

ЮЖНЫЙ КАВКАЗ

ВНУТРИ- И ВНЕШНЕПОЛИТИЧЕСКАЯ СТРАТЕГИЯ ГРУЗИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Научная статья

З.Т. Золоева

*Северо-Осетинский государственный университет
им. Коста Левановича Хетагурова
Владикавказ, Российская Федерация
ORCID: <https://orcid.org/0009-0002-3118-7499>
E-mail: 4noiabria@mail.ru*

Б.Г. Койбаев

*Северо-Осетинский государственный университет
им. Коста Левановича Хетагурова
Владикавказ, Российская Федерация
ORCID: <https://orcid.org/0000-0002-2841-960X>
E-mail: koibaevbg@mail.ru*

Для современных государств угрозы информационной безопасности представляют серьезный вызов, так как они носят как внешнеполитический, так и внутривнутриполитический характер. Информационные угрозы, возникающие в контексте международных отношений, часто исходят от определенных внешнеполитических субъектов, амбиции которых заключаются в стремлении к установлению контроля над информационным полем. Настоящая статья посвящена комплексному анализу основных направлений государственной политики Грузии в области обеспечения информационной безопасности, а также выявлению внутренних и внешних угроз национальной безопасности в информационной сфере. В статье систематизированы ключевые нормы и политико-правовые инструменты, применяемые страной для обеспечения информационной безопасности; выявлены общие тенденции развития государственной политики. В связи с этим рассматриваются структуры государственного аппарата Грузии, ответственные за реализацию государственной политики в данной области. Авторы также уделяют внимание вопросам нормативно-правового регулирования информационной безопасности в Грузии. В работе использован ряд методов исследования, среди которых особое значение имеют метод анализа, метод кейс-стади и метод научной объективности. Использование данных методов позволило наиболее полно раскрыть тему исследования. Полученные выводы позволяют оценить текущую ситуацию в сфере обеспечения информационной безопасности и обозначить перспективные направления для усиления информационной безопасности страны.

Ключевые слова: государственная политика, государственная безопасность, информационная безопасность, информационные технологии, кибербезопасность, стратегия, политическая система, цифровая трансформация, политические институты, Грузия.

Для цитирования: Золоева З.Т., Койбаев Б.Г. 2026 Внутри- и внешнеполитическая стратегия Грузии по обеспечению информационной безопасности // Постсоветские исследования. 2026. Т. 9. № 4. С. 515–523.

GEORGIA'S DOMESTIC AND FOREIGN POLICY STRATEGY FOR ENSURING INFORMATION SECURITY

Research article

Z.T. Zoloeva

*Kosta Levanovich Khetagurov North Ossetian State University
Vladikavkaz, Russian Federation
ORCID: <https://orcid.org/0009-0002-3118-7499>
E-mail: 4noiabria@mail.ru*

B.G. Koibaev

*Kosta Levanovich Khetagurov North Ossetian State University
Vladikavkaz, Russian Federation
ORCID: <https://orcid.org/0000-0002-2841-960X>
E-mail: koibaevbg@mail.ru*

Threats to information security pose a serious challenge for modern States, as they are both foreign and domestic in nature. Information threats that arise in the context of international relations often come from certain foreign policy actors whose ambitions are to establish control over the information field. This article is devoted to a comprehensive analysis of the main directions of the state policy of Georgia in the field of information security, as well as the identification of internal and external threats to national security in the information sphere. The article systematizes the key norms and political and legal instruments used by the country to ensure information security, identifies general trends in the development of public policy. In this regard, the structures of the Georgian state apparatus responsible for the implementation of state policy in this area are being considered. The authors also pay attention to the issues of regulatory regulation of information security in Georgia. The work uses a number of research methods, among which the following are of particular importance: method of analysis, case study method and scientific objectivity method. The use of these methods made it possible to fully reveal the research topic. The findings make it possible to assess the current situation in the field of information security and identify promising areas for strengthening the country's information security.

Key words: *state policy, state security, information security, information technology, cybersecurity, strategy, political system, digital transformation, political institutions, Georgia.*

For citation: *Zoloeva Z.T., Koibaev B.G. 2026. Georgia's Domestic and Foreign Policy Strategy for Ensuring Information Security // Postsovetskie issledovaniya = Post-Soviet Studies. 2026. Vol. 9. № 4. P. 515–523. (In Russ.)*

Цифровые технологии сегодня проникают в различные аспекты повседневной жизни граждан. Большое влияние они оказывают и на функционирование политической системы, трансформируя традиционные формы взаимодействия власти и общества [Zoloeva, Koibaev, 2025: 178], а также модернизируя взаимодействие политических институтов на международной арене. В этих условиях формируются как новые возможности для демократизации [Дудайти, 2025: 750], повышения транспарентнос-

ти и эффективности государственного управления [Conde: 8], так и появляются новые риски и угрозы [Domínguez, 2020: 43], среди которых особо выделяются угрозы безопасности государства в информационном пространстве [Fernandez-Osorio, Villalba-García, Velandia-Pardo, 2024: 12].

