АНАЛИТИЧЕСКАЯ ЗАПИСКА

41 / 2023

Угрозы международной информационной безопасности в эпоху Индустрии 4.0

РСМД
Российский совет по международным делам

Сергей Себекин

РОССИЙСКИЙ СОВЕТ ПО МЕЖДУНАРОДНЫМ ДЕЛАМ

Автор:
канд. ист. наук **С.А. Себекин**

Редакторская группа:
Е.О. Карпинская (ответственный редактор), канд. полит. наук **А.Ю. Толстухина,**
канд. ист. наук **С.М. Гаврилова** (выпускающий редактор)

Российский совет по международным делам (РСМД) — один из ведущих аналитических центров страны, ориентированных на проведение исследований в области международных отношений, выработку практических рекомендаций по вопросам внешней политики и международных отношений в интересах российских органов государственной власти, бизнеса и некоммерческих организаций. Совет создан решением учредителей в соответствии с распоряжением Президента Российской Федерации от 2 февраля 2010 года.

РСМД объединяет усилия экспертного сообщества, органов государственной власти, бизнес-кругов и гражданского общества с целью повышения эффективности внешней политики России. В проведении исследований Совет опирается на широкую сеть российских и зарубежных экспертов, в которую входит порядка 1000 ведущих специалистов по международной политике и мировой экономике, а также по отдельным странам и регионам.

Президент РСМД, член-корреспондент РАН Игорь Иванов занимал пост министра иностранных дел РФ в 1998–2004 гг. и секретаря Совета Безопасности РФ в 2004–2007 гг. Генеральный директор Совета — Иван Тимофеев. Научным руководителем Совета является Андрей Кортунов.

УЧРЕДИТЕЛИ

Министерство иностранных дел Российской Федерации

Министерство образования и науки Российской Федерации

Российская академия наук

Российский союз промышленников и предпринимателей

Информационное агентство «Интерфакс»

Высказанные в аналитической записке мнения отражают исключительно личные взгляды и исследовательские позиции авторов и могут не совпадать с точкой зрения Некоммерческого партнерства «Российский совет по международным делам».

Полный текст аналитической записки опубликован на интернет-портале НП РСМД.

Источник фото на обложке: picture alliance / Zoonar | DANKO N / Vostock Photo

Угрозы международной информационной безопасности в эпоху Индустрии 4.0

Введение

Сегодня мир вступает в новую технологическую эпоху — эпоху «четвертой промышленной революции», или Индустрии 4.0, которая по своей значимости и объему глобальных изменений за единицу времени, привнесенных в развитие человечества, по всей видимости, превзойдет все предыдущие промышленные революции вместе взятые.

Индустрия 4.0 непосредственно повлияет на темпы и масштабы производства вследствие массового внедрения цифровых технологий и систем искусственного интеллекта (ИИ), изменит структуру управления различными процессами, спровоцирует стремительный рост экономики, повлияет на международную и национальную политику.

Однако помимо очевидных преимуществ, обусловленных развитием Индустрии 4.0, новая технологическая эпоха способна не просто существенным образом видоизменить ландшафт информационных угроз, но также стимулировать формирование нового мирового порядка и повлиять на систему международной безопасности. В данной записке будет рассмотрено, какие угрозы информационной безопасности способна продуцировать Индустрия 4.0 и какие вызовы она ставит перед системой глобальной информационной безопасности.

Актуальность темы обусловлена все возрастающим внедрением более продвинутых цифровых технологий и их влиянием на жизнь общества, которая, соответственно, все больше будет подвержена новым информационным угрозам, что делает необходимым анализ данной проблематики и поиск путей противодействия новым вызовам.

Ключевые технологии и природа Индустрии 4.0

Прежде чем переходить к анализу новейших угроз, нужно разобраться, что представляет из себя сама Индустрия 4.0.

В основе четвертой промышленной революции лежит массовое внедрение новейших цифровых технологий во все сферы общественной жизни — производство, экономику, политику, здравоохранение, образование и т.д.

В качестве отличительных черт нового технологического уклада можно выделить:

1. Развитие и распространение киберфизических систем (от англ. *cyber-physical system*, или *CPS*), суть которых состоит в объединении любых физических процессов, с одной стороны, и вычислительных процессов — с другой[1].
2. Рост роли данных, интеллектуального и творческого потенциала как главных производственных ресурсов[2].
3. Рост объемов данных, вычислительной мощности и возможностей подключения[3].
4. Принципиально новые возможности и инструменты не только сбора, хранения и обработки, но и анализа данных[4].
5. Новые формы и качественно иной уровень взаимодействия между человеком и человеком, человеком и машиной, машиной и машиной, а также между человеком, машиной и определенными процессами, что

ОБ АВТОРЕ:

Себекин Сергей Александрович — кандидат исторических наук, эксперт Института актуальных международных проблем Дипломатической академии МИД России.

