Влияние цифровизации на международную информационную безопасность и социальные риски управленческих процессов

УДК 5.4.7 DOI 10.26425/2658-347X-2025-8-2-77-86

Получено 17.05.2025 Доработано после рецензирования 11.06.2025 Принято 15.06.2025

Мкртумова Ирина Владимировна[1,2]

Д-р социол. наук, проф. каф. социологии, психологии управления и истории[1], проф. каф. политического анализа и социально-психологических процессов[2]

ORCID: 0000-0003-3106-2485

E-mail: lmkrtumova@yandex.ru

[1]*Государственный университет управления, г. Москва, Россия*

[2]*Российский экономический университет имени Г.В. Плеханова, г. Москва, Россия*

Прокопьева Сабина Сергеевна[3]

Менеджер по предоставлению премиальных сервисов

ORCID: 0009-0006-3549-9974

E-mail: sabinaprokopyeva@gmail.com

[3]*Акционерное общество «Лаборатория Касперского», г. Москва, Россия*

АННОТАЦИЯ

Рассматривается влияние цифровизации на международную информационную безопасность, анализируются новые вызовы и угрозы, возникающие в связи с расширением цифрового пространства. Авторы определяли социальные риски управленческих процессов, обусловленные цифровой трансформацией. Исследование опиралось на теорию цифровых коммуникаций М. Кастельса, определение З. Баумана текучести цифровой реальности, на идеи Ш. Забофф об управленческой подмене информационных платформ. Основными методами эмпирических исследований были обзоры литературы, вторичный анализ существующих работ по данной теме, осуществленные авторами. По итогам анализа авторы высказали предположение, что цифровизация представляет собой, с одной стороны, мощный ресурс для развития управленческих систем, но с другой стороны – источник новых угроз, прежде всего в области международной информационной безопасности и социальных рисков. Принимая во внимание трансграничный характер цифровых процессов, исследователи отмечают, что необходим комплексный подход к их регулированию, предполагающий развитие международного цифрового права; координацию усилий государств в области кибербезопасности; повышение цифровой грамотности среди управленцев; внедрение этических принципов в алгоритмическое управление. В результате были выявлены социальные риски управленческих процессов, а также определен вектор их минимизации и усиления международной кооперации и информационной безопасности в условиях цифровой экономики.

Ключевые слова

Цифровизация, информационная безопасность, управленческий процесс, социальные риски, киберугрозы, киберпространство, цифровой суверенитет, цифровая трансформация

Для цитирования

Мкртумова И.В., Прокопьева С.С. Влияние цифровизации на международную информационную безопасность и социальные риски управленческих процессов//Цифровая социология. 2025. Т. 8. № 2. С. 77–86.

Impact of digitalisation on international information security and social risks of management processes

Received 17.05.2025 Revised 11.06.2025 Accepted 15.06.2025

Irina V. Mkrtumova[1,2]

Dr. Sci. (Sociol.), Prof. at the Sociology, Psychology of Management and History Department[1], Prof. at the Political Analysis and Socio-Psychological Processes Department[2]

ORCID 0000-0003-3106-2485

E-mail: Imkrtumova@yandex.ru

[1]*State University of Management, Moscow, Russia*

[2]*Plekhanov Russian University of Economics, Moscow, Russia*

Sabina S. Prokopyeva[3]

Manager for the Provision of Premium Services

ORCID: 0009-0006-3549-9974

E-mail: sabinaprokopyeva@gmail.com

[3]*Joint-Stock Company "Kaspersky Lab", Moscow, Russia*

ABSTRACT

The article considers the impact of digitalisation on international information security, analyses new challenges and threats arising from the expansion of digital space. The authors have determined the social risks of management processes caused by digital transformation. The study is based on M. Castells' theory of digital communications, Z. Bauman's definition of the fluidity of digital reality, and Sh. Zuboff's ideas about the managerial substitution of information platforms. The main methods of empirical research are literature reviews, secondary analysis of existing works on the topic conducted by the authors of the article. Based on the results of the analysis, the authors suggest that digitalisation represents, on the one hand, a powerful resource for the development of management systems, but, on the other hand, a source of new threats, above all, in the field of international information security and social risks. Considering the cross-border nature of digital processes, a comprehensive approach to their regulation is required, which implies the development of international digital law; coordination of efforts of states in the field of cybersecurity; improvement of digital literacy among managers; introduction of ethical principles in algorithmic management. As a result, the social risks of management processes are identified, and the vector of their minimisation and strengthening international cooperation and information security in the digital economy is determined.

