ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2226-7867-2025-15-2-50-55
УДК: 32.001:004.056(045)

Риски цифровой политики

М.Е. Левченко
Липецкий государственный технический университет, Липецк, Российская Федерация

АННОТАЦИЯ

Цифровизация политических процессов создает новые риски, оказывающие влияние как на стабильность политических институтов и управление, так и на граждан, и общественное мнение. Интернет стал огромным хранилищем различных данных, среди которых персональные сведения миллионов пользователей. К сожалению, такая информационная насыщенность оборачивается серьезной проблемой: регулярные утечки персональных данных делают граждан легкой мишенью для манипуляций, ставя под угрозу их цифровую и реальную безопасность. Киберугрозы, направленные на политические институты, могут привести к манипулированию результатами выборов, несанкционированному доступу к конфиденциальной информации и подрыву общественного доверия к демократическим процессам. В статье раскрыты подходы к исследованию рисков в области цифровой политики, проанализированы типологии рисков, произведен обзор основных цифровых рисков и угроз (доминируют кибератаки, несанкционированный доступ к данным), фейковых новостей и дезинформации. Сформулирована взаимосвязь между видами рисков в общем, цифровыми рисками в частности, примерами рисков, возможными негативными политическими последствиями, а именно подрывом целостности избирательной системы, эрозией демократии, компрометацией правительственных учреждений и ростом дипломатической напряженности. Правительствам и компаниям нужно поддерживать непрерывный процесс мониторинга и внедрять новые практики и технологии по минимизации цифровых рисков, а гражданам быть ответственнее при работе с персональными данными. Предметом дальнейших обсуждений в данной области может стать исследование общественного мнения граждан в вопросе доверия к государственным структурам в условиях цифровизации социальных, экономических и политических процессов.

Ключевые слова: цифровая политика; цифровой риск; утечки информации; политические последствия; цифровизация; кибератака; манипулирование избирателями

***Для цитирования*: Левченко М.Е. Риски цифровой политики. *Гуманитарные науки. Вестник Финансового университета*. 2025;15(2):50-55. DOI: 10.26794/2226-7867-2025-15-2-50-55**

ORIGINAL PAPER

Risks of Digital Policy

M.E. Levchenko
Lipetsk State Technical University, Lipetsk, Russian Federation

ABSTRACT

The digitalization of political processes creates new risks that can affect both the stability of political institutions and governance, as well as citizens and public opinion. The Internet has become a huge repository of various data, including personal information of millions of users. Unfortunately, such information saturation turns into a serious problem: regular leaks of personal data make citizens an easy target for manipulation, threatening their digital and real security. Cyber threats aimed at political institutions can lead to manipulation of election results, unauthorized access to confidential information and the undermining of public trust in democratic processes. The article reveals approaches to the study of risks in the field of digital policy, analyzes risk typologies, provides an overview of the main digital risks and threats, among which cyber attacks, unauthorized access to data, fake news and disinformation dominate. The relationship between the types of risks in general, digital risks in particular, examples of risks, possible negative political consequences are formulated, namely undermining the integrity of the electoral system, eroding democracy, compromising state institutions and increasing diplomatic tensions. Governments and companies need to maintain a continuous process of monitoring and implementing new practices and technologies to minimize digital risks, and citizens need to be more responsible when working with personal data. The subject of further discussions in this area may be a study of public opinion on the issue of trust in government agencies in the context of digitalization of social, economic and political processes.

Keywords: digital politics; digital risk; information leaks; political consequences; digitalization; cyberattack; voter manipulation

***For citation*: Levchenko M.E. Risks of digital policy. *Humanities and Social Sciences. Bulletin of the Financial University*. 2025;15(2):50-55. DOI: 10.26794/2226-7867-2025-15-2-50-55**

ВВЕДЕНИЕ

В непрерывном процессе цифровизации всех сфер жизни вопросы безопасности в области цифровой политики приобретают первостепенное значение. Вместе с новыми возможностями и преимуществами цифровые технологии несут в себе и значительные риски, и, как следствие, негативные последствия при их наступлении.

Интернет — глобальное хранилище различных данных, включая персональные сведения миллионов пользователей. К сожалению, такая информационная насыщенность оборачивается серьезной проблемой: регулярные утечки персональных данных делают граждан легкой мишенью для мошеннических манипуляций, ставя под угрозу их цифровую и реальную безопасность.

Киберугрозы, направленные на политические институты, могут привести к манипулированию результатами выборов, несанкционированному доступу к конфиденциальной информации и подрыву общественного доверия к демократическим процессам.