[1] World Economic Forum Documentary: The Fourth Industrial Revolution // YouTube.com. 2016. 18 July. URL: https://www.youtube.com/watch?v=kpW9JcWxKq0;
Чулок А. Четыре промышленные революции // Постнаука. 2021. 25 марта. URL: https://postnauka.ru/wtf/155993

[2] Индустрия 4.0 // Kaspersky.Lab ; Ведомости. URL: http://kaspersky.vedomosti.ru/industrii/industry4

[3] Baur C., Wee D. Manufacturing's next act // McKinsey & Company. 2015. June. P. 1. URL: https://www.mckinsey.com/capabilities/operations/our-insights/manufacturings-next-act

[4] Ibid.

будет достигаться благодаря инновационным датчикам, сенсорам и устройствам для взаимодействия[5].

6. Внедрение глобальных централизованных техно-экосистем, объединяющих цифровые системы, технологии и людей, которые будут взаимодействовать между собой в режиме реального времени для достижения максимальной эффективности различных процессов.

Индустрия 4.0 — закономерный продукт научно-технологического развития и результат конвергенции огромного спектра различных технологий: искусственного интеллекта, робототехники, интернета вещей, облачных вычислений, больших данных, *5G* (а в будущем *6G* и более новых поколений сетей), *3D*-печати, био- и нейро- технологий, виртуальной и дополненной реальности и т.д.[6]

Угрозы информационной безопасности, продуцируемые технологиями Индустрии 4.0

В силу своей специфики и ключевых характеристик четвертая промышленная революция способна существенным образом изменить ландшафт информационных угроз и привести к пропорциональному росту их количественных и качественных показателей.

Очевидные вызовы роста количества и качества кибер/информационных угроз будут связаны как с дальнейшим развитием интернета вещей и увеличением количества подключенных устройств, так и с расширением их функционала — превращением в «умные» девайсы со встроенными алгоритмами ИИ, внедрением датчиков для «взаимодействия» с внешним миром и т.д., что существенно увеличивает «поверхность атаки», создает новые возможности для злонамеренного воздействия и делает их не только отличными целями информационных атак, но также средствами достижения негативных эффектов в реальном мире. С развитием Индустрии 4.0 подключенными окажутся более «динамичные» роботизированные устройства (объекты, системы) с большей автономностью в своих действиях, которые могут совершать какие-либо «манипуляции» в реальном мире. Масштабы внедрения и качественные характеристики новых видов подключаемых устройств с широким функционалом будут только расти — это и роботизированные манипуляторы, беспилотные аппараты (дроны, беспилотный транспорт и т.д.), сложные промышленные системы критической инфраструктуры, и даже персональные устройства и бытовые приборы.

За счет увеличения количества подключенных устройств дальнейшее распространение и развитие получат атаки типа «отказ в обслуживании», или *DDoS*-атаки (от англ. *denial-of-service*), которые могут стать еще более мощными, изощренными и деструктивными.

Появление все новых типов подключенных «умных» устройств интернета вещей, а также стремительное увеличение их количества с новой силой поднимает вопрос о конфиденциальности персональных данных. Эти «супергаджеты» с определенным функционалом (распознавание голоса, идентификация по биометрии, ИИ-ассистент), передающие данные в облако, будут служить инструментом генерации, обработки, хранения и передачи данных — маршрута передвижения, показателей здоровья, что мы потребляем и в каких количествах, наши предпочтения и т.д. Новый функционал не просто делает возможным взлом этих устройств, но и создает новые возможности для получения несанкционированного доступа к персональной информации и ее последующего использования в злонамеренных целях и даже удаленного искажения и манипулирования ею, что может привести к негативным последствиям.

Под еще большей угрозой окажутся и объекты критической инфраструктуры. Информационная атака на промышленное предприятие способна саботировать не только его работу и парализовать производство, но и привести к остановке всех взаимосвязанных процессов

[5] Baur C., Wee D. Manufacturing's next act. P. 1; Industry 4.0: the Computerization of Manufacturing // IK4-Tekniker. 2016. 7 March. URL: https://www.tekniker.es/en/industry-4-0-the-computerization-of-manufacturing

[6] Miller J. Cybersecurity considerations for industry 4.0 // BitLyft. 2021. 21 June. URL: https://www.bitlyft.com/resources/cybersecurity-considerations-industry-40

в рамках общей производственной экосистемы и затем отразиться на экономике страны или глобальном экономическом порядке[7].

