nauka.me. 2013-2025

ISSN 2413-2888

URL - http://nauka.me

Выпуск 2 Том . 2024

Влияние цифровизации на международные отношения: вызовы и перспективы

Гребенщикова Екатерина Алексеевна
Владивостокский государственный университет
Российская Федерация, Владивосток

Чернышов Тимофей Александрович
Владивостокский государственный университет
Российская Федерация, Владивосток

Аннотация

В современном мире, на фоне цифровой революции, процесс цифровизации превращается в неотъемлемый компонент международной политики, экономики и культуры. Стремительное развитие информационных и коммуникационных технологий оказывает значительное влияние на международные отношения, внося как вызовы, так и перспективы. Целью настоящего доклада является анализ воздействия цифровизации на международные отношения, выявление вызовов и перспектив, а также практические рекомендации для эффективного управления этими процессами. Данный доклад рассматривает влияние цифровизации на глобальную арену, обозначая ряд вызовов, включая кибербезопасность, приватность данных и цифровой разрыв. В то же время выявляются перспективы, такие как стимулирование экономического роста, углубление международного сотрудничества, инновации в сферах образования и здравоохранения, а также повышение уровня международной безопасности. Доклад подчеркивает, что эффективное управление процессом цифровизации требует сотрудничества и координации на международном уровне. Доклад может предложить практические рекомендации для государственных и негосударственных акторов по эффективному управлению цифровыми вызовами. В контексте кибертерроризма описываются меры национальной и международной безопасности, такие как подписание соглашений и проведение обучающих мероприятий для граждан. Для сокращения цифрового разрыва обсуждаются инициативы Организации

Объединенных Наций (ООН) и других международных организаций, направленные на обеспечение всеобщего подключения к Интернету и сокращение неравенства в доступе к информационно-коммуникационным технологиям. Особое внимание уделяется выработке правил ответственного поведения государств в информационном пространстве, с учетом рисков международной информационной безопасности и интересов всех сторон. Приведены статические данные, суммированы экспертные оценки 2024 г., даны аналитические прогнозы.

Ключевые слова: цифровизация, международные отношения, информационно-коммуникационные технологии, кибербезопасность, международное сотрудничество, информационная безопасность, цифровые вызовы, кибертерроризм, цифровой разрыв, информационное пространство, глобальная арена, устойчивое развитие, международные организации

Дата публикации: 25.12.2024

Ссылка для цитирования:

Гребенщикова Е. А. , Чернышов Т. А. Влияние цифровизации на международные отношения: вызовы и перспективы // nauka.me. – 2024. – Выпуск 2.
URL: https://nauka.me/s0031752-7-1/. DOI: 10.18254/S241328880031752-1

1 В современном мире цифровые технологии проникают во все сферы нашей жизни, открывая новые возможности, но также создавая и новые вызовы. Понятие «цифровизация» активно обсуждается учеными и экспертами из разных стран, хотя единого определения пока не выработано. Под цифровизацией мы понимаем комплексное внедрение передовых цифровых решений, таких как: искусственный интеллект, большие данные, интернет вещей и др. в самые разные области жизни государства и общества – промышленность, медицину, образование, государственное управление и так далее.

2 Цифровая трансформация нашего мира набирает обороты и становится одной из наиболее значимых и стабильных глобальных тенденций последних лет. Учёные и аналитики отмечают многогранность этого феномена. С одной стороны, повсеместное распространение инновационных технологий приносит человечеству неоспоримые преимущества. Так, во время пандемии COVID-19, когда традиционные формы жизни и работы были серьезно нарушены, благодаря цифровым решениям миллионы людей смогли сохранить относительно нормальный уровень жизни и доступ к услугам.

3 Вместе с тем, стремительная цифровизация оказывает масштабное влияние на международные отношения и геополитический ландшафт, создавая как новые возможности для сотрудничества, так и потенциальные вызовы и угрозы, требующие пристального внимания мирового сообщества. Рассмотрим некоторые из наиболее актуальных вызовов более подробно.