Цель настоящей статьи — исследование влияния цифровых рисков на политическую сферу. Задачи исследования: раскрыть подходы к исследованию рисков в области цифровой политики; соотнести цифровые риски и возможные политические последствия при их наступлении.

ПОДХОДЫ К ИССЛЕДОВАНИЮ ЦИФРОВОЙ ПОЛИТИКИ

Цифровизация — мировая тенденция сбора, накопления и обработки информации — позволяет решать многие задачи быстрее, удобнее, эффективнее, и национальные правительства поддерживают данный процесс на всех уровнях общества и отраслях экономики. Однако внедрение цифровых технологий влечет за собой появление уязвимостей и, как следствие, рисков, которые необходимо вовремя предотвращать. Несмотря на то, что процесс цифровизации этапов избирательного процесса начался относительно давно, внедрение новых технологий требует постоянной адаптации существующих методов управления рисками и исследования данной области научным сообществом.

Связь между демократией и избирателями, а также негативную тенденцию в применении цифровых медиа-платформ в политических целях отмечает исследователь Х. Унвер [1]. Такие ученые, как И. Линьков, Б.Д. Трамп, К. Пуансатте-Джонс, М. Флорин анализируют стратегии управления цифровизацией и подчеркивают, что правительства различных стран до сих пор не пришли к единому мнению в данном вопросе [2]. Исследования Е. Трере выявили использование цифровых инструментов партиями Мексики для саботажа, незаконного сбора данных и угроз активистам. Исследователь относит цифровые технологии к области высокого риска [3].

Цифровая политика — это совокупность действий, направленных на регулирование процессов цифровой трансформации общества и цифровизации, включая управление данными, обеспечение кибербезопасности, развитие цифровой экономики, защиту прав пользователей, а также использование цифровых технологий для разработки политических решений и коммуникации. Так, например, В.К. Левашов и О.В. Гребняк отмечают трансформационный потенциал цифрового управления в Российской Федерации [4, с. 80], а в Уругвае цифровая политика является инструментом «повышения эффективности управления результативностью государственной деятельности» [5, с. 59].

Развитие цифровой политики тесно связано с внедрением инновационных технологий, что создает не только новые возможности, но и определенные угрозы. В этом контексте важно учитывать понятие «цифровой риск».

Отечественные исследователи А.И. Рудской, А.И. Боровиков, П.И. Романов и О.В. Колосова описывают данный термин как негативные последствия, связанные с внедрением новых технологий [6], а зарубежные — Ф. Курти, Д. Герлах, С. Казинник — как риск потерь в результате цифровых инцидентов, вызванных как внутренними, так и внешними факторами, включая третьих лиц [7].

Е.В. Янченко описывает «цифровой риск» как «термин, охватывающий все цифровые возможности, обусловливаемый ИКТ, автоматизацией обработки данных, автоматизацией решений» и отмечает, что «к цифровым рискам приводит использование цифровых технологий» [8, с. 2247].

Испанский исследователь Х. Фернандес делает вывод, что цифровые риски — это угроза не только для кибербезопасности. Он отмечает, что «под цифровыми рисками понимаются все преобразования, вызванные цифровизацией, которые могут угрожать основным аспектам нашей текущей жизни в экономическом, политическом или социальном плане» [9, с. 4].

Основываясь на представленном обзоре источников, можно сделать вывод, что цифровые риски — это угрозы и негативные последствия, возникающие из-за внедрения и использования цифровых технологий. Влияние цифровых рисков распро-

страняется не только на кибербезопасность, но и на экономические, политические и социальные аспекты жизни.

ЦИФРОВЫЕ РИСКИ И ИХ ВЛИЯНИЕ НА ПОЛИТИЧЕСКУЮ СФЕРУ

Цифровизация политических процессов создает новые риски, которые могут повлиять как на стабильность политических институтов и управление, так и на граждан и общественное мнение. С одной стороны, цифровые риски для политики должны обладать соответствующей спецификой, но с другой стороны, правильным будет рассмотреть риски, свойственные обычным организациям, и на их основе сформулировать область рисков для политической сферы.

Так, Е.В. Янченко выделяет наиболее важными «следующие виды рисков и угроз в деятельности организации: стратегические, технологические, операционные, сторонние, нормативные, кибернетические, риски устойчивости, утечки данных, конфиденциальности» [8, с. 2248]. А.В. Тимченко считает, что преобладающим цифровым риском является «недостаточный уровень оценки возможных угроз со стороны системы государственного управления, и как следствие — недостаточную динамику их отражения в текущей повестке государственной политики» [10, с. 103].

