DOI 10.35775/PSI.2025.75.10.013
УДК 32.327

М.М. АБДУЖАЛИЛОВА
магистрант кафедры теории и истории
международных отношений РУДН имени Патриса Лумумбы,
Россия, г. Москва

К.Х. САЛИМЗОДА
соискатель кафедры государственного
управления и национальной безопасности Российской академии народного хозяйства и государственной службы
при Президенте Российской Федерации,
Россия, г. Москва

Д.Д. ХИДИРОВА
магистрант кафедры теории и истории
международных отношений РУДН имени Патриса Лумумбы,
Россия, г. Москва

СОВРЕМЕННОЕ СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРАНАХ ОДКБ

В современных международных отношениях информационная безопасность приобретает стратегическое значение для государств-членов Организации Договора о коллективной безопасности (ОДКБ). Цель статьи заключается в детальном анализе современного состояния информационной безопасности в странах ОДКБ и выявлении ключевых вызовов, тенденций и направлений коллективного сотрудничества. Особое внимание уделяется влиянию глобальных киберугроз на национальные стратегии и необходимость гармонизации подходов всех стран-участниц. Методологическая база исследования включает сравнительный анализ национальных стратегий, официальных документов и публикаций по информационной безопасности. Результаты исследования показывают, что страны ОДКБ сталкиваются с общими киберугрозами, однако уровень их готовности и механизмы реагирования существенно различаются. В работе подчеркивается важность обмена передовым опытом и регулярного проведения совместных учений для повышения коллективной устойчивости. Наиболее высокий уровень информационной безопасности наблюдается в России и Казахстане, тогда как Таджикистан и Киргизия остаются с низким уровнем готовности, что ограничивает эффективность коллективных механизмов реагирования. Анализ выявил недостаточную координацию и обмен информацией между государствами, а также частичное применение международных стандартов ISO/IEC 27000. Кроме того, рассмотрены перспективы внедрения инновационных технологий мониторинга угроз и цифровых платформ для совместного реагирования. Исследование делает вывод о необходимости совершенствования национальных правовых механизмов, укрепления координации и внедрения совместных инструментов защиты от киберугроз. Применение международных стандартов, регулярные совместные учения и создание платформ для обмена

информацией могут существенно повысить устойчивость информационных систем государств-участников ОДКБ.

Ключевые слова: *ОДКБ, информационная безопасность, киберугрозы, международное сотрудничество, коллективная безопасность, координация, правовые механизмы, цифровая инфраструктура, стандарты ISO/IEC 27000, обмен информацией, киберустойчивость.*

В последние годы информационная безопасность стала одним из ключевых элементов коллективной и национальной безопасности для государств-членов Организации Договора о коллективной безопасности (ОДКБ). Рост цифровизации государственных органов и критической инфраструктуры значительно повысил значение киберугроз и необходимость выработки согласованных мер защиты. Кроме того, увеличение числа трансграничных кибератак делает региональное сотрудничество еще более необходимым и стратегически значимым для всех стран-участниц.

Современная статистика указывает на устойчивый рост числа сложных киберинцидентов, направленных на государственные учреждения, банковский сектор, энергетическую и телекоммуникационную инфраструктуру. Эти тенденции подчеркивают, что безопасность цифрового пространства становится неотъемлемой частью национального суверенитета, что требует комплексного подхода и активного участия международных организаций. Для ОДКБ это означает необходимость формирования единого пространства доверия и стандартизированных механизмов обмена информацией, что на данный момент остается ограниченным [9. С. 15].

Несмотря на значительный прогресс в создании нормативной и институциональной базы, государства сталкиваются с серьезными вызовами, такими как недостаточная координация, различия в уровне технической оснащенности, слабая подготовка кадров и отсутствие единых критериев оценки киберустойчивости. Особое внимание в данном контексте уделяется подготовке квалифицированного персонала, повышению технической компетентности и внедрению современных систем мониторинга угроз.