В этой связи Т. Зеделашвили отмечает, что «развитие технологий породило виртуальный мир, а виртуальный мир породил альтернативные пространства реальности, что дало агрессорам возможность осущест-

влять кибератаки, кибершпионаж и кибервойну» [ზედელაშვილი, 2022: 33].

Перед государствами в этих условиях стоят как внешнеполитические угрозы, связанные с попытками оказания воздействия на политические альянсы, индивидуальных личностей и социальные группы, так и внутривнутриполитические, в связи с чем необходимо отметить существование угрозы, реализуемых посредством использования передовых информационных технологий с целью подрыва основ политической системы [Gamon, 2017: 80], нарушения территориальной целостности и суверенитета государств [Кухарский, 2020: 5], дестабилизации устоявшихся социальных норм и размывания традиционных ценностей.

Государства Южного Кавказа, реагируя на данные угрозы, реализуют государственную политику в сфере обеспечения информационной безопасности [Койбаев, Золоева, 2024: 7] и становления цифрового суверенитета [Минбалева, 2024: 134; Давтян, 2025: 560]. В данной статье на примере Грузии будет предпринята попытка рассмотреть особенности реализации государственной политики в данной сфере.

В этой связи важно подчеркнуть, что в соответствии с исследованием, опубликованным на сайте Национального индекса кибербезопасности (NCSI), Грузия в 2025 г. заняла 22-е место в мире и 16-е – в Европе¹, что свидетельствует о высоком уровне обеспечения кибербезопасности в стране.

В то же время в стране проблема обеспечения информационной безопасности стоит достаточно остро. Так, например, в январе 2025 г. была полностью выведена из строя система оплаты общественного транспорта в Тбилиси. Наблюдаются случаи распространения недостоверной информации и нарушения правил хранения персональных данных². В связи с этим руководством Грузии неоднократно подчеркивалась важность обеспечения информационной безопасности и ее влияние на функционирование

государственных институтов и экономики страны³.

Основополагающим документом Грузии, определяющим угрозы, риски и вызовы и устанавливающим основные направления политики безопасности, является Концепция национальной безопасности, принятая Парламентом Грузии 23 декабря 2011 г. В соответствии с данной Концепцией целью Грузии является создание системы информационной безопасности, в которой пагубные последствия любой кибератаки будут сведены к минимуму, а после такой атаки можно будет в кратчайшие сроки полностью восстановить функционирование информационной инфраструктуры⁴. Анализ положений Концепции позволяет сделать вывод о том, что Грузия рассматривает Россию как источник угроз своей информационной безопасности, обвиняя ее в кибератаках в 2008 г. Однако данные факты не были доказаны, не было также принято официальное судебное решение, которое признало бы прямое участие государственных органов Российской Федерации в этих атаках.

Представляется, что Концепция национальной безопасности Грузии нуждается в обновлении с учетом современных реалий и эффективного реагирования на современные угрозы и вызовы, стоящие перед страной, так как с момента ее принятия прошло уже 15 лет, во многом изменилась геополитическая ситуация, информационные технологии развиваются экспоненциальными темпами, что способствует появлению новых угроз и вызовов, с которыми сталкиваются государства.

Важно также отметить, что впервые Концепция национальной безопасности Грузии была принята в июле 2005 г.: тогда Россия рассматривалась как партнер, но

³ Премьер Грузии рассказал о вызовах кибербезопасности. URL: <https://sputnik-georgia.ru/20230621/premer-gruzii-rasskazal-o-vyzovakh-kiberbezopasnosti-278777020.html> (дата обращения: 10. 03.2026).

⁴ საქართველოს პარლამენტის დადგენილება, საქართველოს ეროვნული უსაფრთხოების კონცეფციის // დამტკიცების შესახებ. 08.07.2005. № 1895. URL: <https://www.matsne.gov.ge/ka/document/view/43156?publication=0> (дата обращения: 10. 03.2026).

¹ National Cyber Security index. URL: <https://ncsi.ega.ge/ncsi-index> (дата обращения: 10. 03.2026).

