К.А. Панцерев, Д.А. Рущин, Д.О. Матяшова, М.В. Шудрик

ОБЕСПЕЧЕНИЕ И ПРОДВИЖЕНИЕ ЦИФРОВОЙ ГИГИЕНЫ В КОНТЕКСТЕ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Международная онлайн-конференция, Университет Хайдарабада, Индия, 24–25 марта 2021 года*

© Панцерев Константин Арсеньевич – доктор политических наук, профессор, Санкт-Петербургский государственный университет, Санкт-Петербург; e-mail: pantserev@yandex.ru
© Рущин Дмитрий Александрович – кандидат исторических наук, доцент, Санкт-Петербургский государственный университет, Санкт-Петербург; e-mail: ruschin@mail.ru
© Матяшова Дарья Олеговна – студентка, Санкт-Петербургский государственный университет, Санкт-Петербург; e-mail: dasham0708@mail.ru
© Шудрик Максим Владимирович – студент, Санкт-Петербургский государственный университет, Санкт-Петербург; e-mail: st086412@student.spbu.ru

24–25 марта 2021 года в дистанционном формате состоялась двухдневная международная онлайн-конференция «Обеспечение и продвижение цифровой гигиены в контексте развития искусственного интеллекта» («Accelerating Actions and Promoting Digital Wellness in the context of Artificial Intelligence») под эгидой Межправительственной программы ЮНЕСКО «Информация для всех» (UNESCO Intergovernmental Information for All Programme – IFAP). Организаторами конференции выступили Индийский центр передового опыта в области информационной этики (India Centre of Excellence for Information Ethics – ICEIE) и Центр цифрового образования, стажировок и ресурсов (Centre for Digital Learning, Training and Resources – CDLTR), находящиеся в составе Университета Хайдарабада (Индия).

25 марта в рамках конференции состоялся круглый стол «Злонамеренное использование искусственного интеллекта: вызовы международной информационно-психологической безопасности» (Malicious Use of Artificial Intelligence: Challenging the International Psychological Security), в котором приняли участие Мариус Вакарелу, профессор Национальной школы политических и административных исследований (Румыния); Константин Панцерев, доктор политических наук, профессор Санкт-Петербургского государственного университета; Пьер-Эммануэль Томанн, профессор Университета Лион-3 (Франция). В качестве сопредседателей выступили доктор исторических наук, профессор, ведущий научный сотрудник Дипломатической академии МИД РФ Евгений Пашенцев и организатор мероприятия – доктор политических наук, профессор Института права и национальной безопасности Российской академии народного хозяйства и государственной службы при Президенте РФ Дарья Базаркина, которые также представили доклады.

Круглый стол прошел при академической поддержке Международной группы исследователей угроз информационно-психологической безопасности, обусловленных злонамеренным использованием искусственного интеллекта (International Research Group of Specialists on the Threats to International Psychological Security through the Malicious Use of Artificial Intelligence (Research MUAI). Финансовую поддержку двух докладов в рамках мероприятия оказал Российский фонд фундаментальных исследований в рамках научного проекта № 21–514–92001.

Первым с концептуальным докладом, посвященным возможному злонамеренному использованию технологий искусственного интеллекта (ИИ), выступил Е.Н. Пашенцев. В своем выступлении он отметил возросшую роль технологий ИИ в формировании информационной повестки дня в современном мире и то, к каким негативным последствиям может привести злонамеренное использование таких технологий. Способствуют нарастанию угрозы следующие условия: отделение интересов доминирующих групп от национальных интересов и социально ориентированных моделей развития с одной стороны и достаточно высокий уровень развития технологий искусственного интеллекта и наличие соответствующей инфраструктуры, с другой. Менее технологически развитые государства не могут эффективно защитить себя от возможной информационной атаки с применением передовых технологий со стороны высокоразвитых государств, кроме как полностью отключившись от Интернета. Но подобные крайне жесткие меры вряд ли приведут к ожида-

* Исследование поддержано Санкт-Петербургским государственным университетом, проект № 73555239

емым положительным результатам. Скорее наоборот, они будут способствовать дальнейшему скатыванию подобных государств на периферию мировых информационно-коммуникационных процессов. В этом контексте Е.Н. Пашенцев спрогнозировал, что, принимая во внимание наблюдающийся сегодня глубокий кризис демократических институтов и нарастающую геополитическую конфронтацию, риски злонамеренного использования ИИ будут только расти.