4 Кибербезопасность становится одной из главных проблем эпохи цифровизации. Активное использование цифровых систем разного уровня повышает риски кибератак, хакерских взломов и кибершпионажа со стороны злоумышленников. По данным российской компании «Солар Секьюрити»,

специализирующейся на кибербезопасности, в 2023 году около 20% зарегистрированных инцидентов были классифицированы как сложные целевые атаки. Наибольшую угрозу для отечественных организаций представляли профессиональные хакерские группировки из азиатского региона, главной целью которых является кибершпионаж и кража данных[1]. Кроме того, примерно 15 проукраинских группировок активно совершали разрушительные атаки против российских структур. Подобные кибератаки наносят серьезный ущерб, ставят под угрозу национальную безопасность и дестабилизируют ситуацию на международной арене. По прогнозам компании Cybersecurity Ventures, ежегодные убытки мировой экономики от киберпреступности достигнут $10,5 триллионов к 2025 году[2]. Согласно данным компании AV-Test, в 2023 году было обнаружено 30 миллионов новых образцов вредоносного программного обеспечения[3]. Это фактически отражает двукратное снижение показателя по сравнению с предыдущим годом[4]. Согласно Webroot Threat Report от 2020 года, в 2019 году 93,6% наблюдаемого вредоносного ПО было полиморфным, то есть способным постоянно модифицировать свой код для уклонения от обнаружения. Тем не менее, наблюдается внедрение инструментов на основе машинного обучения, которые могут выявлять общие характеристики между любым приложением и известными семействами вредоносных программ[5]. Согласно отчету Webroot Threat Report 2022, 45% корпоративных ПК и 53% потребительских ПК, ранее подвергшихся заражению, были повторно инфицированы в течение того же года[6]. Исследование Университета Мэриленда 2007 года установило, что злоумышленники ранее атаковали компьютеры и сети с частотой в 1 атаку каждые 39 секунд[7]. Отчет Интернет-преступного центра за 2022 год зафиксировал 800 944 жалоб, что соответствует одной успешной атаке каждые 0,65 секунды[8]. Следует отметить, что данные не включают в себя попытки атак или незарегистрированные инциденты. Согласно Cyberthreat Defense Report 2023 компании CyberEdge Group, 84,7% опрошенных организаций были затронуты успешными кибератаками[9]. Этот показатель снизился по сравнению с 85,3% в 2022 году и 86,2% в 2021 году. Также атаки с использованием программ-вымогателей (ransomware) могут быть чрезвычайно затратными. Например, атака, связанная с вредоносным ПО NotPetya, обошлась транспортной компании Maersk более чем в 200 миллионов долларов[10]. Согласно отчету Sophos «The State of Ransomware 2023», в 2023 году средняя глобальная стоимость устранения последствий атаки программ-вымогателей возросла до 1,82 миллиона долларов, что более чем в два раза превышает средний показатель 2021 года ($761,106)[11]. Организации в Сингапуре, ЮАР, Испании и Швейцарии с наибольшей вероятностью подвергаются атакам программ-вымогателей. В Индии распространенность этой угрозы особенно высока – 84% организаций сталкивались с ransomware. Южная Африка занимает второе место по частоте таких инцидентов – 78%[12]. Согласно данным Лаборатории Касперского, в третьем квартале 2023 года было обнаружено более 1800 новых мобильных троянцев-вымогателей (Kaspersky Labs). В 2023 году Йемен, Бангладеш и Южная Корея возглавили список стран, наиболее атакуемых программами-вымогателями по доле пользователей (Kaspersky Labs). Таким образом, активное использование цифровых технологий на всех уровнях повышает риски кибератак, взломов и кибершпионажа со стороны злоумышленников. Наибольшую угрозу для организаций представляют профессиональные хакерские группировки из

азиатского региона, специализирующиеся на кибершпионаже и краже данных, а также проукраинские группировки, проводящие разрушительные атаки. Согласно прогнозам, ежегодные глобальные убытки от киберпреступности к 2025 году могут достигнуть $10,5 триллионов, что свидетельствует о масштабе проблемы. Несмотря на снижение количества новых образцов вредоносного ПО, они становятся все более изощренными, способными постоянно видоизменять свой код, что затрудняет их обнаружение, однако развиваются и методы на основе машинного обучения для выявления таких полиморфных угроз. Проблема повторного заражения компьютеров остается актуальной, что указывает на необходимость совершенствования средств защиты и процедур реагирования на инциденты. Атаки с использованием программ-вымогателей представляют особую опасность, нанося колоссальный ущерб и затраты на ликвидацию последствий, что делает этот вид угрозы одним из наиболее серьезных вызовов для организаций.