² Naprys E. Entire Georgian country population exposed in a massive data leak. URL: <https://cybernews.com/security/entire-georgian-country-population-exposed> (дата обращения: 10. 02.2026).

уже обозначался курс на евроинтеграцию и сотрудничество с НАТО. При этом отмечались слабость единой государственной информационной политики и зависимость управления от ненадежной информации¹. Как отмечает Д. Меликян, сравнивая положения Концепции национальной безопасности 2005 и 2011 гг., «изменения в Концепции коснулись лишь взаимоотношений с Россией и ее восприятия властями и общественностью Грузии» [Меликян, 2014: 78].

Закон Грузии «Об информационной безопасности» от 5 июня 2012 г. имеет большое значение для политической жизни страны, так как он заложил основы регулирования сферы информационной безопасности, определил роли государственных и частных секторов, а также механизмы контроля в этой области². Анализ данного документа позволяет сделать вывод о том, что в нем в качестве взаимозаменяемых используются термины «информационная безопасность» и «кибербезопасность». Между тем эти понятия обладают существенными различиями [Козлова, Довгаль, 2021: 88]. Понятие «информационная безопасность» является более широким, предполагает защиту данных в любой форме и включает также понятие «кибербезопасность», которая связана с обеспечением защиты только цифровой среды, от каких-либо внешних вмешательств.

Важно отметить, что в обществе неоднократно осуществлялась критика данного Закона. Так, например, в 2020 г. Институт исследований демократии указывал на риски, связанные с поправками к Закону. По мнению организации, эти поправки наделяли Службу государственной безопасности Грузии неоправданно широкими полномочиями на доступ к информационным ресурсам³.

¹ საქართველოს პარლამენტის დადგენილება, საქართველოს ეროვნული უსაფრთხოების კონცეფციის // დამტკიცების შესახებ. 08.07.2005. № 1895. URL: <https://www.matsne.gov.ge/ka/document/view/43156?publication=0> (дата обращения: 10. 03.2026).

² Закон Грузии от 5.06.2012 № 6391-Іс «Об информационной безопасности». URL: <https://matsne.gov.ge/ru/document/view/1679424?publication=4> (дата обращения: 10. 02.2026).

³ *Bzhalava K.* DRI on the amendments to the Law of Georgia on Information Security. URL: [Следует заметить, что информационная безопасность определялась как составная часть национальной безопасности, согласно Закону Грузии «О порядке планирования и координации политики национальной безопасности», принятому 4 марта 2015 г. В ст. 3 данного Закона среди сфер политики национальной безопасности прямо упоминается информационная безопасность наряду с государственной обороной, внешней и внутренней безопасностью, социально-экономической и энергетической безопасностью, гражданской безопасностью и правопорядком⁴.](https://mes-</p>
</div>
<div data-bbox=)

В 2012 г. была ратифицирована разработанная Советом Европы Конвенция о преступности в сфере компьютерной информации ETS № 185. Представляется, что принятие данной Конвенции соответствовало общей внешнеполитической линии страны, направленной на интеграцию в европейские структуры, и демонстрировало готовность Грузии соответствовать международным стандартам и укреплять механизмы сотрудничества в уголовно-правовой сфере.

В настоящее время открыта к подписанию Конвенция против киберпреступности, принятая Резолюцией Генеральной Ассамблеи ООН № 79/243 от 24.12.2024. Представляется, что данная Конвенция обладает большим потенциалом для координации усилий государств в борьбе с трансграничной киберпреступностью. В связи с этим присоединение Грузии к данной Конвенции оказало бы положительное влияние на обеспечения информационной безопасности и стабильное функционирование политической системы страны.

Важное место в процессе реализации государственной политики Грузии в исследуемой сфере занимала стратегия Национальная стратегия кибербезопасности на 2021–2024 гг. и План действий, утвержденные 30 сентября 2021 г. Важно отметить,

senger.com.ge/issues/4732_september_22_2020/4732_khatia1.html (дата обращения: 10. 03.2026).

⁴ Закон Грузии от 4.03.2015 № 3126-Іс «О порядке планирования и координации политики национальной безопасности». URL: <https://matsne.gov.ge/en/document/download/2764463/2/ru/pdf> (дата обращения: 10. 03.2026).

что, согласно данному документу, кибербезопасность рассматривалась как неотъемлемая часть национальной безопасности.

Важно отметить, что, несмотря на постоянное возрастание количества рисков и угроз в информационном пространстве, в Грузии с 2024 г. отсутствует национальная стратегия в области кибербезопасности. Представляется, что это является негативной тенденцией, в стране существует необходимость в разработке и принятии новой национальной стратегии кибербезопасности с учетом современных вызовов и угроз.

