности в отдельных странах и регионах, что представляет весьма серьезную угрозу международной информационно-психологической безопасности.

В конечном итоге, автор делает вывод о том, что странам Африки следует разработать эффективные наднациональные инструменты, направленные на повышение уровня своей информационной защищенности и недопущения дальнейшего злонамеренного использования работающих на основе искусственного интеллекта технологий. До тех пор, пока этого не произойдет, представляется маловероятным, что африканские страны хотя бы приблизятся к решению проблемы обеспечения их информационной безопасности, а значит, их информационное пространство будет и впредь подвергаться масштабным кибератакам, представляющим серьезную угрозу не только безопасности отдельных людей, но и всей системе национальной безопасности государства.

Ключевые слова: страны Африки южнее Сахары, информационные технологии, стратегическая коммуникация, искусственный интеллект, информационно-психологическая безопасность, инновации

Благодарность. Статья выполнена при финансовой поддержке СПбГУ. Проект № 73555239 «Искусственный интеллект и наука о данных: теория, технология, отраслевые и междисциплинарные исследования и приложения».

Для цитирования: Панцерев К.А. Существующие практики и риски злонамеренного использования искусственного интеллекта в странах Африки к югу от Сахары. *Азия и Африка сегодня*. 2021. № 10. С. 31-37. DOI: 10.31857/S032150750016841-7

Existing practice and risks of malicious use of artificial intelligence in Sub-Saharan Africa

© Konstantin A. Pantserev[a], 2021

[a] Saint-Petersburg State University. Saint-Petersburg, Russia
ORCID ID: 0000-0002-2164-9525; pantserev@yandex.ru

Abstract. The necessity of the development of advanced technologies is considering as the essential condition for the ensuring of the world leadership in the contemporary world. But the rapid growth of such technologies and their implementation into all spheres of our life increase the risk of their malicious use in the future. African countries are no exception in this regard. They regularly become victims of cyber-attacks, which every year become more and more high-tech.

There has been undertaken in the article the analysis of the existing practice and risks of malicious use of advanced technologies in Sub-Saharan Africa. The author notes that today the banking sector is most exposed to cyber-attacks. But advanced technologies are gradually beginning to be used also for the mind management and creating the public opinion convenient for perpetrators who are aimed on the increase of social tension in certain countries or the entire regions. Undoubtedly even the possibility of such attacks poses a very serious threat to international information and psychological security. Finally, the author comes to the conclusion that African countries should develop effective supranational instruments aimed at improving their information security and preventing further malicious use of advanced technologies. Until this happens, it seems unlikely that African countries will even come close to solving the problem of ensuring their information security. So 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 the entire national security system of the state.

Keywords: States of Sub-Saharan Africa, Information Technologies, Strategic Communication, Artificial Intelligence, Information and Psychological Security, Innovations

Acknowledgment. This research was supported by the St. Petersburg State University, project № 73555239 "Artificial Intelligence and the Data Science: Theory, Technology, Sectoral and Interdisciplinary Research and Applications".

For citation: Konstantin A. Pantserev. Existing practice and risks of malicious use of artificial intelligence in Sub-Saharan Africa. *Aziya i Afrika segodnya*. 2021. № 10. Pp. 31-37. (In Russ.). DOI: 10.31857/S032150750016841-7

ВВЕДЕНИЕ

В современном мире непременным условием обеспечения лидирующих позиций на мировой арене для любого государства является развитие прорывных технологий. Особое внимание при этом уделяется созданию технологий на основе искусственного интеллекта (ИИ), возможности которого растут с каждым днем. Однако следует иметь в виду, что современные информационные технологии развиваются настолько быстрыми темпами, что становится очевидным, что за ними «не поспевают ни правовое регулирование в отдельных странах, ни система международного права, ни существующие механизмы контроля» [1].

В этом как раз и заключается главный вызов цифровой эпохи. Все разработанные в последние годы технологические новации призваны сделать нашу жизнь проще, однако отсутствие эффективных механизмов контроля, равно как и надлежащей нормативно-правовой базы резко повышают риск злонамеренного использования таких технологий.

