Государственное и муниципальное управление. Ученые записки. 2025. № 4. С. 218–224
State and Municipal Management. Scholar Notes. 2025;(4):218–224

Научная статья
УДК 32+352+004
EDN NNKHSH

Кибербезопасность в органах местного самоуправления: системный обзор и анализ основных проблем

Екатерина Ильинична Хубулури

Ростовский государственный университет путей сообщения, Ростов-на-Дону, Россия,
ehubuluri@yandex.ru, https://orcid.org/0000-0002-4005-8712

Аннотация

Введение. Кибербезопасность стала важнейшей проблемой в современном городском управлении, поскольку местные органы власти теперь не только отвечают за управление традиционной инфраструктурой, но и обеспечивают защиту цифровых систем и данных граждан во всё более цифровизированных «умных» городах. Несмотря на важность надёжных мер кибербезопасности, существует серьёзная проблема: местные органы власти зачастую недостаточно подготовлены к противодействию растущим киберугрозам. Это несоответствие подчёркивает необходимость всестороннего изучения проблем, препятствующих эффективной кибербезопасности в местных органах власти.

Цель. Выявить важнейшие проблемы в сфере обеспечения кибербезопасности, с которыми сталкиваются местные органы власти, а также сформулировать конкретные рекомендации, которые помогут городским политикам, администраторам и исследователям повысить устойчивость к киберугрозам в этой важной, но малоизученной области.

Методы. В исследовании используется системный обзор литературы с использованием трехэтапной методики PRISMA (предпочтительные элементы отчетности для системных обзоров и метаанализов).

Результаты. В ходе системного анализа мы выявили и классифицировали основные проблемы, препятствующие принятию эффективных мер по обеспечению кибербезопасности в местных органах власти. Проблемы перечислены в порядке убывания частоты их упоминания в литературе. Этот рейтинг отражает распространенность и предполагаемое влияние каждой проблемы в контексте кибербезопасности местных органов власти.

Выводы. Среди множества выявленных проблем наиболее распространёнными оказались явная нехватка финансирования и дефицит квалифицированных кадров. Эти проблемы не только часто упоминаются в существующей литературе, но и усугубляются жёсткими бюджетными ограничениями, в рамках которых обычно работают местные органы власти. Еще одной серьезной проблемой для местных органов власти является отсутствие надежной политики в области кибербезопасности или нормативных требований, учитывающих уникальные потребности местных органов власти. Отсутствие стандартизированных систем управления кибербезопасностью в местных органах власти препятствует разработке и реализации эффективных стратегий безопасности, что приводит к несогласованности в вопросах кибербезопасности между различными ведомствами. По мере того как мы все глубже погружаемся в эпоху цифровых технологий, безопасность нашей цифровой инфраструктуры становится синонимом безопасности наших сообществ. Следовательно, необходимо в срочном порядке пересмотреть подход к кибербезопасности и рассматривать её не как необязательные расходы, а как важнейшую инвестицию в общественную безопасность и доверие. Таким образом, требуется принятие незамедлительных мер в нескольких ключевых областях. Во-первых, необходимо стратегически перераспределить бюджеты, чтобы обеспечить принятие необходимых мер по кибербезопасности. Во-вторых, следует уделить первоочередное внимание разработке и внедрению комплексной политики кибербезопасности. В-третьих, необходимо развивать сотрудничество как внутри государственных структур, так и между ними, а также с частным и академическим секторами. Такое сотрудничество может привести к объединению ресурсов, обмену опытом и разработке экономически эффективных решений.