Анализ существующих источников показывает, что большинство исследований сосредоточено либо на национальных стратегиях, либо на отдельных аспектах коллективной безопасности. При этом отсутствуют систематические сопоставления подходов всех государств-участниц ОДКБ, что затрудняет объективную оценку текущего состояния и препятствует разработке гармонизированных решений. Данный пробел особо актуален в условиях растущей зависимости государств от цифровых технологий и усложнения геополитической обстановки [15. С. 89].

Кроме того, ограниченная интеграция международных стандартов ISO/IEC 27000, а также недостаточный и нерегулярный обмен информацией между государствами создают дополнительные препятствия для укрепления коллективной устойчивости. Отсутствие единой методологии оценки и обмена данными приводит к тому, что страны реагируют на инциденты несогласованно, что снижает эффективность коллективных мер безопасности [19. С. 102].

Основная цель данного исследования заключается в критическом анализе современного состояния информационной безопасности в странах ОДКБ, вы-

явлении ключевых недостатков и проблем, а также оценке эффективности существующих коллективных механизмов реагирования. В рамках исследования предполагается определить направления для совершенствования правовой базы, укрепления координации и внедрения современных совместных инструментов защиты от киберугроз.

Кроме того, работа направлена на разработку практических рекомендаций, которые могут быть использованы для повышения эффективности национальных стратегий, усиления взаимодействия между государствами-участниками и улучшения подготовки к коллективным операциям по обеспечению кибербезопасности.

Следует подчеркнуть, что в работах российских авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 2; 3; 7; 12; 14; 17; 18; 20; 22; 26; 27].

Однако проблему обеспечения информационной безопасности в странах ОДКБ нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

ОДКБ была создана после распада Советского Союза и нацелена на региональное сотрудничество в сфере безопасности. Изначально приоритет отдавался военному сотрудничеству, однако с начала 2000-х годов вопросы информационной безопасности, киберугроз и цифрового шпионажа стали стратегическими приоритетами, что отражает процесс адаптации коллективного подхода к безопасности ОДКБ к требованиям современности, как отмечает Выходец. Переориентация организации на цифровые угрозы была обусловлена не только технологическим прогрессом, но и появлением новых форм противоборства, в которых киберпространство стало использоваться как инструмент политического давления и подрыва внутригосударственной стабильности. Вследствие этого государства-участники усилили внимание к созданию совместных механизмов мониторинга, обмена оперативной информацией и координации ответных мер, что позволило постепенно формировать основы коллективной киберустойчивости в рамках ОДКБ [4. С. 84].

Члены ОДКБ разрабатывают национальные стратегии в области информационной безопасности, отражающие приоритеты и уровень цифровой зрелости каждого государства. Несмотря на общие подходы к обеспечению киберустойчивости, национальные документы существенно различаются по степени детализации, уровню технологической оснащенности и механизмам международного взаимодействия.

Сравнительный анализ национальных стратегий и программ государств-членов ОДКБ в сфере обеспечения информационной безопасности.

Армения. Армения, в соответствии с Национальной стратегией безопасности 2020 года и соответствующими законодательными инициативами, предприняла быстрые шаги по институционализации кибербезопасности. Государственные учреждения обеспечены централизованным центром реагирования на компьютерные инциденты (CSIRT), что укрепляет межведомственную координацию. Для критической инфраструктуры внедряются регулярные оценки киберрисков и аудиты соответствия. Для повышения технического потенциала налажено со-

трудничество с международными организациями, такими как ITU и DCAF, а правовая база обеспечивает обмен информацией между государственными и частными структурами. Дополнительно реализуются образовательные и сертификационные программы для подготовки специалистов, а также проводятся национальные кибертренировки. Эти меры направлены на комплексное укрепление стратегической и оперативной устойчивости Армении в сфере информационной безопасности.