Один из основных вызовов информационной безопасности в эпоху Индустрии 4.0 связан с глобальным внедрением систем искусственного интеллекта и автоматизацией различных процессов, что подразумевает ограничение участия человека в контуре управления. Этот вызов амбивалентен и продуцирует, с одной стороны, угрозы информационно-технического характера, связанные с исключением человека из каких-либо физических процессов, а с другой — угрозы информационно-психологического характера, связанные в свою очередь с исключением человека из процесса принятия решений, что в некоторых случаях вызывает морально-этические вопросы и опасения касательно выдачи ошибочных результатов.

В будущем наибольшую тревогу, связанную с глобальной автоматизацией, вызывает возможность осуществления воздействий в отношении автономных систем и аппаратов под управлением ИИ и перехвата контроля над ними, и даже их удаленного перепрофилирования — внесения изменений в операционную систему и программу действий для организации их внештатной работы, что делает возможным создание колоссального спектра эффектов. В будущем беспилотные аппараты будут повсеместно внедряться во все сферы человеческой жизни — в качестве личного транспорта, производственные, логистические и прочие процессы. Выход из-под контроля автоматизированного устройства способен не просто саботировать работу целых отраслей, но и приводить к физическим разрушениям окружающей инфраструктуры и даже угрозе здоровью и жизни людей.

Особую опасность в этом плане представляют боевые автономные системы. Возможность перехвата контроля над ними вызывает серьезные опасения и может привести к выводу их из строя и нивелированию текущих оперативных преимуществ, или же к их совершенно неизбирательному применению в отношении как комбатантов, так и гражданских лиц, объектов гражданской инфраструктуры, что может привести к ужасным последствиям, гибели людей, огромному материально-экономическому ущербу и т.д.

ИИ внедряется и в более чувствительные процессы, такие как принятие решений на основе анализа данных. Подключение систем ИИ к принятию решений в полном смысле никак нельзя назвать исключением человека из этого процесса, являющегося сугубо когнитивным[8]. Здесь снова возникают риски с его возможным удаленным перепрофилированием, что чревато последующим искаженным анализом данных и генерацией ошибочных и даже опасных решений в таких областях, как анализ стратегической ситуации и ускорение разработки стратегий для реализации военно-политических задач.

Также ИИ может использоваться для осуществления особо изощренных и сложных кибератак на объекты информационно-коммуникационных технологий[9]. Спектр применения технологий ИИ для организации кибератак очень широк:

1. масштабирование кибератак — многократное увеличение их мощности, скорости и объемов, а также продолжительности воздействия[10];
2. повышение автономности кибератак и усиление вредоносного ПО, что значительно сократит участие человека в управлении и организации на определенных этапах вторжения[11];
3. поиск уязвимостей, анализ целевой среды, получение данных о структуре систем (сетей), выбор метода проникновения, адаптация под параметры атакуемой системы

[7] Хантимиров Р. Индустрия 4.0: цифровые уязвимости новой промышленной революции // Tproger. 28/06.2021. URL: https://tproger.ru/articles/industrija-4-0-cifrovye-ujazvimosti-novoj-promyshlennoj-revoljucii/

[8] Помимо этого, полное исключение человека является нецелесообразным в силу необходимости морально-этической легитимации принимаемых ИИ решений.

[9] Здесь и далее в этом разделе мы будем использовать слово «кибер», так как оно, на наш взгляд, лучше отражает характер описываемых воздействий.

[10] AI-powered cyber-attacks: It's not a fair game // DarkTrace. 2022. URL: https://www.darktrace.com/en/supercharged-ai/; Guembe B. (et al.) The Emerging Threat of Ai-driven Cyber Attacks: A Review // Applied Artificial Intelligence. An International Journal. 2022. Vol. 36. Issue 1. P. 77, 94, 95, 105. URL: https://www.tandfonline.com/doi/pdf/10.1080/08839514.2022.2037254

[11] The Next Paradigm Shift: AI-Driven Cyber-Attacks. DarkTrace. DarkTrace Research White Paper. 2021. 6 p.; Zouave E. (et al.) Artificially intelligent cyberattacks // Totalförsvarets forskningsinstitut FOI. 2020. URL: https://www.statsvet.uu.se/digitalAssets/769/c_769530-l_3-k_rapport-foi-vt20.pdf

и самостоятельный выбор наиболее оптимального метода воздействия с целью оказания большего негативного эффекта[12];