Ключевые слова: кибербезопасность, киберугроза, местное самоуправление, муниципалитет, городское управление, государственные структуры, местные органы власти, общественная безопасность
Для цитирования: Хубулури Е. И. Кибербезопасность в органах местного самоуправления: системный обзор и анализ основных проблем // Государственное и муниципальное управление. Ученые записки. 2025. № 4. С. 218–224. EDN NNKHSH

Original article

Cybersecurity in local governments: a systematic review and analysis of key issues

Ekaterina I. Hubuluri

Rostov State Transport University, Rostov-on-Don, Russia,
ehubuluri@yandex.ru, https://orcid.org/0000-0002-4005-8712

Abstract

Introduction. Cybersecurity has become a major issue in modern urban governance, as local governments are now not only responsible for managing traditional infrastructure, but also ensuring the protection of digital systems and citizens' data in increasingly digitalized smart cities. Despite the importance of reliable cyber security measures, there is a serious problem: local governments are often insufficiently prepared to counter growing cyber threats. This discrepancy highlights the need for a comprehensive study of the issues that hinder effective cybersecurity in local governments.

Purpose. To give an idea of the most important cybersecurity issues faced by local authorities, as well as formulate specific recommendations that will help city politicians, administrators and researchers to increase resilience to cyber threats in this important but little-studied area.

Methods. This study uses a systematic literature review using the three-step PRISMA methodology (Preferred Reporting Elements for and Meta-analyses).

Results. In the course of a systematic analysis, we have identified and classified the main significant problems that hinder the adoption of effective cybersecurity measures in local authorities. The problems are listed in descending order of the frequency of their mention in the literature. This ranking reflects the prevalence and perceived impact of each issue in the context of local government cybersecurity.

Conclusions. Among the many problems identified, the most common were a clear lack of funding, a shortage of qualified personnel, and a lack of cybersecurity policies or regulatory requirements. These problems are not only frequently mentioned in the existing literature, but are also compounded by the tight budget constraints under which local governments usually operate. Another major challenge for local governments is the lack of robust cybersecurity policies or regulatory requirements that address the unique needs of local governments. The lack of standardized cybersecurity management systems in local governments hinders the development and implementation of effective security strategies, leading to inconsistencies in cybersecurity issues between different agencies. As we move deeper into the digital age, the security of our digital infrastructure is becoming synonymous with the security of our communities. Therefore, it is urgently necessary to rethink the approach to cybersecurity and consider it not as an unnecessary expense, but as an essential investment in public safety and trust. Therefore, immediate action is required in several key areas. First, it is necessary to strategically reallocate budgets to ensure that the necessary cybersecurity measures are taken. Secondly, priority should be given to the development and implementation of a comprehensive cybersecurity policy. Thirdly, it is necessary to develop cooperation both within and between government agencies, as well as with the private and academic sectors. Such cooperation can lead to pooling resources, sharing experiences, and developing cost-effective solutions.

Keywords: cybersecurity, cyber threat, local government, municipality, city government, government agencies, local authorities, public safety

For citation: Hubuluri E. I. Cybersecurity in local governments: a systematic review and analysis of key issues. *State and Municipal Management. Scholar Notes.* 2025;(4):218–224. (In Russ.). EDN NNKHSH

Введение

Экспоненциальный технологический прогресс нашего времени, наряду с огромными преимуществами, также несёт в себе значительные риски для пользователей и общества в целом. Кибербезопасность – одна из наиболее значимых социально-технологических проблем, с которыми в настоящее время сталкиваются практически все государственные учреждения независимо от их типа и размера. Местные органы власти, играющие ключевую роль в городском управлении, особенно уязвимы для угроз кибербезопасности среди государственных организаций из-за ограниченного бюджета на информационные технологии (ИТ) и непоследовательных мер безопасности. Эти ограничения приводят к использованию устаревших систем и отсутствию комплексной киберподготовки сотрудников, что повышает риск утечки данных и подрывает доверие общественности. По мере того как эти организации продвигают инициативы по созданию «умных» городов, взаимосвязанность городских цифровых систем ещё больше повышает их уязвимость.

