

## Коммуникационный менеджмент и стратегическая коммуникация в государственном управлении

*Пащенко Е.Н.*

### Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно-психологической безопасности и пути их нейтрализации<sup>1</sup>

*Пащенко Евгений Николаевич* — доктор исторических наук, профессор, ведущий научный сотрудник, Дипломатическая академия МИД РФ; профессор, МГУ имени М.В. Ломоносова; директор Международного центра социально-политических исследований и консалтинга, Москва, РФ.

E-mail: [icspsc@mail.ru](mailto:icspsc@mail.ru)

SPIN-код РИНЦ: [4582-3350](https://elibrary.ru/4582-3350)

#### Аннотация

В статье представлен анализ новых угроз международной информационно-психологической безопасности, обусловленных быстрым внедрением в различные сферы общественной жизни искусственного интеллекта (ИИ), а также его злонамеренным использованием со стороны агрессивных акторов международных отношений. По сравнению с позитивным использованием ИИ, аспект злонамеренного использования ИИ, связанный с угрозами международной информационно-психологической безопасности, гораздо менее изучен. В статье представлены лишь некоторые из методов злонамеренного использования искусственного интеллекта: окно возможностей для такого использования неуклонно растет, качество и глубина проникновения в общественное сознание с помощью ИИ увеличиваются. Это закономерно происходит по мере совершенствования технических возможностей ИИ и растущего запроса на такие возможности со стороны эгоистических групп интересов в условиях нарастающего мирового кризиса, снижения уровня жизни основной части населения большинства стран, роста социальной и имущественной поляризации, опасного роста геополитического соперничества. Автор дает определение международной информационно-психологической безопасности, предлагает возможные классификации злонамеренного использования ИИ по степени реализации возможностей, территориальному охвату, размеру наносимого ущерба, скорости и формам распространения. Кроме того, определены цели и задачи злонамеренного использования ИИ, представлена авторская оценка некоторых текущих и перспективных угроз такого использования в контексте угроз международной информационно-психологической безопасности. Исследование подтверждает, что злонамеренное использование ИИ поднимает угрозы международной информационно-психологической безопасности на качественно новый уровень, требующий адекватного анализа и реакции со стороны общества и государственных органов власти.

#### Ключевые слова

Искусственный интеллект, сильный искусственный интеллект, слабый искусственный интеллект, международная информационно-психологическая безопасность, международная безопасность, перспективные технологии.

DOI: 10.24411/2070-1381-2019-10013

<sup>1</sup> Статья подготовлена в рамках научных исследований, выполненных при поддержке гранта СПбГУ № 26520757.

### **Введение**

За два последних года очевидный успех в развитии систем искусственного интеллекта (ИИ) позволил выйти на новый уровень исследований как в оценке перспектив развития человеческой цивилизации на основе новых технологий, так и в анализе собственно угроз международной информационно-психологической безопасности (МИПБ). Впервые к проблематике социальной роли ИИ автор обращался в своих ранних публикациях начала 1990-х гг., но тогда исследования не получили своего развития по причине незрелости предпосылок для прогресса в этой области технических наук, деградации исследовательской и производственной базы страны.

Достижения последних лет как в теории, так и в практике развития ИИ позволили вновь вернуться к отложенной на время теме. Отражением этого послужил ряд исследований, выполненных на основе участия автора в грантовом проекте Санкт-Петербургского университета<sup>2</sup>. В последние два года удалось рассмотреть общие проблемы развития отрасли ИИ и ее перспективы в России и за рубежом, неоднозначное влияние ИИ на развитие человечества. Появившиеся источники позволили выделить пять сценариев будущего развития общества, дать им характеристику, рассмотреть вопрос социальных последствий возможного создания сильного искусственного интеллекта [Strategic Communication in EU-Russia Relations 2018; Strategic Communication in EU-Russia Relations 2020], а также определить некоторые аспекты безопасности принимаемых в этой сфере решений, выделить особенности информационно-психологического воздействия на социум с опорой на ИИ в рамках неустойчивых динамических социальных равновесий (НДСР) (авторская концепция НДСР изложена прежде всего на международной конференции по киберпротивоборству и безопасности в ЮАР в 2019 г. [Pashentsev 2019a]).

Системный подход к развитию ИИ позволил добиться определенных научных и практических результатов в исследовании злонамеренного использования искусственного интеллекта (ЗИИИ) с точки зрения угроз МИПБ, синергетического эффекта последствий такого использования [Bazarkina, Pashentsev 2019; Pashentsev 2019c; Averkin et al. 2019], рассмотреть некоторые частные аспекты этой проблемы: появление прогностического оружия на основе ИИ [Пашенцев 2016], противостояние нелегальной иммиграции с опорой на ИИ [Pashentsev 2019b], возможные новые угрозы со стороны террористов с использованием возможностей ИИ и методы их нейтрализации на основе современных и перспективных технологий [Pashentsev 2019d].

---

<sup>2</sup> «Инновационные методологии обеспечения информационной безопасности» (ID 26520757 Санкт-Петербургского государственного университета (02.07.2018–31.12.2020)).

Методология исследования, лежащего в основе данной статьи, базируется на системном подходе к оценке роли ИИ в сфере МИПБ, с особым вниманием к роли ЗИИИ. Выполнение поставленных научных задач потребовало привлечения нескольких групп первичных и вторичных источников. Среди первичных источников можно выделить официальные публикации государственных органов ряда стран и международных организаций, статистические данные, материалы опросов, сообщения в СМИ. Вторичные источники — это прежде всего монографии и исследовательские статьи, дающие оценку процессам и явлениям в исследуемой области. Сравнительный анализ и тематические исследования полезны для получения результатов, которые служат основой для определения критериев эффективности ЗИИИ и его нейтрализации в условиях неустойчивых динамических социальных равновесий.

### ***Определение и уровни МИПБ. Цель, задачи и классификации ЗИИИ***

МИПБ — защищенность системы международных отношений от негативных информационно-психологических воздействий, связанных с разнообразными факторами международного развития. Среди последних можно выделить целенаправленную деятельность различных государственных, негосударственных и наднациональных акторов по частичной/полной, локальной/глобальной, кратковременной/долгосрочной, латентной/открытой дестабилизации международного положения с целью получения конкурентных преимуществ вплоть до физического уничтожения противника.