5 Другой важной проблемой цифровой эпохи становится обеспечение приватности и защиты персональных данных граждан. По мере того, как все большие объемы разнообразной информации собираются, хранятся и передаются в цифровом виде, возрастают риски ее утечки или несанкционированного использования. Так, специалисты компании «Лаборатории Касперского» отмечают, что только за первый квартал 2024 года количество кибератак на мобильные устройства выросло в 5,2 раза по сравнению с тем же периодом предыдущего года[13]. Потенциальные нарушения приватности и неправомерное обращение с личными данными людей могут подорвать доверие между государствами и обострить ситуацию в международных отношениях.

6 Международные организации предпринимают усилия для регулирования вопросов защиты персональных данных и прав человека в цифровой среде. Публикуются различные рекомендации, декларации, готовятся к принятию новые нормативные акты в этой сфере. Однако темпы цифровизации опережают развитие правовой базы, поэтому дискуссия о балансе между инновациями и правами человека в изменяющемся мире требует активного продолжения.

7 Цифровой разрыв между развитыми и развивающимися странами в доступе к современным технологиям является еще одной серьезной проблемой, которую необходимо решать на международном уровне. По статистике ООН, почти 40% жителей планеты до сих пор не имеют постоянного доступа к интернету, причем большинство из них – женщины из бедных стран. Разрыв в цифровизации отчетливо прослеживается между регионами[14]. Если в государствах с высоким уровнем дохода 87% населения пользуются интернетом, то в наименее развитых странах этот показатель составляет всего 17%. Внутри стран доступность цифровых технологий также определяется социально-экономическим статусом граждан, в том числе и в благополучных обществах. Согласно результатам анализа, проведенного учеными на основе данных обследований Росстата за 2016-2019 годы, в России наблюдается существенный цифровой разрыв между регионами. Этот разрыв связан с неравенством в доступе к персональным компьютерам и сети интернет, различиями в уровне цифровых знаний и навыков населения, а также разницей в конечных результатах применения компьютеров и интернета. Таким образом, в России существует

серьезное цифровое неравенство между регионами[15]. Таким образом, существующее цифровое неравенство не только сдерживает прогресс, но и несет в себе серьезные риски для международной безопасности. Линии геополитических разломов, разделяющие богатых и бедных, переносятся в виртуальную среду, провоцируя рост напряженности и конфликтов на глобальном уровне. Преодоление цифрового разрыва требует скоординированных усилий мирового сообщества – оказания помощи отстающим странам в развитии инфраструктуры, совершенствования законодательства, подготовки квалифицированных кадров. Необходимо международное сотрудничество для выработки правил цивилизованного и ответственного поведения государств в глобальном информационном пространстве с учетом мнений правительств, деловых кругов, экспертов и гражданского общества. Только так можно будет избежать новых угроз миру и стабильности.

8 Несмотря на существующие вызовы, процесс цифровой трансформации открывает перед глобальным сообществом и широкие позитивные перспективы. Во-первых, цифровые технологии являются мощным драйвером экономического роста. Создание инновационных цифровых платформ, развитие электронной коммерции, внедрение новейших IT-решений дают импульс техническому прогрессу и появлению новых отраслей и рынков. Это позволяет повысить эффективность производства, стимулировать международную торговлю и улучшить качество жизни населения. Во-вторых, цифровизация облегчает коммуникацию и взаимодействие между государствами, создавая благоприятные условия для многостороннего сотрудничества. Примером такого партнерства может служить совместная инициатива России и Китая по сопряжению строительства Евразийского экономического союза и проекта «Один пояс – один путь». В рамках данной программы стороны развивают тесное взаимодействие по цифровой тематике и уже подписали ряд важных соглашений. В-третьих, внедрение цифровых решений открывает новые горизонты для таких сфер как образование и здравоохранение, особенно в развивающихся странах. Дистанционные технологии обучения и телемедицина способны обеспечить гораздо более широкий доступ к качественным услугам, снизив тем самым неравенство между регионами мира. Наконец, цифровизация предоставляет новые возможности для повышения международной безопасности. Современные IT-инструменты позволяют более эффективно отслеживать и пресекать деятельность террористических и экстремистских группировок, противодействовать киберпреступности и другим трансграничным угрозам.