Цифровая трансформация местных органов власти все чаще подвергает их риску с точки зрения кибербезопасности. Многочисленные исследования указывают на рост частоты и серьезности кибератак, что в последние годы стало серьезной проблемой для местных органов власти. В своём новаторском исследовании Дегтерев Д.А., Рамич М.С. и др. выяснили, насколько распространены проблемы с кибербезопасностью в органах местного самоуправления [1]. Результаты исследования показывают, что органы местного самоуправления постоянно подвергаются частым кибератакам. Около 28% органов местного самоуправления подвергались ежечасным или более частым кибератакам, а 19% – атакам хотя бы раз в день.

Несмотря на растущее число угроз для местных органов власти, существует огромный пробел в знаниях о конкретных проблемах и решениях, типах и методах атак, инструментах, а также доступных платформах и стандартах для местных органов власти в вопросах кибербезопасности. Недостаток научных исследований также заметен во многих статьях, рассмотренных в рамках данного исследования. В своём исследовании Зиновьева Е.С. указала, что за период с 2000 по середину 2021 г. ей удалось найти только три статьи, в которых конкретно рассматривались кибератаки на местные органы власти [2]. Так же она отметила, что «несмотря на признанную необходимость внедрения стратегий кибербезопасности и правовых норм, до сих пор проводилось мало исследований, подтверждающих эффективность принятых решений на практике или анализирующих реальные примеры киберпреступлений в государственных учреждениях, особенно на уровне местных органов власти» [3]. В большинстве существующих статей используется описательный подход: авторы фокусируются на значимости и распространённости киберугроз, не предлагая теоретических основ или эмпирически обоснованных стратегий для понимания проблем кибербезопасности.

Исследователи выявили серьёзную нехватку комплексных структур управления, включающих в себя политику, стандартизированные практики, обучение кибербезопасности и стратегии восстановления, которые имеют решающее значение для обеспечения надёжной кибербезопасности. Они рекомендуют обратить внимание на эти проблемы управления как на важный шаг на пути к укреплению кибербезопасности местных органов власти [4]. Основываясь на этих рекомендациях, данное исследование использует системный обзор литературы для тщательного выявления и анализа проблем в сфере кибербезопасности, с которыми сталкиваются местные органы власти как с технической точки зрения, так и с точки зрения управления городским хозяйством, а также для выработки рекомендаций. При этом рассматривается следующий исследовательский вопрос: с какими конкретными проблемами сталкиваются местные органы власти при внедрении эффективной системы кибербезопасности и какие практические меры могут помочь решить эти проблемы. В ходе обзора литературы выявляются соответствующие научные статьи в области кибербезопасности и местного самоуправления, после чего проводится их тщательный анализ и критическая оценка [5]. Наконец, анализ и обзор приводят к обсуждению и формулированию выводов.

Методы

В исследовании используется системный обзор литературы с использованием трехэтапной методики PRISMA (Предпочтительные элементы отчетности для системных обзоров и метаанализов). Первый этап (планирование) применения PRISMA включает в себя формулировку цели исследования, исследовательских вопросов, списка ключевых слов, а также критериев включения и исключения статей. Второй этап (проведение обзора) предполагает изучение соответствующих статей, а третий этап (отчётность и распространение) включает в себя анализ и обобщение результатов.

Результаты и обсуждение

Академическое внимание к вопросам кибербезопасности в местных органах власти началось в 2012 г., что совпало с двумя параллельными, но взаимосвязанными явлениями. Во-первых, в этот период произошёл стремительный технологический подъём, связанный с развитием облачных вычислений, аналитики данных и устройств Интернета. Местные органы власти активно внедряли эти технологии для повышения операционной эффективности, улучшения качества государственных услуг и расширения участия граждан.