*Уровни МИПБ.* Согласно многим последним отчетам, таким как отчеты ООН, Всемирного экономического форума, Банка Америки, Мерилла Линча, Всемирного института Маккинзи, Оксфордского университета и других [Frey, Osborne 2017; Pol, James 2017]<sup>3</sup>, 30% и более рабочих мест исчезнут в ближайшие 2–3 десятилетия в

---

<sup>3</sup> См. также: World Development Report 2016. Digital Dividends. Overview. Washington: International Bank for Reconstruction and Development, 2016 // World Bank Group [Электронный ресурс]. URL: <https://openknowledge.worldbank.org/bitstream/handle/10986/23347/210671EnSum.pdf?sequence=11&isAllowed=y> (дата обращения: 10.10.2019); Creative Disruption. Bank of America, Merrill Lynch, 2015 // FrankDiana [Электронный ресурс]. URL: <https://frankdiana.net/2015/11/16/a-report-on-creative-disruption/> (дата обращения: 10.10.2019); Technology at Work v.2.0. The Future is not what it used to be. Oxford: Global Perspectives and Solutions, 2016 // Oxford Martin School [Электронный ресурс]. URL: [https://www.oxfordmartin.ox.ac.uk/downloads/reports/Citi\\_GPS\\_Technology\\_Work\\_2.pdf](https://www.oxfordmartin.ox.ac.uk/downloads/reports/Citi_GPS_Technology_Work_2.pdf) (дата обращения: 10.10.2019); A Future that Works. Automation, Employment, and Productivity. January 2017 Executive Summary. McKinsey Global Institute, 2017 // McKinsey & Company [Электронный ресурс]. URL: <https://www.mckinsey.com/~/media/mckinsey/featured%20insights/Digital%20Disruption/Harnessing%20Automation%20for%20a%20future%20that%20works/MGI-A-future-that-works-Executive-summary.ashx> (дата обращения: 14.09.2019); Robots and industrialization in developing countries. United Nations Conference on Trade and Development Policy Brief. 2016. № 50 // UNCTAD [Электронный ресурс]. URL: [https://unctad.org/en/PublicationsLibrary/presspb2016d6\\_en.pdf](https://unctad.org/en/PublicationsLibrary/presspb2016d6_en.pdf) (дата обращения: 10.10.2019); The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution. Executive

результате процессов роботизации производства, финансов, услуг и управления, включая высокооплачиваемые должности. В 2016 г. Всемирный банк опубликовал доклад, в котором говорится, что в ближайшие десятилетия более 65% рабочих мест в развивающихся странах будут поставлены под угрозу ускоряющимся развитием технологий<sup>4</sup>.

Не только возможная массовая безработица в результате внедрения ИИ, но и возможность утраты полного (в достаточно далеком будущем) и частичного (в настоящем и ближайшем будущем) контроля за искусственным интеллектом — в центре внимания специалистов, государственных органов и широкой общественности.

Большая часть опасений связана, однако, с реальной угрозой, исходящей не от ИИ как такового, а от ЗИИИ. И эта тревога вполне обоснована: за быстро растущим внедрением ИИ в общественную жизнь, ростом его возможностей, а также увеличением практики и возможностей ЗИИИ не поспевают ни правовое регулирование в отдельных странах, ни система международного права, ни существующие механизмы контроля. Поле для ЗИИИ здесь широкое — неоправданное применение дронов, угрозы кибератак на элементы инфраструктуры, манипуляции с криптовалютами, использование ботов в кампаниях по подрыву репутации отдельных личностей, организаций и стран и многое другое. Отнюдь неслучайно многие исследования и аналитические доклады о восприятии ИИ обществом свидетельствуют о высоком уровне обеспокоенности населения социальными последствиями внедрения ИИ [Fastand, Horvitz 2016; Holder et al. 2018]<sup>5</sup>.

Объективные и субъективные негативные факторы и последствия развития ИИ составляют *первый уровень угроз* МИПБ, а ЗИИИ — *второй*. Средствами и методами информационно-психологического противоборства (ИПП) (хотя и не только его) можно поднять уровень восприятия вышеназванных угроз выше или опустить ниже адекватного. Более того, применение в ИПП ИИ позволяет уже сегодня и позволит в гораздо большей мере в будущем сделать явные и скрытые кампании информационно-психологического воздействия более эффективными и опасными. Поэтому ЗИИИ,

---

Summary. Geneva: World Economic Forum, 2016 // World Economic Forum [Электронный ресурс]. URL: [http://www3.weforum.org/docs/WEF\\_Future\\_of\\_Jobs.pdf](http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf) . (дата обращения: 14.10.2019).

<sup>4</sup> World Development Report 2016. Digital Dividends. Overview. Washington: International Bank for Reconstruction and Development, 2016 // World Bank Group. P. 23. [Электронный ресурс]. URL: <https://openknowledge.worldbank.org/handle/10986/23347> (дата обращения: 10.10.2019).

<sup>5</sup> См. также: 2019 Artificial Intelligence Survey // Edelman [Электронный ресурс]. URL: <https://www.edelman.com/research/2019-artificial-intelligence-survey> (дата обращения: 14.09.2019); AI Today, AI Tomorrow: Awareness, Acceptance and Anticipation of AI — A Global Consumer Perspective. ARM, 2017 // ARM [Электронный ресурс]. URL: <http://pages.arm.com/rs/312-SAX-488/images/arm-ai-survey-report.pdf> . (дата обращения: 10.10.2019).

нацеленные в значительной мере на нанесение ущерба в информационно-психологической сфере, заслуживают самостоятельного и самого пристального внимания, представляя особый *третий уровень угроз МИПБ*. Первые два уровня в разной мере влияют на сознание и поведение человека. Однако воздействие на третьем уровне может на определенном этапе развития обеспечить краткосрочный или долгосрочный контроль эгоистических групп влияния над общественным сознанием, внезапную дестабилизацию ситуации в той или иной стране или международной обстановки в целом.

*Цель ЗИИИ.* В рамках гибридной войны с помощью материальных средств воздействия в различных сферах (экономической, политической, военной и др.) субъекты международных отношений осуществляют негативное опосредованное и непосредственное воздействие на общественное сознание противника, а также нередко и на свое собственное состояние, своих союзников, нейтральных акторов. Например, экономические санкции имеют своей задачей не только материально ослабить/уничтожить противника, но и через рост его экономических проблем снизить готовность целевых групп воздействия к дальнейшему сопротивлению. Военно-политическая конфронтация с противником на основе захватнических интересов и политики массового геноцида населения других народов наносит трудно исправимый ущерб менталитету и психике народа страны-агрессора. В то же время средства ИПП всегда нацелены на нанесение непосредственного (хотя часто латентного) удара по общественному сознанию и (через победу в этой сфере) бескровную общую победу над противником. ЗИИИ в контексте МИПБ как раз и нацелено на получение перевеса в ИПП за счет количественно и качественно-новых форм воздействия на индивидуальное и общественное сознание. По сути, в современном глобальном мире речь идет о гибридной войне в рамках системы международных отношений, которая никогда в истории полностью не прекращалась, но имеет свои периоды закономерного обострения. Мы явно и надолго вступили в переходный период развития человечества в целом и системы международных отношений в частности, который сопровождается нелинейно нарастающим ИПП.

ЗИИИ может решать следующие задачи:

- спровоцировать целевые группы на неадекватную реакцию на несуществующий фактор общественного развития в интересах заказчика информационно-психологического воздействия. Аудитория видит то, что не существует.

- представить ложную интерпретацию существующего фактора общественного развития и таким образом также вызвать искомую целевую реакцию. Аудитория видит то, что существует, но в ложном свете.
- существенным и опасным образом усилить (уменьшить) общественную реакцию на реальный фактор общественного развития. Аудитория видит то, что существует, но реагирует неадекватным образом.

Автором предложена следующая классификация ЗИИИ по степени реализации его возможностей:

- существующая практика ЗИИИ;
- существующие возможности ЗИИИ, которые еще не были использованы на практике (такая вероятность связана с широким спектром быстро развивающихся новых возможностей ИИ — не все они сразу входят в спектр реализованных возможностей ЗИИИ);
- будущие возможности ЗИИИ на основе текущих разработок и будущих исследований (оценка должна быть дана на ближайшую, среднесрочную и долгосрочную перспективы);
- неопознанные риски — «неизвестное в неизвестном». Не все разработки в сфере ИИ можно точно оценить. Готовность встретить неожиданные скрытые риски имеет решающее значение.

