Балановский В.Л., Подъяконов В.М., Алборова М.Б. Вызовы и риски современного мира в цифровой среде // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 6(32) с. 75–79

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

ВЫЗОВЫ И РИСКИ СОВРЕМЕННОГО МИРА В ЦИФРОВОЙ СРЕДЕ

[1]Балановский В.Л., [2]Подъяконов В.М., [3]Алборова М.Б.
[1]Академия военных наук, Москва, Россия (119330 Москва, Университетский пр., 14)
[2]Военный университет МО РФ, Москва, Россия (125047 Москва, Большая Садовая ул., 14)
[3]Центр Международной информационной безопасности МГИМО МИД России, Москва, Россия (119454, г.Москва, просп. Вернадского, 76, корп. В.), e-mail: alborova2205@mail.ru

В статье рассматриваются основные возможности и риски информационного общества, обусловленные вхождением в постиндустриальный технологический уклад, цифровизацией, техно-гуманитарным дисбалансом и некоторыми другими феноменами цифровой эпохи.

Ключевые слова: Цифровая эпоха, информационное общество, постиндустриальный технологический уклад, искусственный интеллект, цифровизация, вызовы цифровой эпохи.

CHALLENGES AND RISKS OF THE MODERN WORLD IN THE DIGITAL ENVIRONMENT

[1]Balanovsky V.L., [2]Podyakonov V.M., [3]Alborova M.B.
[1]Academy of Military Sciences, Moscow, Russia (119330 Moscow, Universitates pr., 14)
[2]Military University of the Ministry of Defense of the Russian Federation, Moscow, Russia (125047 Moscow, Bolshaya Sadovaya st., 14)
[3]Center for International Information Security, MGIMO, Ministry of Foreign Affairs of Russia, Moscow, Russia (119454, Moscow, Prospekt Vernadskogo, 76, building V), e-mail: alborova2205@mail.ru

The article examines the main opportunities and risks of the information society caused by the entry into the post-industrial technological order, digitalization, techno-humanitarian imbalance and some other phenomena of the digital age.

Keywords: digital age, information society, post-industrial technological structure, artificial intelligence, digitalization, challenges of the digital age.

Цифровая цивилизация формируется стремительно и становится драйвером для развития инновационных технологий, имеющих как положительные, так и отрицательные стороны. Скорость, многоспекторность и масштабность изменений, которые влияют на жизнь современного общества имеют беспрецедентный характер и требуют высокого уровня анализа текущих явлений для понимания как их значимости, так и рисков.

Человечество все больше погружается в новый технологический мир цифровизации, нано, био и когно технологий, плотно взаимодействующих с передовыми ИКТ. В этих условиях Интернет сеть стала основной информационной инфраструктурой, связав многие процессы в единое глобальное пространство. Количество интернет-пользователей растет

ежегодно, в 2023 г., согласно отчёту Global Digital 2023, уже насчитывает 5, 16 миллиарда,[1] а это значит, что более 60 % населения земли является пользователями Интернета. Обостряется борьба за лидерство в управлении этим стратегическим ресурсом.

Технологическая сила государств на современном этапе во многом определяется наличием у него своей собственной комплексной инфраструктуры, базой данных (хранение информации), суперкомпьютеров (обработка данных), а также корневых серверов и доступа к широкополосному Интернету (передача информации). Не маловажную роль имеет и полноценная система подготовки и переподготовки кадров, способных не только успешно работать с уже созданными технологиями, но и быстро и творчески реагировать на вызовы и риски, возникающие в условиях современных противоречий и угроз информационного пространства. Динамически развивающаяся научно-технологическая составляющая является значимым фактором конкурентоспособности на международной арене и необходимым элементом обеспечения государственного суверенитета.