Keywords

Digitalisation, information security, management process, social risks, cyber threats, cyber space, digital sovereignty, digital transformation

For citation

Mkrtumova I.V., Prokopyeva S.S. (2025) Impact of digitalisation on international information security and social risks of management processes. *Digital sociology*. Vol. 8, no 2, pp. 77–86. DOI: 10.26425/2658-347X-2025-8-2-77-86

ВВЕДЕНИЕ / INTRODUCTION

Цифровизация стремительно трансформирует не только экономику и социальную сферу, но и системы государственного и корпоративного управления. На фоне глобального внедрения цифровых технологий усиливается зависимость управленческих решений от цифровой инфраструктуры, что влечет за собой рост киберугроз, цифрового неравенства и снижение прозрачности алгоритмических решений. Международный характер цифровых коммуникаций делает вопросы информационной безопасности ключевыми в повестке глобального управления.

Актуальность проблемы обусловлена тем, что при всех преимуществах цифровой трансформации ее побочные эффекты – от утечек данных до социальной поляризации – могут подорвать доверие к институтам и создать предпосылки для международных конфликтов.

Цели статьи – исследовать влияние цифровизации на международную информационную безопасность и выявить связанные с ней социальные риски в управленческой сфере.

Задачи исследования заключаются в проведении обзора современной научной и аналитической литературы по данной проблематике, а также в определении ключевых угроз, возникающих в результате цифровизации управленческих процессов. Задачей является и определение вектора минимизации рисков и усиления международной кооперации.

Структура статьи включает введение, обзор источников и методологию, анализ выявленных рисков и выводы.

МЕТОДЫ И МАТЕРИАЛЫ / METHODS AND MATERIALS

Исследование базируется на междисциплинарном подходе, сочетающем:

– PESTLE-анализ (англ. political, economic, social, technological, legal, environmental – политические, экономические, социальные, технологические, правовые, природные факторы) для оценки факторов, влияющих на управленческие риски;

– контент-анализ нормативных актов, стратегий цифровой трансформации и докладов международных организаций (ITU (англ. International Telecommunication Union – Международный союз электросвязи), WEF (англ. World Economic Forum – Всемирный экономический форум), Организация Объединенных Наций (далее – ООН);

– сравнительный анализ международных практик регулирования цифровой среды и подходов к обеспечению кибербезопасности.

Материалами исследования стали 20 источников, включая научные публикации, отчеты, аналитические записки и международные нормативные документы периода 2018–2024 гг.

Методологические основы исследования. Теория секьюритизации Б. Бузана и концепция цифрового суверенитета (англ. digital sovereignty) рассматриваются авторами статьи в качестве теоретической рамки анализа цифровых угроз как вызовов национальной безопасности[1]. Теория была разработана учеными Копенгагенской школы (Б. Бузаном, О. Уивером, Я. де Вильде) в 1990-е гг. как критика традиционных подходов к безопасности[2]. Ключевая идея Б. Бузана состоит в том, что безопасность – это не объективная данность, а результат речевого акта, когда некая угроза объявляется экзистенциальной, что оправдывает чрезвычайные меры. Ученый разделяет процесс секьюритизации на три этапа. Первый этап – выделение агентом (правительством, средствами массовой информации, экспертами) угрозы (например, кибератаки). Второй – ее признание аудиторией (обществом, международными организациями) критической. Третий – легитимация исключительных мер, к которым автор относит цензуру, санкции, милитаризацию киберпространства. Примером секьюритизации может быть закон о «суверенном интернете» (Российская Федерация (далее – РФ, Россия), 2019 г.) как ответ на «внешние угрозы»[3].

Б. Бузан выделяет такие риски, как подавление инакомыслия под видом защиты от дезинформации, гиперболизация угроз (например, TikTok как «шпионский инструмент» Китайской Народной Республики (далее – КНР, Китай). Управленческие выводы автора состоят в выделении риска подмены безопасности политическими интересами. Он предлагает в качестве решения прозрачные критерии секьюритизации (например, через независимые аудиты).

Концепция цифрового суверенитета не имеет единого основателя – концепция развивалась параллельно в Европейском союзе (далее – ЕС),

[1] Баранов Н. Тема «Теория секьюритизации в анализе политики». Режим доступа: https://www.nicbar.ru/politology/study/politicheskie-problemy-mezhdunarodnykh-otnoshenij-globalnogo-i-regionalnogo-razvitiya/tema-teoriya-sekyuritizatsii-v-analize-politiki (дата обращения: 10.05.2025).

[2] Там же.

[3] Федеральный закон от 01.05.2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон „О связи“ и Федеральный закон „Об информации, информационных технологиях и о защите информации“». Режим доступа: http://www.kremlin.ru/acts/bank/44230 (дата обращения: 10.05.2025).

Китае и Соединенных Штатах Америки (далее – США). В академических кругах существуют ссылки на исследование Л. Денардис (The global war for internet governance, 2014 г.), которая систематизировала научные дискуссии по данному вопросу [DeNardis, 2014].

Концепция цифрового суверенитета формировалась постепенно, ключевые вехи ее теоретизации и политического оформления связаны с идеями М. Кастельса, Дж.П. Барлоу, Д. Поста и других авторов. Истоки формирования концепции (1990–2000-е гг.) связаны с влиянием работы М. Кастельса о сетевом обществе, где контроль над цифровыми потоками становится аналогом территориального суверенитета [Кастельс, 2009].