Беларусь. Беларусь сосредоточилась на обеспечении информационной безопасности через усиление национальной системы мониторинга и контроля информационного пространства. Созданы механизмы централизованного реагирования на компьютерные инциденты, усилены регуляторные требования для критически важных объектов и расширены полномочия уполномоченных органов. Проводится развитие системы кибершпионажа и анализа угроз, что позволяет снизить зависимость от внешних ресурсов. Практическое внедрение включает регулярные проверки соответствия стандартам и обмен информацией с частным сектором. Эти меры направлены на повышение оперативной готовности и укрепление национальной устойчивости к внешним киберугрозам [6. С. 65].

Казахстан. Казахстан реализует концепцию «Киберщит» и многослойную архитектуру защиты национальной цифровой инфраструктуры. Созданы национальные центры анализа киберугроз и структуры SOC, проводится сертификация государственных и критических систем. Внедряются международные стандарты ISO/IEC, а также регулярные национальные кибертренировки. Особое внимание уделяется взаимодействию с частными операторами цифровых услуг и обмену информацией. Эти меры позволяют Казахстану усилить стратегическое лидерство в регионе и повысить готовность к совместным действиям по киберзащите (1. С. 5).

Кыргызстан. Кыргызстан сосредоточен на обновлении законодательной базы и формировании единых стандартов защиты государственных информационных систем. Созданы национальные и ведомственные группы реагирования на инциденты, реализуются образовательные программы и международные проекты по повышению квалификации персонала. Несмотря на ограниченные ресурсы, построены пилотные центры и базовые механизмы защиты критически важных объектов. Данные меры направлены на постепенное наращивание национальной и региональной устойчивости к киберугрозам, при сохранении зависимости от внешней поддержки в случае крупных инцидентов [21. С. 1].

Россия. Россия применяет комплексную государственную политику, объединяющую юридические, технические и организационные меры. Усилена защита критической инфраструктуры, введены строгие стандарты для операторов, стимулируется развитие отечественных технологий и независимых решений. Проводятся масштабные национальные кибертренировки, развиваются кибервойска и активно осуществляется международное сотрудничество в области кибердипломатии. Эти меры обеспечивают высокую степень готовности, координации и стратегического лидерства России в регионе [24. С. 1].

Таджикистан. Таджикистан, обладая ограниченными ресурсами, сосредоточен на создании базовой нормативно-правовой базы и базовых механизмов защиты критически важных систем. Реализуются программы подготовки специалистов и технического усиления с поддержкой международных партнеров. Постепенно развиваются системы реагирования на инциденты и раннего пред-

упреждения, однако национальные центры остаются с ограниченными возможностями. Эти меры направлены на повышение устойчивости страны при сохранении необходимости внешней поддержки и сотрудничества (2. С. 1).

Между национальными стратегиями стран-участниц ОДКБ существуют заметные несоответствия и недостатки координации, что существенно ограничивает эффективность коллективного подхода к информационной безопасности. Как отмечает Зайцев, различия в приоритетах, уровнях технической готовности и применении международных стандартов создают препятствия для согласованного реагирования на киберугрозы, подчеркивая необходимость укрепления совместных механизмов и регулярного обмена информацией [8. С. 16].

ОДКБ создала различные правовые и институциональные механизмы для обеспечения информационной безопасности. Однако между ними наблюдаются несоответствия и проблемы координации. Фролов отмечает, что совместные документы ОДКБ в области информационной безопасности не полностью согласованы с национальными законами стран-участниц, что снижает эффективность коллективных усилий по защите информации и подчеркивает необходимость гармонизации законодательства и улучшения координации между государствами [25. С. 82].

Страны ОДКБ стремятся разрабатывать совместные системы реагирования на киберугрозы, однако эффективность этих систем во многом определяется уровнем подготовки и координации государств-участников. Медведев подчеркивает, что киберзащитные возможности России значительно выше, чем у других стран-участников, и эта диспропорция снижает общую эффективность коллективных механизмов реагирования [11. С. 35].