Закон «О защите персональных данных», принятый в 2023 г., регулирует обработку персональных данных в Грузии с использованием различных средств. В соответствии с данным Законом, обязательным является назначение лица, ответственного за защиту данных в организациях. Ужесточаются требования к согласию на рассылки и расширены полномочия Службы защиты персональных данных, которая может проводить проверки и накладывать штрафы за первые нарушения. Тем не менее меры защиты информации, предусмотренные данным Законом, не предотвратили крупную утечку данных, произошедшую в 2025 г.

Важно также отметить, что в Грузии введены меры уголовно-правовой ответственности за совершение киберпреступлений. В этой связи в Уголовном кодексе Грузии содержится ряд статей: 284, 285, 286, 286¹, 286². Статьи 286¹, 286² были добавлены в Уголовный кодекс Грузии в 2021 г. Статья 286¹ предусматривает ответственность за нарушение компьютерных данных или системы с целью получения финансовой выгоды, а ст. 286² устанавливает уголовную ответственность за создание поддельных официальных компьютерных данных¹.

Закрепление ответственности за совершение киберпреступлений играет важную роль в развитии политической системы государства, так как напрямую связано с обеспечением национальной безопасности, стабильности институтов власти, доверия

граждан и международного сотрудничества. В условиях цифровизации киберпространство становится важным полем политических, экономических и информационных противостояний, что требует эффективных механизмов противодействия.

Грузия активно сотрудничает с другими государствами и международными организациями в сфере информационной безопасности, что обусловлено растущими угрозами в цифровом пространстве. Так, по мнению А. Гоциридзе, занимавшего должность директора Бюро кибербезопасности Министерства обороны Грузии в 2014–2016 гг., «для надежной киберобороны необходимы инфраструктура, юридическая поддержка и многонациональное сотрудничество» [Горидзе, 2016: 56].

Важно отметить, что Грузия осуществляет сотрудничество в исследуемой сфере как на двусторонней, так и на многосторонней основе и принимает участие в различных международных инициативах. Например, в 2018 г. Грузия и Великобритания подписали меморандум о сотрудничестве в сфере кибербезопасности. Документ предусматривал координацию действий, развитие критической инфраструктуры и повышение устойчивости к кибератакам².

Грузия тесно взаимодействует с США, Великобританией, Эстонией и Литвой в сфере кибербезопасности³. В частности в 2021 г. Грузия, Украина и Литва подписали меморандум о совместной работе в сфере кибербезопасности⁴.

Важно также отметить, что для Грузии характерно участие неправительственных

² Грузия и Великобритания договорились сотрудничать в сфере кибербезопасности. URL: <https://sputnik-georgia.ru/20181108/Gruziya-i-Velikobritaniya-dogovorilis-sotrudnicat-v-sfere-kiberbezopasnosti-242856284.html> (дата обращения: 10. 03.2026).

³ Грузия достигла значительных результатов в сфере кибербезопасности. URL: <https://sputnik-georgia.ru/20230621/gruziya-dostigla-znachitelnykh-rezultatov-v-sfere-kiberbezopasnosti-premer-278787217.html> (дата обращения: 10. 03.2026).

⁴ Приходько В. Украина, Литва и Грузия подписали договор о совместной работе в сфере кибербезопасности. URL: <https://www.osnmedia.ru/world/ukraina-litva-i-gruziya-podpisali-dogovor-o-sovmestnoj-rabote-v-sfere-kiberbezopasnosti> (дата обращения: 10. 03.2026).

¹ Уголовный кодекс Грузии. № 2287 от 22.07.1999. URL: <https://matsne.gov.ge/ru/document/view/16426.?publication=282> (дата обращения: 10. 03.2026).

организаций в обеспечении кибербезопасности, прежде всего, посредством осуществления сотрудничества с государственными структурами, реализации образовательных программ, тренингов, различных исследований и получения международного финансирования для укрепления цифровой защиты, где активное участие принимают США и ЕС¹.

Так, например, в 2022 г. Национальная комиссия по регулированию энергетики и водоснабжения Грузии (GNERC) подписала меморандум о сотрудничестве с Национальной ассоциацией кибербезопасности с целью повышения осведомленности о кибербезопасности (NCSA), совместной организации информационных встреч, обучения и тренингов, укрепления устойчивости кибербезопасности и информационного общества².