Идеи киберпространства как новой сферы были предложены Дж.П. Барлоу («Декларация независимости киберпространства», 1996 г.)[4] и Д. Постом (теория киберсуверенитета, 2002 г.) [Михалевич, 2021], которые первыми подняли тему конфликта между государством и анархией интернета.

Политическое оформление произошло в 2010 г. В ЕС термин «цифровой суверенитет» впервые был официально использован в 2013 г. в докладе Европейской комиссии European Digital Agenda[5], где акцент делался на независимости от ИТ-гигантов (ИТ – информационные технологии) США. Ключевыми документами являются протокол ЕС GDPR (англ. General Data Protection Regulation – Общий регламент по защите данных) 2016 г., который осуществляет контроль над данными[6]; Gaia-X – инициатива по разработке объединенной инфраструктуры безопасных данных для Европы, представленная в 2019 г., обеспечивает инфраструктурную независимость.

ОБСУЖДЕНИЕ / DISCUSSION

Проблематика цифровизации и ее последствий для международной безопасности активно обсуждается в трудах зарубежных и отечественных исследователей. Согласно М. Кастельсу, цифровые сети становятся новой формой власти, перераспределяющей доступ к информации и влияющей на глобальные процессы [Кастельс, 2009]. З. Бауман рассматривает цифровую эпоху как пространство текучей модерности, где исчезают традиционные границы между государствами, личной и публичной сферами [Бауман, 2013].

Ш. Забофф поднимает проблему надзора и манипуляции в условиях цифрового капитализма, подчеркивая, что информационные платформы все чаще подменяют собой институты управления [Zuboff, 2019]. В работах российских авторов акцент делается на рисках автоматизации, снижении роли человека в принятии решений и росте зависимости алгоритмов [Греков, 2021; Вяткин, 2020].

Э.М. Альшами, Ф.М. Алотаиби и М. Карипиду в статье «Цифровая трансформация и проблемы кибербезопасности в эпоху глобализации» анализируют проблемы кибербезопасности в условиях глобализации и цифровой трансформации [Альшами, Алотаиби, Карипиду, 2022]. Авторы отмечают, что рост взаимосвязи стран через цифровые сети увеличивает уязвимость государственных и экономических систем перед внешними угрозами. Особое внимание уделено вопросам межгосударственного сотрудничества, стандартизации протоколов безопасности и необходимости создания стандартного правового поля для противодействия киберпреступности. Статья содержит сравнительный анализ ситуации в разных регионах мира и предлагает стратегические рекомендации по обеспечению устойчивости. Анализируются риски для государственных систем, экономики и общества, а также предлагаются стратегии межгосударственного сотрудничества в рамках расширения пространства.

А. Петров, Д. Иванов в 2023 г. исследовали влияние цифровых технологий на национальную и международную безопасность, на экономику и развитие систем безопасности [Петров, Иванов, 2023]. Они выделили проблемы расширения суверенитета, гибридных угроз и необходимости многостороннего регулирования киберпространства. Авторы рассматривают влияние цифровых технологий на безопасность как на суше, так и на море. Анализируется эволюция угроз, начиная от классического шпионажа и заканчивая гибридными формами воздействия, включая дезинформацию и кибератаки на критическую инфраструктуру. В работе подчеркивается необходимость разработки многих аспектов обеспечения безопасности в киберпространстве. Также рассматриваются вопросы этики и ответственности при использовании искусственного интеллекта (далее – ИИ) и больших данных.

Социальные риски цифровой трансформации – дезинформацию и поляризацию в онлайн-пространстве – изучали Б. Мартенс и К.Д. Рааб [Мартенс, Рааб, 2021]. Авторы осуществили анализ социальных рисков цифровых трансформаций,

[4] Barlow J.P. A Declaration of the Independence of Cyberspace. Режим доступа: https://www.eff.org/cyberspace-independence (дата обращения: 10.05.2025).

[5] European Parliament. Digital Agenda for Europe. Режим доступа: https://www.europarl.europa.eu/ftu/pdf/en/FTU_2.4.3.pdf (дата обращения: 11.05.2025).

[6] European Union. General data protection regulation (GDPR). Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:310401_2 (дата обращения: 11.05.2025).

включая распространение дезинформации, поляризацию мнений и возникновение информационных пузырей. Ученые рассматривают влияние алгоритмических платформ на демократические процессы и общественную стабильность. Исследованы такие социальные последствия цифровизации, как распространение дезинформации и общественная поляризация. Авторы представляют алгоритмы социальных сетей, обеспечивающие формирование информационных пузырей, где пользователи сталкиваются только с мнениями, совпадающими со своими собственными представлениями. Это приводит к снижению толерантности к иным мнениям, радикализации и утрате доверия к институту демократии. Предлагаются пути решения проблем: регулирование контента, повышение цифровой грамотности, развитие медиаобразования.