Анализ текущего уровня информационной безопасности стран ОДКБ. Страны члены ОДКБ, чтобы укрепить информационную безопасность, проводят масштабные кибертренировки, защищают критическую инфраструктуру и внедряют комплексные стандарты для операторов;

Россия проводит масштабные кибертренировки, защищает критическую инфраструктуру и внедряет комплексные стандарты для операторов, что, как отмечает Выходец, отражает стратегический подход к обеспечению кибербезопасности [4. С. 84].

Казахстан создает национальные SOC, применяет международные стандарты ISO/IEC и развивает центры анализа угроз, опираясь на рекомендации Национальных стратегий Казахстана; это повышает готовность к совместным действиям и укрепляет региональное лидерство [13. С. 14].

Армения формирует CSIRT и проводит регулярную оценку рисков критической инфраструктуры, что способствует укреплению стратегической и оперативной устойчивости, несмотря на ограниченные ресурсы, как подчеркивает Лапшин [10. С. 42].

Беларусь усиливает национальный мониторинг, централизованное реагирование на инциденты и обмен информацией с частным сектором; при этом интеграция с международными стандартами остается ограниченной, указывает Фролов [25. С. 82].

Кыргызстан постепенно создает национальные и ведомственные группы реагирования, реализует образовательные программы и привлекает международную поддержку; однако слабая техническая база делает страну зависимой от внешней помощи, как показывает Третьяков [23. С. 18].

Таджикистан сосредоточен на создании базовой нормативно-правовой базы и подготовке специалистов, однако низкая техническая готовность ограничивает эффективность коллективной защиты, отмечает Медведев [11. С. 36].

Все страны ОДКБ, согласно Эрмолову, направляют усилия на повышение устойчивости к киберугрозам через координацию, обмен информацией и внедрение международных стандартов, обеспечивая более высокий уровень коллективной безопасности региона [29. С. 14].

Национальные стратегии и сопутствующие документы стран-участниц были подвергнуты сравнительному анализу, что позволило выявить как общие тенденции и лучшие практики, так и значительные различия в подходах и недостатки в координации между государствами.

Эффективность правовых и институциональных механизмов, созданных в рамках ОДКБ, была тщательно оценена с учетом выявленных несоответствий и проблем координации, что позволило определить ключевые области для совершенствования коллективного подхода к информационной безопасности.

Были проанализированы усилия стран ОДКБ по внедрению международных стандартов информационной безопасности, таких как ISO/IEC 27000, и тщательно оценен уровень их практического применения, что позволило выявить как достижения, так и существующие пробелы в стандартизации.

Законы об информационной безопасности стран-членов должны быть обновлены и приведены в полное соответствие с международными стандартами. Следует разработать превентивные меры против кибератак с внедрением тяжелых санкций за нарушения. В качестве успешных примеров в литературе приводятся реформы Беларуси и Казахстана, что подтверждается официальными национальными документами [13. С. 14].

Третьяков подчеркивает, что для критической инфраструктуры и государственных информационных систем каждая страна-член должна создавать локальные центры кибербезопасности. Он также указывает на необходимость проведения регулярных национальных киберучений и симуляций для накопления опыта персонала. Программы обучения и сертификации, по мнению Третьякова, должны быть тщательно разработаны и внедрены для повышения профессиональной квалификации специалистов [23. С. 18].

Для дата-центров, государственных сетей и критических систем стран-членов необходимо создать системы оценки рисков и постоянного мониторинга. Как отмечает Медведев, также следует формировать экстренные подразделения для оперативного реагирования на киберугрозы [11. С. 37].

Общие системы раннего оповещения требуют создания механизмов моментального обмена данными и уведомлений о кибератаках между странами-членами. Лапшин указывает, что сокращение времени реагирования на киберинциденты значительно повысит коллективную безопасность [10. С. 42].

В рамках ОДКБ необходимо регулярно проводить киберучения и кризисные симуляции во всех странах-членах. Третьяков отмечает, что образовательные программы должны быть ориентированы на развитие технических навыков и компетенций по управлению кризисными ситуациями [23. С. 20].