Важно и необходимо использовать независимые команды разных специалистов и сам ИИ для оценки возможностей ЗИИИ.

Мы также можем предложить следующие варианты классификации ЗИИИ:

- по территориальному охвату: местный, региональный, глобальный;
- по степени наносимого ущерба: незначительный, значительный, крупный, катастрофический;
- по скорости распространения: медленный, быстрый, стремительный;
- по форме распространения: открытый, скрытый.

### ***Угрозы МИПБ посредством ЗИИИ***

Среди возможных угроз ЗИИИ, которые могут вызвать серьезное дестабилизирующее воздействие на социально-политическое развитие той или иной страны и системы международных отношений, включая сферу МИПБ, выделим следующие:

*Рост комплексных всеохватывающих систем с активным или ведущим участием ИИ* повышает риск злонамеренного перехвата контроля над такими системами. Многочисленные объекты инфраструктуры, например роботизированные самообучающиеся транспортные системы с централизованным управлением посредством ИИ, могут стать удобной мишенью для высокотехнологичных терактов. Перехват контроля над системой управления транспортом в крупном городе может привести к многочисленным жертвам. Это, несомненно, вызовет панику и создаст информационно-психологический климат, облегчающий дальнейшие враждебные действия. Например, программа DeepLocker была разработана в качестве доказательства концепции IBM Research, чтобы понять, как совокупность уже существующих технологий ИИ и вредоносных компьютерных программ может быть использована для создания новой, очень защищенной породы вредоносных программ, которые скрывают свое вредоносное намерение до тех пор, пока не достигнет конкретной жертвы<sup>6</sup>.

*Перепрофилирование коммерческих систем искусственного интеллекта.* Коммерческие системы могут быть использованы во вред (даже не всегда намеренно). Возможно использование беспилотных летательных аппаратов или автономных транспортных средств для доставки взрывчатых веществ и организации аварий [Brundage et al. 2018, 27]. Серия серьезных катастроф, особенно с участием известных лиц, может иметь международный резонанс и нанести ущерб МИПБ.

*Создание «deepfakes».* «Deepfake» (от deep learning — «глубинное обучение» и fake — «подделка») — метод синтеза человеческого изображения и/или голоса на основе использования ИИ. Жертвами создания порно-«deepfakes» уже стали актрисы Скарлетт Йоханссон, Мэйси Уильямс, Тейлор Свифт, Мила Кунис и многие другие знаменитости. Любители «deepfakes» начали использовать технологию для создания достоверных цифровых видео мировых лидеров, в том числе президентов Владимира Путина и Дональда Трампа, бывшего президента США Барака Обамы и кандидата в президенты Хиллари Клинтон. Эксперты предупреждают, что «deepfakes» могут быть достаточно реалистичным, чтобы манипулировать будущими выборами и

---

<sup>6</sup> Kirat D., Jang J., Stoecklin M.Ph. DeepLocker — concealing targeted attacks with AI locksmithing // Black Hat [Электронный ресурс]. URL: <https://www.blackhat.com/us-18/briefings/schedule/#deeplocker---concealing-targeted-attacks-with-ai-locksmithing-11549> (дата обращения: 14.09.2019); Stoecklin M.Ph. DeepLocker: How AI Can Power a Stealthy New Breed of Malware // Security Intelligence [Электронный ресурс]. URL: <https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/> (дата обращения: 14.09.2019).



глобальной политикой уже в 2020 г.<sup>7</sup>, что делает их потенциально опасным средством влияния на поведение как отдельных лиц, так и больших целевых групп воздействия. При соответствующей подготовке «deepfakes» в рамках ИПП могут спровоцировать финансовую панику, торговую или «горячую» войну. Видео, где премьер-министр Беньямин Нетаньяху или другие правительственные чиновники Израиля говорят, например, о предстоящих планах захвата иерусалимской Храмовой горы и мечети Аль-Акса, могут распространиться, как лесной пожар, на Ближнем Востоке<sup>8</sup>. Потенциально опасно распространение технологии «deepfake» и тем, что люди не захотят доверять никаким видео- или аудиоматериалам<sup>9</sup>.

*Технология «Fake People».* После продажи первого произведения искусства, созданного ИИ, в начале 2018 г. алгоритмы глубокого обучения теперь работают с портретами несуществующих людей. Компания NVIDIA недавно поделилась результатами работы генеративной конкурентной сети (generative adversarial network, GAN), обученной самостоятельно генерировать изображения людей [Karras et al. 2019]. За основу был взят условно бесконечный массив изображений реальных лиц, поэтому нейросеть узнает и применяет в работе множество мелких деталей. Она может нарисовать сотню лиц в очках, но с разной прической, текстурой кожи, морщинами и шрамами, добавить возрастные признаки, культурные и этнические черты, эмоции, настроение или результаты воздействия внешних факторов — от ветра в волосах до неровного загара. Еще в 2017 г. те же специалисты из NVIDIA проводили схожий эксперимент, но тогда изображения лиц были слишком грубыми, подделку распознавали сразу. Сегодня нейросеть работает несравнимо лучше, рисует лица в большом разрешении. И нет проблемы приказать ей создать, например, несуществующего внебрачного ребенка известной личности, чтобы устроить провокацию. Фамильное сходство на картинке будет стопроцентно убедительным.

*Установка и закрепление повестки дня.* Исследования показывают, что боты составили более 50% всего интернет-трафика в 2016 г. Организации, которые

---

<sup>7</sup> Palmer A. Experts warn digitally-altered ‘deepfakes’ videos of Donald Trump, Vladimir Putin, and other world leaders could be used to manipulate global politics by 2020 // Daily Mail [Электронный ресурс]. URL: <https://www.dailymail.co.uk/sciencetech/article-5492713/Experts-warn-deepfakes-videos-politicians-manipulated.html> (дата обращения: 14.09.2019).

<sup>8</sup> ‘I Never Said That!’ The High-Tech Deception of ‘Deepfake’ Videos // The Times of Israel [Электронный ресурс]. URL: <https://www.timesofisrael.com/i-never-said-that-the-high-tech-deception-of-deepfake-videos/> (дата обращения: 14.09.2019).

<sup>9</sup> Waddel K. The impending war over deepfakes // Axios [Электронный ресурс]. URL: <https://www.axios.com/the-impending-war-over-deepfakes-b3427757-2ed7-4fbc-9edb-45e461eb87ba.html> (дата обращения: 14.09.2019).



искусственно продвигают контент, могут манипулировать повесткой дня: чем чаще люди видят определенный контент, тем более важным они его считают [Horowitz et al. 2018, 5–6]. Ущерб репутации с помощью ботов во время политических кампаний, например, может быть использован террористическими группами для привлечения новых сторонников или организации убийств политиков.