Искусственный интеллект в этой связи не является исключением, а наша быстро растущая зависимость от компьютеризированных интеллектуальных систем делает нас крайне уязвимыми перед лицом злоумышленников, которые также используют технологии на основе искусственного интеллекта как для удовлетворения своих личных потребностей, так и для нанесения непоправимого урона критически важной инфраструктуре [2]. Данное обстоятельство создает серьезную угрозу международной информационно-психологической безопасности.

РИСКИ ЗЛОНАМЕРЕННОГО ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СТРАНАХ АФРИКИ К ЮГУ ОТ САХАРЫ

На первый взгляд, может показаться, что угрозы, связанные с возможным злонамеренным использованием искусственного интеллекта, имеют в Африке второстепенное значение в силу общего относительно невысокого уровня (по сравнению с развитыми странами западной цивилизации) развития *IT*-сферы. Однако это не совсем так. Данное обстоятельство обусловлено, прежде всего, тем, что за последние два десятилетия странам Африки все-таки удалось добиться существенных успехов в развитии рынка ИКТ. Но в то же самое время, взяв твердый курс на внедрение на своей территории прорывных технологий, указанные государства практически не уделяли внимания необходимости обеспечения своей информационной безопасности. В результате, страны Африки регулярно становятся жертвами кибератак, которые с каждым годом, по мере развития информационных технологий, становятся все более высокотехнологизированными.

Согласно официальным данным, общий объем ущерба от деятельности киберпреступников в Африке превысил $3,5 млрд. При этом наибольший ущерб приходится на Нигерию ($649 млн). На втором месте находится Кения ($210 млн), а на третьем - ЮАР ($157 млн) [3]. Что касается конкретных сфер деятельности, которые в наибольшей степени подвергаются кибератакам, наиболее уязвимым является банковский сектор африканских стран. Его доля в общем количестве кибератак составляет 23%, затем следуют правительственные структуры различного уровня (19%), электронная торговля (16%), система мобильных переводов (13%) и телекоммуникация (11%) [4].

Применение работающих на основе искусственного интеллекта технологий открывает практически неограниченные возможности для злоумышленников и позволяет им обходить любую киберзащиту. В частности, благодаря передовым технологиям киберпреступники могут:

- скрывать вредоносный код в официальных, безопасных приложениях;
- влиять на голосовую или визуальную аутенфикацию;
- получать закрытые ключи для контроля устройств;
- проводить интеллектуальные атаки на системы и сети;
- имитировать надежные компоненты системы [5];
- манипулировать массовым сознанием благодаря умелому использованию поддельного видео (технология дипфейкс).

И с каждым годом количество киберпреступлений неуклонно растет. Так, одна только Кения всего за три месяца 2019 г. (с апреля по июнь) столкнулась более чем с 26 млн кибератак. С нашей точки зрения, подобный стремительный рост числа кибератак за столь короткий промежуток времени обусловлен тем, что цифровая инфраструктура африканских стран по-прежнему крайне плохо укомплектована программными средствами, которые способны противостоять интеллектуальным кибератакам и свыше 60% африканских предприятий не обучают своих сотрудников в сфере кибербезопасности. К этому следует добавить, что свыше 90% крупных африканских компаний тратят менее $10 000 на обеспечение своей кибербезопасности [4]. Все эти факты в своей совокупности объясняют, почему Африка - крайне привлекательный регион для различного рода киберпреступников.

В подтверждение данного тезиса мы хотели бы привести отчет с говорящим названием - «Африка: новая безопасная гавань для киберпреступников?», который был подготовлен и опубликован еще в апреле 2013 г. компаний *Trend Micro*, которая является признанным мировым лидером в сфере производства технологических решений, направленных на обеспечение кибербезопасности [6].

