



**Зарина Тамерлановна
ЗОЛОЕВА,**

старший преподаватель
кафедры теоретико-
исторических
правовых дисциплин
Северо-Осетинского
государственного
университета имени Коста
Левановича Хетагурова,
кандидат юридических наук
4noiabria@mail.ru
362025, Россия,
г. Владикавказ,
ул. Ватутина, д. 44–46

Обеспечение кибербезопасности в государствах Южного Кавказа: сравнительно-правовой анализ

Аннотация. Статья посвящена сравнительно-правовому анализу подходов государств Южного Кавказа — Грузии, Азербайджана и Армении — к обеспечению кибербезопасности. Исследование обеспечения кибербезопасности на Южном Кавказе актуально в силу ряда факторов, связанных с геополитической ситуацией, технологическим развитием, угрозами кибератак и необходимостью обеспечения цифровой стабильности государств региона. Этот вопрос приобретает особую значимость в условиях растущей цифровизации, использования киберпространства в политических и военных целях, а также в контексте конкуренции глобальных и региональных акторов за влияние в регионе. Цель работы — проанализировать правовые механизмы регулирования кибербезопасности в трех государствах и выявить существующие проблемы в этой сфере. В ходе исследования рассмотрены ключевые нормативные правовые акты и документы стратегического планирования Грузии, Азербайджана и Армении в сфере обеспечения кибербезопасности.

На основе анализа выявлены общие тенденции, сделаны выводы о различиях в подходах указанных стран к обеспечению кибербезопасности, выявлены общие проблемы региона в сфере кибербезопасности.

Ключевые слова: информационное право, киберпространство, информационная безопасность, кибератаки, кибербезопасность, правовое регулирование кибербезопасности, Южный Кавказ, Грузия, Азербайджан, Армения

DOI: 10.17803/2311-5998.2026.142.6.120-127

Zarina T. ZOLOEVA,

Senior Lecturer, Department of Theoretical and Historical
Legal Disciplines, Kosta Levonovich Khetagurov
North Ossetian State University, Cand. Sci. (Law)

4noiabria@mail.ru

44–46, ul. Vatutina, Vladikavkaz,
Russia, 362025

Ensuring Cybersecurity in the South Caucasus States: a Comparative Legal Analysis

Abstract. This article provides a comparative legal analysis of the approaches of the South Caucasus states — Georgia, Azerbaijan, and Armenia — to ensuring cybersecurity. Research into cybersecurity in the South Caucasus is relevant due to a number of factors related to the geopolitical situation, technological development, the threat of cyberattacks, and the need to ensure

digital stability in the region. This issue is particularly significant in the context of increasing digitalization, the use of cyberspace for political and military purposes, and the competition between global and regional actors for influence in the region. The objective of this study is to analyze the legal mechanisms regulating cybersecurity in the three states and identify existing challenges in this area. The study examines key regulatory legal acts and strategic planning documents of Georgia, Azerbaijan, and Armenia in the area of cybersecurity. Based on the analysis, common trends were identified and conclusions were drawn about the differences in countries' approaches to ensuring cybersecurity. Common problems in the region were identified: a shortage of qualified personnel; dependence on foreign technologies; gaps in legislation; data leaks; low levels of information literacy among the population; and duplication of authority between agencies.

Keywords: information law, cyberspace, information security, cyberattacks, cybersecurity, legal regulation of cybersecurity, the South Caucasus, Georgia, Azerbaijan, Armenia

Введение

В настоящее время для государств Южного Кавказа проблема обеспечения кибербезопасности стоит достаточно остро в связи с довольно частыми случаями утечек конфиденциальной информации и кибератак. В январе 2025 г. стало известно о масштабной утечке данных граждан Грузии¹. В 2024 г. в Азербайджане в сеть попали личные данные граждан в результате кибератак². В Армении были зафиксированы массовое распространение фейковой информации, утечки данных, DDoS-атаки³ и т.д. Кроме того, для данных государств сохраняется проблема недостатка квалифицированных кадров и обладания навыками информационной и медийной грамотности, что требует развития правового обеспечения в сфере формирования культуры информационной и кибербезопасности⁴ и соблюдения кибергигиены. Сохраняется и проблема зависимости от зарубежных технологий.