*Целевая трансформация образов.* Эксперимент в лаборатории массовой информации Массачусетского технологического института окрестили «Машина кошмаров». Результаты доступны в Интернете. Алгоритмы глубокого обучения используются для превращения обычных, повседневных образов в страшные, зловещие картинки. К ним относятся фотографии популярных достопримечательностей, таких как римский Колизей и Капитолийский холм в Вашингтоне, а также лиц политиков, таких как Дональд Трамп и Хиллари Клинтон<sup>10</sup>. В другом разделе сайта размещены «лица с привидениями», к которым был добавлен намек на шрамы. Посетителей специализированного сайта просят выбрать, какие из них самые страшные<sup>11</sup>. Исследователь MIT Media Lab Пинар Янардаг Делул в интервью Washington Post задает вопрос: «...может ли ИИ вызвать более мощные внутренние реакции, более похожие на то, что мы видим в фильме ужасов?» Даже весьма невинные эксперименты исследователей из MIT Media Lab дают утвердительный ответ на этот вопрос. К сожалению, те, кто будет использовать подобные наработки в целевых информационно-психологических операциях, об этом открыто не напишут, и нельзя исключить использование подобной технологии в целях опасных для МИПБ уже сегодня. Фактически исследователи из MIT Media Lab открыто предупреждают о такой возможности.

Данная технология позволяет многократно и быстро увеличить и направить вал негативных образов на целевые аудитории в любой точке мира, быстро подстраиваясь под ее скрытые и часто неосознанные ожидания, увеличивая эффективность воздействия. При этом расходы на такие информационно-психологические операции с участием ИИ несравнимо меньше, чем если бы этим попытались заниматься массы людей. Опять-таки секретность операции обеспечить несравненно легче. Одна программа сама по себе не «болтает», а небольшой штат специалистов по контролю за операцией легче контролируем, чем тысячные армии традиционных пропагандистов.

---

<sup>10</sup> Capitol Hill (Toxic) // Nightmare Machine. Horror Imagery Generated by Artificial Intelligence [Электронный ресурс]. URL: <http://nightmare.mit.edu/#portfolioModal22> (дата обращения: 14.09.2019).

<sup>11</sup> Scary or Not // Nightmare Machine. Horror Imagery Generated by Artificial Intelligence [Электронный ресурс]. URL: <http://nightmare.mit.edu/faces> (дата обращения: 14.09.2019).

«Отравленные данные». Эффекты обучения алгоритмов в значительной степени зависят от данных, на основе которых проводится обучение. Может оказаться, что эти данные были неверны и искажены, то ли случайно, то ли по чьему-то злему умыслу (в последнем случае это называется «отравлением» данных), что скажется на работе алгоритма. Чат-бот Microsoft под названием «Tay.ai» должен был выглядеть как обычная девочка-подросток и привлекать к разговору подростков в социальных сетях. Но менее чем через день после своего дебюта Тай неожиданно превратился в тролля, любящего Гитлера и критикующего феминистку. Так что же пошло не так? Оказалось, что «добрые» интернет-пользователи быстро научили бота ругаться и читать отрывки из книги «Моя борьба» Адольфа Гитлера<sup>12</sup>. Это отличный пример отравления данных, используемых для машинного обучения. Математическая модель, используемая для анализа компьютерных вирусов, обрабатывает в среднем миллион файлов в день, как нейтральных, так и вредных. Из-за того, что ландшафт угроз постоянно меняется, изменения модели передаются на продукты, установленные на стороне клиента в виде обновления антивирусных баз данных. К сожалению, хакер может генерировать вредоносные файлы, очень похожие на безобидные, и отправлять их в антивирусную лабораторию. Такие действия постепенно стирают грань между безобидными и вредными файлами — в результате модель может давать ложную тревогу<sup>13</sup>.

*Анализ тональности* — класс методов контент-анализа в компьютерной лингвистике, предназначенный для автоматизированного выявления в текстах эмоционально окрашенной лексики и тем самым мнений авторов об объектах, о которых идет речь в тексте. Анализ тональности обеспечивается широким спектром источников, таких как блоги, статьи, форумы, опросы и т.д. Это может быть очень эффективным инструментом в ИПП.

ИИ, машинное обучение и анализ тональности позволяют предсказывать будущее путем анализа прошлого, потенциально такая возможность выгодна и для ЗИИИ различными государственными и негосударственными акторами. Особенно велико значение *прогностического оружия*: методов предсказательной аналитики на основе больших данных и с использованием ИИ, которые позволяют, получая данные о будущих событиях, корректировать будущее из настоящего в интересах субъекта

---

<sup>12</sup> Reese H. Why Microsoft's 'Tay' AI bot went wrong // TechRepublic [Электронный ресурс]. URL: <https://www.techrepublic.com/article/why-microsofts-tay-ai-bot-went-wrong/> (дата обращения: 14.09.2019).

<sup>13</sup> С какими проблемами сталкиваются создатели искусственного интеллекта // WebZnam [Электронный ресурс]. URL: [https://webznam.ru/blog/sozdateli\\_iskusstvennogo\\_intellekta/2018-11-12-777](https://webznam.ru/blog/sozdateli_iskusstvennogo_intellekta/2018-11-12-777) (дата обращения: 14.09.2019).

воздействия и вопреки объективным интересам объекта такого воздействия. К примеру, программа EMBERS (Early Model Based Event Recognition Using Surrogates — «Распознавание событий на основе ранних моделей с применением суррогатов») была запущена Агентством передовых исследований в сфере разведки (Intelligence Advanced Research Projects Activity, IARPA) в 2012 г. Программа прогнозирует значимые события, такие как социальные беспорядки, вспышки заболеваний, результаты выборов. EMBERS представляет детальные прогнозы, включая дату, место, тип события, характеристику протестного населения, определяя при этом возможную погрешность. Программа оперирует как открытыми источниками информации (например, Twitter), так и более сложными и качественными информационными продуктами, например экономическими индикаторами, обрабатывая около 5 млн сообщений в день. Только по возможностям гражданского протеста EMBERS дает свыше 50 прогнозов на 30 дней вперед [Doyle et al. 2014].

Можно представить, что на основе комбинации техник психологического воздействия, сложных систем ИИ и больших данных в ближайшие годы появятся *синтетические информационные продукты*, похожие «на модульный вредоносный софт... Однако действовать они будут не на неодушевленные предметы, социальные сети и т.п., а на человека и массы как на психобиофизические существа. В подобном синтетическом информационном продукте будут содержаться программные модули, которые введут массы людей в депрессию», после чего скрытые суггестивные программы, апеллируя к привычкам, стереотипам, психофизиологии, побудят людей выполнять строго определенные действия [Ларина, Овчинский 2018, 126–127].

За ограниченностью в объеме настоящей статьи мы представили лишь некоторые из методов ЗИИИ: окно возможностей ЗИИИ неуклонно растет, качество и глубина проникновения в общественное сознание увеличиваются. Это закономерно происходит по мере совершенствования технических возможностей ИИ и растущего запроса на такие возможности со стороны эгоистических групп интересов в условиях нарастающего мирового кризиса, снижения уровня жизни основной части населения большинства стран, роста социальной и имущественной поляризации, опасного роста геополитического соперничества. Отметим, что мы опирались в наших предшествующих исследованиях и данной статье на результаты открытых источников, что в данной ситуации, разумеется, недостаточно для точного определения уровня и размаха данной угрозы для России и всего международного сообщества.

Дальнейшее результативное рассмотрение темы настоящей статьи не в последнюю очередь требует налаживания международного научного сотрудничества.