В этом отчете указывается на 2 ключевых обстоятельства, которые, по мнению автора документа, способствуют росту киберпреступности в Африке: массовый доступ к системе оптоволоконной широкополосной связи, который способствует быстрому увеличению количества Интернет-пользователей, и отсутствие развитого законодательства в сфере обеспечения кибербезопасности. При этом мы видим, что за последние годы, несмотря на то, что в целом ряде африканских стран все-таки были приняты законы, направленные на защиту персональных данных и борьбу с киберпреступностью, каких-либо позитивных изменений в этой сфере не произошло, а резкое увеличение количества киберпреступлений в Африке представляет серьезную угрозу как для личной, так и для национальной и даже международной информационно-психологической безопасности африканских стран.

Одной из наиболее масштабных кибератак принято считать утечку персональных данных жителей Южно-Африканской Республики, которая случилась в 2017 г. [7]. В сети Интернет в свободном доступе появились доступные для скачивания файлы, содержащие личную информацию миллионов южноафриканцев, как живых, так и уже умерших: их паспортные данные (*national identity number*), сведения о семейном положении, размере дохода, сведения о работе и занимаемой должности, а также информацию о собственности. Примечательно, что подобную утечку данных нельзя назвать в полном смысле хакерской атакой, поскольку вся эта информация о пользователях была размещена на сайте компании по обработке данных - *Dracore Data Sciences* без какой-либо дополнительной защиты [8]. Совершенно очевидно, что было исключительно вопросом времени, когда эти сведения попадут в руки злоумышленников, которые теперь могут ими распоряжаться по своему усмотрению.

Помимо подобных случаев, которые имеют все признаки преступной халатности, регулярно с массированными кибератаками сталкиваются африканские банки. В качестве примера мы хотели бы привести кибератаку на расположенный в Руанде Акционерный банк ("*Equity Bank*"). Прежде всего, следует отметить, что этот банк первым в Африке стал предлагать услуги в сфере он-лайн и мобильного банкинга на основе технологии, которая соединяет воедино банкинг и телефонию. Вот почему этот банк оказался столь привлекательным для киберпреступников. Был даже создан преступный синдикат, который состоял из 8-ми кенийцев, трех руандийцев и одного угандийца. Они пытались организовать хакерскую атаку на компьютерную систему банка, но у них ничего не вышло, и они были арестованы полицией Руанды. Однако в процессе расследования этого уголовного дела была доказана причастность этих людей и к организации похожих хакерских атак в Кении и Уганде [9].

Таким образом, на основе вышеизложенного, можно сделать вывод о том, что необходимость обеспечения кибербезопасности, на сегодняшний день, является главным условием обеспечения национальной безопасности стран Африки. Вот почему сегодня большое количество африканских стран начинает уделять повышенное внимание обеспечению своей информационной безопасности.

Так, например, в Кении в начале 2019 г. было арестовано свыше 130 хакеров и мошенников [9], но, несмотря на все эти меры, в Африке наблюдается существенный рост киберпреступности, а финансовые потери от подобных высокотехнологичных преступлений представляют серьезную угрозу не только для региона Восточной Африки, но для всего континента.

Однако, что немаловажно, помимо хакерских атак на африканские банки с целью кражи денежных средств, которые представляют серьезную угрозу информационной безопасности личности в цифровом пространстве, в странах Африки передовые технологии постепенно начинают применяться с целью мани-

пулирования массовым сознанием и созданием необходимого злоумышленникам общественного мнения, направленного на рост социальной напряженности.

Наиболее подходящей технологией в этой связи является функционирующая на основе алгоритмов искусственного интеллекта технология создания поддельного видео. Сама по себе технология создания фейковых видеороликов, которые еще именуют дипфейками либо глубинными фейками, представляет собой метод синтеза изображения при помощи соответствующих алгоритмов, работающих на основе искусственного интеллекта.