4. превращение кибератак в «невидимые» для обнаружения («маскировка» вредоносной активности)[13];
5. осуществление более точечных кибератак — вредоносное ПО сможет поражать лишь конкретные цели, не вызывая непропорциональных и ненужных эффектов. Более того, возможно использование анализа больших данных с целью адаптации кибератаки к конкретной цели (например, организации, производству, системе и т.д.). Это же касается и фишинга — с применением ИИ злоумышленники смогут генерировать персонализированные текстовые сообщения для конкретных лиц[14];
6. повышение эффективности и разрушительности *DDoS*-атак — они станут мощнее, быстрее, повысится как временная продолжительность воздействия, так и количество зараженных устройств. ИИ будет более эффективно распространять вредоносное ПО и создавать бот-сети, сокращая участие человека в этом процессе[15];
7. «прогнозирование» степени успеха кибератаки на основе анализа больших данных и всех известных случаев вредоносного воздействия[16];
8. составление успешной стратегии кибератаки;
9. быстрый подбор паролей, подмена сигнатур, автоматическое создание эксплойтов и т.д.[17]

Таким образом, ИИ способен создавать совершенно новое, сложное по своим характеристикам кибероружие нового поколения. Кибератаки с задействованным в них ИИ способны привести к очень серьезным последствиям. Они будут обладать гораздо большей степенью «инвазивности», точности, смогут вызывать лишь необходимые эффекты или же целый каскад эффектов, надолго парализовать работу ведомства или предприятия, скрытно находясь в системе и осуществляя длительное воздействие, приводя к систематическим сбоям в работе. Все это потребует кардинального пересмотра стратегий кибербезопасности и задействованию технологий ИИ в кибероборонe. Решения по обеспечению кибербезопасности на основе ИИ будут сканировать системы на наличие уязвимостей и автоматически генерировать исправления («заплатки»), молниеносно адаптироваться под изменяющиеся угрозы, анализировать вредоносные сигнатуры и т.д. В связи с этим нас, возможно, ждет сдвиг всей парадигмы кибербезопасности. ИИ будет использован как в кибероборонительных, так и кибернаступательных целях, и мы увидим, как кибератака под управлением ИИ пытается преодолеть кибероборону ИИ.

Кроме того, в условиях информационной войны ИИ будет применяться в целях информационно-психологического воздействия на массовое сознание, манипулирования общественным мнением, эффективного распространения пропаганды и т.д., что может привести к подрыву международной информационно-психологической стабильности[18]. Уже сегодня создаются конкретные технологии воздействия с применением ИИ в отношении как отдельных индивидуумов, так и общественных процессов и социальных групп.

[12] Guembe B. (et al.) The Emerging Threat of Ai-driven Cyber Attacks. P. 77, 78, 95, 101-103, 105; Dixon W., Eagan N. 3 ways AI will change the nature of cyber attacks // World Economic Forum. 2019. 19 June.
URL: https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/

[13] Интеллектуальное вредоносное ПО с алгоритмами машинного обучения по мере накопления опыта сможет обходить системы безопасности (самый простой пример — обход спам-фильтров) и выдавать злонамеренную деятельность за штатную работу системы. См.: The Next Paradigm Shift: AI-Driven Cyber-Attacks. DarkTrace; AI-powered cyber-attacks: It's not a fair game; Guembe B. (et al.) The Emerging Threat of Ai-driven Cyber Attacks. P. 77, 78, 94-95, 105.

[14] Goldman S. Crippling AI cyberattacks are inevitable: 4 ways companies can prepare // VentureBeat. 2022. 16 May.
URL: https://venturebeat.com/2022/05/16/crippling-ai-cyberattacks-are-inevitable-4-ways-companies-can-prepare/

[15] Zouave E. (et al.) Artificially intelligent cyberattacks // Totalförsvarets forskningsinstitut FOI. 2020.
URL: https://www.statsvet.uu.se/digitalAssets/769/c_769530-l_3-k_rapport-foi-vt20.pdf

[16] Dheap V. AI in cybersecurity: A balancing force or a disruptor? // RSA Conference. 2017.
URL: https://www.rsaconference.com/industry-topics/presentation/ai-in-cybersecurity-a-balancing-force-or-a-disruptor

[17] Guembe B. (et al.) The Emerging Threat of Ai-driven Cyber Attacks. P. 94; Zouave E. (et al.) Artificially intelligent cyberattacks. P. 21.
URL: https://www.statsvet.uu.se/digitalAssets/769/c_769530-l_3-k_rapport-foi-vt20.pdf

[18] Bazarkina D. Yu., Pashentsev E.N. Artificial Intelligence and New Threats to International Psychological Security // Russia in Global Affairs. 2019. No. 1. URL: https://eng.globalaffairs.ru/articles/artificial-intelligence-and-new-threats-to-international-psychological-security; Pashentsev E. Experts on the Malicious Use of Artificial Intelligence and Challenges to International Psychological Security. Edition of the International Center for Social and Political Studies and Consulting. Moscow: LLC «SAM Polygraphist», 2021. 62 p.

Перечислим некоторые из них.