Отсутствие комплексной политики и руководящих принципов является серьёзной проблемой в сфере кибербезопасности для местных органов власти. Муниципалитеты, у которых есть официальная политика в области кибербезопасности, лучше справляются с управлением конфиденциальной информацией доступом, проведением плановых проверок и операций по обеспечению безопасности, а также с обучением своих сотрудников в области кибербезопасности. В исследовании, в котором участвовала фокус-группа экспертов в области информационных технологий и кибербезопасности, исследователи назвали политику в области кибербезопасности ключевым фактором в обеспечении стратегических и единообразных мер по обеспечению кибербезопасности в местных органах власти. Аналогичным образом Понька Т.И., Рамич М.С. и др. в своём исследовании, посвящённом местному самоуправлению в КНР, подчеркнули важность нормативно-правовой базы для обеспечения кибербезопасности местных органов власти [6]. Более того, недостатки в политике могут привести к несогласованности в вопросах контроля доступа, нарушению целостности и поставить под угрозу критически важные системы и доступность данных.

Вопросы регулирования также являются серьёзной проблемой для обеспечения кибербезопасности местных органов власти. Важной проблемой является недостаточная осведомлённость местных органов власти о вопросах кибербезопасности и их влияние на эти вопросы, что приводит к разрыву между разработкой политики и её практической реализацией. Такая недостаточная прозрачность может привести к недостаточному выделению ресурсов и вниманию к вопросам кибербезопасности, в результате чего местные органы власти становятся уязвимыми для киберугроз. Недостаточная политическая и бюрократическая поддержка также существенно затрудняет разработку и внедрение эффективных мер кибербезопасности.

Кроме того, крайне важно уделять приоритетное внимание кибербезопасности на руководящем уровне. Без поддержки со стороны вышестоящих должностных лиц инициативы в области кибербезопасности не будут набирать обороты. Несогласованность в работе по соблюдению нормативных требований и недостаточное понимание этих требований могут препятствовать созданию комплексной системы кибербезопасности. Местным органам власти приходится ориентироваться в сложной системе законов и нормативных актов, зачастую не имея достаточных ресурсов и опыта. Отсутствие контроля и соблюдения политики и практик в области кибербезопасности может привести к неэффективным стратегиям и формированию в организации культуры безразличия к рискам в сфере кибербезопасности.

Политика в области кибербезопасности должна содержать подробные разделы, в которых описывается позиция местных органов власти в отношении кибербезопасности, определяются роли, обязанности и стандарты, соответствующие принципам кибербезопасности, а также регулярно пересматриваться и обновляться, чтобы соответствовать динамичному ландшафту угроз. Местные органы власти могут сотрудничать с научными учреждениями для разработки политики и стандартов в области кибербезопасности, учитывая ограниченность своих ресурсов. Такое сотрудничество должно гарантировать, что политика местных органов власти в области кибербезопасности будет соответствовать политике «умных городов», обеспечивая единый подход к борьбе с киберугрозами и их эффективное устранение [7].

Исследователи часто ссылаются на ограниченность ресурсов, особенно с точки зрения бюджетных ассигнований, как на одну из основных проблем, препятствующих развитию кибербезопасности в местных органах власти. Исследователи назвали несколько причин ограниченного финансирования этого сектора.

Во-первых, ошибочное представление о киберугрозах – о том, что эти небольшие государственные организации не являются основными целями киберпреступников, – является одним из основных факторов, способствующих недостаточному финансированию кибербезопасности. Такое представление обычно возникает из-за нерегулярного информирования избранных лидеров и лиц,

принимающих решения, о нарушениях кибербезопасности [8]. Во-вторых, сложная и динамичная природа кибербезопасности с постоянно меняющимся ландшафтом угроз и мерами противодействия может обескураживать. В-третьих, местные органы власти часто работают в условиях жёстких финансовых ограничений, и кибербезопасность остаётся «менее значимой» в списке конкурирующих приоритетов по сравнению с другими обязанностями, требующими финансовых вложений. Кибербезопасность, будучи относительно новой сферой, часто не получает должного внимания и финансирования. Учитывая все эти сложности, можно прийти к выводу, что не стоит инвестировать без чёткого понимания окупаемости таких вложений, особенно если преимущества, такие как сохранение конфиденциальности данных, неосязаемы и часто остаются незамеченными.