Эта технология открывает широкие возможности для злонамеренного использования и представляет серьезную угрозу для личной, национальной и международной информационно-психологической безопасности, поскольку она дает возможность злоумышленнику заставить любого политика сказать все, что он хочет, а затем опубликовать эту фейковую речь на *YouTube* или *Facebook*, либо на поддельном сайте известных СМИ или на поддельном профиле того или иного политика в социальных сетях. Фейковое видео может достаточно быстро стать вирусным в сети и привести, в конечном итоге, к концу политической карьеры того или иного человека или даже вызвать кризис в отношениях между странами.

Одним из наиболее показательных из пока еще не многочисленных примеров использования «высоких» технологий с целью разжигания массового недовольства и напряженности в отношениях между отдельными африканскими странами является активное применение поддельных видеороликов во время прокатившейся по ЮАР в 2019 г. на почве ксенофобских настроений волны беспорядков и насилия, после того, как водители грузовиков устроили забастовку в знак протеста против трудоустройства иностранцев.

В ходе состоявшихся в начале сентября 2019 г. в Йоханнесбурге массовых погромов принадлежащих иностранцам предприятий были убиты 12 человек. И, несмотря на то, что среди убитых на самом деле не оказалось ни одного нигерийца (из 12 убитых 10 человек были гражданами ЮАР, а 2 - Зимбабве) в социальных сетях появились поддельные видеоролики и изображения, на которых якобы были изображены нападения и убийства нигерийцев либо их массовая депортация [10].

С целью дальнейшего разжигания массового недовольства в сети также появилось вырванное из контекста видео, на котором изображено горящее здание, которое на самом деле расположено в Индии в штате Гуджарат, но на видео утверждалось, что пожар произошел в ЮАР [11].

В результате, Нигерия отозвала делегацию с крупной международной конференции, проходившей в Южной Африке, и заявила об эвакуации своих граждан из этой страны. Это вынудило ЮАР принести Нигерии официальные извинения за серию ксенофобских нападений, которые привели к всплеску напряженности между двумя странами, и заверить своих нигерийских партнеров в том, что все случае массовых погромов принадлежащих нигерийцам предприятий будут тщательным образом расследованы [12].

С нашей точки зрения, подобная апробация злонамеренного использования передовых технологий с целью разжигания конфликта между двумя государствами в регионе, в котором многие страны имеют неурегулированные споры и претензии друг к другу, представляет весьма серьезную угрозу международной информационно-психологической безопасности, поскольку любое такое боестолкновение может перерасти в очередной полномасштабный вооруженный конфликт на континенте. Это означает, что станам Африки следует направить все свои усилия на повышение уровня своей информационной безопасности и недопущения дальнейшего злонамеренного использования работающих на основе искусственного интеллекта технологий.

СТРАНЫ АФРИКИ НА ПУТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Сегодня целый ряд африканских стран начинает активно работать над обеспечением свое информационной безопасности. Руанда, например, в 2015 г. разработала и предложила Национальную политику в сфере обеспечения кибербезопасности: был создан Национальный центр компьютерной безопасности и реагирования, в задачи которого как раз и входит обнаружение и предотвращение киберугроз. В стране также разработан направленный на борьбу с киберкризисами Национальный план действий в чрезвычайных ситуациях в киберпространстве. Наконец, в Руанде в 2016 г. был принят Закон об информационных и коммуникационных технологиях, в котором содержатся положения о злонамеренном использовании компьютерных технологий с целью совершения преступлений, которые предусматривают уголовную ответственность за несанкционированный доступ к данным.

В Кении в 2014 г. была разработана собственная Национальная стратегия по кибербезопасности, в соответствии с которой были приняты поправки в Закон об информации и связи с целью криминализации несанкционированного доступа к компьютерной информации. Помимо этого, в Кении был также создан Национальный координационный центр реагирования на компьютерные преступления, направленный на налаживание регионального и международного сотрудничества в этой сфере.