1. Технология дипфейков (от англ. *deepfake*) на основе искусственного интеллекта (включая алгоритмы машинного обучения) посредством синтеза изображения и голоса конкретного человека позволяет создавать фейковые видео якобы с его участием[19]. По мере совершенствования и улучшения качества эта технология будет получать все большее распространение и может применяться в целях дестабилизации общественно-политической ситуации, стать угрозой национальной безопасности и даже привести к конфликтам[20].
2. Целевое автоматизированное профилирование — составление психологических портретов и классификация целевых интернет-пользователей на основе анализа открытых данных социальных сетей, интернет-ресурсов, поисковых запросов и т.д., что позволит выявлять их психологические особенности и даже прогнозировать будущие психологические состояния с целью последующего оказания необходимого воздействия и мотивирования их к осуществлению определенных действий[21].
3. Распространение с помощью чат-ботов деструктивной информации среди широкой аудитории с целью политической пропаганды, популяризации экстремистских идей, ценностных установок и т.д. Используя технологии машинного обучения, продвинутые ИИ-боты могут обучаться в человеческой среде, а затем имитировать людей (и даже конкретных лиц) и использовать изощренные приемы психологической обработки с целью манипуляции как личным, так и общественным мнением и сознанием[22]. Более того, в будущем это будут *3D*-чат-боты с человеческой внешностью и синтезированным голосом, что лишь усилит эффект убеждения[23].
4. Прогнозирование будущих событий на основе анализа больших данных — экономических показателей, климатических изменений, возможных вспышек и волн эпидемий, распространения лесных пожаров и т.д.[24] Результаты прогнозов могут быть не только полезны, но и использованы в злонамеренных целях для дестабилизации общественно-политической и экономической ситуации.
5. Применение технологии «отравленных данных»[25] в целях информационно-психологического воздействия. Так, «отравлению» вполне могут подвергнуться ИИ-чат-боты с целью последующего их использования для продвижения деструктивной информации.

Информационные угрозы в эпоху Индустрии 4.0

Сама по себе Индустрия 4.0 и продуцируемые ею информационные угрозы способны спровоцировать серьезные сдвиги во всей существующей[26] системе МИБ. Мы вступаем в новую эру угроз информационной безопасности, которые будут способны вызывать более масштабные последствия, и ставить под угрозу не только национальную, но и международную безопасность.

В условиях глобальной технологической и экономической взаимосвязанности мы можем наблюдать «эффект кибербабочки» — информационная атака в отношении како-

[19] Bazarkina D. Yu., Pashentsev E.N. Artificial Intelligence and New Threats to International Psychological Security // Russia in Global Affairs. 2019. No. 1; Пашенцев Е.Н. Искусственный интеллект и безопасность: что во благо, а что во зло? : интервью / вел Моисеев А. / Международная жизнь. 21.10.2019. URL: https://interaffairs.ru/news/show/24219

[20] Helmus T.C. Artificial Intelligence, Deepfakes, and Disinformation: A Primer. Rand Corporation. 2022. July. P. 6. URL: https://www.rand.org/pubs/perspectives/PEA1043-1.html

[21] Bilal M. (et al.) Social Profiling: A Review, Taxonomy, and Challenges // Cyberpsychology, Behavior and Social Networking. Vol. 22. Issue 7. Pp. 433-450. DOI: 10.1089/cyber.2018.0670; Brundage M. (et al.) The malicious use of artificial intelligence: forecasting, prevention, and mitigation // Oxford: Future of Humanity Institute.

[22] Woolley S.C., Howard P.N. Political Communication, Computational Propaganda, and Autonomous Agents // International Journal of Communication. 2016. No. 10. P. 4885. URL: https://ijoc.org/index.php/ijoc/article/view/6298

[23] Bazarkina D. Yu., Pashentsev E.N. Malicious Use of Artificial Intelligence // Russia in Global Affairs. 2020. No. 4. URL: https://eng.globalaffairs.ru/articles/malicious-use-ai/#

[24] Bazarkina D. Yu., Pashentsev E.N. Artificial Intelligence and New Threats to International Psychological Security; Пашенцев Е.Н. Искусственный интеллект и безопасность: что во благо, а что во зло? : интервью / вел Моисеев А. / Международная жизнь. 21 октября. 2019. URL: https://interaffairs.ru/news/show/24219

[25] «Отравление данных» — технология, при которой алгоритм обучается на ошибочных или деструктивных данных (иногда заведомо), что сказывается на его работе и чревато неправильным анализом поступающей информации с последующей генерацией искаженных результатов.

[26] См. подробнее: Мартиросян А.Ж. Формирование системы обеспечения безопасности киберпространства: монография / отв. ред. И.О. Анисимов / Дипломатическая академия МИД России. Москва: Проспект, 2022. 120 с.