Мы живем в эпоху экспоненциального роста количества технологий. Наиболее успешно развиваются многочисленные приложения искусственного интеллекта для анализа больших объемов данных, создаются новые возможности для сети связи 5G, активно распространяется технология блокчейна. Технологии искусственного интеллекта открывают новые направления в области машинного обучения, эволюции вычислений планировании и так далее. Уже сегодня использование приложений ИИ выросло многократно и применяется в авиации, космосе, медицине, банковской сфере, безопасности критической инфраструктуры и др. В последние годы технологии ИИ применяются в сфере правопорядка и национальной обороны.

Развитие данной технологии позволяет сформировать качественно новые условия для экономической и социальной сферы в жизни общества. Совершенно очевидно, что государства, лидирующие в этом направлении, получают конкурентное преимущество.

В 2017 г. Президент России В.В. Путин подчеркивая значение технологии искусственного интеллекта сказал, что страна, добившаяся лидерства в данной сфере «будет властелином мира»[2], осознание роли и инновационного потенциала искусственного интеллекта требует и от Российской Федерации формирования комплекса мер как по разработке данной технологии, так и по подготовке кадров в этом направлении. Важно отметить, что у России есть качественная научная и практическая база для реализации технологии ИИ.

Инновации приводят к изменению жизни общества, трансформируя его, создавая с одной стороны уникальные возможности, с другой стороны формируя риски и потенциальные угрозы. Важно вовремя анализировать деструктивный потенциал, который заложен в инновационных технологиях и может негативно отразиться на всех сферах общественной жизни. Уже сегодня мы видим глобальные изменения в экономике, на рынке труда, все больше меняются социальные запросы, трансформируются моральные ценности. Развивающиеся социальные сети создают информационную среду, в которой с помощью инновационных технологий возможно манипулировать общественным сознанием применяя дипфейки и

[1] Цифровой 2023: глобальный обзорный отчет. https://datareportal.com/reports/digital-2023-global-overview-report (дата обращения: 08.05.2023)

[2] Открытый урок «Россия, устремленная в будущее» // 01.09.2017 URL: http://kremlin/ ru/events/president/news/55493 (дата обращения: 08.05.2023)

расставляя акценты с определенным контекстом[3]. В совокупности с этой проблемой необходимо рассматривать и вопрос информационного воздействия на подрастающее поколение. Современные технологии социального инжениринга широко используются для управления обществом.

Рассматривая широкие возможности ИИ нельзя не заострить внимание на вопросах угроз безопасности, связанных с применением подобных технологий, причем риски могут быть как технического характера (использование результатов анализа больших баз данных в преступных целях), так и социального (применение ИИ технологий очевидно меняет рынок труда, сокращаются многие профессии, растет безработица).

Нельзя не отметить и риски для национальной безопасности, которые проявляются на фоне обострения технологической конкуренции и цифрового разрыва, что в свою очередь ведет ущемлению интересов стран, не имеющих подобных технологий. Кроме того, деструктивный потенциал искусственного интеллекта может быть использован для вмешательства во внутреннюю политику стран, влияния на протестные настроения, рост агрессии и паники.

Важно отметить, что отставание в технологическом прогрессе ведет к рискам сохранения суверенности государств, их уязвимости в новом мире цифры, подобная ситуация становится новым цивилизационным вызовом, с котором столкнулось человечество в XXI веке.

В 2020 г. выступая на заседании Генассамблеи ООН, Генеральный секретарь ООН Антониу Гутерриш отметил, что новые технологии используются для преступлений, разжигания ненависти, распространения ложной информации и эксплуатации людей.[4]

Разработка и повсеместное внедрение цифровых информационных технологий проявили все три основных направления угроз: гражданское, военное и преступное. Новым фактором современных угроз для всего мирового сообщества стало использование многомерного потенциала сети Интернет и других цифровых ИКТ международными криминальными структурами. В условиях современного геополитического кризиса количество киберпреступлений увеличилось значительно, а ущерб от них для мировой экономики, по оценкам ООН в 2023 году вырастет до 10, 5 трлн долл.