К наиболее перспективным угрозам, исходящим от технологий искусственного интеллекта, профессор Е.Н. Пашенцев отнес, прежде всего, злонамеренное использование функционирующих на основе технологий искусственного интеллекта ботов. Это могут быть боты, интегрированные в социальные сети, различные чат-боты, а также торговые боты. Другие же технологии ИИ, такие как анализ настроений в обществе, дипфейки[1] либо предсказательная аналитика, с точки зрения Е.Н. Пашенцева, менее изучены как инструменты формирования повестки дня.

С точки зрения Е.Н. Пашенцева, появление новых угроз, связанных с современными информационными технологиями обусловлено следующими факторами: 1) резкое увеличение объема генерируемой информации, 2) повышение скорости генерации и распространения информации, 3) правдоподобность информации, 4) усиление интеллектуального и эмоционального воздействия, 5) возможности обработки аналитических данных, 6) рост возможностей прогнозной аналитики на основе ИИ, 7) методы убеждения, 8) новые возможности интеграции в процесс принятия решений.

В конце своего выступления профессор Е.Н. Пашенцев порекомендовал:

– создать на национальном и международном уровне научно-аналитические и мониторинговые центры, которые бы выявляли угрозы злонамеренного использования ИИ и разрабатывали бы рекомендации по нейтрализации этих угроз;

– оказывать любую организационную, финансовую и политическую поддержку международным междисциплинарным исследовательским группам, занимающимся изучением угроз злонамеренного использования ИИ;

– проводить международные междисциплинарные научно-практические конференции по данной проблематике.

[1] Deepfake – создание и публикация ложной информации в виде видео, аудио и фотографий.

Доклад Мариуса Вакарелу был посвящен вопросам морали и использования инструментов искусственного интеллекта в политических кампаниях. Рассуждая о тесной взаимосвязи между политикой, вопросами морали и ИИ в наши дни, М. Вакарелу особенно подчеркнул необходимость правильного применения технологий ИИ при проведении политических кампаний. По его мнению, мотивация к власти и самореализации через власть отличает политиков от других граждан, которые готовы в первую очередь предпринимать меры по улучшению исключительно собственных условий жизни. Это различие, в совокупности с социальной ролью политиков, требует специальных институтов, которые бы обучали вести политическую жизнь.

М. Вакарелу отметил, что избирательные кампании заставляют политиков внедрять любые технологии, которые могут оказаться полезными для достижения конечной цели. Технологии ИИ, с одной стороны, способны резко увеличить количество акций в рамках той или иной политической кампании, а с другой – лучше изучить ожидания избирателей. Как следствие, возникает проблема соотношения морали и политики, поскольку плохое управление, равно как и проведение политических кампаний, основанных исключительно на аморальных принципах, при помощи технологий ИИ, может привести не только к сильному социальному недовольству, но и к изменению политического режима. В связи с этим М. Вакарелу делает вывод, что, несмотря на все потенциальные преимущества, которые несет активное внедрение технологий ИИ во все сферы человеческой жизни, включая проведение политических кампаний, ИИ может нанести большой вред политической культуре. С точки зрения ученого, в XXI веке одной из основных политических задач является нахождение правильного баланса между использованием инструментов искусственного интеллекта и моральными нормами.

Доклад К.А. Панцерева «Существующая практика злонамеренного использования ИИ в странах Африки к югу от Сахары» был посвящен проблеме обеспечения информационной безопасности в Африке. В своем выступлении ученый отметил, что на протяжении двух десятилетий страны Африки к югу от Сахары предпринимали значительные усилия, направленные на быстрое развитие своего информационно-телекоммуникационного сектора. Но проблема заключается в том, что любые

технологические новинки, которые призваны упростить нашу жизнь, могут также использоваться злоумышленниками с целью незаконного обогащения либо, что намного хуже, нанесения значительного урона критически важной инфраструктуре государства. В частности: скрывать вредоносные коды в официальных, безопасных приложениях; влиять на голосовую или визуальную аутентификацию; установить контроль над любым устройством при помощи закрытых ключей; организовать кибер-атаку с использованием технологий ИИ, которую крайне сложно выявить; сымитировать надежные компоненты системы.