го-либо объекта (тем более критической инфраструктуры) может парализовать не только его работу, но и привести к более глобальным последствиям — политической и социальной нестабильности, экономическому коллапсу, экологической катастрофе и даже межгосударственным конфликтам и т.д.

Новые технологии несут в себе глобальные вызовы и для международной информационно-психологической безопасности. Все вышеописанные ИИ-технологии могут применятся в рамках информационных войн и в целом будут использоваться для формирования определенной повестки дня (в первую очередь — политической) в интересах тех или иных акторов. Отдельным лицам, индивидам, группам и даже обществам могут быть навязаны какая-либо информация или определенные представления о текущей ситуации в политике, экономике, состоянии экологии и т.д. Этого можно добиться с помощью запрограммированной в соответствии с определенными идеологическими, политическими и прочими ценностными установками армии ИИ-чат-ботов, которая будет массово продвигать определенную повестку в общественное сознание в соцсетях. Дипфейки могут повлиять на результаты выборов, усугубить межнациональные разногласия, снизить доверие к действующим международным и национальным институтам, медиа, СМИ и т.д. ИИ-алгоритмы также смогут интеллектуально настраивать пользовательский контент в различных приложениях, социальных сетях и т.д. В глобальном масштабе алгоритмы, настраивающие контент под конкретные целевые аудитории, могут усиливать нарастающую поляризацию в обществе, убеждая группы в правоте своих убеждений и существенно снижая таким образом уровень критического мышления в целом.

ИИ на основе обработки и анализа огромных массивов данных о прошлых и текущих состояниях какой-либо сферы в конкретных государствах и регионах может применяться для прогнозирования ситуации, выявления рисков и целенаправленного моделирования негативных сценариев развития государств в таких областях, как медицина, экология, экономическое развитие, уровень образования, безопасность и т.д. Например, ИИ может применяться для анализа и обработки огромного массива информации о состоянии здоровья населения (на основе открытых или похищенных персональных данных пациентов), уровне смертности, распространенных заболеваниях, размерах финансирования сферы и ее приоритетности, наличия медицинской инфраструктуры и т.д., и последующего прогнозирования состояния здоровья населения, выявления рисков и даже моделирования факторов, способствующих неблагоприятному развитию сферы, что может негативно повлиять на психологическую стабильность всего общества. Аналогичным образом ИИ может проанализировать текущее состояние экологии на определенной территории и смоделировать варианты ухудшения окружающей среды, что может сказаться на различных отраслях экономики и инвестиционной привлекательности (например, в сфере туризма демографии, общих вопросах перспективного развития территорий и т.д.). Прогнозирование с помощью ИИ негативных сценариев в экономике (например, потенциального экономического кризиса) также может сказаться на инвестиционной привлекательности конкретных отраслей, территорий и государств, и привести к снижению экономического роста. Преднамеренное использование этих данных в злонамеренных целях может способствовать неблагоприятному развитию ситуации, привести к психологической дестабилизации общества и в условиях наличия реальных проблем даже стимулировать развитие целенаправленных внешних и внутренних угроз.

Существенно повышаются возможности того, что технологии Индустрии 4.0 будут использоваться для решения военно-политических задач. Международное сообщество давно ведет обсуждение вопроса о недопущении эскалации кибер/информационных конфликтов и их перехода к реальной конфронтации с применением традиционных вооруженных сил, и стремится снизить влияние информационных угроз как эскалационного фактора в международной и межгосударственной политике[27].

[27] Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии. М.: ИМЭМО РАН, 2020. С. 12;
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности : Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года [по докладу Первого комитета (A/73/505)] 73/27 / Генеральная Ассамблея ООН: Семьдесят третья сессия. Пункт 96 повестки дня. 11.12.2018. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement/

Тем не менее информационные угрозы Индустрии 4.0 существенно усиливают эти риски. Информационные атаки потенциально могут привести к таким последствиям, которые достигнут уровня прямого вооруженного нападения и повлекут за собой ответ с применением традиционных вооруженных сил, и тогда конфликт способен «выйти» за пределы противоборства в кибер/информационном пространстве и перейти в традиционную область военных действий.

Мощнейшим фактором, который усиливает риски эскалации, является внедрение и применение смертоносных автономных систем и увеличение вероятности осуществления в отношении них информационных атак. Например, во время боевых действий с применением смертоносных автономных систем контроль над некоторыми из них может быть перехвачен третьими лицами, что может привести к сильнейшей эскалации, так как повлечет за собой прямые обвинения одной из противоборствующих сторон, чьи системы были перехвачены, в нарушении правил ведения войны.