Деятельность неправительственных организаций в Грузии часто поддерживается как государственными, так и международными инициативами. Однако после принятия Закона «О прозрачности иностранного влияния» от 28 мая 2024 г. США и Евросоюз сократили прямое финансирование правительства Грузии, что косвенно затронуло и некоммерческие организации, зависимые от государственных программ.

Важное место в процессе реализации государственной политики Грузии в сфере обеспечения информационной безопасности занимает ограничение доступа к незаконной информации. При выявлении незаконного контента государственные органы, правоохранительные структуры или заинтересованные стороны могут подать запрос на удаление или блокировку информации. Если контент размещен на онлайн-платформе, ее администрация обязана выполнить предписания суда или запросы от правоохранительных органов. Ключевую роль

в данном процессе играет Национальная комиссия по коммуникациям (GNCC).

К информации, распространение которой в Грузии запрещено, в том числе в Интернете, относятся, в частности: клевета; материалы, разжигающие ненависть или насилие на основе расы, национальности, религии, политических убеждений и других признаков; детская порнография; незаконное использование авторских и смежных прав, товарных знаков и других объектов интеллектуальной собственности; государственная тайна и др. В 2024 г. в Грузии были введены дополнительные ограничения на распространение информации, что связано с принятием Закона «О семейных ценностях и защите несовершеннолетних», который запрещает пропаганду ЛГБТ (30 ноября 2023 г. Верховный суд Российской Федерации признал это движение экстремистским) и смену пола³.

Особую важность, по нашему мнению, представляет исследование политических институтов, ответственных за реализацию государственной политики в сфере информационной безопасности. В структуре органов государственного управления Правительство Грузии играет центральную роль в формировании и реализации государственной политики в сфере информационной безопасности. Министерство юстиции через подведомственное ему Агентство по обмену данными осуществляет разработку и реализацию государственной политики в сфере информационной безопасности. Группа помощи по реагированию на компьютерные инциденты (CERT.GOV.GE) занимается выявлением, анализом и реагированием на кибератаки.

Министерство обороны Грузии через подведомственное ему Бюро кибербезопасности отвечает за информационную безопасность в сфере обороны. Управление кибератаками в отношении субъектов критической информационной системы в сфере обороны осуществляет Группа помощи

¹ США и ЕС решили увеличить финансирование НКО в Грузии на фоне Закона об иноагентах. URL: https://tsargrad.tv/news/ssha-i-es-reshili-velichit-finansirovanie-nko-v-gruzii-na-fone-zakona-ob-inoagentah_tah_1035444 (дата обращения: 10. 03.2026).

² Нацкомиссия по энергетике и Ассоциация кибербезопасности Грузии подписали меморандум. URL: <https://ru.rt.com/swxh> (дата обращения: 10. 03.2026).

³ Закон Грузии от 17.09.2024 № 4437-XVIтс-пХс «О семейных ценностях и защите несовершеннолетних». URL: <https://matsne.gov.ge/ru/document/view/6283110?publication=0> (дата обращения: 10. 02.2026).

Бюро кибербезопасности по реагированию на компьютерные инциденты.

Министерство внутренних дел Грузии также имеет в своем распоряжении отдел компьютерной цифровой криминалистики, который анализирует и исследует цифровые доказательства [Бәззәҗзәбәдә, 2020: 30]. Кроме того, в Генеральной прокуратуре Грузии также создано специальное подразделение прокуроров и следователей по борьбе с киберпреступностью.

Следует заметить, что в соответствии с Законом «О порядке планирования и координации политики национальной безопасности» от 4.03.2015 за планирование политики в области национальной безопасности ответственен Совет национальной безопасности.

Таким образом, в Грузии сформирована система органов государственной власти, каждый из которых отвечает за конкретные аспекты обеспечения информационной безопасности. Однако, как отмечают Р. Ларссон и Г. Квашилавава, в Грузии существуют проблемы дублирования полномочий между силовыми структурами, недостатка квалифицированных специалистов, неразвитости информационно-коммуникационной инфраструктуры, что затрудняет эффективное реагирование на угрозы в сфере информационной безопасности.

Политика в сфере обеспечения информационной безопасности играет ключевую роль в развитии политической системы и политической жизни страны, так как она

напрямую влияет на стабильность государства, суверенитет, эффективность управления, доверие граждан и противодействие внешним угрозам. В Грузии уделяется достаточно большое внимание вопросам обеспечения информационной безопасности. Государственная стратегия Грузии в области информационной безопасности направлена на укрепление цифрового суверенитета, обеспечение защиты критически важной инфраструктуры.