Приведя несколько примеров злонамеренного использования передовых технологий, К.А. Панцерев делает вывод, что, уделяя в последние годы большое внимание развитию на своей территории информационно-телекоммуникационной индустрии, страны Африки к югу от Сахары практически не предпринимали никаких усилий по укреплению своей информационной безопасности, в том числе в вопросах, связанных с использованием технологий ИИ. В подтверждение своих слов К. А. Панцерев привел достаточно любопытные статистические данные: сегодня более 60% африканских предприятий не обучают своих сотрудников кибербезопасности, а более 90% крупных африканских компаний тратят менее 10 000 долларов США на обеспечение своей кибербезопасности. Это делает африканские предприятия особенно уязвимыми перед лицом таких угроз, как интеллектуальные атаки на компьютерные системы предприятий, воздействие на голосовую или визуальную аутентификацию, сокрытие вредоносных кодов в официальных приложениях и ряд других.

Нигерия, Кения и ЮАР входят в топ-3 африканских государств, которые терпят наибольшие убытки от киберпреступлений. Чтобы нивелировать угрозы, исходящие от злонамеренного использования передовых технологий в Африке, К.А. Панцерев рекомендовал включить проблему обеспечения кибербезопасности и противодействия злонамеренному использованию ИИ в панафриканскую повестку дня.

В 2014 году в Малабо (Экваториальная Гвинея) была принята Конвенция Африканского союза о кибербезопасности и защите персональных данных. На сегодняшний день Конвенцию подписали 14 африканских стран, а ратифицировали только 8 – Ангола, Гана, Гвинея, Мозамбик, Маврикий, Намибия, Руанда, Сенегал. Примечательно, что Кения, Нигерия и Южная Африка – региональные лидеры в сфере развития информационно-коммуникационных технологий – воздержались от подписания этого важного документа. С точки зрения К.А. Панцерева, появление этого документа следует рассматривать как важное событие, которое доказывает, что африканские страны понимают, что им следует разработать совместный механизм, направленный на прекращение дальнейшего распространения киберпреступности. Но в то же самое время процесс подписания и ратификации Конвенции показывает, что сегодня существует ряд серьезных противоречий между различными африканскими странами по вопросу обеспечения кибербезопасности. Документ все еще не может вступить в силу, поскольку ее должны ратифицировать не менее 15 африканских стран.

Конвенция может рассматриваться только как некий программный документ, который определяет важнейшие направления сотрудничества в информационной сфере (особенно в сфере противодействия киберпреступности) межу различными африканскими странами. Данное обстоятельство заставляет К.А. Панцерева сделать вывод, что наднациональные институты плохо работают в Африке из-за серьезных противоречий между странами, которые препятствуют налаживанию взаимовыгодного сотрудничества даже по такому важному вопросу, как кибербезопасность.

Пьер-Эммануэль Томанн в своем выступлении осветил проблемы регулирования ИИ в ЕС. Он особенно подчеркнул, что современный мир сталкивается с растущей геополитической фрагментацией и изменением прежних геополитических иерархий. Имеющая место сегодня геополитическая конфронтация, с его точки зрения, подготавливает почву для гибридной войны, которая всегда включает информационно-психологический компонент.

Злонамеренное использование ИИ, применяемого на тактическом уровне, может иметь важные последствия в конфликте или борьбе за геополитическое влияние, особенно если ИИ используется таким образом, что ведет к росту влияния одного или нескольких государств. По словам П.-Э. Томанна, это обстоятельство способно дестабилизировать систему международных отношений и создать несбалансированные новые геополитические иерархии. Вопреки общепринятой идее о том, что цифровая революция обязательно вызывает экономическую децентрали-

зацию, на самом деле, возможно, что ИИ спровоцирует глобальное движение в сторону сосредоточения власти в руках горстки государств и частных акторов.