Недавнее исследование Р. Сингх и Н. Патель было посвящено проблемам кибербезопасности и социальной уязвимости в эпоху цифровизации [Сингх, Патель, 2024]. Работа сосредоточена на пересечении кибербезопасности и социальной уязвимости. Авторы рассматривают, как цифровизация связана с различными заболеваниями, особенно в странах Африки. Обсуждаются психологические и социальные последствия цифровых технологий, включая тревожные расстройства, обусловленные личной автономией и снижением уровня доверия к государственным и корпоративным структурам. Предлагаются стратегии повышения цифровой устойчивости общества.

Цифровые технологии, несомненно, являются мощным катализатором трансформации управления на всех уровнях. Постоянно наблюдаются создание новых форм взаимодействия между государственными, экономическими и социальными институтами, повышение скорости принятия решений и в определенной степени рост их прозрачности за счет внедрения цифровых платформ.

Исследователи изучают масштабные цифровые инновации в сфере платформизации финансовой и предпринимательской деятельности, которые трансформируют ежедневные практики институтов государственного управления, крупных экономических и промышленных гигантов, компаний цифровой индустрии [Мкртумова, Ашкар, Чижов, Янчук, 2025]. Авторы выявили и описали некоторые важные социальные результаты создания и развития новых цифровых мегаплатформ, таких как портал «Госуслуги». Так, государственная информационная платформа аккумулировала запросы россиян на предоставление большинства социальных услуг. Столичная мегаплатформа «Мос.ру» внедрила принцип «одного окна» для москвичей. Гигант банковской сферы «Сбер» создал и выстроил собственную метаплатформу вокруг потребностей людей в финансах, банковском обслуживании, бизнесе, страховании, электронной коммерции, а также в продуктах, доставке еды, лекарственных средствах, транспорте и др. У ресурса работает свой GigaChat2 и многочисленные платформенные решения.

Однако стоит отметить и обратную сторону медали. Автоматизация процессов и все большее использование платформенных решений ведут к постепенной замене традиционных форм человеческого участия в управлении. Это, в свою очередь, порождает снижение контроля за принятием решений, особенно в отношении алгоритмических процессов, и увеличивает общественное недоверие к «черному ящику» алгоритмов [Мкртумова, 2023]. Необходимы механизмы, обеспечивающие прозрачность и подотчетность алгоритмических систем, а также инструменты для контроля и корректировки их работы со стороны человека.

Ученые Института статистических исследований и экономики знаний Национального исследовательского университета «Высшая школа экономики» (далее – НИУ ВШЭ) в 2025 г. проанализировали тенденции цифровизации государственных услуг (далее – госуслуги) населению по итогам прошлого года[7]. Взаимодействие граждан и государства все заметнее переходит в цифровую плоскость. Так, только 13 % россиян не заходят в интернет для получения госуслуг, а 86,7 % в 2024 г. полностью или частично получили государственные и муниципальные услуги онлайн. Ученые НИУ ВШЭ установили, что пользователи заходят на электронные порталы («Госуслуги») чаще всего за нужной информацией (77,6 %) и результатами предоставления услуг (47,1 %), для осуществления обязательных платежей (54 %), получения или отправки документов (40,3 %). Каждый второй пользователь госуслуг (55 %) получает их исключительно онлайн.

Международные организации, такие как ITU [International Telecommunication Union, 2023], WEF[8] и UNDP (англ. United Nations Development Programme – Программа развития ООН), указывают на необходимость создания глобальных

[7] Национальный исследовательский университет «Высшая школа экономики». Цифровизация государственных услуг. Режим доступа: https://issek.hse.ru/news/1039474722.html (дата обращения: 12.05.2025).

[8] World Economic Forum. The global risks report 2024. 19th edition. Insight report. Режим доступа: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (дата обращения: 12.05.2025).

механизмов регулирования киберпространства и цифрового сотрудничества. Так, в новом «Докладе о человеческом развитии на 2025 г.», опубликованном ООН, показано, как ИИ может ускорить развитие[9]. В документе отмечено, что около 50 % респондентов по всему миру считают, что их работа может быть автоматизирована, и свыше 60 % опрошенных высказали предположение, что цифровизация положительно повлияет на их занятость, создав возможности для работы.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ / RESEARCH RESULTS

Проведенное исследование выявило ряд ключевых тенденций и проблем, связанных с цифровой трансформацией и ее влиянием на различные сферы общественной жизни, а также на международную безопасность.

Цифровизация влияет на все сферы жизни современного общества: от государственного управления до личных коммуникаций. Глобальная сеть становится центральной платформой для распространения информации, формирования общественного мнения и трансляции стратегических интересов государств и корпораций. Эта трансформация привела к созданию единого информационного пространства, где границы между национальными государствами становятся все более условными.