В 2019 г. оформилась международная группа специалистов по угрозам МИПБ посредством ЗИИИ, которая успешно сотрудничает в проведении совместных научных исследований и международных конференций и научных семинаров<sup>14</sup>. Так, участники группы сформировали панельную группу «Злонамеренное использование искусственного интеллекта и международная информационно-психологическая безопасность»<sup>15</sup> на II Международной конференции «Информация и коммуникация в цифровую эпоху: явные и неявные воздействия». Конференция проходила в рамках Межправительственной программы ЮНЕСКО «Информация для всех» (IFAP) и XI Международного IT-форума с участием стран БРИКС и ШОС в Ханты-Мансийске 9–12 июня 2019 г. В заключительном документе конференции были учтены наиболее важные результаты деятельности группы<sup>16</sup>.

Обсуждение проблем злонамеренного использования ИИ продолжилось на научно-исследовательском семинаре «Искусственный интеллект и вызовы международной психологической безопасности». Семинар был организован Центром евроатлантических исследований и международной безопасности Дипломатической академии МИД России и Международным Центром социально-политических исследований и консалтинга при академической поддержке Европейско-российской экспертной сети коммуникационного менеджмента (ЕРЭСМ) и кафедры международной безопасности и внешнеполитической деятельности Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации. Участники семинара приняли итоговый документ «За сотрудничество между странами, экспертными сообществами и организациями гражданского общества в борьбе со злонамеренным использованием искусственного интеллекта и дестабилизацией международной информационно-психологической

---

<sup>14</sup> Автор настоящей публикации является ее инициатором и координатором.

<sup>15</sup> *Bazarkina D., Smirnov M. Artificial Intelligence and International Psychological Security: Academic Discussion in Khanty-Mansiysk and Moscow* // L'institut International de la Recherche Scientifique [Электронный ресурс]. URL: [http://www.institut-irs.com/pages/article/artificial\\_intelligence\\_and\\_international\\_psychological\\_security](http://www.institut-irs.com/pages/article/artificial_intelligence_and_international_psychological_security) (дата обращения: 14.09.2019).

<sup>16</sup> *Second International Conference "Tangible and Intangible Impact of Information and Communication in the Digital Age". Khanty-Mansiysk, Russian Federation 9 – 12 June 2019* // L'institut International de la Recherche Scientifique [Электронный ресурс]. URL: [http://institut-irs.com/pages/article/second\\_international\\_conference\\_tangible\\_and\\_intangible\\_impact\\_of\\_information\\_and\\_communication\\_in\\_the\\_digital\\_age](http://institut-irs.com/pages/article/second_international_conference_tangible_and_intangible_impact_of_information_and_communication_in_the_digital_age) (дата обращения: 14.09.2019).

безопасности и демократических институтов» и сформировали рабочую группу по ее реализации<sup>17</sup>.

На X Международной научной конференции «Влияние великих держав на безопасность малых государств», организованной факультетом безопасности в Охриде (Македония), член группы, председатель-основатель Международного института научных исследований (Марракеш) д-р Фатима Румате представила доклад «Злонамеренное использование искусственного интеллекта и Международная психологическая безопасность: последствия и решения».

В сентябре 2019 г. в Острове (Чехия) на конференции Международной ассоциации нечетких систем и Европейского общества нечеткой логики и технологий (EUSFLAT 2019) был представлен доклад четырех российских специалистов на тему «Искусственный интеллект в контексте психологической безопасности: теоретические и практические аспекты» [Averkin et al. 2019]. На второй Международной конференции «Противодействие незаконным поставкам оружия в контексте борьбы с международным терроризмом» в Москве был представлен доклад на тему «Угроза овладения террористами технологиями информационно-психологического воздействия на базе искусственного интеллекта и возможные пути ее нейтрализации»<sup>18</sup>.

В начале октября 2019 г. обсуждение проблем ЗИИИ в контексте развития ИИ в Латинской Америке состоялось на Иberoамериканском форуме в рамках двух панелей: «Новые возможности искусственного интеллекта и социальные, политические

---

<sup>17</sup> For Cooperation between Countries, Expert Communities and Civil Society Organizations against the Malicious Use of Artificial Intelligence and the Destabilization of the International Psychological Security and Democratic Institutions. The Final Document of the International Research Seminar “Artificial Intelligence and Challenges to International Psychological Security”, Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation. Moscow, June 14, 2019 // Geopolitica Estului [Электронный ресурс]. URL: <https://geopoliticaestului.ro/for-cooperation-between-countries-expert-communities-and-civil-society-organizations-against-the-malicious-use-of-artificial-intelligence-and-the-destabilization-of-the-international-psychological-se/> (дата обращения: 14.09.2019).

<sup>18</sup> Prof. Evgeny Pashentsev on How to Stop Terrorist Psychological Campaigns, Enhanced by Artificial Intelligence // International Institute for Scientific Research — IIRS (Marrakech) [Электронный ресурс]. URL: [http://institut-irs.com/pages/article/prof\\_evgeny\\_pashentsev\\_on\\_how\\_to\\_stop\\_terrorist\\_psychological\\_campaigns](http://institut-irs.com/pages/article/prof_evgeny_pashentsev_on_how_to_stop_terrorist_psychological_campaigns) (дата обращения: 14.09.2019); Terrorist Psychological Campaigns enhanced by Artificial Intelligence technologies and their neutralization // ASRIE (Roma). September 11, 2019. [Электронный ресурс]. URL: <http://www.asrie.org/2019/09/terrorist-psychological-campaigns-enhanced-by-artificial-intelligence-ai-technologies-and-their-neutralization/> (дата обращения: 14.09.2019); How to Stop Terrorist Psychological Campaigns, Enhanced by Artificial Intelligence, by Professor Evgeny Pashentsev // Asociației Geopolitica Estului (A.G.E.) [Электронный ресурс]. URL: <https://geopoliticaestului.ro/how-to-stop-terrorist-psychological-campaigns-enhanced-by-artificial-intelligence-by-professor-evgeny-pashentsev/> (дата обращения: 14.09.2019).

и психологические вызовы в Латинской Америке» и «Информационно-психологическое противоборство в современном мире и Латинской Америке»<sup>19</sup>.

На «Европейской конференции по влиянию ИИ и робототехники» в Оксфорде дискуссия будет продолжена на мини-треке «Вредоносное использование искусственного интеллекта: новые вызовы для демократических институтов и политической стабильности»<sup>20</sup>.

В ведущих международных издательствах готовятся к изданию книги, в которых тема развития ИИ, ЗИИИ и МИПБ является одной из главных. В монографии «Стратегическая коммуникация в отношениях ЕС и России: напряженность, вызовы и возможности» [Strategic Communication in EU-Russia Relations 2020] анализируются общие риски развития ИИ. В книге «Терроризм и передовые технологии в информационно-психологическом противоборстве: новые риски, новые возможности противодействия террористической угрозе» с участием 18 специалистов из 11 стран (ред. Д.Ю. Базаркина, Г. Саймонз, Е.Н. Пашенцев, Nova Science Publishers) целый раздел будет посвящен информационно-психологическим угрозам с использованием ИИ, исходящим от террористов, и методам их нейтрализации. В конце 2020 г. планируется представить коллективную монографию на тему «Искусственный интеллект и угрозы международной психологической безопасности».