Свою достаточно развитую нормативно-правовую базу в сфере обеспечения кибербезопасности имеет Уганда. В этой стране был принят специальный Закон о неправомерном использовании компьютеров, который обеспечивает защиту электронных транзакций и дает возможность осуществлять мониторинг и перехват подозрительных сообщений. Помимо этого, в Уганде также создана Национальная группа реагирования на чрезвычайные ситуации в киберпространстве и специализированный Национальный информационно-консультативный и технологический орган, в задачи которого входит обеспечение технической поддержки и обучение в сфере кибербезопасности [9].

Таким образом, опираясь на вышеизложенные факты, можно сделать вывод о том, что Руанда, Кения и Уганда приняли ряд мер, направленных на борьбу с киберугрозами и защиту данных в киберпространстве. С нашей точки зрения, эти меры следует признать эффективными, но они не являются достаточными для комплексного и всестороннего решения проблемы.

На наш взгляд, невозможно решить все стоящие перед странами Африки задачи в указанной сфере только посредством внедрения различных запретительных мер на государственном уровне в отдельных африканских странах. Особенно подчеркнем, что проблема обеспечения информационной безопасности - это достаточно сложная, многомерная задача, комплексное решение которой возможно только посредством привлечения всех заинтересованных сторон, которые включают в себя представителей различных органов власти, топ-менеджеров крупных компаний, представителей банковского сектора и гражданского общества. При этом особенно следует сделать акцент на необходимости активизации сотрудничества в указанной сфере между всеми африканскими странами.

В этой связи в Африке была даже создана специализированная Африканская ассоциация по информационной безопасности (*African Information Security Association - AISA*). Эта Ассоциация была создана в 2006 г. как один из ключевых результатов Международной конференции по компьютерной безопасности и киберпреступлениям в Африке *(International Conference on Computer Security and Cybercrime in Africa*). Миссией Ассоциации является развитие информационной безопасности в Африке. Войти в состав Ассоциации может любая заинтересованная сторона, которая обеспокоена обеспечением информационной безопасности - отдельные люди, организации и различные правительственные структуры.

Согласно информации, представленной на сайте, основная деятельность Ассоциации нацелена на то, чтобы делиться передовым мировым опытом в области обеспечения информационной, компьютерной и интернет-безопасности и организовывать различные кампании по борьбе с киберпреступностью в Африке - прежде всего путем организации и проведения семинаров, конференций, публикации книг и журналов, ведения веб-сайтов, блогов, а также разработки различных руководящих принципов безопасности, консультаций. Отдельное важное направление деятельности Ассоциации - проведение ежегодного мониторинга уровня информационной безопасности в Африке [13].

Но более чем за 10 лет работы Ассоциации нам так и не удалось найти сколько-нибудь значимые результаты ее деятельности, а контент ее веб-сайта по-прежнему остается достаточно скудным.

Из других важных инициатив, демонстрирующих попытку африканских стран выработать единый подход к обеспечению информационной безопасности, следует отметить принятую в 2014 г. в Малабо (Экваториальная Гвинея) Конвенцию Африканского Союза в сфере кибербезопасности и защиты персональных данных (*African Union Convention on Cyber Security and Personal Data Protection*) [14]. Появление этого документа следует рассматривать как важный шаг, который доказывает стремление африканских стран выработать совместные механизмы, нацеленные на дальнейшую борьбу с киберпреступностью. Но в то же самое время сам процесс подписания и последующей ратификации этого документа свидетельствует о наличии серьезных противоречий между отдельными африканскими странами в сфере обеспечения кибербезопасности.

По состоянию на сегодняшний день, эта Конвенция была подписана только 14 африканскими странами, а ратифицировали ее только 8 - Ангола, Гана, Гвинея, Мозамбик, Маврикий, Намибия, Руанда, Сенегал. Примечательно, что ни Кения, ни Нигерия, ни ЮАР - страны, которые считаются региональными лидерами в сфере развития информационных технологий - не подписали этот документ. В этой связи Конвенция

до сих пор не вступила в силу, поскольку ее должны ратифицировать не менее 15 стран ее подписавших. Таким образом, сегодня эту Конвенцию можно рассматривать всего лишь как очередной программный документ, который пытается регулировать одно из наиболее важных направлений сотрудничества в информационной сфере, связанное с обеспечением кибербезопасности.