9 Таким образом, процесс цифровой трансформации, хоть и сопряжен с множеством сложных вызовов, несет в себе колоссальный позитивный потенциал для развития человеческой цивилизации. Ключевая задача мирового сообщества – научиться управлять этим процессом, максимизируя его преимущества и минимизируя риски. Это требует тесной координации усилий государств, международных организаций, частного сектора и гражданского общества на глобальном уровне.

10 Угроза кибертерроризма сегодня приобретает глобальный масштаб и требует консолидированных усилий всего международного сообщества. Многие государства уже принимают на национальном уровне необходимые меры для

обеспечения кибербезопасности и защиты критической инфраструктуры. Так, в 2009 году страны-участницы Шанхайской организации сотрудничества подписали Соглашение об обеспечении международной информационной безопасности, где кибертерроризм был обозначен как одна из главных угроз. Активную работу в данной сфере проводят и другие международные организации, осознавая всю опасность этого вида преступлений.

11 В России вопросы повышения защищенности информационной инфраструктуры и ее устойчивого функционирования определены в качестве приоритетных в Доктрине информационной безопасности. Федеральный закон «О безопасности критической информационной инфраструктуры РФ» также является фундаментом для построения системы кибербезопасности в стране. Созданы Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА) и Национальный координационный центр по компьютерным инцидентам. Роскомнадзор наделен полномочиями и обязанностями по противодействию киберпропаганде, с чем он, по-видимому, справляется достаточно эффективно[16]. Важнейшим направлением противодействия киберугрозам является просвещение и обучение граждан – проведение образовательных мероприятий по распознаванию фишинговых атак, вредоносного контента, формированию навыков цифровой грамотности и правовой культуры. Положительным примером служит ежегодный Единый урок по кибербезопасности для школьников[17].

12 Контртеррористическое управление ООН реализует комплекс инициатив, связанных с использованием новых технологий, таких как анализ открытых цифровых источников, применение беспилотников и другие для эффективного сбора данных в борьбе с терроризмом при строгом соблюдении прав человека. Отдельная программа ООН по кибербезопасности направлена на укрепление потенциала государств и частных структур в сфере предотвращения, смягчения последствий и восстановления после возможных кибератак террористов на критически важные объекты[18].

13 Проблема цифрового неравенства также находится в фокусе внимания мирового сообщества. На глобальном уровне реализуется ряд программ и инициатив, направленных на сокращение разрыва в доступе к цифровым технологиям. Так, например, ООН приняла Дорожную карту цифрового сотрудничества, ставящую цель обеспечить повсеместное подключение к интернету на планете к 2030 году[19]. Комиссия по широкополосной связи при МСЭ и ЮНЕСКО более десяти лет ведет работу по преодолению неравенства в доступе к ИКТ. Инициатива «Giga» ЮНИСЕФ и МСЭ нацелена на подключение к интернету всех школ мира. ПРООН поддерживает программы ликвидации гендерного цифрового разрыва[20].

14 Важную роль в развитии цифровых технологий играют крупные IT-корпорации. Однако при решении трансграничных проблем информационной безопасности, киберпреступности, защиты персональных данных им приходится опираться на государства, обладающие необходимой легитимностью и правосубъектностью.

15 Взаимозависимость глобального цифрового пространства не позволяет ни одной стране или компании в одиночку управлять процессами цифровой трансформации. Поэтому крайне важно развивать многостороннее сотрудничество по преодолению цифрового разрыва с участием государств, бизнеса, научного сообщества, гражданского общества. При этом приоритетное внимание должно уделяться вопросам информационной безопасности. В этих условиях одной из ключевых задач становится выработка правил ответственного поведения государств в глобальном информационном пространстве. Эти нормы должны учитывать риски для международной инфобезопасности при одновременном задействовании ресурсов и интересов всех вовлеченных сторон. Координирующая роль в данном процессе отводится государствам.

16 Таким образом, глобальные вызовы цифрового неравенства требуют консолидированного отклика со стороны мирового сообщества при тесном взаимодействии различных акторов – правительств, компаний, экспертов, общественных организаций. Только на основе многостороннего партнерства возможно построить более справедливое и безопасное цифровое будущее для всех стран и народов.