Кибератаки — одна из главных угроз для правительства: политические партии, избирательные системы — основные мишени для хакеров, чья основная цель — конфиденциальные данные или дестабилизация работы информационных систем. К.Ф. Азубуике отмечает, что спуфинг в большинстве своем поддерживается государствами [11], а по мнению Р. Шендлера, нападения хакеров влекут значительные социальные риски и снижение доверия к правительству [12].

Другой способ влияния на политику — дезинформация, направленная в первую очередь на граждан и избирателей, основная цель которой — распространение ложной или вводящей в заблуждение информации через медиа. Исследование[1] Оксфордского университета в 2019 г. показало, что количество стран, где организованы кампании по манипулированию социальными сетями, выросло с 28 до 70 за период 2017–2019 гг.

Проблема влияния на избирательный процесс ярко выражается в публикациях профильных специалистов. В докладе[2] спецпрокурора Р. Мюллера о российском вмешательстве в выборы президента США в 2016 г. не доказано влияние России на избирательный процесс США, а доклад[3] А. Манойло, посвященный вмешательству США в избирательный процесс России, содержит весомые аргументы (описаны конкретные механизмы давления) это подтверждающие.

Т.Л. Каминская отмечает, что «наибольшую эффективность в плане влияния на ценности общества и коммуникативное поведение в социуме» оказывает распространение через социальные сети, мессенджеры и блоги адаптированной для аудитории платформы информации. Эффект такой коммуникации может привести к «переходу из цифрового активизма в оффлайн в виде протестных митингов и флэшмобов» [13, с. 100]. Если учитывать данное предположение, то распространение фейковой информации может нанести вред как государству, так и простым гражданам, которые не будут знать реальных целей протестной акции.

В процессе цифровизации повышается риск несанкционированного доступа к персональным данным. Отечественный исследователь А.С. Селюк отмечает, что в 2022 г. в России зафиксировано рекордное количество утечки персональной информации, а также приводит статистику преступлений с использованием цифровых технологий, исходя из которой наблюдается «низкая степень раскрываемости таких преступлений» [14].

Несмотря на подобные инциденты, согласно аналитическому отчету[4] Экспертно-Аналитического центра InfoWatch доля России в мировом распределении утечек сократилась почти в два раза (с 10,8 до 5,7%), а более трети всех утечек в мире произошли в США.

На основе рассмотренных рисков автором настоящей статьи приводится соотношение цифровых рисков и наступление возможных полити-

[1] Bradshaw S., Howard P.N. The global disinformation order: 2019 global inventory of organised social media manipulation // Oxford: University of Oxford, 2019. URL: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf

[2] Mueller R.S. III. Report on the Investigation into Russian Interference in the 2016 Presidential Election, Volumes I and II (Redacted Version of April 18, 2019). Washington, D.C.: U.S. Department of Justice, 2019. 449 с.

[3] Манойло А.В. Вторжение. Вмешательство США в выборы в Российской Федерации в ходе президентских кампаний 1996–2018 гг. Доклад. 2018. 40 с.

[4] Аналитический отчет: исследование утечек информации в мире за 2022–2023 гг. 2024. 23 с. URL: https://www.infowatch.ru/sites/default/files/analytics/files/issledovaniye-utechek-informatsii-v-mire-za-2022-2023-gody.pdf

ческих последствий (см. *таблицу*). Виды рисков и ключевые области управления основаны на типологии Е.В. Янченко, но автор добавил этический и социальный виды риска.

ВЫВОДЫ

С каждым годом количество новых технологий и угроз в области цифровой политики будет возрастать. Правительствам и компаниям нужно под-

Таблица / Table

Влияние цифровых рисков на политические последствия / Impact of Digital Risks on Policy Implications