Результаты анализа указывают на серьезную эскалацию угроз в сфере международной информационной безопасности. Наблюдается значительный рост числа кибератак, случаев цифрового шпионажа и вмешательства в политические процессы других государств. Эти деструктивные действия, осуществляемые как государственными, так и негосударственными факторами, подрывают международную стабильность и создают напряженность в отношениях между странами. Данные ITU (2023 г.) подтверждают эту тенденцию: более половины стран-членов организации сообщают о масштабных инцидентах в киберпространстве, что подчеркивает необходимость усиления международного сотрудничества в сфере кибербезопасности и разработки эффективных мер противодействия киберугрозам[10].

КИБЕРУГРОЗЫ, МЕЖДУНАРОДНАЯ И НАЦИОНАЛЬНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / CYBER THREATS, INTERNATIONAL AND NATIONAL INFORMATION SECURITY

Цифровая трансформация, как было указано, при всех ее преимуществах несет в себе и значительные социальные риски. Исследование выявило несколько ключевых проблем. Прежде всего нужно отметить феномен цифрового неравенства. Он выражен в том, что неравномерное распределение цифровой инфраструктуры приводит к исключению из глобальных процессов регионов с низким уровнем развития. Это усугубляет существующее социальное неравенство и создает барьеры для экономического и социального развития.

Унификация информационной среды генерирует новые вызовы. К наиболее распространенным относятся:

– глобализация информационной угрозы – кибератаки, дезинформация и манипуляции в цифровом пространстве могут исходить из любой точки мира и затрагивать миллионы пользователей;

– уязвимость критической инфраструктуры – стратегические объекты, транспорт, учреждения здравоохранения и государственного управления все чаще становятся жертвами киберпреступников;

– нарушения суверенитета в цифровом пространстве.

Под национальной информационной безопасностью понимаются меры по защите информации, информационных систем и сетей от несанкционированного доступа, использования, изменений, распространения внешних угроз, особенно если это связано с интересами национальной безопасности в современной сложной геополитической ситуации.

Цифровизация усилила масштабы и сложность киберугроз. Согласно данным международных организаций, таких как ООН и Интерпол (англ. International Criminal Police Organization – Международная организация уголовной полиции), количество кибератак ежегодно растет, увеличиваясь в геометрической прогрессии. Особую опасность представляют такие формы угрозы, как:

– кибератаки на государственные структуры, направленные на дискредитацию финансового аудита, шпионаж или дестабилизацию экономики;

– дезинформационные кампании, использующие технологии ботов, фейковые новости и алгоритмический таргетинг для манипуляции общественным мнением;

[9] Национальный исследовательский университет «Высшая школа экономики». Цифровизация государственных услуг. Режим доступа: https://issek.hse.ru/news/1039474722.html (дата обращения: 12.05.2025).

[10] International Telecommunication Union. Facts and figures 2023. Режим доступа: https://www.itu.int/itu-d/reports/statistics/facts-figures-2023/index/ (дата обращения: 12.05.2025).

– распространение незаконного экстремистского и террористического контента, содействие радикализации молодежи и возникновение новых угроз глобальной безопасности;

– цифровой суверенитет, который, будучи инструментом управления рисками, иногда сам становится источником новых социальных угроз (изоляция, цензура).

МЕЖДУНАРОДНАЯ ПРАКТИКА ПРИМЕНЕНИЯ КОНЦЕПЦИИ ЦИФРОВОГО СУВЕРЕНИТЕТА / INTERNATIONAL PRACTICE OF APPLYING THE CONCEPT OF DIGITAL SOVEREIGNTY

В Китае эксперт Китайской академии наук Ц. Сяопин в работе Cyber sovereignty (2015 г.) обосновал право государств регулировать интернет [Fang, 2018]. В 2017 г. был принят Закон о кибербезопасности КНР – основной нормативно-правовой акт, регулирующий сферу интернет-безопасности Китая. Опубликован 7 ноября 2016 г., вступил в силу 1 июня 2017 г. Закон регламентирует действия поставщиков сетевых продуктов и услуг по сбору, хранению и обработке пользовательских данных, определяет порядок и специфику обеспечения безопасности информационной инфраструктуры в стратегически важных отраслях. Главной целью принятия закона провозглашается защита национального киберсуверенитета КНР.