17 Процесс глобальной цифровой трансформации открывает перед человечеством колоссальные возможности, но одновременно несет серьезные вызовы и риски. Внедрение инновационных технологий способствует экономическому росту, развитию новых отраслей, повышению эффективности производства и международной торговли. Цифровые коммуникации облегчают взаимодействие между государствами, создавая благоприятные условия для многостороннего сотрудничества и интеграционных проектов, таких как инициатива «Один пояс – один путь». Важнейшим позитивным аспектом цифровизации является расширение доступа к качественному образованию и здравоохранению, снижение неравенства. Современные IT-решения также открывают новые возможности для обеспечения международной безопасности, борьбы с терроризмом и киберпреступностью.

18 Вместе с тем, цифровая эпоха сопряжена с серьезными вызовами, среди которых кибертерроризм, проблема защиты персональных данных, риски для информационной безопасности государств. Угроза кибертерроризма носит глобальный характер и требует консолидированных усилий всего мирового сообщества. Многие страны уже принимают меры на национальном уровне, разрабатывают образовательные программы для граждан, развивают правовую базу. На международной арене реализуются профильные инициативы ООН, других организаций. Отдельным серьезным вызовом остается проблема цифрового неравенства - разрыва в доступе к современным технологиям между странами и социальными группами. Его преодоление требует масштабных совместных усилий по развитию инфраструктуры, реализации специальных программ и проектов.

19 Таким образом, грамотное управление процессами цифровизации при максимальном задействовании ее позитивного потенциала и минимизации рисков является одной из ключевых задач мирового сообщества. Для ее успешного решения необходимы тесная координация и многостороннее сотрудничество

государств с участием бизнеса, научного сообщества, гражданского общества. Центральную роль при этом должен играть выверенный политико-правовой регулятор на национальном и международном уровнях, основанный на гармонизации различных интересов и строгом соблюдении принципов информационной безопасности.

Примечания:

1. Хакеры нацелились на госсектор. – Текст : электронный // Российская газета:

2. Тренд на «белых хакеров»: будущее индустрии кибербезопасности. – Текст: электронный // FORBES: [сайт]. 2024. – URL: >>>> (дата обращения: 14.06.2024).

3. Malware. – Текст: электронный // av-test.org: [сайт]. 2024. – URL: >>>> (дата обращения: 14.06.2024).

4. 300+ Terrifying Cybercrime and Cybersecurity Statistics (2024 EDITION). – Текст: электронный // comparitech.com: [сайт]. 2024. – URL: >>>>

5. Nastiest Malware 2023. – Текст: электронный // community.opentextcybersecurity.com: [сайт]. 2023. – URL: >>>> (дата обращения: 14.06.2024).

6. 2022 BrightCloud® Threat Report. – Текст: электронный // www-cdn.webroot.com: [сайт]. 2022. – URL: >>>> (дата обращения: 14.06.2024).

7. Study: Hackers Attack Every 39 Seconds. – Текст: электронный // eng.umd.edu: [сайт]. 2007. – URL: >>>> (дата обращения: 14.06.2024).

8. 2022 Internet crime report. – Текст: электронный // Federal bureau of investigation: [сайт]. 2022. – URL: >>>> (дата обращения: 14.06.2024).

9. Cyberthreat Defense Report. – Текст: электронный // CyberEdge Group: [сайт]. 2023. – URL: >>>> (дата обращения: 14.06.2024).

10. NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million. – Текст: электронный // FORBES: [сайт]. 2017. – URL: >>>> (дата обращения: 14.06.2024).

11. The State of Ransomware 2023. – Текст: электронный // SOPHOS: [сайт]. 2023. – URL: >>>> (дата обращения: 14.06.2024).

12. IT threat evolution in Q3 2023. Mobile statistics. – Текст: электронный // Securelist by Kaspersky: [сайт]. 2023. – URL: >>>> (дата обращения: 14.06.2024).

13. Эксперты оценили масштаб атак хакеров на пользователей Android в России. – Текст: электронный // RBC: [сайт]. 2024. – URL: >>>> (дата обращения: 14.06.2024).