Вид риска / Type of risk [8, с. 2248]	**Цифровой риск / Digital risk**	**Пример / Example**	**Политические последствия / Political implications**	**Область управления / Management area**
Кибернетические (киберпространство)	Кибератака на избирательную систему	Взлом демократического национального комитета США (2016). Взлом предвыборной кампании Э. Макрона (2017)	Подрыв целостности избирательных систем. Эрозия демократии. Дипломатическая напряженность	«Укрепление платформы, сетевой архитектуры; безопасность приложений; управление уязвимостями и мониторинг безопасности»
Утечка данных	Нарушения конфиденциальности данных	Утечки данных в РФ (2022). Cambridge Analytica (2018)	Внедрение более строгих законов о защите данных. Общественный резонанс. Нагрузка на правоохранительную систему	«Обеспечение защиты данных в цифровой экосистеме на различных этапах жизненного цикла; области управления фокусом будут касаться классификации, хранения, обработки, шифрования данных и т.д.»
	Кибершпионаж	Атака на SolarWinds (2020)	Компрометация правительственных учреждений	
Этические / социальные риски	Кампании по дезинформации	Вмешательство в выборы США (2016). Референдум по Brexit (2016)	Манипулирование поведением избирателей. Поляризация общества. Сомнение избирателей в легитимности результатов выборов	Мониторинг СМИ, сотрудничество с платформами, аутентификация контента, разработка плана реагирования на кризисные ситуации
	Дипфейки	Использование дипфейков в политических кампаниях	Ущерб репутации. Дезинформация избирателей	

Источник / Sourse: составлено автором / complied by the author.

держивать непрерывность процесса мониторинга и совершенствовать технологии по минимизации цифровых рисков, а гражданам быть внимательнее с хранением и размещением персональных данных.

В статье раскрыты подходы к исследованию рисков в области цифровой политики, проанализированы типологии рисков, произведен обзор основных цифровых рисков и угроз, среди которых доминируют кибератаки, несанкционированный доступ к данным, фейковые новости и дезинформация.

Проведенное исследование помогло выявить взаимозависимость между видами рисков в общем и цифровыми рисками в частности, проанализировать примеры рисков и возможные от них негативные политические последствия (подрыв целостности избирательной системы, эрозию демократии, компрометацию правительственных учреждений и рост дипломатической напряженности).

Предметом дальнейших обсуждений в данной области может стать исследование общественного мнения граждан в вопросе доверия к государственным структурам в условиях цифровизации социальных, экономических и политических процессов.

СПИСОК ИСТОЧНИКОВ

1. Unver H.A. Digital challenges to democracy: Politics of automation, attention, and engagement. *Journal of International Affairs*. 2017;71(1);127-146. URL: https://www.jstor.org/stable/26494368
2. Linkov I., Trump B.D., Poinsatte-Jones K., Florin M.-V. Governance strategies for a sustainable digital world. *Sustainability*. 2018;10(2);1-13. DOI: 10.3390/su10020440
3. Treré E. The dark side of digital politics: Understanding the algorithmic manufacturing of consent and the hindering of online dissidence. *IDS Bulletin*. 2016;47(1);127-138. DOI: 10.19088/1968-2016.111
4. Левашов В.К., Гребняк О.В. Цифровая культура российского общества и государства. *Социологические исследования*. 2020;5;79-89. DOI: 10.31857/S 013216250009401-4
5. Неверов К.А. Интероперабельность как рекурсивный процесс: цифровая платформа Уругвая. *Латинская Америка*. 2021;4;56-68. DOI: 10.31857/S 0044748X0013483-0
6. Рудской А.И., Боровков А.И., Романов П.И., Колосова О.В. Пути снижения рисков при построении в России цифровой экономики. Образовательный аспект. *Высшее образование в России*. 2019;28(2);9-22. DOI: 10.31992/0869-3617-2019-28-2-9-22
7. Curti F., Gerlach J., Kazinnik S. Cyber risk definition and classification for financial risk management. *Journal of Operational Risk*. 2023;18(2);28-37. DOI: 10.21314/JOP.2022.036
8. Янченко Е.В. Риски организации в условиях цифровизации экономики. *Креативная экономика*. 2022;16(6);2239-2256. DOI: 10.18334/ce.16.6.114838
9. Fernández J.V. The risk of digitalization: Transforming government into a digital Leviathan. *Indiana Journal of Global Legal Studies*. 2023;30(1)3-13. DOI: 10.2979/gls.2023.a886160
10. Тимченко А.В. Риски и угрозы тотальной цифровизации: возможности и потенциал управляемости. *Российский журнал правовых исследований*. 2022;9(1);99-106. DOI: 10.17816/Rjls99747
11. Azubuike C.F. Cyber security and international conflicts: an analysis of state-sponsored cyber attacks. *Nnamdi Azikiwe Journal of Political Science*. 2023;8(3);101-114. URL: https://najops.org.ng/index.php/najops/article/view/70
12. Shandler R., Gomez M.A. The hidden threat of cyber-attacks: Undermining public confidence in government. *Journal of Information Technology & Politics*. 2023;20(4);359-374. DOI: 10.1080/19331681.2022.2112796
13. Каминская Т.Л. Ответственность за медиаконтент и проблема цензурирования коммуникационного пространства России. *Гуманитарные науки. Вестник Финансового университета*. 2021;11(2):96-101. DOI: 10.26794/2226-7867-2021-11-2-96-101
14. Селюк А.С. Защита персональных данных в цифровом пространстве. *Вестник Университета имени О.Е. Кутафина*. 2023;2(102);110-119. DOI: 10.17803/2311-5998.2023.102.2.110-119