Исследование опыта правового обеспечения кибербезопасности государств Южного Кавказа представляет большой научный интерес в связи с недостаточной

¹ Entire Georgian country population exposed in a massive data leak. URL: <https://cybernews.com/security/entire-georgian-country-population-exposed/> (дата обращения: 10.03.2026).

² Госслужба: Предотвращены целевые кибератаки на сайты государственных учреждений // URL: https://azertag.az/ru/xeber/gossluzhba_predotvrashcheny_celevye_kiberataki_na_saity_gosudarstvennyh_uchrezhdeniy_video-3301240 (дата обращения: 10.03.2026).

³ Все по-старому: российские аналитики назвали главную причину киберуязвимости Армении // URL: <https://am.sputniknews.ru/20250905/vse-po-staromu-rossiyskie-analitiki-nazvali-glavnyuyu-prichinu-kiberuyazvimosti-armenii-92904749.html> (дата обращения: 10.03.2026).

⁴ Полякова Т. А., Минбалеев А. В., Троян Н. А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023. № 5. С. 131.



разработанностью данной проблематики и особым, стратегически важным для России географическим расположением данных государств.

Подходы государств Южного Кавказа к правовому регулированию кибербезопасности

В соответствии с исследованием, опубликованным на сайте Национального индекса кибербезопасности, Грузия в 2025 г. заняла 22-е место в мире и 16-е — в Европе⁵, Армения в данном рейтинге заняла 95-е, а Азербайджан — 52-е место. Эти данные свидетельствуют о том, что среди государств Южного Кавказа и в мире Грузия достигла высоких результатов в сфере обеспечения информационной безопасности.

Государства Южного Кавказа, реагируя на современные угрозы, формируют свою правовую базу в сфере обеспечения информационной безопасности⁶, кибербезопасности и построения цифрового суверенитета⁷, демонстрируя разные подходы, что, вероятно, связано с их современными геополитическими ориентациями, уровнем социально-экономического и политического развития.

В конституциях Грузии, Азербайджана и Армении содержатся нормы, косвенно связанные с обеспечением кибербезопасности, например, через защиту персональных данных (ст. 34 Конституции Армении); тайну связи (ст. 33 Конституции Армении, ст. 32 Конституции Азербайджанской Республики); провозглашение права на доступ к информации о деятельности публичных учреждений (ст. 18 Конституции Грузии), права свободно получать и распространять информацию (ст. 18 Конституции Грузии, ст. 50 Конституции Азербайджанской Республики) и др. В Конституции Грузии закреплено право каждого человека на доступ к Интернету и его свободное использование (п. 4 ст. 17), что, по нашему мнению, представляет собой основу для дальнейшего расширения правового статуса граждан в контексте киберправа.

Основополагающим документом Грузии, определяющим угрозы, риски и вызовы, основные направления политики безопасности, является Концепция национальной безопасности Грузии, в соответствии с которой целью страны является создание системы информационной безопасности, в которой пагубные последствия любой кибератаки будут сведены к минимуму⁸. Анализ Концепции

⁵ National Cyber Security index // URL: <https://ncsi.ega.ee/ncsi-index/> (дата обращения: 10.03.2026).

⁶ Койбаев Б. Г., Золоева З. Т. Развитие информационного общества в Азербайджанской Республике. Владикавказ : Северо-Осетинский государственный университет имени К. Л. Хетагурова, 2024. С. 7.

⁷ Лолаева А. С. Суверенитет 2.0: защита национальных интересов в эпоху цифровых гибридных войн // Российская правовая система: в поисках национальной идентичности : сборник докладов XIV Московской юридической недели : в 6 ч., Москва, 26—29 ноября 2024 года. М. : Университет имени О.Е. Кутафина (МГЮА), 2025. С. 408.

⁸ საქართველოს პარლამენტის დადგენილება «საქართველოს ეროვნული უსაფრთხოების კონცეფციის» დამტკიცების შესახებ 23.12.2011. № 5589-რს // URL: <https://www.matsne.gov.ge/ka/document/view/43156?publication=0> (дата обращения: 10.03.2026).

показывает, что данный документ 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 15 лет, во многом изменилась геополитическая ситуация, появились новые угрозы.