В РФ концепция «суверенного интернета» была предложена в 2012 г. И.О. Щеголевым – Министром связи и массовых коммуникаций России[11], занимавшим эту должность в Правительстве с 12 мая 2008 г. по 21 мая 2012 г, – и реализована в 2019 г. Закон о «суверенном интернете» — неформальное название Федерального закона от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон „О связи“ и Федеральный закон „Об информации, информационных технологиях и о защите информации“». Вступил в силу 1 ноября 2019 г. Его цель – создание независимой инфраструктуры для бесперебойного функционирования интернета в России. Она позволит обеспечить работоспособность сайтов в случае невозможности подключения российских операторов связи к зарубежным корневым серверам интернета. Суверенный интернет – это концепция, предполагающая создание отдельной сегментированной сети, которая сохранит работоспособность в случае отключения от мировой инфраструктуры интернета. Основная идея – обеспечение безопасности и защиты национальных интересов в сети путем ограничения доступа к определенным внешним ресурсам и контенту. Концепция основана на идее, что страны имеют право управлять своими интернет-ресурсами в соответствии со своими ценностями и интересами. Это может включать создание локализованных интернет-инфраструктур, а также политики и нормативных актов, регулирующих поток информации в страну и из страны.

В сентябре 2020 г. А.В. Крутских, специальный представитель Президента РФ по вопросам международного сотрудничества в области информационной безопасности (2014–2023 гг.), рассказал, что источники DDoS-атак (англ. Distributed Denial of Service – распределенный отказ от обслуживания) на инфраструктуру Центральной избирательной комиссии и других государственных органов во время проведения голосования по поправкам в Конституцию фиксировались на территории США, Великобритании, Украины и ряда стран Содружества Независимых Государств.

Современные интерпретации концепции цифрового суверенитета оформлены в академических исследованиях Дж.С. Ная (The future of power, 2021 г.)[12], который рассматривает цифровой суверенитет как элемент мягкой силы. Критику концепции как инструмента авторитаризма осуществил М.Э. Вагнер (Петербургский международный юридический форум 2025 г.)[13], (табл. 1).

[11] Материалы по выбранной персоне. Щеголев, Игорь Олегович. Режим доступа: http://www.kremlin.ru/catalog/persons/65/biography (дата обращения: 12.05.2025).

[12] Nye J.S. Jr. The future of power. Режим доступа: https://www.files.ethz.ch/isn/154756/issuesinsights_vol11no08.pdf (дата обращения: 12.05.2025).

[13] Росконгресс. Милош Вагнер. Цитаты. Режим доступа: https://roscongress.org/speakers/vagner-milosh/quotes/?utm_referrer=https%3A%2F%2Fyandex.ru%2 (дата обращения: 12.05.2025).

Таблица 1. **Концепция цифрового суверенитета. Ключевые даты и документы**

Table 1. Concept of digital sovereignty. Key dates and documents

Год	Событие/документ	Автор/страна	Основное содержание
1996	Декларация независимости киберпространства	Дж.П. Барлоу (США)	Трактовка независимости киберпространства

Окончание табл. 1

Год	Событие/документ	Автор/страна	Основное содержание
2013	European Digital Agenda	ЕС	Первое официальное использование термина
2017	Закон о кибербезопасности КНР	Китай	Модель государственного контроля
2019	Закон о «Суверенном интернете» – Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон „О связи“ и Федеральный закон „Об информации, информационных технологиях и о защите информации“»	РФ	Модель государственного контроля
2021	The future of power	Дж.С. Най (США)	Суверенитет как ресурс влияния

Составлено авторами по материалам исследования / *Compiled by the authors on the materials of the study*

Международная политическая практика реализации концепции цифрового суверенитета включает несколько основных документов. Так, в США принята Доктрина ответственного цифрового суверенитета (Белый дом, 2023 г.), в которой обосновывается баланс между безопасностью и открытостью. В Индии политика цифрового самообеспечения (2020 г.) содержит запрет TikTok, поддержку локальных ИТ.

ЕС использует регламент GDPR для ограничения Meta. В контексте информационной безопасности GDPR – это законодательный акт союза, который регулирует обработку персональных данных граждан ЕС. Он устанавливает строгие требования к тому, как организации должны собирать, хранить и защищать личные данные, а также предоставляет гражданам расширенные права в отношении их информации.

Китай для обеспечения безопасности использует систему «Великий китайский файрвол» (англ. Great Firewall of China) – это комплексная система интернет-цензуры, внедренная правительством КНР для мониторинга, фильтрации и блокировки небезопасного интернет-контента для пользователей внутри страны. Основные цели этой системы – контролировать информацию и ограничивать доступ к небезопасным веб-сайтам и онлайн-сервисам, контент которых власти Китая считают вредным. Также блокируется информация, связанная с порнографией, азартными играми или насилием (табл. 2).

Управление данными и инфраструктурой как атрибут государственного суверенитета включает право государства контролировать цифровое пространство на своей территории. В первую очередь это данные граждан (например, GDPR в ЕС); критическая инфраструктура (киберзащита энергосетей); цифровые платформы (например, блокировка Google/Amazon в Китае).

[14] European Parliament. Digital Agenda for Europe. Режим доступа: https://www.europarl.europa.eu/ftu/pdf/en/FTU_2.4.3.pdf (дата обращения: 11.05.2025).

