DOI: 10.22394/2073-2929-2024-03-83-90

специальность: 5.1.5

EDN: WAVWMQ

Анализ законодательства стран ЕАЭС в области борьбы с киберпреступностью

Клюканова Т. М.*, Виниченко А. Т., Христинченко К. Ю.
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления РАНХиГС), Санкт-Петербург, Российская Федерация
*e-mail: tatianam1211@mail.ru

РЕФЕРАТ

В статье представлен анализ законодательства о кибербезопасности в странах — участницах Евразийского экономического союза (ЕАЭС). Рассмотрены основные аспекты правового регулирования киберпреступности в отдельных странах, а также выявлены проблемы и недостатки в законодательстве. Обсуждаются устаревшие нормы и неоднозначности в законодательстве, неспособные адекватно реагировать на современные вызовы киберпреступности. Подчеркивается важность комплексного подхода к обеспечению кибербезопасности, который включает не только правовое регулирование, но и технические, организационные и образовательные меры. Сравнительно-правовой метод исследования законодательства позволил выявить общие тенденции, различия и эффективность принимаемых мер в борьбе с киберпреступностью.

Цель. Анализ законодательства стран Евразийского экономического союза в области кибербезопасности и борьбы с киберпреступностью, выявление общих тенденций и различий, оценка эффективности принятых мер, а также определение направлений для дальнейшего улучшения кибербезопасности в регионе.

Задачи. Осуществление анализа законодательства стран — участниц ЕАЭС в сфере кибербезопасности, оценка принимаемых мер по противодействию киберпреступности, выявление общих тенденций и различий в нормативных подходах, определение направлений для совершенствования правовой базы и практических мер в области борьбы с киберпреступностью.

Методология. При осуществлении анализа правовых актов стран — участниц ЕАЭС по кибербезопасности и киберпреступности применены диалектический подход, а также сравнительный, системный и функциональный методы исследования общих тенденций и различий, дана оценка эффективности применения законодательства в противодействии киберугрозам, проведена идентификация проблем и предложены направления для совершенствования правовой базы с учетом современных вызовов в области кибербезопасности.

Результаты. Сформулированы предложения по улучшению обмена информацией и опытом, разработке общих стратегий и стандартов в области кибербезопасности, сокращению числа успешных кибератак за счет совместных усилий, а также по повышению уровня защищенности информационных систем и данных благодаря совместным техническим и организационным мерам.

Выводы. Сотрудничество между странами — участницами ЕАЭС в области кибербезопасности может привести к сокращению числа киберпреступлений, повышению уровня защищенности информационных систем и данных, стимулированию инновационного развития в цифровой сфере, а также укреплению доверия к электронным сервисам и развитию цифровой экономики в регионе, что является ключевыми аспектами в современном информационном обществе.

Ключевые слова: кибербезопасность, Евразийский экономический союз (ЕАЭС), борьба с киберугрозами, борьба с киберпреступностью, проблемы в законодательстве, организационные меры, защита

Для цитирования: Клюканова Т. М., Виниченко А. Т., Христинченко К. Ю. Анализ законодательства стран ЕАЭС в области борьбы с киберпреступностью // Евразийская интеграция: экономика, право, политика. 2024. Т. 18. № 3. С. 83–90.
https://doi.org/10.22394/2073-2929-2024-03-83-90. EDN: WAVWMQ

Analysis of the Legislation of the EEU Countries in the Field of Combating Cybercrime

Tatyana M. Klyukanova*, Karina T. Vinichenko, Kirill Yu. Khristinchenko
Russian Presidential Academy of National Economy and Public Administration (North-West Institute of Management), Saint Petersburg, Russian Federation
*e-mail: tatianam1211@mail.ru