Ключевым документом Грузии в исследуемой сфере является также Закон «Об информационной безопасности» 2012 г., который закрепляет определения понятий «информационная безопасность», «киберпространство», «кибератака» и другие; устанавливает права и обязанности публичного и частного секторов, а также механизмы государственного контроля⁹. Анализ данного документа позволяет сделать вывод о том, что в нем в качестве взаимозаменяемых используются термины «информационная безопасность» и «кибербезопасность».

Национальная стратегия кибербезопасности на 2021—2024 гг. также играла важную роль в обеспечении кибербезопасности, которая рассматривалась как часть национальной безопасности страны¹⁰. Однако в Грузии с 2024 г. отсутствует стратегия в данной области, что, по нашему мнению, негативно влияет на обеспечение кибербезопасности.

Кроме того, в Грузии действует Закон «О защите персональных данных», принятый 14.06.2023, который регулирует обработку данных на территории страны, включая автоматизированные и неавтоматизированные системы, что, по нашему мнению, непосредственно влияет на устойчивость информационных систем к киберугрозам.

В Концепции национальной безопасности Азербайджанской Республики, принятой 23.05.2007, закреплено, что политика информационной безопасности страны базируется на комплексе мер по защите государственных, общественных и частных информационных ресурсов, а также на обеспечении национальных интересов в информационной сфере¹¹. Однако данная Концепция имеет ряд существенных недостатков, связанных с чрезмерной фокусировкой на конкретных угрозах, недостаточной проработкой некоторых аспектов безопасности, а также с институциональными пробелами.

В Азербайджане также действует Закон «О персональных данных» от 11.05.2010, который регулирует сбор, обработку и защиту персональных данных, включая трансграничную передачу. Однако критерии отнесения данных к категориям конфиденциальных или общедоступных не всегда четко определены, что создает простор для толкований и может приводить к нарушениям прав субъектов данных.

⁹ Закон Грузии от 05.06.2012 № 6391-Іс «Об информационной безопасности» // URL: <https://matsne.gov.ge/ru/document/view/1679424?publication=4> (дата обращения: 10.02.2026).

¹⁰ საქართველოს მთავრობის დადგენილება «საქართველოს კიბერუსაფრთხოების 2021—2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ». 30.09.2021. № 482 // URL: <https://matsne.gov.ge/ka/document/view/5263611?publication=0> (дата обращения: 10.03.2026).

¹¹ Концепция национальной безопасности Азербайджанской Республики. Утв. распоряжением Президента Азербайджанской Республики от 23.05.2007 № 2198 // URL: <https://ir.rudn.ru/books/b1/p5/01.pdf> (дата обращения: 10.03.2026).



Указ Президента Азербайджана от 29.12.2004 «О мерах по обеспечению информационной безопасности в государственных органах Азербайджанской Республики» обязывает не включать в состав информационных систем и сетей связи, а также других информационных систем и сетей, используемых для обмена информацией (в том числе глобальной информационной сети Интернет), информационные системы, сети связи и персональные компьютеры, на которых обрабатывается служебная информация, содержащая государственную тайну либо служебную информацию ограниченного распространения¹².

В Азербайджанской Республике вопросы кибербезопасности получили закрепление сравнительно недавно — 28.08.2023 распоряжением Президента Азербайджанской Республики была утверждена Стратегия информационной и кибербезопасности на 2023—2027 гг.¹³ Однако, как показал ее анализ, определения термина «кибербезопасность» в тексте не содержится. В то же время она учитывает современные тренды и проблемы кибербезопасности и делает упор на выявление рисков безопасности в информационном пространстве, а также на укрепление готовности к угрозам, связанным с информационной агрессией и искажением фактов, нарушением национальных ценностей, и борьбу с киберпреступностью.

Представляется, что данная Стратегия демонстрирует новый подход, характеризующий переходом от модели реактивного реагирования на кибератаки и иные инциденты, к построению целостной национальной экосистемы кибербезопасности. Кроме того, в качестве ее особенности необходимо назвать комплексный подход, охватывающий не только технические аспекты, но и совершенствование законодательства, международное сотрудничество и др.

Представляется важным также отметить, что Азербайджан активно продвигает концепцию цифрового нейтралитета, настаивая на том, что кибертехнологии не должны использоваться для вмешательства во внутренние дела других стран.