Помимо этого, технологии и информационные угрозы Индустрии 4.0 ставят на повестку дня множество вопросов перед существующим «традиционным» международным правом, которое было сформировано в «доинформационную индустриальную» эпоху, когда решающим фактором достижения военно-политических задач и влияния на стратегическую обстановку были обычные вооружения, и поэтому оно довольно плохо адаптировано для урегулирования вопросов, связанных с информационными угрозами Индустрии 4.0.

Так, много неординарных правовых вопросов возникает в связи с возможностью осуществления кибератак в отношении боевых автономных систем и перехвата над ними контроля. Как одной из сторон, чьи машины были взломаны, доказать свою невиновность? Как приписать ответственность за эти действия какому-либо актору? Будут ли в таком случае нести ответственность производители боевых систем и программного обеспечения по статье «несоблюдение правил безопасности при производстве»? Являются ли в таком случае взломщики полноправными участниками боевых действий?

Напомним, что атрибуция — один из серьезных камней преткновения в современном праве, когда на международном уровне очень трудно доказать причастность кого-либо к совершению кибератаки. Также отсутствует единая методология атрибуции и предоставления исчерпывающей доказательной базы международному сообществу, что усложняет возможность доказательства причастности третьих лиц к вмешательству в боевые системы. Пока международное право не готово полноценно ответить на эти вопросы. На настоящий момент международно-правовая атрибуция носит спекулятивно-субъективный характер и может быть использована для решения собственных политических задач или в качестве инструмента информационной войны для подрыва имиджа стратегического соперника[28].

Международное право довольно плохо адаптировано для решения проблемы отнесения информационных воздействий к акту агрессии — как информационно-технического, так и информационно-психологического характера, и на сегодняшний день до сих пор не выработано адекватных критериев квалифицирования.

Множество вопросов вызовет и квалифицирование в качестве акта агрессии воздействий информационно-психологического характера с применением технологий ИИ. Подобные воздействия носят амбивалентную природу, связанную, с одной стороны, с характером воздействия, который является информационно-психологическим, с другой стороны — с инструментом воздействия — то есть ИИ, полноценное применение которого можно ожидать в перспективе, и ни одна из составляющих этого сложносоставного воздействия в полной мере не попадает в поле регулирования международного права с точки зрения их квалифицирования как акта агрессии. Определение психологического воздействия с применением ИИ как акта агрессии осложняется тем фактом, что эффект от него невозможно измерить.

[28] Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии. М.: ИМЭМО РАН, 2020. С. 86.

Представляется, что главнейшим критерием, по которому информационные атаки будут квалифицироваться как акт агрессии и таким образом приравниваться к применению силы — произведенные типы эффектов и последствий от таких воздействий, при оказании которых они могут быть равносильны вооруженному нападению.

Более того, систему глобальной информационной безопасности могут ждать и некоторые «институциональные» изменения. Так, обсуждение вопросов обеспечения международной информационной безопасности в рамках ООН очень долгое время было прерогативой лишь национальных государств. С 2018 г. по инициативе России в рамках ООН функционирует Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (РГОС ООН), которая предусматривает включение в процесс обсуждения профильного вопроса мультистейкхолдеров, в том числе представителей частного сектора. Более того, сегодня компании самостоятельно инициируют разработку и продвижение своих собственных глобальных проектов в сфере обеспечения международной информационной безопасности, так как они сами и их клиенты страдают от кибератак. Именно частный сектор управляет львиной долей всей важнейшей мировой информационной инфраструктуры, а также производит контент, программное и аппаратное обеспечение, и именно он — главнейший драйвер развития ключевых технологий Индустрии 4.0 (систем искусственного интеллекта, автономных аппаратов, сетей нового поколения, облачных вычислений, интернета вещей, виртуальной и дополненной реальности и т.д.). В связи с этим можно предположить, что с развитием Индустрии 4.0 и эволюции ландшафта киберугроз на повестке дня неизбежно встанет вопрос об увеличении роли частного сектора в обсуждении вопросов международной информационной безопасности в рамках ООН.

Наконец, трансформации, которые могут происходить в системе глобальной информационной безопасности, в целом связаны не только с качественно новыми и перспективными информационными угрозами, но и со складывающейся стратегической и политической ситуацией на мировой арене.

Представляется, что наиболее отягчающие обстоятельства связаны с тем, что качественная эволюция и изменение ландшафта информационных угроз будет происходить, как показывает опыт и текущая ситуация, параллельно если не с деградацией, то возможной будущей фрагментацией глобальной системы обеспечения международной информационной безопасности.

Переговорный процесс в ООН, скорее всего, продолжится, но он может замедлиться. В свете этого необходимо помнить, что невозможность координировать свои усилия под эгидой ООН ставит под угрозу становление всеобщей системы глобальной информационной безопасности. Вопрос установления общепризнанных универсальных правил ответственного поведения в информационном пространстве вновь рискует быть отложенным на годы вперед, что в условиях эволюции информационных угроз в эпоху Индустрии 4.0 чревато печальными последствиями.