Публикации в российских и зарубежных академических журналах подробных обзоров выступлений российских и зарубежных специалистов по проблемам международной информационно-психологической безопасности [Базаркина, Дурсунова 2018; Базаркина, Ласурия 2019; Bifulchi, Pashentsev, Shilina 2018] содействуют более широкому распространению среди специалистов нового направления в области обеспечения международной безопасности.

Распространению представлений о существующих и перспективных угрозах МИПБ посредством ЗИИИ и методах их нейтрализации способствуют и многочисленные публикации за последние два года в СМИ, в том числе обзоров авторских научных исследований членов международной группы<sup>21</sup>; выступлений членов группы на научных и научно-практических мероприятиях на тему ИИ и МИПБ

---

<sup>19</sup> Programme // Russia and Iberoamerica in the Global World. Fourth International Forum (1 – 3 October 2019) [Электронный ресурс]. URL: <http://iberorus.spbu.ru/en/page/program2019> (дата обращения: 14.09.2019).

<sup>20</sup> ECIAIR Mini Tracks // Academic Conferences and Publishing International [Электронный ресурс]. URL: <https://www.academic-conferences.org/conferences/eciair/eciair-call-for-papers/eciair-mini-tracks/> (дата обращения: 14.09.2019).

<sup>21</sup> Например, обзоры исследования Д.Ю. Базаркиной и Е.Н. Пашенцева по ИИ и МИПБ на сайте РИА «Новости», а также портала Sputnik (материал доступен на английском, испанском и китайском языках).



за последние два года в России, Чехии, Италии, Белоруссии, Марокко, Македонии, Франции, Уругвае, Румынии, Аргентине, Бразилии, ЮАР, Великобритании<sup>22</sup>; интервью членов группы на русском, английском, французском, испанском, итальянском, румынском, китайском языках, опубликованные в России, Марокко, Испании, Румынии, Аргентине, Италии, Кубе, Эквадоре, Франции и др. странах, имеющих не менее 800 репостов на страницах новостных агентств, сайтов университетов, профессиональных блогов.

Системы [PURE](#)<sup>23</sup> в СПбГУ и «[Истина](#)» в МГУ имени М.В. Ломоносова, [РЛАСИ](#) и [EU-RU-CM Network](#) позволяют эффективно представить освещение в СМИ научных достижений в области МИПБ и ЗИИИ.

Сотрудничество специалистов по вопросам ЗИИИ и МИПБ успешно развивается и по линии международных ассоциаций: Европейско-российской экспертной сети коммуникационного менеджмента<sup>24</sup> и Российско-латиноамериканской ассоциации стратегических исследований<sup>25</sup>. Таким образом, можно констатировать, что проблематика международной информационно-психологической безопасности в контексте угроз ЗИИИ закрепились на начальном уровне восприятия части международного научного сообщества, а также, хотя и в меньшей мере, в бизнес-среде и среди лиц, участвующих в разработке и принятии государственных решений.

Подготовлен проект создания международного исследовательского центра «Искусственный интеллект и проблемы международной информационно-психологической безопасности», его реализация потребует времени прежде всего по финансовым причинам.

---

<sup>22</sup> См., например: Искусственный интеллект и проблемы обеспечения международной информационно-психологической безопасности. Круглый стол «Свобода выражения мнений в цифровой среде в контексте обсуждения проблематики международной информационной безопасности на профильных международных площадках» МИД РФ. 28 ноября 2018 г. // Pure [Электронный ресурс]. URL: <https://pureportal.spbu.ru/ru/activities/искусственный-интеллект-и-проблемы-обеспечения-международной-инфо> (дата обращения: 29.09.2019).

<sup>23</sup> Искусственный интеллект и проблемы обеспечения международной информационно-психологической безопасности. Круглый стол «Свобода выражения мнений в цифровой среде в контексте обсуждения проблематики международной информационной безопасности на профильных международных площадках» МИД РФ. 28 ноября 2018 г. // Pure [Электронный ресурс]. URL: <https://pureportal.spbu.ru/ru/activities/искусственный-интеллект-и-проблемы-обеспечения-международной-инфо> (дата обращения: 29.09.2019);

<sup>24</sup> European — Russian Communication Management Network (EU-RU-CM Network) [Электронный ресурс]. URL: <http://globalstratcom.ru/eurucmnet/> (дата обращения: 14.09.2019).

<sup>25</sup> Russian-Latin American Strategic Studies Association (RLASSA) [Электронный ресурс]. URL: <http://globalstratcom.ru/russian-latin-american-strategic-studies-association/> (дата обращения: 14.09.2019).



### **Заключение**

Осмысление человеком новых угроз, количество которых будет только расти, отстает от стремительно меняющихся реалий современного мира. Различные государственные и негосударственные акторы смогут применить быстро дешевающие и распространяющиеся средства ИИ для нанесения ущерба обществу. В складывающейся ситуации необходимы междисциплинарные исследовательские проекты, чтобы выяснить, как применение ИИ может усилить «традиционные» средства воздействия на общественное сознание и противостоять ЗИИИ.

В настоящей статье выделены лишь некоторые из возможностей ЗИИИ, которые могут представлять большую опасность для МИПБ. Эксперты из разных стран предупреждают о новых и перспективных рисках по мере быстрого развития технологий. Список таких рисков будет продолжать увеличиваться, но мы надеемся, что это будет происходить вместе со способностью общества противостоять новым угрозам. Важно не упустить момент и снизить издержки нашего реагирования на эти новые угрозы. Ошибки особенно недопустимы из-за возможных глобальных катастрофических последствий МИПБ в условиях нарастания кризиса современной цивилизации, резкого обострения межгосударственных противоречий. Одним из негосударственных акторов, способных серьезно угрожать МИПБ в будущем посредством ЗИИИ, является международный терроризм, что следует учитывать в долгосрочной стратегии России по обеспечению национальной информационно-психологической безопасности и усилиях на международной арене по созданию предпосылок для устойчивого и безопасного развития человечеств в условиях новых высокотехнологичных угроз общественному сознанию.

Не только ведущим в технологическом отношении государствам, но и всем странам ООН, видимо, необходимо найти более эффективный механизм сотрудничества, направленного на минимизацию ЗИИИ. Сделать это будет крайне непросто, но необходимо, причем в достаточно сжатые сроки.

Помимо ИИ, вся сумма новых технологий требует качественных изменений в человеческом обществе как на уровне государственных и общественных институтов, так и на уровне человеческого индивидуума. Для индивидуума требуются качественные изменения в его ментальных, физических способностях, уровне этических норм и социальной ответственности с целью использовать качественно новые возможности, минимизировать качественно новые риски и обеспечить поступательное развитие социума. Альтернатива таким изменениям —

самоуничтожение (быстрое или относительно постепенное) человечества и ликвидация возможности старта новой прогрессивной цивилизации, уважающей свои корни, но идущей вперед в своем развитии. Большая позитивная определенность, осмысленность, последовательность в таком движении в будущее — лучшее лекарство против террористов. Всякая неопределенность, колебания, отсрочка назревших решений и, главное, отсутствие стратегического видения и соответствующих действий будут играть на руку асоциальным группам, включая террористические организации.