Однако в стране проблема обеспечения информационной безопасности в настоящее время стоит остро, так как не редкими являются случаи кибератак, распространения недостоверной информации, нарушений правил хранения персональных данных. В Грузии в настоящее время отсутствует концепция информационной безопасности, наблюдается проблема неразвитости критической информационной инфраструктуры и недостатка квалифицированных специалистов, также есть изъяны в реализации законодательства и др.

Растущие внутренние и международные вызовы повышают риски использования информационных технологий в целях манипуляций и дезинформации. Для их преодоления необходим комплексный подход: разработка национальной стратегии, усиление межведомственной координации, увеличение инвестиций в инфраструктуру и образование, а также совершенствование законодательства и политических механизмов контроля.

ЛИТЕРАТУРА

Горидзе А. Защита киберпространства в Грузии // *Per Concordiam*. № 2. 2016. URL: <https://perconcordiam.com/ru/защита-киберпространства-в-грузии> (дата обращения: 18.03.2026).

Даевян В.С. Цифровой суверенитет на Южном Кавказе: вызовы интеграции в международные цифровые коридоры // *Вестник Российского университета дружбы народов*. Серия: Политология. 2025. Т. 27. № 3. С. 560–578.

Дудайти А.К. Современные вызовы государственной власти в Грузии: политическая оценка // *Постсоветские исследования*. 2025. Т. 8. № 7. С. 746–758.

Козлова Н.Ш., Довгаль В.А. Кибербезопасность и информационная безопасность: сходства и отличия // *Вестник Адыгейского государственного университета*. Серия: Естественно-математические и технические науки. 2021. № 3 (286). С. 88–97.

Койбаев Б.Г., Золоева З.Т. Развитие информационного общества в Азербайджанской Республике. Владикавказ: Северо-Осетинский государственный университет им. К.Л. Хетагурова, 2024. 172 с.

Кухарский А.Н. Информационная безопасность политического процесса как элемент государственного и муниципального управления России: автореф. дис. ... канд. полит. наук. Екатеринбург, 2020. 25 с.

Меликян Д. Внешняя политика Грузии после парламентских выборов 1 октября 2012 г. // Центральная Азия и Кавказ. 2014. Т. 17. № 1. С. 78–88.

Минбалеев А.В. Обеспечение кибербезопасности и международной информационной безопасности в системе обеспечения информационного суверенитета // Правовое обеспечение суверенитета России: проблемы и перспективы: сборник докладов XXIV Международной научно-практической конференции и XXIV Международной научно-практической конференции юридического факультета МГУ им. М.В. Ломоносова в рамках XIII Московской юридической недели. Москва, 21–24 ноября 2023 г.: в 4 ч. М.: Издательский центр Университета им. О.Е. Кутафина (МГЮА), 2024. С. 134–137.

Conde R.C. Ciberpolítica y gobernanza. Estrategias de gobernanza para el empoderamiento de la Ciudadanía Digital. Xalapa, Veracruz, México, 2024. 282 p. (На исп. яз.) [*Конде Р.К.* Киберполитика и управление. Стратегии управления для расширения прав и возможностей цифрового гражданства. Халапа, Веракрус, Мексика, 2024. 282 с.]

Domínguez D. Sistema de Seguridad Cibernética Nacional frente a los ciberataques como amenaza a la seguridad nacional // Revista de Ciencia e Investigación en Defensa – CAEN. 2020. № 1. P. 43–48. (На исп. яз.) [*Домингес Д.* Национальная система кибербезопасности сталкивается с кибератаками как угрозой национальной безопасности // CAEN: журнал науки и исследований в области обороны. 2020. № 1. С. 43–48.]

Fernández-Osorio A.E., Villalba-García L.F., Velandia-Pardo E.F. Gobernanza policéntrica, big data e inteligencia artificial: herramientas para la seguridad ciudadana en Colombia // Revista Criminalidad. 2024. № 66 (3). P. 11–25. (На исп. яз.) [*Фернандес-Осорио А.Е., Вильяльба-Гарсия Л.Ф., Веландия-Пардо Э.Ф.* Полицентрическое управление, большие данные и искусственный интеллект: инструменты обеспечения безопасности граждан в Колумбии // Журнал преступности. 2024. № 66 (3). С. 11–25.]

Gamon V. Internet, la nueva era del delito: cibercrimen, ciberterrorismo, legislación y ciberseguridad, Internet, the new age of crime: cybercrime, cyberterrorism, legislation and cybersecurity // URVIO: Revista Latinoamericana de Estudios de Seguridad. 2017. № 20. P. 80–93. (На исп. яз.) [*Гамон В.* Интернет, новая эра преступности: киберпреступность, кибертерроризм, законодательство и кибербезопасность // URVIO: латиноамериканский журнал исследований безопасности. 2017. № 20. С. 80–93.]