На наш взгляд, данное обстоятельство лишний раз свидетельствует о том, что любые наднациональные институты и инструменты в африканских условиях работают крайне плохо. Связано это с тем, что у стран Африки существует много противоречий, которые в своей совокупности препятствуют им выработать единые рабочие инструменты, направленные на решение наиболее значимых проблем континента, в т.ч. и в сфере обеспечения информационной и кибербезопасности.

В этой связи относительного успеха сумела добиться лишь Нигерийская ассоциация по информационной безопасности (*Information Security Society of Africa - Nigeria - ISSAN*), которой удалось превратиться в реальную платформу для сотрудничества и обмена мнениями между всеми заинтересованными сторонами - банками, телекоммуникационными компаниями, правительственными структурами, государственными регуляторами, *IT*-компаниями, консультантами в сфере информационной безопасности и юристами. При этом особенно подчеркивается, что это некоммерческая организация, направленная на обеспечение защиты нигерийского киберпространства, прежде всего банковской и правительственной систем. Эту задачу Ассоциация решает посредством проведения комплекса мероприятий, направленных на знакомство всех заинтересованных сторон с передовой практикой в указанной сфере [15].

ЗАКЛЮЧЕНИЕ

На основе вышеизложенного можно сделать вывод о том, что:

1. Страны Африки, расположенные к югу от Сахары, по-прежнему страдают от различного рода киберпреступлений, которые в эпоху бурного развития работающих на основе искусственного интеллекта технологий становятся все более высокотехнологизированными;

2. Проблема обеспечения информационно-психологической, информационной и кибербезопасности - общая проблема всех африканских стран, препятствующая их устойчивому социально-экономическому развитию;

3. Африканские страны предприняли значительные усилия, направленные на выработку единого видения в сфере борьбы с киберпреступлениями. Но все их попытки разработать эффективные наднациональные инструменты, которые бы регулировали борьбу с киберпреступностью на панафриканском уровне и учитывали бы интересы подавляющего большинства стран Африки в этой сфере, провалились. С нашей точки зрения, данное обстоятельство наглядно демонстрирует наличие серьезных противоречий среди африканских стран, которые в своей совокупности препятствуют установлению взаимовыгодного сотрудничества даже в такой важной сфере, как обеспечение информационной безопасности. Но до тех пор, пока этого не произойдет, представляется маловероятным, что африканские страны хотя бы приблизятся к решению этой проблемы, а значит, их информационное пространство будет и впредь подвергаться масштабным кибератакам, представляющим серьезную угрозу не только безопасности отдельных людей, но и всей системе национальной безопасности государства.

ЛИТЕРАТУРА / REFERENCES

1. Пашенцев Е. Н. Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно-психологической безопасности и пути их нейтрализации. *Государственное управление. Электронный вестник.* 2019. № 76, с. 279-300. http://www.elibrary.ru/item.asp?id=41254064 (accessed 29.06.2021)

Pashentsev E.N. 2019. Malicious Use of Artificial Intelligence: New Challenges for International Psychological Security and Ways of their Neutralization. P*ublic administration. Electronic bulletin.* № 76 (In Russ.). http://www.elibrary.ru/item.asp?id=41254064 (accessed 29.06.2021)

2. Bazarkina D., Pashentsev E. 2019. Artificial Intelligence and New Threats to International Psychological Security. *Russia in Global Affairs.* № 17(1), pp. 147-170. https://eng.globalaffairs.ru/articles/artificial-intelligence-and-new-threats-to-international-psychological-security (accessed 29.06.2021)

3. Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line. https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf (accessed 01.07.2021)

4. Isiavwe D. 2020. Cybersecurity Threat Evolution: Perspectives from Africa. https://www.issan.org.ng/download/cyber-security-threat-evolution (accessed 05.07.2021)