14. Преодолеть цифровой колониализм. – Текст: электронный // Валдай: [сайт]. 2023. – URL: >>>> (дата обращения: 14.06.2024).

15. Цифровой разрыв. Чем он грозит России и каковы его масштабы?. – Текст: электронный // Национальный исследовательский университет «Высшая школа экономики»: [сайт]. 2021. – URL: >>>> (дата обращения: 14.06.2024).

16. Есть ли у России шанс победить в мировой кибервойне. – Текст: электронный // Московский комсомолец: [сайт]. 2022. – URL: >>>> (дата обращения: 14.06.2024).

17. Троян Н.А. Влияние цифровых технологий на повышение уровня культуры информационной безопасности граждан России / Н.А. Троян. – Текст: электронный // Мониторинг правоприменения. – 2023. – №1 (46). – URL: URL: >>>> (дата обращения: 13.06.2024). С. 20-26.

18. Кибербезопасность. – Текст: электронный // Контртеррористическое управление ООН: [сайт]. 2017. – URL: >>>> (дата обращения: 14.06.2024).

19. Report of the Secretary-General Roadmap for Digital Cooperation JUNE 2020. – Текст: электронный // ООН: [сайт]. 2020. – URL: >>>> (дата обращения: 14.06.2024).

20. Международно-политическое измерение цифрового разрыва. – Текст: электронный // Российский совет по международным делам (РСМД): [сайт]. 2021. – URL: >>>> (дата обращения: 14.06.2024).

Библиография:

1. Хакеры нацелились на госсектор. – Текст : электронный // Российская газета:

2. [офиц. сайт]. – Москва, 2023. – URL: https://rg.ru/2023/12/14/hakery-nacelilis-na-gossektor.html (дата обращения: 14.06.2024).

3. Тренд на «белых хакеров»: будущее индустрии кибербезопасности. – Текст: электронный // FORBES: [сайт]. 2024. – URL: https://www.forbes.ru/forbes-agenda/514198-trend-na-belyh-hakerov-budusee-industrii-kiberbezopasnosti (дата обращения: 14.06.2024).

4. Malware. – Текст: электронный // av-test.org: [сайт]. 2024. – URL: https://www.av-test.org/en/statistics/malware/ (дата обращения: 14.06.2024).

5. 300+ Terrifying Cybercrime and Cybersecurity Statistics (2024 EDITION). – Текст: электронный // comparitech.com: [сайт]. 2024. – URL: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/ (дата обращения: 14.06.2024).

6. Nastiest Malware 2023. – Текст: электронный // community.opentextcybersecurity.com: [сайт]. 2023. – URL: https://community.opentextcybersecurity.com/threat-reports-176/nastiest-malware-2023-355907 (дата обращения: 14.06.2024).

7. 2022 BrightCloud® Threat Report. – Текст: электронный // www-cdn.webroot.com: [сайт]. 2022. – URL: https://www-cdn.webroot.com/1316/5956/7965/BrightCloud_All_Threat_Report_Mid-Year_Letter_REP_AMER_EN_3.pdf (дата обращения: 14.06.2024).

8. Study: Hackers Attack Every 39 Seconds. – Текст: электронный // eng.umd.edu: [сайт]. 2007. – URL: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds (дата обращения: 14.06.2024).

9. 2022 Internet crime report. – Текст: электронный // Federal bureau of investigation: [сайт]. 2022. – URL: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (дата обращения: 14.06.2024).

10. Cyberthreat Defense Report. – Текст: электронный // CyberEdge Group: [сайт]. 2023. – URL: https://cyberedgegroup.com/cdr/ (дата обращения: 14.06.2024).

11. NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million. – Текст: электронный // FORBES: [сайт]. 2017. – URL: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#586fa6c74f9a (дата обращения: 14.06.2024).

12. The State of Ransomware 2023. – Текст: электронный // SOPHOS: [сайт]. 2023. – URL: https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf (дата обращения: 14.06.2024).

13. IT threat evolution in Q3 2023. Mobile statistics. – Текст: электронный // Securelist by Kaspersky: [сайт]. 2023. – URL: https://securelist.com/it-threat-evolution-q3-2023-mobile-statistics/111224/ (дата обращения: 14.06.2024).