В Армении важное место в системе регулирования отношений в исследуемой сфере занимает Стратегия кибербезопасности, принятая в 2017 г., в которой основной упор делается на защиту критически важной информационной инфраструктуры¹⁴. На наш взгляд, важно отметить, что в Стратегии акцент сделан на необходимость сотрудничества государственного и частного секторов с целью защиты критически важной информационной инфраструктуры частного сектора от кибератак, включая банковский сектор, государственные услуги и телекоммуникации.

С 04.01.2026 в Армении вступил в силу Закон «О кибербезопасности», который определяет кибербезопасность как комплекс организационных, технических

¹² Azərbaycan Respublikası Prezidentinin Fərmanı 29.12.2004-cü il № 172 «Azərbaycan Respublikasının dövlət orqanlarında informasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlər haqqında» // URL: <https://e-qanun.az/framework/5572> (дата обращения: 10.03.2026).

¹³ Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023—2027-ci illər üçün Strategiyası // URL: <https://itkk.gov.az/az/strategiya/strategiya-haqqinda> (дата обращения: 10.03.2026).

¹⁴ Стратегия кибербезопасности Армении 2017 г. // Единый веб-сайт для публикации правовых актов. URL: <https://www.e-draft.am/projects/581/about> (дата обращения: 10.03.2026).

и программных мер по защите информации в цифровых системах и сетях. Закон нацелен на создание безопасного киберпространства и защиту критически важной инфраструктуры, государственных и частных информационных систем¹⁵. Здесь следует подчеркнуть, что Закон обязывает частные компании соблюдать нормы кибергигиены и сообщать о киберинцидентах в органы государственной власти, а также четко определяет перечень критически важных объектов.

Проведенный анализ позволяет сделать вывод о том, что в государствах Южного Кавказа правовое обеспечение в сфере кибербезопасности находится в стадии формирования. Однако сохраняется проблема наличия пробелов в законодательстве этих государств, а также сохраняется несоответствие мировым стандартам кибербезопасности¹⁶. По нашему мнению, в условиях постоянного совершенствования информационных технологий и возрастания количества киберугроз существует необходимость дальнейшего совершенствования нормативно-правовой базы¹⁷, включая ужесточение ответственности за кибератаки, а также разработки законов, учитывающих успешные международные практики.

Развитие институциональных механизмов в сфере обеспечения кибербезопасности в государствах Южного Кавказа

Важную роль в обеспечении кибербезопасности играют и институциональные механизмы. Так, в результате исследования установлено, что в государствах Южного Кавказа применяются разные подходы к наименованию и статусу органов, ответственных за обеспечение кибербезопасности. Так, в Грузии обеспечение кибербезопасности относится к компетенции таких органов, как Бюро кибербезопасности при Министерстве обороны, Группа помощи Бюро кибербезопасности, Агентство по обмену данными при Министерстве юстиции.

В Азербайджане вопросы обеспечения кибербезопасности подведомственны Государственной службе специальной связи и информационной безопасности, а также Службе электронной безопасности при Министерстве цифрового развития и транспорта.

В Республике Армения вопросы обеспечения информационной безопасности отнесены к компетенции Службы национальной безопасности при Правительстве Республики Армения, а также автономного органа, формируемого Национальной группой реагирования на компьютерные чрезвычайные ситуации.

¹⁵ ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՕՐԵՆԸ «ԿԻԲԵՐԱՆԱՎՏԱՆԳՈՒԹՅԱՆ ՄԱՍԻՆ» Ընդունվել է 04.12.2025. № ՅՕ-442-Ն // URL: <http://www.parliament.am/legislation.php?sel=show&id=10064&lang=arm&enc=utf8> (дата обращения: 10.03.2026).

¹⁶ *Мкртчян А. Р.* Сравнительный анализ правовых стандартов кибербезопасности: Республика Армения и международное право // Международная Восемнадцатая годовичная научная конференция : сборник научных статей, Ереван, 2—6 декабря 2024 года. Ереван : Российско-Армянский (Славянский) университет, 2025. С. 95—104.

¹⁷ *Койбаев Б. Г., Усова Ю. В., Золоева З. Т.* Особенности реализации государственной политики в сфере развития информационного общества в Азербайджанской Республике // Современная наука и инновации. 2023. № 2 (42). С. 170.



Таким образом, в государствах Южного Кавказа сформирован организационный механизм противодействия угрозам кибербезопасности, однако исследователи отмечают проблемы дублирования полномочий силовых структур¹⁸, отсутствия скоординированного подхода¹⁹. Представляется, что это может затруднять эффективное реагирование на кибератаки, в связи с чем существует необходимость в модернизации.