Бюджетные ограничения оказывают каскадный эффект на общее состояние кибербезопасности местных органов власти и вызывают множество других проблем. Дефицит бюджета не только препятствует найму высококвалифицированных специалистов по кибербезопасности из-за невозможности обеспечить конкурентоспособную заработную плату, но и ограничивает важнейшие инициативы в области обучения и повышения компетентности. Кроме того, эти бюджетные ограничения существенно ограничивают возможности инвестирования в исследования и разработки в области кибербезопасности, из-за чего местные органы власти становятся уязвимыми перед возникающими киберугрозами.

Местные органы власти часто сталкиваются с техническими и инфраструктурными проблемами в своих экосистемах кибербезопасности. Эта проблема, во многом обусловленная бюджетными ограничениями, проявляется по-разному. Бюджетные ограничения часто вынуждают эти организации полагаться на устаревшие механизмы безопасности. Финансовые ограничения также препятствуют модернизации инфраструктуры безопасности и внедрению передовых инструментов кибербезопасности. Каждое слабое звено, будь то устаревшее программное обеспечение или непропатченная сеть, является потенциальной точкой входа для кибератак. Поэтому местные органы власти не должны пренебрегать распределением бюджета в пользу обеспечения кибербезопасности или идти на компромисс в этом вопросе [9].

Местные органы власти сталкиваются с всё более сложными техническими и операционными проблемами, особенно в борьбе со сложными и изощрёнными киберугрозами. Недостаток знаний о виртуальной среде у сотрудников и лиц, принимающих решения, ещё больше усугубляет эту уязвимость. Этот недостаток проявляется не только в общей неосведомлённости о кибербезопасности среди сотрудников, не связанных с информационными технологиями, но и в отсутствии конкретных технических знаний, необходимых ИТ-специалистам в местных органах власти. Крайне важно понимать нюансы управления типами данных, знать подходящие инструменты для их обработки, хранения и обслуживания, а также разбираться в распространённых кибератаках и инструментах, необходимых для их предотвращения. Каждая категория данных имеет свои уникальные уязвимые места, требующие разного уровня защиты [10].

Например, персональные данные могут быть уязвимы для кражи личных данных, а инфраструктурные данные могут привести к сбоям в работе жизненно важных служб. Понимание различных типов киберугроз также крайне важно для ИТ-специалистов, чтобы они могли правильно расставить приоритеты в мерах по обеспечению кибербезопасности, особенно учитывая их постоянно меняющийся характер. Например, программы-вымогатели могут шифровать данные, а утечка данных приводит к раскрытию конфиденциальной информации. Фишинговые схемы могут обманом заставить сотрудников раскрыть свои пароли или перейти по вредоносным ссылкам. Инструменты и методы, предназначенные для борьбы с этими угрозами, варьируются от брандмауэров и антивирусного ПО до систем обнаружения вторжений и алгоритмов машинного обучения [11].

Сотрудничество с научными учреждениями или частными компаниями может способствовать разработке комплексной политики кибербезопасности, в которой будут чётко прописаны рекомендации, обязанности и процедуры по обеспечению кибербезопасности. Такие стратегии не только делают кибербезопасность более доступной, но и способствуют формированию культуры осведомлённости и ответственности в сфере кибербезопасности, что крайне важно в условиях ограниченных ресурсов [12]. Такой подход к саморегулированию и управлению кибербезопасностью на основе политики может стать эффективной и экономичной альтернативой официальной сертификации, особенно для небольших местных органов власти или организаций с ограниченными финансовыми ресурсами.