Zoloeva Z.T., Koybaev B.G. Features of the development of e-government in the Republic of Azerbaijan // Modern Science and Innovations. 2025. № 3 (51). P. 171–177. (На англ. яз.) [*Золоева З.Т., Койбаев Б.Г.* Особенности развития электронного правительства в Азербайджанской Республике // Современная наука и инновации. 2025. № 3 (51). С. 171–177.]

ზედელაშვილი თ. კიბერუსაფრთხოების სამხედრო პოლიტიკური განზომილება 21-ე საუკუნეში // საერთაშორისო სამეცნიერო-პრაქტიკული კონფერენციის ნაშრომთა კრებული «ეროვნული უსაფრთხოების აქტუალური საკითხები». გორი, 2022. გ. 33–47. (На груз. яз.) [*Зедელაшвили Т.* Военно-политическое измерение кибербезопасности в XXI веке // Материалы Международной научно-практической конференции «Актуальные вопросы национальной безопасности». Гори, 2022. С. 33–47.]

ნაგეტვარიძე ვ. ელექტრონული მმართველობის დანერგვა საქართველოში: პრობლემები და პერსპექტივები. პოლიტიკის მეცნიერების დოქტორის აკადემიური ხარისხის მოსაპოვებლად წარდგენილი დისერტაცია. თბილისი, 2020 170 გ. (На груз. яз.) [*Нагетваридзе В.* Внедрение электронного управления в Грузии: проблемы и перспективы: дис. ... докт. полит. наук. Тбилиси, 2020. 170 с.]

REFERENCES

Goridze A. Zashchita kiberprostranstva v Gruzii // Per Concordiam. № 2. 2016. URL: <https://perconcordiam.com/ru/защита-киберпространства-в-грузии> (data obrasheniya: 18.03.2026). (In Russ.) [*Goridze A.* Cyberspace Protection in Georgia // Per Concordiam. № 2. 2016. URL: <https://perconcordiam.com/ru/защита-киберпространства-в-грузии> (data accessed: 18.03.2026).]

Davyan V.S. Tsifrovoy suverenitet na Yuzhnom Kavkaze: vyzovy integratsii v mezhdunarodnyye tsifrovyye koridory // Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: Politologiya. 2025. T. 27. № 3. S. 560–578. (In Russ.) [*Davyan V.S.* Digital Sovereignty in the South Caucasus: Challenges of Integration into International Digital Corridors // Bulletin of Peoples' Friendship University of Russia. Series: Political Science. 2025. Vol. 27. № 3. P. 560–578.]

Dudayti A.K. Sovremennyye vyzovy gosudarstvennoy vlasti v Gruzii: politicheskaya otsenka // Post-sovetskiye issledovaniya. 2025. T. 8. № 7. S. 746–758. (In Russ.) [*Dudaiti A.K.* Modern Challenges to State Authority in Georgia: Political Assessment // Post-Soviet Studies. 2025. Vol. 8. № 7. P. 746–758.]

Conde R.C. Cyberpolitics and Governance. Governance Strategies for the Empowerment of Digital Citizenship. Xalapa, Veracruz, Mexico, 2024. 282 p.

Domínguez D. National Cybersecurity System Facing Cyberattacks as a Threat to National Security // CAEN: Journal of Science and Research in Defense. 2020. № 1. P. 43–48.

Fernández-Osorio A.E., Villalba-García L.F., Velandia-Pardo E.F. Polycentric Governance, Big Data and Artificial Intelligence: Tools for Citizen Security in Colombia // Criminality Journal. 2024. № 66 (3). P. 11–25.

Gamon V. Internet, the new age of crime: cybercrime, cyberterrorism, legislation and cybersecurity. // URVIO: Latin American Journal of Security Studies. 2017. № 20. P. 80–93.

Koybayev B.G., Zoloyeva Z.T. Razvitiye informatsionnogo obshchestva v Azerbaydzhanskoy Respublike. Vladikavkaz: Severo-Osetinskiy gosudarstvennyy universitet im. K.L. Khetagurova, 2024. 172 s. (In Russ.) [*Koybaev B.G., Zoloeva Z.T.* Development of the Information Society in the Republic of Azerbaijan. Vladikavkaz: North Ossetian State University named after K.L. Khetagurov, 2024. 172 p.]