С точки зрения П.-Э. Томанна, основное внимание Европейского Союза в отношении искусственного интеллекта, сконцентрировано на его этических, нормативных и экономических аспектах в контексте регулирования общего рынка ЕС. 19 февраля 2020 года Европейская Комиссия опубликовала Белую книгу по ИИ и Доклад об аспектах безопасности и ответственности ИИ, но в этих документах не рассматриваются вопросы разработки и использования ИИ в военных целях.

По словам П.-Э. Томанна ЕС стремится взять на себя лидерство во второй цифровой революции и сделать акцент на использовании промышленных данных (поскольку битва за частные данные была проиграна), которые являются основным двигателем технологий искусственного интеллекта. Но проблема ЕС заключается в деиндустриализации Европы (особенно в ее южных регионах), а также в отсутствии долгосрочной общей стратегии, направленной на развитие технологий ИИ.

Отсутствие единых взглядов на геополитическую картину мира, равно как и единой позиции в отношении искусственного интеллекта и цифровизации среди государств-членов ЕС является, с точки зрения П.-Э. Томанна, серьезным препятствием для выработки консолидированной стратегии ЕС в указанной области и для развития международного сотрудничества в борьбе со злонамеренным использованием ИИ и защите международной информационно-психологической безопасности.

Ученый убежден, что позиция ЕС в отношении ИИ, с ее основным акцентом на этические вопросы, недостаточна для того, чтобы внести позитивный вклад в улучшение равновесия в международных отношениях. ЕС и его международные партнеры смогут продвигать этическое измерение ИИ только в том случае, если он достигнет позиции силы и суверенитета, а не позиции зависимости и слабости. В то же время следует иметь в виду, что сила и суверенитет вне инновационной модели развития могут усилить международную конкуренцию в самой Европе и в мире. В этой связи, делает вывод французский исследователь, было бы разумным объединить ориентированный на человека подход к ИИ с доктриной баланса сил, которая предполагает более равный доступ к ИИ и создание крупных глобальных альянсов для борьбы со злонамеренным использованием технологий ИИ, угрожающим информационно-психологической безопасности и геополитической стабильности.

Д.Ю. Базаркина в докладе, посвященном злонамеренному использованию искусственного интеллекта террористическими организациям, подчеркнула, что военное поражение так называемого «Исламского государства» (ИГ) спровоцировало переход от прямых вооруженных столкновений к удаленным атакам в рамках сетевой структуры, где коммуникации в виртуальном пространстве играют ключевую роль. В этом контексте терроризм приобретает много общего с киберпреступностью, используя передовые технологии как для пропаганды, так и для физического уничтожения людей.

ИИ способен изменить механизм вербовки новых сторонников в ряды террористических организаций, прежде всего в связи с его возможностями выстроить индивидуализированный контент. Вербовщику-человеку всегда требовалось время, чтобы лучше узнать потенциального объекта вербовки и начать общение с ним в социальных сетях или мессенджерах. После этого, как правило, вербовщик задает объекту вербовки ряд личных вопросов (есть ли у последнего желание жениться, наличие каких-либо проблем в профессиональной сфере и т.д.), выясняя его уязвимые места. После этого вербовщик обещает объекту вербовки именно то, чего ему не хватает в жизни – счастье в браке, стабильность, признание, профессиональный рост, реализацию его способностей и т.д. Достижение всех этих целей увязывается, конечно же, со вступлением в ряды террористической организации.

Сегодня возможности ИИ стремительно растут не только в отслеживании цифровых следов человека, но и в построении контента. Например, анализ настроений поведения жертвы в цифровой среде может сократить время, необходимое для изучения ее привычек, сильных сторон и уязвимостей. Распознавание лиц позволяет отслеживать появление фото/видео объекта вербовки даже на тех ресурсах, на которых он не зарегистрирован.