Заключение

В исследовании рассматриваются проблемы, с которыми сталкиваются местные органы власти при обеспечении кибербезопасности. Это малоизученная, но крайне важная область исследований в связи с растущим значением цифровых преобразований и инфраструктуры «умных городов». Среди множества выявленных проблем наиболее распространёнными оказались явная нехватка финансирования, дефицит квалифицированных кадров и отсутствие политики в области кибербезопасности или нормативных требований. Эти проблемы не только часто упоминаются в существующей литературе, но и усугубляются жёсткими бюджетными ограничениями, в рамках которых обычно работают местные органы власти. Ограниченный бюджет не только препятствует технологическому прогрессу, но и влияет на найм квалифицированного персонала и проведение обучающих программ, что, в конечном счёте делает цифровую инфраструктуру местных органов власти уязвимой для кибератак. Мы считаем, что, несмотря на противоположные точки зрения, согласно которым первоочередное внимание уделяется решению финансовых проблем, а не долгосрочным инвестициям в безопасность, кибербезопасность должна рассматриваться как неотъемлемый аспект деятельности местных органов власти.

Список источников

1. Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций: образование, наука, новая экономика. 2021. Т. 16. № 3. С. 7–33. EDN: RHBSFR. https://doi.org/10.17323/1996-7845-2021-03-01.

2. Зиновьева Е.С. Кибersдерживание и цифровая дилемма безопасности в американском экспертном дискурсе // Международные процессы. 2019. Т. 17. № 3(58). С. 51-65. EDN: LVKPIA. https://doi.org/10.17994/IT.2019.17.3.58.4.

3. Зиновьева Е.С. Формирование цифровых границ и информационная глобализация: анализ с позиций критической географии // Полис. Политические исследования. 2022. № 2. С. 8–21. EDN: AJDIQL. https://doi.org/10.17976/jpps/2022.02.02.

4. Зиновьева Е.С., Шитьков С.В. Цифровой суверенитет в практике международных отношений // Международная жизнь. 2023. № 3. С. 38–51. EDN: HBTQYT

5. Себекин С.А. Система международной информационной безопасности в условиях политической турбулентности // Вестник Санкт-Петербургского университета. Международные отношения. 2023. Т. 16. № 2. С. 170-190. EDN: JQHKPU. https://doi.org/10.21638/spbu06.2023.205

6. Понька Т.И., Рамич М.С., У Ю. Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // Вестник Российского университета дружбы народов. Сер. Международные отношения. 2020. Т. 20. № 2. С. 382–394. EDN: UANODL. https://doi.org/10.22363/2313-0660-2020-20-2-382-394

7. Ребро О.И., Гладышева А., Сучков М.А., Сушенцов А.А. Категория «Цифрового суверенитета» в современной мировой политике: вызовы и возможности для России // Международные процессы. 2021. Т. 19. № 4(67). С. 47-67. EDN: QPXXVU. https://doi.org/10.17994/1X2021.19.4.67.6

8. Лебедева М.М. Новый мировой порядок: параметры и возможные контуры // Полис. Политические исследования. 2020. № 4. С. 24-35. EDN: DNORYR. https://doi.org/10.17976/ jpps/2020.04.03

9. Сафранчук И.А., Лукьянов Ф.А. Современный мировой порядок: адаптация акторов к структурным реалиям // Полис. Политические исследования. 2021. № 4. С. 14–25. https://doi.org/10.17976/jpps/2021.04.03. EDN: JVPZJB

10. Конышев В.Н., Парфенов Р.В. Гибридные войны: между мифом и реальностью // Мировая экономика и международные отношения. 2019. Т. 63. № 12. С. 56-66. EDN: NQTLHW. https://doi.org/10.20542/0131-2227-2019-63-12-56-66.

11.Истомин И.А. Войны будущего в свете опыта прошлого // Мировая экономика и международные отношения. 2022. Т. 66. № 11. С. 101-114. EDN: IRAVWZ. https://doi.org/10.20542/0131-2227-2022-66-11-101-114

12.Ребро О.И., Гладышева А., Сучков М.А., Сушенцов А.А. Категория «Цифрового суверенитета» в современной мировой политике: вызовы и возможности для России // Международные процессы. 2021. Т. 19. № 4(67). С. 47–67. EDN: QPXXVU. https://doi.org/10.17994/1X2021.19.4.67.6