Таблица 2. **Концепция цифрового суверенитета. Модели реализации**

Table 2. Concept of digital sovereignty. Implementation models

Страна/блок	Подход	Инструменты
Китай	Жесткий государственный контроль	Великий файрвол, закон о кибербезопасности (2017 г.), обязательное хранение данных локально
ЕС	Соблюдение протоколов	GDPR, Digital Markets Act (англ. Закон о цифровых услугах), борьба с монополиями (штрафы Apple/Meta)
РФ	Государственный контроль	Закон о «Суверенном интернете» – Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон „О связи“ и Федеральный закон „Об информации, информационных технологиях и о защите информации“»; налог на ИТ-гиганты

Составлена авторами по материалам источников[14] и [Гриффитс, 2021] / *Compiled by the authors on the materials of the sources[14] and [Griffiths, 2021]*

Также необходимо отметить риски роста социальной изоляции. Несмотря на возможности онлайн-коммуникации, чрезмерное увлечение цифровыми форматами взаимодействия приводит к снижению качества человеческих связей, ослаблению социальных контактов и росту чувства одиночества и социальной изоляции.

Происходит также некоторая утрата автономии, которая выражается в том, что чрезмерная зависимость от цифровых платформ и сервисов снижает способность людей к самостоятельному принятию решений и критическому мышлению. Они становятся зависимыми от алгоритмов и рекомендаций, что ограничивает их свободу выбора и автономию.

Немаловажными являются и психологические риски. Цифровая среда способствует распространению дезинформации, усиливает тревожность и может вызывать цифровую зависимость. Непрерывный поток информации, необходимость всегда быть на связи и соответствовать определенным стандартам, установленным в социальных сетях, негативно сказываются на психическом здоровье людей.

Происходят также деградация коммуникативных практик и рост психологического напряжения. Чрезмерное погружение в цифровую среду приводит к ограничению моделей межличностных коммуникаций: снижается эмпатия, повышается уровень тревожности и зависимости от цифровых устройств. Особую остроту эта проблема приобретает среди подростков и молодежи.

Важным аспектом являются такие феномены, как формирование информационных пузырей и поляризация общества. Алгоритмы рекомендаций в социальных сетях и на онлайн-платформах обеспечивают формирование замкнутых информационных пространств, где пользователи сталкиваются только с мнениями, подтверждающими их собственные. Это ведет к идеологической поляризации, приводит к диалогу и может привести к внутриполитическому конфликту.

Отсутствие единого, общепризнанного международного правового механизма, регулирующего цифровую безопасность, является серьезной проблемой, подрывающей усилия по созданию безопасного и доверительного цифрового пространства. Несмотря на усилия таких организаций, как ООН и Глобальная комиссия по стабильности киберпространства, достичь консенсуса по ключевым вопросам не удается. Геополитические разногласия между странами, различные подходы к регулированию цифровой среды и вопросы суверенитета в киберпространстве препятствуют созданию эффективной архитектуры цифрового доверия. Необходимы поиск компромиссных решений и разработка универсальных норм и принципов, которые могли бы стать основой для международного сотрудничества в сфере цифровой безопасности.

ЗАКЛЮЧЕНИЕ / CONCLUSION

Цифровизация представляет собой как мощный ресурс для развития управленческих систем, так и источник новых угроз, прежде всего в области международной информационной безопасности и социальных рисков. Принимая во внимание трансграничный характер цифровых процессов, отметим, что необходим комплексный подход к их регулированию, предполагающий развитие международного цифрового права; координацию усилий государств в области кибербезопасности; повышение цифровой грамотности среди управленцев; внедрение этических принципов в алгоритмическое управление.

Цифровизация, с одной стороны, открывает широкие возможности для развития общества, но, с другой стороны, создает новые угрозы в сфере национальной информационной безопасности. В эпоху глобализации успешное преодоление этих проблем требует не только принятия мер информационной безопасности на национальном уровне, но и комплексных объединенных усилий многих дружественных государств, международных организаций, технологических компаний и общества. Необходимы разработка и согласование универсальных этических мер по использованию цифровых технологий. Только посредством многопланового сотрудничества можно минимизировать риски и направить цифровую трансформацию на общее благо.

Направления дельнейших исследований связаны с разработкой моделей оценки цифровых рисков, с анализом успешных практик цифрового регулирования в разных странах. Обозначен и вектор исследования роли ИИ в управлении и его социальных последствий. Важно также формирование международной платформы цифрового доверия.

СПИСОК ЛИТЕРАТУРЫ

Альшами Э.М., Алотаиби Ф.М., Карипиду М. Цифровая трансформация и проблемы кибербезопасности в эпоху глобализации. Международный журнал информационной безопасности и киберпреступности. 2022;2(11):5–28.

Бауман З. Текучая современность. Пер. с англ. СПб.: Питер; 2013. 240 с.

Вяткин А.Ю. Социальные последствия цифровой трансформации. Государственная служба. 2020;3:67–72.

Греков И.С. Цифровизация управления: вызовы и риски. Вестник государственного управления. 2021;4:25–34.