В самом недалеком будущем государственным и общественным структурам разных стран предстоит решить следующие задачи:

- поставить теоретические и практические вопросы ЗИИИ против МИПБ на обсуждение на международных площадках (ООН, ЮНЕСКО и др.). Необходимо учесть важность и стратегическую перспективность этой темы в сложной международной обстановке. ЗИИИ против МИПБ при определенных условиях способно ее существенно усложнить и даже спровоцировать кризис в международных отношениях. Существенно и то, что, пока широкая тематика ЗИИИ пользуется определенным вниманием профессиональной общественности и органов власти на Западе, проблема ЗИИИ против МИПБ получила приоритетное рассмотрение именно в работах российских исследователей. Результаты исследований озвучены на авторитетных международных конференциях и опираются на целый ряд публикаций, сформирована международная группа специалистов, поддерживающих это новое направление;
- подтема «Угроза овладения террористами технологиями информационно-психологического воздействия на базе искусственного интеллекта и возможные пути ее нейтрализации» должна получить развитие в теории и практике антитеррористических структур России и других стран;
- изыскать возможности для создания в России исследовательского центра по рассмотрению ЗИИИ против МИПБ;
- исследовать возможности развития широкого (сильного) искусственного интеллекта с учетом возможных угроз для МИПБ уже сегодня;

- крайне важно рассматривать вопросы ЗИИИ против МИПБ в контексте разнообразия моделей социального развития на основе все более широкого внедрения ИИ в общественную жизнь.

**Список литературы:**

Базаркина Д.Ю., Дурсунова Э.Э. Российские специалисты в Латинской Америке: научные мероприятия по проблемам передовых технологий и информационно-психологического противоборства (27 августа – 10 сентября 2018 г.) // Государственное управление. Электронный вестник. 2018. № 71. С. 369–389.

Базаркина Д.Ю., Ласурия Л.Дж. Искусственный интеллект и международная информационно-психологическая безопасность: выступления российских исследователей в ЮАР // Государственное управление. Электронный вестник. 2019. № 75. С. 283–299.

Ларина Е.С., Овчинский В.С. Искусственный интеллект. Большие данные. Преступность. М.: Книжный мир, 2018.

Пашенцев Е.Н. Прогностическое оружие и борьба с терроризмом // Противодействие терроризму. Проблемы XXI века. 2016. № 2. С. 9–16.

Averkin A.N., Bazarkina D.Yu., Pantserev K.A., Pashentsev E.N. Artificial Intelligence in the Context of Psychological Security: Theoretical and Practical Implications // 11<sup>th</sup> Conference of the European Society for Fuzzy Logic and Technology (EUSFLAT 2019). Atlantis Studies in Uncertainty Modelling. 2019. Vol. 1. P. 101–107.

Bazarkina D., Pashentsev E. Artificial Intelligence and New Threats to International Psychological Security // Russia in Global Affairs. 2019. № 1. P. 147–170.

Bifolchi G., Pashentsev E., Shilina M. The 3rd International Conference ‘Transformation of International Relations in the XXI Century: Challenges and Prospects’ (TIR3), Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, 27–28 April 2017. The Issues of Strategic Communication: Russian and Foreign Experience at TIR 3 // Russian Journal of Communication. 2018. № 1. P. 101–104.

Brundage M., Avin Sh., Clark J., Toner H., Eckersley P., Garfinkel B., Dafoe A., Scharre P., Zeitzoff Th., Filar B., Anderson Y., Roff H., Allen G.C., Steinhardt J., Flynn C., Ó hÉigeartaigh S., Beard S., Belfield H., Farquhar S., Lyle C., Crootof R., Evans O., Page M., Bryson J., Yampolskiy R., Amodei D. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Oxford, AZ: Future of Humanity Institute, University of Oxford, 2018.

Doyle A., Katz G., Summers K., Ackermann Chr., Zavorin I., Lim Z., Muthiah S., Butler P., Self N., Zhao L., Lu Ch.-T., Khandpur R.P., Fayed Y., Ramakrishnan N. Forecasting Significant Societal Events Using the EMBERS Streaming Predicative Analytics System // Big Data. 2014. Issue 4. P. 185–195.

Fastand E., Horvitz E. Long-Term Trends in the Public Perception of Artificial Intelligence // arXiv of Cornell University. 2016. URL: <https://arxiv.org/pdf/1609.04904.pdf> (дата обращения: 14.09.2019).

Frey B.C., Osborne A. The Future of Employment: How Susceptible Are Jobs to Computerisation? // Technological Forecasting and Social Change. 2017. Vol. 114. P. 254–280.

Holder Chr., Khurana V., Watts M. Artificial Intelligence: Public Perception, Attitude and Trust. London: Bristows, 2018.

Horowitz M.C., Scharre P., Allen G.C., Frederick K., Cho A., Saravalle E. Artificial Intelligence and International Security. Washington: Center for a New American Security (CNAS), 2018.

Karras T., Laine S., Aila T. A Style-Based Generator Architecture for Generative Adversarial Networks // arXiv of Cornell University. URL: <https://arxiv.org/pdf/1812.04948.pdf> (дата обращения: 14.09.2019).

Pashentsev E. Destabilization of Unstable Dynamic Social Equilibriums through High-Tech Strategic Psychological Warfare // Proceedings of the 14<sup>th</sup> International Conference on Cyber Warfare and Security. Stellenbosch University, South Africa. UK: Academic Conferences and Publishing International Limited, 2019a. P. 322–328.

Pashentsev E. How to Counteract Illegal Mediterranean Migrant Arrivals (IMMA) through Strategic Communication Using AI — A Research and Consultancy Project // Глобальные и региональные аспекты миграционных процессов. М.: Федеральное государственное бюджетное учреждение науки «Институт Европы Российской академии наук», Институт лингвоцивилизационных и миграционных процессов при фонде «Русский мир», 2019b. С. 50–57.

Pashentsev E. Malicious Use of Artificial Intelligence: Challenging International Psychological Security // European Conference on the Impact of AI and Robotics. EM-Normandie Business School, Oxford, 31 October – 1 November 2019. Conference Proceedings. UK: Academic Conferences and Publishing International Limited, 2019c. P. 140–147.

*Pashentsev E.* Sophisticated Technologies in Counteraction to Terrorism in Datafied Society (From Big Data to Artificial Intelligence) // *Understanding the War on Terror: Perspectives, Challenges and Issues*. New York: Nova Science Publishers, 2019d. P. 99–136.

*Pol E., James R.* Robot Induced Technological Unemployment: Towards a Youth-Focused Coping Strategy // *Psychosociological Issues in Human Resource Management*. 2017. № 5(2). P. 169–186.

*Strategic Communication in EU-Russia Relations: Tensions, Challenges and Opportunities* / ed. by E. Pashentsev, E. Vlaeminck. Moscow: ICSPSC, 2018.

*Strategic Communication in EU-Russia Relations: Tensions, Challenges and Opportunities* / ed. by E. Pashentsev. London: Palgrave Macmillan, 2020.