Следует создать совместную цифровую платформу для обмена разведданными о киберугрозах и опытом между странами-членами. Лапшин подчеркивает, что

такая платформа должна включать информацию как на техническом, так и на стратегическом уровне, обеспечивая более эффективное сотрудничество и реагирование.

Внедрение стандартов ISO/IEC 27000 требует от стран-членов приведения процессов информационной безопасности в полное соответствие с международными требованиями. Шевченко отмечает, что это повысит доверие между системами и укрепит коллективную способность к реагированию на киберугрозы [28. С. 24].

Страны ОДКБ должны адаптировать передовые практики кибербезопасности на основе международного опыта. Третьяков подчеркивает, что это способствует развитию потенциала как на техническом, так и на стратегическом уровне, усиливая общую устойчивость к киберугрозам [23. С. 21].

Сотрудничество с международными организациями и другими региональными структурами поддерживает развитие коллективных механизмов защиты. Эрмолов указывает, что внедрение совместных стандартов и механизмов взаимного контроля значительно повышает эффективность коллективной киберзащиты [29. С. 9].

На национальном уровне необходимо усиление правовой базы и киберспособностей. Фролов подчеркивает важность укрепления законодательства и развития киберспособностей для повышения общей устойчивости систем [25. С. 82].

На коллективном уровне следует внедрить координированные системы раннего оповещения, учения и платформы обмена информацией. Иванов в своем исследовании упоминает, что такие меры существенно повышают готовность стран-членов к совместному реагированию на киберугрозы [9. С. 30].

Применение международных стандартов и обмен опытом значительно повысит коллективную информационную безопасность и устойчивость ОДКБ. Эрмолов в своем исследовании рассказывает о том, что совместное использование стандартов и обмен практиками существенно укрепляют коллективную киберустойчивость [29. С. 14].

Исследования и анализ показывают, что Россия и Казахстан обладают самым высоким уровнем информационной безопасности среди стран-членов, тогда как Таджикистан и Кыргызстан остаются на низком уровне готовности и отстают. Медведев отмечает, что эта гетерогенная структура ограничивает эффективность коллективных систем реагирования [11. С. 36].

Обмен данными о киберугрозах между странами-членами крайне недостаточен. Лапшин указывает на то, что совместные системы раннего предупреждения и учения применяются частично, что ограничивает их эффективность [10. С. 43].

Стандарты ISO/IEC 27000 внедрены частично; Шевченко подчеркивает, что в некоторых странах продолжаются проблемы с их соблюдением, что негативно влияет на коллективную информационную безопасность и устойчивость ОДКБ [28. С. 24].

Укрепление национальной правовой базы остается критическим. Доктрина информационной безопасности Российской Федерации рекомендует, чтобы все страны-члены привели законы о цифровой информационной безопасности в соответствие с международными стандартами и повысили санкции до сдерживающего уровня [5. С. 15].

Для критической инфраструктуры и государственных информационных систем необходимо создать центры кибербезопасности в каждой стране, а для пер-

сонала – программы сертификации и обучения под руководством уполномоченных специалистов, на что обращает внимание Третьяков [23. С. 18].

Следует внедрить совместные системы раннего предупреждения, киберучения и платформы обмена информацией. Медведев подчеркивает важность проведения коллективных учений под руководством России и Казахстана и развития потенциала Таджикистана и Кыргызстана [11. С. 36].

Полное применение стандартов ISO/IEC 27000 необходимо обеспечить. Шевченко указывает, что страны-члены должны адаптировать международный опыт и лучшие практики к своим стратегиям [28. С. 27].

Расширение сотрудничества с международными организациями и региональными структурами также критично. Эрмолов отмечает необходимость внедрения совместных стандартов и механизмов контроля [29. С. 9].

Эти рекомендации значительно повысят устойчивость информационных систем стран-членов ОДКБ и коллективный потенциал защиты. Эрмолов подчеркивает, что укрепление правовой, институциональной и технической базы уменьшит воздействие киберугроз и обеспечит доверие между странами, а применение международных стандартов и обмен опытом улучшит региональное сотрудничество [29. С. 14].