Выводы

Правовая база в сфере кибербезопасности в государствах Южного Кавказа формируется на основе национальных законов, документов стратегического планирования и международных обязательств. Законодательные инициативы преимущественно ориентированы на обеспечение безопасности ключевых секторов экономики и системы государственного управления.

Из государств Южного Кавказа вопросы кибербезопасности ранее всех закрепила Грузия. В Армении и Азербайджане нормативные акты, регулирующие данные вопросы, были приняты позднее. До этого регулирование общественных отношений в данной сфере осуществлялось при помощи положений документов, регламентирующих вопросы информационной безопасности.

Анализ текущего состояния правового обеспечения кибербезопасности на Южном Кавказе позволяет сделать вывод о наличии устойчивой тенденции к усилению регуляторных мер в данной сфере. Наблюдается активное создание специализированных институтов, осуществляющих противодействие киберугрозам. При этом темпы и подходы к развитию нормативно-правовой базы в государствах региона существенно различаются. В то же время данные государства сталкиваются с необходимостью адаптации законодательства к быстро меняющейся цифровой среде, что сопровождается нехваткой квалифицированных кадров и необходимостью осуществления международного сотрудничества.

Государства Южного Кавказа демонстрируют разные подходы к правовому регулированию кибербезопасности и разную степень проработки регуляторных механизмов.

Так, подход Грузии в настоящее время характеризуется регулированием кибербезопасности в рамках Закона «Об информационной безопасности».

Республика Армения сделала шаг к системному регулированию посредством принятия Закона «О кибербезопасности», особенностью подхода этой страны является также закрепление необходимости сотрудничества государственного и

¹⁸ Ларссон Р., Квашилава Г. Информационная безопасность Грузии: проблемы развития информационно-коммуникационных технологий и создания программ в этой области // URL: https://ca-c.org.ru/journal/2003/journal_rus/cac-05/15.larrus.shtml (дата обращения: 10.03.2026).

¹⁹ Овакимян А. А. Политика Республики Армения в контексте обеспечения кибербезопасности // Шестнадцатая годовичная научная конференция : сборник научных статей конференции, приуроченной к 25-летию основания РАУ, Ереван, 5—9 декабря 2022 года. Ереван : Российско-Армянский (Славянский) университет, 2023. С. 306—312.

частного секторов с целью защиты критически важной информационной инфраструктуры.

Подход Азербайджанской Республики характеризуется сочетанием национального законодательства об информационной безопасности и документов стратегического планирования в сфере обеспечения кибербезопасности.

БИБЛИОГРАФИЯ

1. *Койбаев Б. Г., Золоева З. Т.* Развитие информационного общества в Азербайджанской Республике. — Владикавказ : Северо-Осетинский государственный университет имени К. Л. Хетагурова, 2024. — 172 с.
2. *Койбаев Б. Г., Усова Ю. В., Золоева З. Т.* Особенности реализации государственной политики в сфере развития информационного общества в Азербайджанской Республике // Современная наука и инновации. — 2023. — № 2 (42). — С. 168—174.
3. *Лолаева А. С.* Суверенитет 2.0: защита национальных интересов в эпоху цифровых гибридных войн // Российская правовая система: в поисках национальной идентичности : сборник докладов XIV Московской юридической недели : в 6 ч., Москва, 26—29 ноября 2024 года. — М. : Университет имени О.Е. Кутафина (МГЮА), 2025. — С. 406—409.
4. *Мкртчян А. Р.* Сравнительный анализ правовых стандартов кибербезопасности: Республика Армения и международное право // Международная Восемнадцатая годичная научная конференция : сборник научных статей, Ереван, 2—6 декабря 2024 года. — Ереван : Российско-Армянский (Славянский) университет, 2025. — С. 95—104.
5. *Овакимян А. А.* Политика РА в контексте обеспечения кибербезопасности // Шестнадцатая годичная научная конференция : сборник научных статей конференции, приуроченной к 25-летию основания РАУ, Ереван, 5—9 декабря 2022 года. — Ереван : Российско-Армянский (Славянский) университет, 2023. — С. 306—312.
6. *Полякова Т. А., Минбалева А. В., Троян Н. А.* Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. — 2023. — № 5. — С. 131—144.