Уязвимость государств становится все очевиднее. Столь масштабное, бесконтрольное применение информационно-коммуникационных технологий может быть использовано для подрыва государственной стабильности и суверенитета[5]. Риски глобального информационного пространства не имеют границ. Осознание и понимание угроз нового технологического мира должно стать основой для значительной работы международного сообщества в сфере обеспечения безопасности в условиях новой реальности.

В Концепции внешней политики Российской Федерации отмечается необходимость: «Формирования и совершенствования международно-правовых основ противодействия использованию информационно-коммуникационных технологий в преступных целях»[6].

3 Булва В.И. Феномен социальных сетей в контексте информационной безопасности / В. И. Булва // Международная жизнь. – 2023. – № 3. – С. 53.

[4] Генсек ООН назвал четыре угрожающих миру «всадника Апокалипсиса» https://ria. ru/ (дата обращения: 8.05.2023).

[5] Международная информационная безопасность: подходы России : Аналитический доклад / А. В. Крутских, Е. С. Зиновьева, В. И. Булва [и др.]. – Москва : Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, 2022. – 48 с.

6 https://www.mid.ru/ru/detail-material-page/1860586/

Важно отметить, что Россия с конца XX века принимает все необходимые меры для обеспечения национальной и международной информационной безопасности, поднимая вопрос о противодействии угрозам нового глобального цифрового мира как на международном уровне, так и на региональном и национальном. 4 декабря 1998 года по инициативе России впервые был принят Генеральной Ассамблеей ООН проект резолюции (№ 53/70) под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»[7]. С этого момента начинается официальный процесс создания международно-правового режима, регулирующего вопросы обеспечения безопасности в новом мире технологий.

Многоаспектность технологических рисков наиболее четко проявилась и в условиях кризиса 2022 года. Очевидное расширение милитаризации глобального информационного пространства становится все более активным. Увеличилось и количество кибератак на критическую информационную инфраструктуру. Сегодня многие страны стали наращивать свои военные возможности в сфере информационно-коммуникационных технологий. Страны блока НАТО открыто заявляют о возможности нанесения превентивных кибердударов по недружественным им государствам. Усиливающиеся международные противоречия создают условия для использования инновационного технологического потенциала для доминирования над развивающимися странами. Глобальное цифровое пространство все больше становится местом для межгосударственной конкуренции и конфликтов.

Российская позиция направлена на приоритет мирного развития информационного пространства, уважение государственного суверенитета, недопущение использования силы или угрозы силой в цифровой среде. На современном этапе необходимо формировать глобальную систему международной информационной безопасности, в рамках которой надо заключить на международном уровне универсальные и юридически обязывающие договоренности в информационной сфере.

Список литературы

1. Бирюков А. В., Алборова М. Б. Социально-гуманитарное измерение международной информационной безопасности. М.: Аспект Пресс, 2019.
2. Крутских А., Бирюков А. Новая геополитика международных научно-технологических отношений // Международные процессы. 2017. № 2. С. 6-26.
3. Ларина Е.С. Человеческое мышление и искусственный интеллект: российский аргумент в международном сотрудничестве // В кн. Международная информационная безопасность: новая геополитическая реальность. М.: Аспект Пресс, 2021. С. 79–85
4. Международная информационная безопасность: теория и практика: В 3 т. / Под общ. ред. А. В. Крутских. М.: Аспект Пресс, 2021.

References

1. Biryukov A.V., Alborova M. B. Social and humanitarian dimension of international information security. M.: Aspect Press, 2019.

7 Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Организация Объединенных Наций. 04.01.1999. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement

2. Krutskikh A., Biryukov A. New geopolitics of international scientific and technological relations // International processes. 2017. No. 2. pp. 6-26.
3. Larina E.S. Human thinking and artificial intelligence: the Russian argument in international cooperation // In the book. International Information Security: A New Geopolitical Reality. Moscow: Aspect Press, 2021. pp. 79-85
4. International information security: theory and practice: In 3 volumes / Under the general editorship of A.V. Krutskikh. M.: Aspect Press, 2021.