Гриффитс Дж. Великий Китайский Файрвол. Пер. с англ. Н.А. Комар, А.В. Ефимовой. М.: Бомбора; 2021. 464 с.

Кастельс М. Информационная эпоха. Экономика, общество и культура. Том 1. Становление сетевого общества. М.: Государственный университет «Высшая школа экономики»; 2009. 608 с.

Мартенс Б., Рааб К.Д. Социальные риски цифровой трансформации: дезинформация и поляризация в онлайн-пространствах. Телематика и информатика. 2021;56.

Михалевич Е.А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность. Вестник Российского университета дружбы народов. Серия: Политология. 2021;2(23):254–264.

Мкртумова И.В. От «Троянского коня» до «Пожирателей фейков»: взгляд социолога на образы информационного поведения и манипуляций. В кн.: Научные исследования в современном мире: проблемы, тренды, перспективы: сборник статей по итогам Научного профессорского форума, 7 февраля 2023 г. М.: Российское профессорское собрание; 2023. С. 228–236.

Мкртумова И.В., Ашкар М., Чижов Д.А., Янчук П.П. Трансформации социальных коммуникаций в условиях цифровой платформизации и создания метавселенных помощи человеку. Цифровая социология. 2025;1(8):42–50.

Петров А., Иванов Д. Влияние цифровых технологий на национальную и международную безопасность: сравнительное исследование. Журнал безопасности. 2023.

Сингх Р., Патель Н. Кибербезопасность и социальная уязвимость в эпоху цифровизации. Журнал кибербезопасности и политики. 2024;1(17):45–62.

ITU. Global Cybersecurity Index 2023. Geneva: International Telecommunication Union; 2023.

DeNardis L. The global war for internet governance. New Haven: Yale University Press; 2014. 288 p.

Fang B. Cyberspace sovereignty. Reflections on building a community of common future in cyberspace. Singapore: Springer Singapore; 2019. 482 p.

Zuboff Sh. The age of surveillance capitalism. The fight for a human future at the new frontier of power. New York: Public Affairs; 2019. 691 p.

REFERENCES

Alshami E.M., Alotaibi F.M., Karipidu M. Digital transformation and cybersecurity challenges in the era of globalization. International Journal of Information Security and Crime. 2022;2(11):5–28. (In Russian). http://doi.org/10.3390/info13020076

Bauman Z. Liquid modernity. Trans. from Eng. St Petersburg: Piter; 2013. 240 p. (In Russian).

Castells M. The information age. Economy, society and culture. Volume 1. The rise of the network society. Moscow: State University “Higher School of Economics”; 2009. 608 p. (In Russian).

DeNardis L. The global war for internet governance. New Haven: Yale University Press; 2014. 288 p.

Fang B. Cyberspace sovereignty. Reflections on building a community of common future in cyberspace. Singapore: Springer Singapore; 2019. 482 p.

International Telecommunication Union. Global cybersecurity index 2023. Geneva: International Telecommunication Union; 2023.

Grekov I.S. Digitalization of governance: challenges and risks. Bulletin of State Administration. 2021;4:25–34. (In Russian).

Griffiths J. The Great Firewall of China. Trans. from Eng. N.A. Komar, A.V. Efimova. Moscow: Bombora; 2021. 464 p. (In Russian).

Martens B., Raab K.D. Social risks of digital transformation: misinformation and polarization in online spaces. Telematics and Informatics. 2021;56. (In Russian).

Mikhalevich E.A. The concept of cyber sovereignty of the People’s Republic of China: development history and essence. RUDN Journal of Political Science. 2021;2(23):254–264. (In Russian). http://doi.org/10.22363/2313-1438-2021-23-2-254-264

Mkrtumova I.V., Ashkar M., Chizhov D.A., Yanchuk P.P. Social communications transformations in the conditions of digital platformization and human assistance metavillages creation. Digital Sociology. 2025;1(8):42–50. (In Russian). https://doi.org/10.26425/2658-347X-2025-8-1-42-50

Mkrtumova I.V. From “Trojan horse” to “Fake eaters”: a sociologist’s view on information behaviour and manipulation. In: Scientific research in the modern world: problems, trends, prospects: Proceedings on the results of the Scientific Professor Forum, February 7, 2023. Moscow: Russian Professorial Assembly; 2023. Pp. 228–236. (In Russian).

Petrov A., Ivanov D. Impact of digital technologies on national and international security: comparative study. Security Journal. 2023.

Singh R., Patel N. Cybersecurity and social vulnerability in the era of digitization. Journal of Cyber Security and Policy. 2024;1(17):45–62. (In Russian).

Vyatkin A.Yu. Social consequences of digital transformation. Public Service Bulletin. 2020;3:67–72. (In Russian).

Zuboff Sh. The age of surveillance capitalism. The fight for a human future at the new frontier of power. New York: Public Affairs; 2019. 691 p.