Kozlova N.Sh., Dovgal' V.A. Kiberbezopasnost' i informatsionnaya bezopasnost': skhodstva i otlichiya // Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya: Yestestvenno-matematicheskkiye i tekhnicheskkiye nauki. 2021. № 3 (286). S. 88–97. (In Russ.) [*Kozlova N.Sh., Dovgal' V.A.* Cybersecurity and Information Security: Similarities and Differences // Bulletin of Adyge State University. Series: Natural, Mathematical and Technical Sciences. 2021. № 3 (286). P. 88–97.]

Kukhar'skiy A.N. Informatsionnaya bezopasnost' politicheskogo protsessa kak element gosudarstvennogo i munitsipal'nogo upravleniya Rossii: avtoref. diss. ... kand. polit. nauk. Yekaterinburg, 2020. 25 s. (In Russ.) [*Kukhar'skiy A.N.* Information Security of the Political Process as an Element of State and Municipal Administration in Russia: Abstract of a PhD Dissertation in Political Science. Yekaterinburg, 2020. 25 p.]

Melikyan D. Vneshnyaya politika Gruzii posle parlamentskikh vyborov 1 oktyabrya 2012 goda // Tsentral'naya Aziya i Kavkaz. 2014. T. 17. № 1. S. 78–88. (In Russ.) [*Melikyan D.* Georgia's Foreign Policy after the Parliamentary Elections of October 1, 2012 // Central Asia and the Caucasus. 2014. Vol. 17. № 1. P. 78–88.]

Minbaleyev A.V. Obespecheniye kiberbezopasnosti i mezhdunarodnoy informatsionnoy bezopasnosti v sisteme obespecheniya informatsionnogo suvereniteta // Pravovoye obespecheniye suvereniteta Rossii: problemy i perspektivy: Sbornik dokladov XXIV Mezhdunarodnoy nauchno-prakticheskoy konferentsii i XXIV Mezhdunarodnoy nauchno-prakticheskoy konferentsii Yuridicheskogo fakul'teta MGU im. M.V. Lomonosova v ramkakh XIII Moskovskoy yuridicheskoy nedeli. V 4-kh chastyakh, Moskva, 21–24 noyabrya 2023 goda. M.: Izdatel'skiy tsentr Universiteta im. O.Ye. Kutafina (MGYUA), 2024. S. 134–137. (In Russ.) [*Minbaleyev A. V.* Ensuring Cybersecurity and International Information Security in the System of Ensuring Information Sovereignty // Legal Support of Russia's Sovereignty: Problems and Prospects: collection of reports from the XXIV International Scientific and Practical Conference and the XXIV International Scientific and Practical Conference of the Law Faculty of Moscow State University named after M.V. Lomonosov within the framework of the XIII Moscow Legal Week. In 4 parts. Moscow, November 21–24, 2023. M.: Publishing Center of the University. O.E. Kutafina (MGYuA), 2024. P. 134–137.]

Napetvaridze V. Implementation of e-Governance in Georgia: Problems and Prospects: dissertation submitted for the academic degree of Doctor of Political Science. Tbilisi, 2020. 170 p.

Zedelashvili T. Military-political dimension of cybersecurity in the 21st century. Proceedings of the International Scientific-Practical Conference «Current Issues of National Security». Gori, 2022. P. 33–47.

Zoloeva Z.T., Koybaev B.G. Features of the development of e-government in the Republic of Azerbaijan // Modern Science and Innovations. 2025. № 3 (51). P. 171–177.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Золоева Зарина Тамерлановна, кандидат юридических наук, старший преподаватель кафедры теоретико-исторических правовых дисциплин Северо-Осетинского государственного университета им. Коста Левановича Хетагурова (Владикавказ, Российская Федерация).
E-mail: 4noiabria@mail.ru

Койбаев Борис Георгиевич, доктор политических наук, кандидат исторических наук, профессор кафедры всеобщей истории, профессор Северо-Осетинского государственного университета им. Коста Левановича Хетагурова (Владикавказ, Российская Федерация).
E-mail: koibaevbg@mail.ru

INFORMATION ABOUT THE AUTHORS

Zarina T. Zoloeva, candidate of law, senior lecturer of the Department of Theoretical and Historical Legal Disciplines of Kosta Levanovich Khetagurov North Ossetian State University (Vladikavkaz, Russian Federation).
E-mail: 4noiabria@mail.ru

Boris G. Koibaev, doctor of political sciences, candidate of historical sciences, professor of the Department of General History, professor of Kosta Levanovich Khetagurov North Ossetian State University (Vladikavkaz, Russian Federation).
E-mail: koibaevbg@mail.ru