14. Эксперты оценили масштаб атак хакеров на пользователей Android в России. – Текст: электронный // RBC: [сайт]. 2024. – URL: https://www.rbc.ru/rbcfreenews/66271e9f9a7947df531fa12f (дата обращения: 14.06.2024).

15. Преодолеть цифровой колониализм. – Текст: электронный // Валдай: [сайт]. 2023. – URL: https://ru.valdaiclub.com/events/posts/articles/preodolet-tsifrovoy-kolonializm/ (дата обращения: 14.06.2024).

16. Цифровой разрыв. Чем он грозит России и каковы его масштабы?. – Текст: электронный // Национальный исследовательский университет «Высшая школа экономики»: [сайт]. 2021. – URL: https://iq.hse.ru/news/465308186.html (дата обращения: 14.06.2024).

17. Есть ли у России шанс победить в мировой кибервойне. – Текст: электронный // Московский комсомолец: [сайт]. 2022. – URL: https://www.mk.ru/politics/2022/03/13/est-li-u-rossii-shans-pobedit-v-mirovoy-kibervoyne.html (дата обращения: 14.06.2024).

18. Троян Н.А. Влияние цифровых технологий на повышение уровня культуры информационной безопасности граждан России / Н.А. Троян. – Текст: электронный // Мониторинг правоприменения. – 2023. – №1 (46). – URL: URL: https://cyberleninka.ru/article/n/vliyanie-tsifrovyh-tehnologiy-na-povyshenie-urovnya-kultury-informatsionnoy-bezopasnosti-grazhdan-rossii (дата обращения: 13.06.2024). С. 20-26.

19. Кибербезопасность. – Текст: электронный // Контртеррористическое управление ООН: [сайт]. 2017. – URL: https://www.un.org/counterterrorism/ru/cybersecurity (дата обращения: 14.06.2024).

20. Report of the Secretary-General Roadmap for Digital Cooperation JUNE 2020. – Текст: электронный // ООН: [сайт]. 2020. – URL: https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf (дата обращения: 14.06.2024).

21. Международно-политическое измерение цифрового разрыва. – Текст: электронный // Российский совет по международным делам (РСМД): [сайт]. 2021. – URL: https://russiancouncil.ru/analytics-and-comments/analytics/mezhdunarodno-politicheskoe-izmerenie-tsifrovogo-razryva/ (дата обращения: 14.06.2024).

The impact of digitalization on international relations: challenges and prospects

Ekaterina Grebenshchikova
Vladivostok State University
Russian Federation
Chernyshov Timofey
Vladivostok State University
Russian Federation, Vladivostok

Abstract

In the modern world, against the backdrop of the digital revolution, the digitalization process is becoming an integral component of international politics, economics and culture. The rapid development of information and communication technologies has a significant impact on international relations, introducing both challenges and opportunities. The purpose of this report is to analyze the impact of digitalization on international relations, identify challenges and prospects, as well as practical recommendations for effectively managing these processes. This report examines the impact of digitalization on the global stage, highlighting a number of challenges including cybersecurity, data privacy and the digital divide. At the same time, prospects are being identified, such as stimulating economic growth, deepening international cooperation, innovation in the fields of education and health, and increasing the level of international security. The report emphasizes that effectively managing digitalization requires cooperation and coordination at the international level. The report can offer practical recommendations for state and non-state actors to effectively manage digital challenges. In the context of cyberterrorism, national and international security measures are described, such as signing agreements and conducting training events for citizens. To reduce the digital divide, initiatives by the United Nations (UN) and other international organizations are being discussed to achieve universal Internet connectivity and reduce inequalities in access to information and communications technologies. Particular attention is paid to developing rules for responsible behavior of states in the information space, taking into account the risks of international information security and the interests of all parties. Static data is provided, expert assessments for 2024 are summarized, and analytical forecasts are given.

Keywords: digitalization, international relations, information and communication technologies, cybersecurity, international cooperation, information security, digital challenges, cyber terrorism, digital divide, information space, global arena, sustainable development, international organizations

Date of publication: 25.12.2024

Citation link:

Grebenshchikova E., Timofey C. The impact of digitalization on international relations: challenges and prospects // nauka.me. – 2024. – Issue 2.
URL: https://nauka.me/s0031752-7-1/. DOI: 10.18254/S241328880031752-1