Угроза усугубляется низкой информированностью населения не только о развитии технологий ИИ, но и о средствах психологического воздействия, используемых террористами. Д.Ю. Базаркина подчеркнула, что, с одной стороны, специалисты в области безопасности должны будут мыс-

лить, как террористы, при оценке рисков внедрения тех или иных технологий ИИ в обществе и государстве (это поможет продумать большее число сценариев и методов противодействия использованию ИИ террористами для управления общественным мнением). С другой стороны, всем ответственным структурам нужно разрабатывать широкие программы просвещения граждан не только в сфере использования ИИ, но также в психологической и политической сферах. Нужно объяснять гражданам, как и какие уязвимые места человеческой психики, реальные жизненные проблемы, политическую ситуацию использует террорист, общаясь со своими аудиториями. Для этого необходим междисциплинарный подход с привлечением специалистов как технического, так и гуманитарного профиля.

Рекомендации, сделанные участниками конференции, включая участников круглого стола, вошли в Хайдарабадскую Декларацию – итоговый документ конференции, который, как ожидается, станет важной вехой в развитии международного научного сотрудничества по проблемам политики в сфере искусственного интеллекта.

Д.А. Рущин

РЕЛИГИОЗНЫЙ ФАКТОР В МЕЖДУНАРОДНОЙ ПОЛИТИКЕ: ВОЗМОЖНОСТИ ДИАЛОГА, ПРАВА ЧЕЛОВЕКА И ИНСТРУМЕНТ ДАВЛЕНИЯ

Международная онлайн-конференция, Москва, 13 мая 2021 года

© Рущин Дмитрий Александрович — кандидат исторических наук, доцент, Санкт-Петербургский государственный университет, Санкт-Петербург; e-mail: ruschin@mail.ru

13 мая 2021 года в Москве состоялась международная онлайн-конференция «Религиозный фактор в международной политике: Возможности диалога, права человека и инструмент давления». В конференции приняли участие ученые, эксперты, журналисты, дипломаты из России, Франции, Конго, Тайваня.

Видный российский богослов, вице-президент Европейской федерации центров по исследованию и информированию о сектах (FECRIS) Александр Дворкин выступил с докладом на тему «Секты как фактор международной политики». По мнению докладчика, секты уже давно ведут международную политическую деятельность. До начала 1990-х годов в США преобладала мощная антисектантская политика, но постепенно отношение властей этой страны к сектам стало меняться по принципу: «Если не можешь противостоять процессу, возглавь его».

В 1998 году Конгресс США принял «Международный Акт о религиозных свободах» (H.R.2431). Тем самым Вашингтон взял на себя миссию гаранта свободы вероисповедования во всем мире. В 2016 году президент США Барак Обама заявил, что соблюдение религиозных свобод в мире является гарантией национальной безопасности США. 12 мая 2021 года государственный секретарь США Энтони Блинкен выступил с докладом о состоянии религиозной свободы в России. Он предъявил к Российской Федерации ряд претензий. Во-первых, критиковал Москву за «гонения» на Общество свидетелей Иеговы и ряд исламских фундаменталистских организаций. Во-вторых, упрекнул российские власти в том, что они оказывают предпочтение Русской Православной Церкви (РПЦ).

А. Дворкин также коснулся деятельности патронируемого США Международного Альянса религиозных свобод (IRFA). По его мнению, эта организация создана для политического давления на Россию. В ней присутствует слишком много бывших советских союзных республик и государств Восточной Европы, имеющих противоречия с РФ.

Еще одной страной, использующей фактор сект и новых религиозных движений, по мнению А. Дворкина, является Индия. В период правления в этой стране партии Индийский Национальный Конгресс (ИНК) до 2014 года индийская политическая элита открещивалась от неоиндуистских организаций. Они являются еретическими с точки зрения ортодоксального индуизма, так как эта религия отвергает прозелитизм. Индусом можно только родиться, принадлежа к определенной варне. Когда же к власти в стране пришла правая националистическая «Бхаратия Джаната Парти» (БДП), руководство Индии стало поддерживать по всему миру псевдоиндуистские организации, выдвинув новую идею о том, что изначальной религией человечества была религия Вед,