Некоторые данные стран-членов недоступны или ограничены. Выходец обращает внимание на то, что киберугрозы постоянно меняются, и текущие анализы со временем могут терять актуальность; рекомендации должны учитывать местные условия при внедрении [4. С. 83].

Заключение. Анализ текущего состояния информационной безопасности в странах ОДКБ показывает значительную неоднородность уровня готовности и способности к коллективному реагированию. В некоторых государствах создана развитая техническая и институциональная база, тогда как другие сталкиваются с ограниченными ресурсами и недостаточной координацией.

Для повышения эффективности коллективной защиты важно укреплять национальные правовые механизмы, развивать инфраструктуру кибербезопасности и обеспечивать подготовку специалистов. Регулярные киберучения, обмен опытом и внедрение международных стандартов помогут повысить общую устойчивость информационных систем региона.

Комплексный подход, объединяющий технические, организационные и стратегические меры, позволит создать согласованную и готовую к угрозам региональную структуру, способную эффективно противостоять современным и будущим киберугрозам.

ПРИМЕЧАНИЯ:

(1) Государство Казахстан // Cyber Shield. 2021.

(2) Национальные показатели NCSI, 2022.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Алаудинов А.А., Манойло А.В.** Когнитивная и ментальная составляющие современной гибридной войны // Вопросы политологии. 2024. № 2.

2. **Буданцев Э.В.** Информационная безопасность как фактор стратегического суверенитета на пространстве Большой Евразии // Евразийский Союз: вопросы международных отношений. 2024. № 6.
3. **Власов М.С.** Особенности информационного противостояния России и США в гибридной войне // Вопросы национальных и федеративных отношений. 2024. № 3.
4. **Выходец Р.С.** Политика обеспечения информационно-психологической безопасности ОДКБ в условиях глобальной стратегической конкуренции // Вестник Российского университета дружбы народов. Международные отношения. 2025. Т. 25. № 1.
5. Доктрина информационной безопасности Российской Федерации. Москва: Министерство обороны РФ, 2017 // http://publication.pravo.gov.ru/Document/View/0001201702060002.
6. Доктрина информационной безопасности Республики Беларусь, 2019.
7. **Жбанов А.М.** Современные тенденции политики кибербезопасности крупных держав // Вопросы политологии. 2024. № 7.
8. **Зайцев М.А.** Сравнительный анализ национальных стратегий информационной безопасности стран ОДКБ // Вестник безопасности. 2022. Т. 10. № 4.
9. **Иванов А.** Киберугрозы и коллективная оборона. Москва: Научный центр безопасности, 2020.
10. **Лапшин В.В.** Координация и обмен информацией в ОДКБ // Журнал региональной безопасности. 2021. Т. 14. № 3.
11. **Медведев С.Г.** Системы коллективного реагирования на киберугрозы // Вестник международных отношений. 2020. Т. 8. № 2.
12. **Медведева В.К., Медведев Н.П.** Постсоветские государства Центральной Азии: ЕАЭС, ОДКБ и геополитические интересы России // Евразийский Союз: вопросы международных отношений. 2025. № 6.
13. Национальные стратегии и программы кибербезопасности Республики Казахстан и Республики Таджикистан. Астана/Душанбе, 2018-2021 // https://cpi.gov.kz/documents/national-cybersecurity-strategy.
14. **Никитин Н.А.** Основные подходы к определению понятия «киберпространство» в контексте международных отношений – зарубежный опыт // Вопросы политологии. 2025. № 6.
15. **Петров С.В.** Современные тенденции киберугроз и стратегия ОДКБ. Москва: Научный журнал безопасности, 2021.
16. **Семёнов И.А.** Информационная безопасность и цифровая устойчивость в Центральной Азии // Журнал международной безопасности. 2021. Т. 12. № 2.
17. **Скуридин А.А., Малявина А.Б., Шевченко А.В., Григорян Д.К.** Перспективы развития ОДКБ: вызовы и возможности в контексте поддержания мира в постсоветских регионах // Евразийский Союз: вопросы международных отношений. 2025. № 1.
18. **Слизовский Д.Е., Медведев Н.П.** Информационные, гибридные и прокси-войны: обзор новейших исследований // Вопросы политологии. 2024. № 12.