REFERENCES

1. Unver H.A. Digital challenges to democracy: Politics of automation, attention, and engagement. *Journal of International Affairs*. 2017;71(1):127-146. URL: https://www.jstor.org/stable/26494368
2. Linkov I, Trump B.D, Poinsatte-Jones K, Florin M.V. Governance strategies for a sustainable digital world. *Sustainability*. 2018;10(2):1-13. DOI: 10.3390/su10020440

3. Treré E. The dark side of digital politics: Understanding the algorithmic manufacturing of consent and the hindering of online dissidence. *IDS Bulletin*. 2016;47(1);127-138. DOI: 10.19088/1968-2016.111
4. Levashov V.K., Grebnyak O.V. Digital culture of Russian society and state. *Sociological Studies*. 2020;5;79-89. (In Russ.). DOI: 10.31857/S 013216250009401-4
5. Neverov K.A. Interoperability as a recursive process: Uruguay's digital platform. *Latin America*. 2021;4;56-68. (In Russ.). DOI: 10.31857/S 0044748X0013483-0
6. Rudskoy, A.I., Borovkov, A.I., Romanov, P.I., Kolosova, O.V. Ways to reduce risks when building the digital economy in Russia. Educational aspect. *Higher Education in Russia*. 2018;28(2);9-22. (In Russ.). DOI: 10.31992/0869-3617-2019-28-2-9-22
7. Curti F., Gerlach J., Kazinnik S. Cyber risk definition and classification for financial risk management. *Journal of Operational Risk*. 2023;18(2):28-37. DOI: 10.21314/JOP.2022.036
8. Yanchenko E.V. Riski organizatsii v usloviyakh tsifrovizatsii ekonomiki: Enterprise's risks amidst digitalization. *Creative economy*. 2022;16(6):2239-2256. (In Russ.). DOI: 10.18334/ce.16.6.114838
9. Fernández J.V. The risk of digitalization: Transforming government into a digital Leviathan. *Indiana Journal of Global Legal Studies*. 2023;30(1):3-13. DOI: 10.2979/gls.2023.a886160
10. Timchenko A.V. Risks and threats of total digitalization: Opportunity and manageability level. *Russian journal of legal studies*. 2022;9(1):99-106. (In Russ.). DOI: 10.17816/Rjls99747
11. Azubuike C.F. Cyber security and international conflicts: an analysis of state-sponsored cyber attacks. *Nnamdi Azikiwe Journal of Political Science*. 2023;8(3):101-114. URL: https://najops.org.ng/index.php/najops/article/view/70
12. Shandler R., Gomez M.A. The hidden threat of cyber-attacks — undermining public confidence in government. *Journal of Information Technology & Politics*. 2023;20(4):359-374. DOI: 10.1080/19331681.2022.2112796
13. Kaminskaya T.L. Responsibility for media content and the problem of censoring the communication space of Russia. *Humanities and Social Sciences. Bulletin of the Financial University*. 2021;11(2):96-101 (In Russ.). DOI: 10.26794/2226-7867-2021-11-2-96-101
14. Selyuk A.S. Protection of personal data in the digital space. *Courier of Kutafin Moscow State Law University*. 2023;(2):110-119. (In Russ.). DOI: 10.17803/2311-5998.2023.102.2.110-119

ИНФОРМАЦИЯ ОБ АВТОРЕ / ABOUT THE AUTHOR

Михаил Евгеньевич Левченко — аспирант, научная специальность «Политические институты, процессы, технологии», Липецкий государственный технический университет, Липецк, Российская Федерация
Mikhail E. Levchenko — postgraduate student, scientific speciality "Political Institutions, Processes, Technologies", Lipetsk State Technical University, Lipetsk, Russian Federation
https://orcid.org/0009-0002-5782-9939
lme@asp48.ru

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.
Conflicts of Interest Statement: The author has no conflicts of interest to declare.

Статья поступила 24.05.2025; принята к публикации 02.06.2025.
Автор прочитал и одобрил окончательный вариант рукописи.
The article was received 24.05.2025; accepted for publication 02.06.2025.
The author read and approved the final version of the manuscript.