*Pashentsev E.N.*

### **Malicious Use of Artificial Intelligence: New Threats to International Psychological Security and Ways to Neutralize Them**

*Evgeny N. Pashentsev* — DSc (History), Professor, Leading Researcher, Diplomatic Academy of the MFA of Russia; Professor, Lomonosov Moscow State University; Director of the International Center for Socio-Political Studies and Consulting, Moscow, Russian Federation.  
E-mail: [icspsc@mail.ru](mailto:icspsc@mail.ru)

#### **Abstract**

The article presents an analysis of new threats to international psychological security caused by the rapid introduction of artificial intelligence (AI) into various spheres of public life, as well as its malicious use by aggressive actors of international relations. Compared to the positive use of AI, the aspect of AI malicious use associated with threats to international psychological security is much less studied. The author presents only some of the methods of artificial intelligence malicious use: the window of opportunities for such use is steadily growing, the quality and depth of penetration into the public consciousness with the help of AI is increasing. This naturally occurs with the improvement of AI technical capabilities and the growing demand for such opportunities on the part of selfish interest groups under the growing global crisis, the decline in the living standards of the majority of the population in the majority of countries, the growth of social and property polarization, the dangerous growth of geopolitical rivalry. The author gives a definition of international psychological security, offers possible classifications of AI malicious use based on implementability, territorial coverage, the degree of damage, and the speed and forms of propagation. The author defines the purpose and objectives of AI malicious use, assesses some current and future threats of such use in the context of threats to international psychological security. The study confirms that the malicious use of AI raises threats to international psychological security to a qualitatively new level that requires an adequate assessment and response from society and public authorities.

#### **Keywords**

Artificial intelligence, strong artificial intelligence, weak artificial intelligence, international information and psychological security, international security, promising technologies.

**DOI:** 10.24411/2070-1381-2019-10013

#### **References:**

Averkin A.N., Bazarkina D.Yu., Pantserev K.A., Pashentsev E.N. (2019) Artificial Intelligence in the Context of Psychological Security: Theoretical and Practical Implications.

11<sup>th</sup> Conference of the European Society for Fuzzy Logic and Technology (EUSFLAT 2019). *Atlantis Studies in Uncertainty Modelling*. Volume 1. P. 101–107.

Bazarkina D., Pashentsev E. (2019) Artificial Intelligence and New Threats to International Psychological Security. *Russia in Global Affairs*. No. 1. P. 147–170.

Bazarkina D.Yu., Dursunova E.E. (2018) Russian Specialists in Latin America: Academic Events on the Problems of Advanced Technologies and Psychological Warfare (August, 27<sup>th</sup> –September 10<sup>th</sup>, 2018). *Gosudarstvennoye upravleniye. Elektronnyy vestnik*. No. 71. P. 369–389.

Bazarkina D.Yu., Lasuriia L.Dz. (2019) Artificial Intelligence and International Psychological Security: Russian Researchers' Presentations in South Africa. *Gosudarstvennoye upravleniye. Elektronnyy vestnik*. No. 75. P. 283–299.

Bifolchi G., Pashentsev E., Shilina M. (2018) The 3rd International Conference 'Transformation of International Relations in the XXI Century: Challenges and Prospects' (TIR3), Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, 27–28 April 2017. The Issues of Strategic Communication: Russian and Foreign Experience at TIR 3. *Russian Journal of Communication*. No. 1. P. 101–104.

Brundage M., Avin Sh., Clark J., Toner H., Eckersley P., Garfinkel B., Dafoe A., Scharre P., Zeitoff Th., Filar B., Anderson Y., Roff H., Allen G.C., Steinhardt J., Flynn C., Ó hÉigearthaigh S., Beard S., Belfield H., Farquhar S., Lyle C., Crootof R., Evans O., Page M., Bryson J., Yampolskiy R., Amodei D. (2018) *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Oxford, AZ: Future of Humanity Institute, University of Oxford.

Doyle A., Katz G., Summers K., Ackermann Chr., Zavorin I., Lim Z., Muthiah S., Butler P., Self N., Zhao L., Lu Ch.-T., Khandpur R.P., Fayed Y., Ramakrishnan N. (2014) Forecasting Significant Societal Events Using the EMBERS Streaming Predicative Analytics System. *Big Data*. Issue 4. P. 185–195.

Fastand E., Horvitz E. (2016) Long-Term Trends in the Public Perception of Artificial Intelligence. *arXiv of Cornell University*. Available: <https://arxiv.org/pdf/1609.04904.pdf> (accessed: 14.09.2019).

Frey B.C., Osborne A. (2017) The Future of Employment: How Susceptible Are Jobs to Computerisation? *Technological Forecasting and Social Change*. Vol. 114. P. 254–280.

Holder Chr., Khurana V., Watts M. (2018) *Artificial Intelligence: Public Perception, Attitude and Trust*. London: Bristows.

Horowitz M.C., Scharre P., Allen G.C., Frederick K., Cho A., Saravalle E. (2018) *Artificial Intelligence and International Security*. Washington: Center for a New American Security (CNAS).

Karras T., Laine S., Aila T. (2019) *A Style-Based Generator Architecture for Generative Adversarial Networks*. arXiv of Cornell University. Available: <https://arxiv.org/pdf/1812.04948.pdf> (accessed: 14.09.2019).

Larina E.S., Ovchinskij V.S. (2018) *Iskusstvennyj intellekt. Bol'shie dannye. Prestupnost'* [Artificial Intelligence. Big Data. Crime]. Moscow: Knizhnyj mir.

Pashentsev E. (2019a) Destabilization of Unstable Dynamic Social Equilibriums through High-Tech Strategic Psychological Warfare. *Proceedings of the 14<sup>th</sup> International Conference on Cyber Warfare and Security*. Stellenbosch University, South Africa. 28 February – 1 March 2019. Reading, UK: Academic Conferences and Publishing International Limited. P. 322–328.

Pashentsev E. (2019b) How to Counteract Illegal Mediterranean Migrant Arrivals (IMMA) through Strategic Communication Using AI — A Research and Consultancy Project. *Global'nye i regional'nye aspekty migracionnykh processov*. Moscow: «Institut Evropy Rossiyskoy akademii nauk», Institut lingvotsivilizatsionnykh i migratsionnykh protsessov pri fonde «Russkiy mir» «Institut Evropy Rossiyskoy akademii nauk», Institut lingvotsivilizatsionnykh i migratsionnykh protsessov pri fonde «Russkiy mir». P. 50–57.

Pashentsev E. (2019c) Malicious Use of Artificial Intelligence: Challenging International Psychological Security. *European Conference on the Impact of AI and Robotics*. EM-Normandie Business School, Oxford, 31 October – 1 November 2019. Conference Proceedings. UK: Academic Conferences and Publishing International Limited. P. 140–147.

Pashentsev E. (2019d) Sophisticated Technologies in Counteraction to Terrorism in Datafied Society (From Big Data to Artificial Intelligence). *Understanding the War on Terror: Perspectives, Challenges and Issues*. New York: Nova Science Publishers. P. 99–136.

Pashentsev E., Vlaeminck E. (eds.) (2018) *Strategic Communication in EU-Russia Relations: Tensions, Challenges and Opportunities*. Moscow: ICSPSC.

Pashentsev E., Vlaeminck E. (eds.) (2020) *Strategic Communication in EU-Russia Relations: Tensions, Challenges and Opportunities*. London: Palgrave Macmillan.

Pashentsev E.N. (2016) Prognostic Weapon and Struggle with Terrorism. *Protivodeystviye terrorizmu. Problemy XXI veka*. No. 2. P. 9–16.

Pol E., James R. (2017) Robot Induced Technological Unemployment: Towards a Youth-Focused Coping Strategy. *Psychosociological Issues in Human Resource Management*. No. 5(2). P. 169–186.