Противодействие деградации МИБ

Международному сообществу необходимо решить ряд проблем, которые усиливают риски и тормозят процесс эффективного противодействия информационным угрозам в новую эпоху. Эти проблемы связаны как с самой Индустрией 4.0, так и со складывающейся на сегодняшний день стратегической ситуацией. Обеспечение МИБ в условиях «форсированных» угроз Индустрии 4.0 потребует еще более тесной координации международных усилий.

Помимо действующих переговорных форматов под эгидой ООН может быть создан специальный международный орган по расследованию киберинцидентов. При этом механизмы работы подобного органа могут включать в себя сбор всей доказательной базы и необходимых данных в интересах расследования, анализ стратегической обстановки и т.д. Важно, чтобы государства предоставляли исчерпывающий пакет доказательств виновности предполагаемого нарушителя вместе с унифицированной методологией проведения атрибуции.

В юрисдикцию данного органа также может входить оценка ущерба, причиненного ин-

формационным воздействием, квалифицирование конкретного воздействия как акта агрессии, независимое и беспристрастное определение пропорциональных издержек, которые могут налагаться на виновника и т.д. Данные механизмы международного регулирования отношений в области информационной безопасности будут призваны снизить риск лишних политических провокаций, связанных с вмешательствами, и уменьшить субъективное и одностороннее приписывание актов воздействия какому-либо субъекту (хотя, конечно, не исключат эти факторы полностью).

В адаптации к новым реалиям Индустрии 4.0 нуждается и существующее международное право. Стремительное развитие информационных технологий может видоизменить или усилить информационные угрозы — как технического, так и психологического характера — которые в будущем могут приводить к непропорциональным и гораздо более разрушительным последствиям, ранее не характерным для подобного рода воздействий. Соответственно, должны быть проработаны адекватные механизмы классификации «новых» информационных атак с точки зрения их отнесения к акту агрессии. Само понятие «акта агрессии» должно быть расширено посредством дополнительных комментариев или протоколов к Резолюции Генеральной Ассамблеи ООН 3314, и, в случае необходимости, включать в себя информационные воздействия.

Один из ключевых вопросов, который на данный момент остается открытым, состоит в том, в какой степени привлекать частный сектор к обсуждению вопросов международной информационной безопасности, так как именно он — главный драйвер развития технологий Индустрии 4.0. В этом плане представляется, что ограничение участия ключевых *IT*-компаний может существенно снизить эффективность диалога в будущем в контексте развития информационных угроз новой эпохи. Поэтому в перспективе странам все же придется согласовать модальности и разработать более эффективные механизмы и форматы привлечения частного сектора к переговорному процессу по вопросу обеспечения МИБ. Однако важно соблюсти баланс между привлечением частного сектора к обсуждению вопросов международной информационной безопасности и ключевой ролью государств в этом процессе.

Безусловно, противодействие новейшим угрозам в эпоху Индустрии 4.0 потребует теснейшей координации между правоохранительными органами, компьютерными группами реагирования на чрезвычайные ситуации (*Computer emergency response team, CERT*) и другими уполномоченными структурами разных стран.

Выводы

Индустрия 4.0 открывает эру высокотехнологичных информационных атак, которые будут способны не просто вызывать гораздо более масштабные и разрушительные последствия в отношении непосредственных объектов воздействия, но и продуцировать экзистенциальные вызовы системе международной информационной безопасности. Новая эпоха потребует гораздо более системных, скоординированных и институциональных мер противодействия форсированным угрозам.

Вместе с тем поиск ответов на новейшие вызовы будет существенно осложняться складывающейся политической обстановкой, которая еще долго будет определять характер взаимодействия между соперничающими государственными и негосударственными субъектами. Таким образом, диалог по вопросу обеспечения МИБ неизбежно находится в заложниках у политических разногласий. В этих условиях государствам будет трудно сотрудничать в сфере определения методологии и предоставления необходимых данных о произошедших инцидентах, привлекать представителей частного сектора из «недружественных» стран к обсуждению вопросов МИБ и т.д.

Однако переговорный процесс по вопросу обеспечения МИБ не должен быть заморожен и фрагментирован. Государства должны иметь определенные инструменты координации по особо острым вопросам. Учитывая взаимосвязанность технологий и процессов в эпоху Индустрии 4.0, в условиях фрагментации усилий процесс обеспечения международной информационной безопасности может находится под угрозой.

Для заметок

Для заметок

Для заметок

Тел.: +7 (495) 225 6283
Факс: +7 (495) 225 6284
welcome@russiancouncil.ru

119049, Москва,
4-й Добрынинский переулок, дом 8

russiancouncil.ru