ABSTRACT
The article presents an analysis of cybersecurity legislation in the member countries of the Eurasian Economic Union (EAEU), focusing on Russia, Kazakhstan, Kyrgyzstan and Belarus. In four parts of the article, the main aspects of the legal regulation of cybercrime in each of these countries are considered, as well as problems and shortcomings in legislation are identified. Outdated norms and ambiguities in legislation that are unable to adequately respond to modern challenges of cybercrime are discussed. The importance of an integrated approach to cybersecurity is emphasized, which includes not only legal regulation, but also technical, organizational and educational measures. It is proposed to conduct a more in-depth analysis and comparison of legislation to identify common trends, differences and the effectiveness of measures taken in the fight against cybercrime.
Aim. Analysis of the legislation of the Eurasian Economic Union (EAEU) member states in the field of cybersecurity and cybercrime prevention, identification of common trends and differences, evaluation of the effectiveness of measures taken, and determination of directions for further improvement of cybersecurity in the region.
Tasks. Analysis of the legislation of the EAEU member states in the field of cybersecurity, evaluation of measures taken to counter cyber threats, identification of common trends and differences in regulatory approaches, determination of directions for improving the legal framework and practical measures in combating cybercrime.
Methods. Analysis of the legal acts of the EAEU member states on cybersecurity and cybercrime, comparative analysis to identify common trends and differences, evaluation of the effectiveness of legislation in countering cyber threats, identification of problems, and proposal of directions for improving the legal framework considering modern challenges in cybersecurity.
Results. Expected improvement in information exchange and experience sharing, development of common strategies and standards in cybersecurity, reduction in the number of successful cyberattacks through joint efforts, and enhancement of the security level of information systems and data through joint technical and organizational measures.
Conclusions. Cooperation among the EAEU member states in cybersecurity can lead to a reduction in the number of cybercrimes, enhancement of the security level of information systems and data, stimulation of innovative development in the digital sphere, and strengthening trust in electronic services and the development of the digital economy in the region, which are key aspects in the modern information society.
Keywords: cybersecurity, Eurasian Economic Union (EAEU), combating cyber threats, legislative issues, organizational measures, comprehensive approach, protection
For citation: Klyukanova T. M., Vinichenko K. T., Khristinchenko K. Yu. Analysis of the Legislation of the EEU Countries in the Field of Combating Cybercrime // Eurasian Integration: Economics, Law, Politics. 2024. Vol. 18. No. 3. P. 83–90. (In Russ.)
https://doi.org/10.22394/2073-2929-2024-03-83-90. EDN: WAVWMQ

Введение

В современном мире цифровые технологии широко проникают во все сферы жизни, обеспечивая удобство и эффективность, но при этом создавая новые угрозы и вызовы. Одной из таких угроз является киберпреступность — преступная деятельность, совершаемая с использованием информационных и коммуникационных технологий. Киберпреступность включает в себя широкий спектр деяний, начиная от хакерских атак и кибершпионажа до финансовых мошенничеств и распространения вредоносного программного обеспечения.

В современном мире киберпреступность является одной из наибольших угроз для любого государства. Страны, объединенные в Евразийский экономический союз (ЕАЭС), осознают необходимость совместных усилий для борьбы с ней и принимают серьезные меры, направленные на обеспечение информационной безопасности. Так, в 2013 г. в Санкт-Петербурге было заключено Соглашение о сотрудничестве в области информационной безопасности между государствами — членами СНГ. Указанный нормативно-правовой акт является основным в области борьбы с киберпреступностью, и страны — участницы ЕАЭС все еще руководствуются им при составлении новых актов в области кибербезопасности[1].

Анализ законодательства стран — членов ЕАЭС в области кибербезопасности и борьбы с киберпреступностью представляет собой актуальную задачу, поскольку каждая из этих стран разрабатывает и принимает законы и меры для защиты своего информационного пространства и обеспечения кибербезопасности граждан и организаций.

В данной статье проводится анализ законодательства стран ЕАЭС в области кибербезопасности, рассмотрены основные положения и меры, принимаемые каждой страной для противодействия киберпреступности, а также выявлены общие тенденции и различия в подходах к решению этой проблемы. Этот анализ позволит лучше понять текущие предпринимаемые меры по борьбе с киберпреступностью в рамках ЕАЭС и определить возможные направления для дальнейших усилий по обеспечению кибербезопасности в регионе.

Помимо широкомасштабных угроз киберпреступности, каждая страна сталкивается с собственными вызовами и особенностями в области кибербезопасности [1; 2; 4–7]. Российская Федерация, будучи одной из крупнейших стран в ЕАЭС, активно разрабатывает и внедряет меры по противодействию киберпреступности, киберугрозам, отражая в них собственные стратегические интересы и специфику информационного пространства.