19. **Смирнов А.П.** Проблемы интеграции международных стандартов в национальные системы ОДКБ // Журнал кибербезопасности. 2020. Т. 7. № 1.
20. **Степовая Д.А.** Безопасность национального киберпространства в условиях информационно-психологического противоборства // Вопросы политологии. 2023. № 5.
21. Стратегия кибербезопасности Кыргызской Республики 2019-2023. Бишкек, 2019.
22. **Сулейманов Э.А.** Реализация информационной политики государства в современных условиях // Евразийский Союз: вопросы международных отношений. 2024. № 2.
23. **Третьяков А.В.** Развитие киберспособностей в странах ОДКБ // Журнал кибербезопасности. 2020. Т. 5. № 1.
24. Указ Президента РФ / Доктрина информационной безопасности. Москва, 2016-2017.
25. **Фролов П.С.** Правовая база информационной безопасности в СНГ // Вестник права. 2018. № 7.
26. **Хопёрская Л.Л.** Евразийская безопасность: концепции и инициативы // Евразийский Союз: вопросы международных отношений. 2025. № 1.
27. **Шавлохов А.К., Максименко Д.И.** Актуальные вопросы обеспечения информационной безопасности населения в условиях военных конфликтов: правовые аспекты // Региональное и муниципальное управление: вопросы политики, экономики и права. 2023. № 3.
28. **Шевченко О.М.** Международные стандарты ISO/IEC 27000 и их применение в странах ОДКБ // Информационная безопасность и стандарты. 2019. № 3.
29. **Эрмолов А.Н.** Международное сотрудничество и коллективная кибербезопасность. Санкт-Петербург: Центр стратегических исследований, 2025.

M.M. ABDUJALILOVA
Master of International Relations,
Department of Theory and History, Patrice Lumumba
Peoples' Friendship University of Russia,
Moscow, Russia

K.H. SALIMZODA
PhD student at the Department of Public
Administration and National Security at the Russian Presidential
Academy of National Economy and Public Administration,
Moscow, Russia

D.D. KHIDIROVA
Master of International Relations,
Department of Theory and History, Patrice Lumumba
Peoples' Friendship University of Russia,
Moscow, Russia

THE CURRENT STATE OF INFORMATION SECURITY IN THE CSTO COUNTRIES

In contemporary international relations, information security has become a strategic priority for the member states of the Collective Security Treaty Organization (CSTO). The main aim of this study is to provide a detailed analysis of the current state of information security in CSTO countries, identifying key challenges, trends, and directions for collective cooperation. Special attention is given to the impact of global cyber threats on national strategies and the need for harmonization of approaches among all member states. The research methodology involves a comparative analysis of national strategies, official documents, and publications on information security. The results show that CSTO countries face common cyber threats, yet their preparedness levels and response mechanisms vary significantly. The study emphasizes the importance of sharing best practices and regularly conducting joint exercises to enhance collective resilience. Russia and Kazakhstan exhibit the highest levels of information security, while Tajikistan and Kyrgyzstan still have low preparedness levels, which limits the effectiveness of collective response mechanisms. The analysis also highlights insufficient coordination and information sharing among member states, as well as the partial implementation of ISO/IEC 27000 international standards. Additionally, the potential for adopting advanced threat monitoring technologies and digital platforms for joint response is examined. The study concludes that legal frameworks at the national level should be fully developed, coordination strengthened, and joint tools for countering cyber threats implemented. The adoption of international standards, regular joint exercises, and the creation of information-sharing platforms can substantially enhance the resilience of information systems in CSTO member states.

Key words: *CSTO, information security, cyber threats, international cooperation, collective security, coordination, legal mechanisms, digital infrastructure, ISO/IEC 27000 standards, information sharing, cyber resilience.*