5. Кибератаки на основе искусственного интеллекта и машинного обучения и как от них защититься. *Cloud Networks.* 04.06.2020. https://zen.yandex.ru/media/id/5e71e35dac36540bbf854c99/kiberataki-na-osnove-mashinnogo-obucheniia-i-kak-ot-nih-za-scititsia-5ed90b0d8e6e074cb42cd4a7 (accessed 05.07.2021)

Cyberattacks on the Basis of Artificial Intelligence and Machine Learning. *Cloud Networks.* 4.06.2020. (In Russ.). https://zen.yandex.ru/media/id/5e71e35dac36540bbf854c99/kiberataki-na-osnove-mashinnogo-obucheniia-i-kak-ot-nih-zascititsia-5ed90b0d8e6e074cb42cd4a7 (accessed 05.07.2021)

6. Kharouni L. 2013. Africa: A New Safe Harbor for Cybercriminals? *Trendmicro.* https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf?_ga=2.144503985.507792652.1626804790-2127745893.1626804790 (accessed 11.07.2021)

7. Mohapi T. What we know so far about South Africa's largest ever data breach. *iAfrikan.* October, 18, 2017. https://iafrikan.com/2017/10/17/south-africas-govault-hacked-over-30-million-personal-records-leaked (accessed 11.07.2021)

8. Mohapi T. Is Dracore Data Sciences responsible for South Africa's largest ever data leak? *iAfrikan.* October, 18, 2017. https://iafrikan.com/2017/10/18/dracore-data-sciences (accessed 11.07.2021)

9. Что сделано для борьбы с киберпреступностью в Восточной Африке. *Новости высоких технологий.* 4.12.2019. https://cdnews.ru/2019/12/04/chto-sdelano-dlja-borby-s-kiberprestupnostju-v-vostochnoj-afrike (дата обращения 17.07.2021)

What has been done for the counteraction the cybercrime in East Africa. *High-Tech News.* 4.12.2019. (In Russ.). https://cdnews.ru/2019/12/04/chto-sdelano-dlja-borby-s-kiberprestupnostju-v-vostochnoj-afrike (accessed 17.07.2021)

10. Faife C. In Africa, Fear of State Violence Informs Deepfake Threat: WITNESS' workshop in South Africa revealed that perceived threats from synthetic media vary greatly by region, especially where repressive government is a factor. *WITNESS.* December 9, 2019. https://blog.witness.org/2019/12/africa-fear-state-violence-informs-deepfake-threat (accessed 18.07.2021)

11. Burning building video from India, not from xenophobic violence in South Africa. *Africa Check.* September 19, 2019. https://africacheck.org/fact-checks/fbchecks/burning-building-video-india-not-xenophobic-violence-south-africa (accessed 18.07.2021)

12. South Africa apologizes to Nigeria over xenophobic attacks. *BBC.* September 17, 2019. https://www.bbc.com/news/world-africa-49726041 (accessed 18.07.2021)

13. African Information Security Association.http://www.jidaw.com/aisa (accessed 21.07.2021).

14. African Union Convention on Cyber Security and Personal Data Protection. 2014. https://issafrica.org/ctafrica/uploads/AU%20Convention%20on%20Cyber%20Security%20and%20Personal%20Data%20Protection.pdf (accessed 21.07.2021)

15. Information Security Society of Africa - Nigeria (ISSAN). https://issan.org.ng (accessed 21.07.2021)

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

Панцерев Константин Арсеньевич, доктор политических наук, профессор, факультет международных отношений, Санкт-Петербургский государственный университет, Санкт-Петербург, Россия.

Konstantin A. Pantserev, Dr.Sc. (Political Science), Professor, Faculty of International Relations, Saint-Petersburg State University, Saint-Petersburg, Russia.

Поступила в редакцию (Received) 06.07.2021

Доработана после рецензирования (Revised) 20.08.2021

Принята к публикации (Accepted) 23.09.2021