Анализ законодательства стран — участниц ЕАЭС по борьбе с киберпреступностью

Анализ законодательства России в области кибербезопасности позволит глубже понять подходы и механизмы, используемые нашей страной для защиты информационной инфраструктуры и борьбы с киберпреступностью. При этом важно рассмотреть как законы, так и практическую реализацию этих законов, чтобы оценить эффективность принимаемых мер и выявить возможные недостатки и улучшения. Поэтому в рамках данной статьи мы обратим внимание на ключевые аспекты законодательства России в области кибербезопасности, проанализируем последние изменения и новации, а также оценим их влияние на уровень киберзащиты в стране.

Терроризм и киберпреступность являются международными угрозами, требующими скоординированных усилий мирового сообщества. Основные международные правовые нормы содержатся в актах ООН и региональных организаций, таких как Содружество Независимых Государств, Шанхайская организация содружества. Россия активно продвигает сотрудничество с этими организациями для эффективной борьбы с терроризмом и киберпреступностью. Политические разногласия, например, между США и Россией затрудняют международное взаимодействие, но Содружество Независимых Государств ра-

[1] Соглашение о сотрудничестве в области информационной безопасности между государствами — членами СНГ (Санкт-Петербург 20.11.2013) [Электронный ресурс] // Бюллетень международных договоров. 2015. № 10. С. 12. URL: http://publication.pravo.gov.ru/Document/View/0001201506040007 (дата обращения: 20.05.2024).

ботает над гармонизацией национального законодательства с международными стандартами. Важную роль играют организации, такие как Интерпол и Бюро по координации борьбы с организованной преступностью Содружества Независимых Государств. Эффективная борьба с этими угрозами требует совместных и скоординированных действий всех государств [3, с. 145].

В некоторых статьях гл. 28 Уголовного кодекса Российской Федерации[1] могут присутствовать неоднозначные формулировки, что может затруднить интерпретацию и применение закона в судебной практике. Как следствие из этого, существует Постановление Пленума Верховного суда Российской Федерации «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»»[2]. Следует отметить, что некоторые положения данной главы могут быть устаревшими или недостаточно гибкими для реагирования на новые вызовы и ситуации в современном обществе. Так, например, Примечание к ст. 272 УК РФ дает понимание передачи информации по сети Интернет, однако не оговаривает передачу информации путем внешних носителей. Несмотря на это, гл. 28 помогает регулировать общественные отношения в области компьютерной безопасности. Законодателю следует принять во внимание, что компьютерные технологии развиваются достаточно быстро, в отличие от законодательства о компьютерных технологиях в силу объективных причин и, зачастую, излишней формализованности.

Необходимо обратить внимание на законодательство других стран — членов Евразийского экономического союза (ЕАЭС), включая Республику Казахстан. Будучи одной из крупнейших экономик региона, Республика Казахстан уделяет большое внимание вопросам кибербезопасности, разрабатывая и внедряя соответствующие законодательные акты и меры.

Анализ законодательства Республики Казахстан в области кибербезопасности позволит нам оценить подходы и механизмы, используемые этой страной для защиты своего информационного пространства и противодействия киберугрозам. Это также предоставит возможность сопоставить подходы Республики Казахстан к борьбе с киберпреступностью с практикой других стран ЕАЭС для выявления общих тенденций или уникальных особенностей в регулировании кибербезопасности.

Законы Республики Казахстан в области кибербезопасности и борьбы с киберпреступностью[3] играют ключевую роль в обеспечении защиты информационного пространства страны. Одним из ключевых документов является Закон «О введении в действие некоторых законодательных актов Республики Казахстан о борьбе с информационными технологиями и киберпреступностью», который вступил в силу в 2015 г. Этот закон включает в себя различные меры по защите информации и борьбе с преступлениями в сфере информационных технологий, регулируя вопросы незаконного доступа к компьютерной информации, кражи, мошенничества и распространения вредоносных программ[4].

Анализ этих законов показывает, что Республика Казахстан стремится к совершенствованию своей правовой базы в области кибербезопасности, адаптируя ее к изменяющимся условиям цифровой среды и новым угрозам. Эти законы предоставляют четкие правила и стандарты, способствующие улучшению защиты информации и снижению рисков кибератак.

Однако эффективная борьба с киберпреступностью требует не только правового регулирования, но и комплексного подхода, включающего технические, организационные и образовательные меры.

---

1 Уголовный кодекс Российской Федерации. М. : Эксмо, 2024. 320 с.

2 Постановление пленума Верховного суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 23.05.2024).