References

1. Degterev D.A., Ramich M.S., Piskunov D.A. The approaches of the USA and China to global cyberspace governance: the «new bipolarity» in the «network society». *Bulletin of International Organizations: education, Science, New Economy.* 2021;16(3):7–33. EDN: RHBSFR. (In Russ.). https://doi.org/10.17323/1996-7845-2021-03-01

2. Zinovieva E.S. Cyber support and the digital security dilemma in American expert discourse. *International processes.* 2019;17(3(58)):51–65. EDN: LVKPIA (In Russ.). https://doi.org/10.17994/IT.2019.17.3.58.4

3. Zinovieva E.S. The formation of digital borders and information globalization: an analysis from the perspective of critical geography. *Polis. Political Studies*. 2022;(2):8–21. EDN: AJDIQL (In Russ.). https://doi.org/10.17976/jpps/2022.02.02

4. Zinovieva E.S., Shitkov S.V. Digital sovereignty in the practice of international relations. *International life.* 2023;(3):38–51. EDN: HBTQYT (In Russ.)

5. Sobekin S.A. The system of international information security in the context of political turbulence. *Bulletin of St. Petersburg University. International relations.* 2023;16(2):170-190. EDN: JQHKPU (In Russ.). https://doi.org/10.21638/spbu06.2023.205

6. Ponka T.I., Ramich M.S., U. Y. Information policy and information security of the PRC: development, approaches and implementation. *Bulletin of the Peoples' Friendship University of Russia. Ser. International Relations*. 2020;20 (2):382–394. EDN: UANODL (In Russ.). https://doi.org/10.22363/2313-0660-2020-20-2-382-394

7. Rebro O.I., Gladysheva A., Suchkov M.A., Sushentsov A.A. The category of «Digital sovereignty» in modern world politics: challenges and opportunities for Russia. *International Processes.* 2021;19(4(67)):47–67. EDN: QPXXVU (In Russ.). https://doi.org/10.17994/1X2021.19.4.67.6

8. Lebedeva M.M. New World order: parameters and possible contours. *Polis. Political Studies*. 2020;(4):24-35. EDN: DNORYR (In Russ.). https://doi.org/10.17976/jpps/2020.04.03

9. Safranchuk I.A., Lukyanov F.A. Modern world order: adaptation of actors to structural realities. *Polis. Political Studies*. 2021;(4):14–25. EDN: JVPZJB (In Russ.). https://doi.org/10.17976/jpps/2021.04.03

10. Konyshev V.N., Parfenov R.V. Hybrid Wars: between myth and reality. *World Economy and International Relations.* 2019;63(12):56–66. EDN: NQTLHW (In Russ.). https://doi.org/10.20542/0131-2227-2019-63-12-56-66

11. Istomin I.A. The wars of the future in the light of the experience of the past. *World Economy and International Relations.* 2022;66(11):101–114. EDN: IRAVWZ (In Russ.). https://doi.org/10.20542/0131-2227-2022-66-11-101-114

12. Rib O.I., Gladysheva A., Suchkov M.A., Sushentsov A.A. The category of «Digital sovereignty» in modern world politics: challenges and opportunities for Russia. *International Processes.* 2021;19(4(67)):47–67. EDN: QPXXVU (In Russ.). https://doi.org/10.17994/1X2021.19.4.67.6

Информация об авторе

Е. И. Хубулури – доктор политических наук, профессор кафедры «Государственное и муниципальное управление», Ростовский государственный университет путей сообщения.

Information about the authors

E. I. Hubuluri– Dr. Sci. (Polit.), Professor, Department of State and Municipal Administration, Rostov State Transport University.

Автор заявляет об отсутствии конфликта интересов.
The author declares that there is no conflict of interest.

Статья поступила в редакцию 21.10.2025; одобрена после рецензирования 25.11.2025; принята к публикации 26.11.2025.
The article was submitted 21.10.2025; approved after reviewing 25.11.2025; accepted for publication 26.11.2025.