3 Закон Республики Казахстан «О доступе к информации» от 16.10.2015 № 401-V ЗРК [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=39415981 (дата обращения: 23.05.2024); Закон Республики Казахстан от 24.11.2015 № 418 «Об информатизации» с изменениями и дополнениями по состоянию на 20.08.24 [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=33885902 (дата обращения: 23.05.2024); Закон Республики Казахстан от 21.03.2013 № 94-V ЗРК «О персональных данных и их защите» [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 23.05.2024).

4 Постановление Правительства Республики Казахстан от 30.06.2017 № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)» [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/P1700000407 (дата обращения: 23.05.2024).

В условиях быстрого развития киберугроз и технологических изменений, законодательство должно постоянно обновляться и совершенствоваться, чтобы эффективно реагировать на новые вызовы и угрозы в сети. Поэтому, помимо законов, важно также уделять внимание практической реализации этих законов, оценивать их эффективность и выявлять возможные недостатки для последующих улучшений.

Кыргызская Республика, как и другие страны — члены ЕАЭС, сталкивается с вызовами в области кибербезопасности и принимает меры для борьбы с этой угрозой. Одним из важных шагов в этом направлении является разработка законов, направленных на противодействие киберпреступности и обеспечение безопасности в информационной среде. Борьба с киберпреступностью отражена в Уголовном кодексе Кыргызской Республики[1].

В рамках данного Уголовного кодекса рассматриваются различные аспекты противодействия киберугрозам, включая:

- несанкционированный доступ к компьютерной информации;
- создание вредоносных программных продуктов;
- киберсаботаж;
- массовое распространение электронных сообщений.

Анализ законодательства Кыргызской Республики в области кибербезопасности показывает, что государство уделяет серьезное внимание информационной безопасности и противодействию киберпреступности. Установленные наказания демонстрируют стремление Кыргызстана к эффективной борьбе с киберугрозами и защите интересов общества в цифровой среде. Однако, как и в других странах, эффективная борьба с киберпреступностью требует комплексного подхода, включающего не только правовое регулирование, но и технические, организационные и образовательные меры.

Рассмотрение законодательства Республики Таджикистан в области кибербезопасности представляет собой важный шаг для понимания подходов и мер, принимаемых этой страной для защиты информационной инфраструктуры и борьбы с киберпреступностью. Анализ законов, регулирующих сбор, хранение, обработку и передачу информации, а также установленных стандартов и требований для организаций и государственных учреждений в контексте кибербезопасности дает полное понимание законодательной базы Республики Таджикистан в этой области и позволяет выявить сходства и различия с другими странами — членами ЕАЭС и определить эффективность принимаемых мер для обеспечения кибербезопасности в регионе.

Рассматривая, каким образом в Республике Таджикистан борются с преступлениями в сфере кибербезопасности, необходимо сказать о том, что ученые отмечают недостаточность профессиональных навыков для борьбы с киберпреступлениями. Так 82% сотрудников аппаратных ведомств отметили, что не располагают достаточными навыками и знаниями в сфере компьютерных технологий. Однако нужно отметить, что сейчас в Республике Таджикистан идет активная подготовка квалифицированных кадров, в том числе в университетах и в специализированных академиях внутренних дел. Необходимо отметить, что ежегодно Республика Таджикистан направляет в Российскую Федерацию сотрудников внутренних дел на курсы повышения квалификации в сфере компьютерной безопасности. Положения Уголовного кодекса Республики Таджикистан схожи с положениями Уголовного кодекса Российской Федерации. Так, в Уголовном кодексе Республики Таджикистан[2] гл. 28 посвящена преступлениям в области информационной безопасности. Всего указанным преступлениям посвящено семь статей. К ним относятся следующие составы преступлений:

- неправомерный доступ к компьютерной информации;
- модификация компьютерной информации;
- компьютерный саботаж;
- незаконное завладение компьютерной информацией;

---

[1] Уголовный кодекс Кыргызской Республики. 02.02.2017 № 19 [Электронный ресурс]. URL: https://cbd.minjust.gov.kg/111527/edition/1186183/ru (дата обращения: 23.05.2024).

[2] Уголовный кодекс Республики Таджикистан от 21.05.1998 № 574 [Электронный ресурс]. URL: https://continent-online.com/Document/?doc_id=30397325 (дата обращения: 23.05.2024).

- изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети;
- разработка, использование и распространение вредоносных программ;
- нарушение правил эксплуатации компьютерной системы или сети.

В области борьбы с киберпреступностью Республики Беларусь также существуют проблемные аспекты. Так, в стране отсутствует специализированный орган по борьбе с киберпреступлениями, однако существует определенный план действий по борьбе с кибертерроризмом. Уголовный кодекс Республики Беларусь содержат гл. 31 «Преступления против компьютерной безопасности»[1], в которой пять статей посвящены указанным преступлениям. Указанные статьи направлены прежде всего на защиту от преступлений от несанкционированного доступа к компьютерной информации. Отдельно следует выделить ст. 212, в которой содержатся положения о хищении путем использования компьютерной техники. Указанная статья содержит два основных способа совершения хищения: 1) с помощью специальных программ, 2) путем внесения в компьютер ложной информации. Существенной проблемой в законодательстве так же, как и в Российской Федерации, являются достаточно устаревшие нормы уголовного права в области киберпреступности. Уголовный кодекс Республики Беларусь не содержит достаточного количества статей, охватывающих все виды киберпреступлений. Законодательство не учитывает последние тенденции в сфере киберпреступности, такие как криптовалютные мошенничества или же атаки на критически важную инфраструктуру.

Заключение

В контексте рассмотрения законодательства Российской Федерации, Республики Казахстан, Кыргызской Республики, Республики Таджикистан и Республики Беларусь в области кибербезопасности становится ясно, что эти страны уделяют значительное внимание борьбе с киберпреступностью и обеспечению информационной безопасности.

Сравнение законодательства в области кибербезопасности позволили выявить общие тенденции, различия и эффективность мер, принимаемых каждой страной для борьбы с киберпреступностью. Принимая во внимание сложность и динамичность цифровой среды, а также угрозы, которые несет киберпреступность, понимание подходов и мер каждой страны становится ключевым для обеспечения кибербезопасности в регионе.

Однако для более глубокого понимания эффективности принимаемых мер и сопоставления подходов каждой страны необходимо провести анализ законодательства в области кибербезопасности всех стран — участниц ЕАЭС. Данный анализ позволит выявить общие стратегии, уникальные особенности и потенциальные области для улучшения в борьбе с киберугрозами. Введение для данного анализа должно учитывать уже проведенное рассмотрение законодательств Российской Федерации, Республики Казахстан, Кыргызской Республики, Республики Таджикистан и Республики Беларусь в области кибербезопасности.

В контексте изучения законодательства стран — членов ЕАЭС становится ясно, что государства-участники имеют схожие положения в своих уголовных кодексах, посвященных киберпреступлениям, а также демонстрируют определенные различия в подходах к противодействию киберугрозам. Однако совершенствование существующей правовой базы и разработка единой стратегии кибербезопасности в регионе остаются приоритетными задачами. Для этого страны должны активизировать сотрудничество и обмен информацией о своем законодательстве и практиках в области кибербезопасности. Кроме того, необходимо разработать общие стандарты и стратегии, а также укрепить сотрудничество в технической и организационной сферах. Только такой комплексный подход позволит эффективно противодействовать киберугрозам и обеспечить стабильную кибербезопасность в регионе.

[1] Уголовный кодекс Республики Беларусь [Электронный ресурс]. URL: https://pravo.by/document/?guid=3871&p0=hk9900275 (дата обращения: 23.05.2024).

Проведенное исследование базируется на анализе информации, полученной из открытых источников по предметной области исследования, в том числе уголовных кодексах Российской Федерации, Республики Беларусь, Республики Казахстан, Кыргызской Республики, Республики Узбекистан, Республики Таджикистан, подписанной в ноябре 2011 г. Декларации о Евразийской экономической интеграции, Договоре о Евразийском экономическом союзе от 29.05.2014, принятом в 2009 г. Таможенном кодексе и др.

Научная новизна проведенного исследования заключается в рекомендациях по доработке существующей правовой базы по формированию специальной единой правовой программы и разработке единой стратегии, направленных на обеспечение кибербезопасности для стран ЕАЭС.

Результаты проведенного исследования могут быть использованы для разработки общих стандартов и стратегии, а также укрепления сотрудничества в технической и организационной сферах.

Литература

1. *Бабаева З. Ш.* Актуальные аспекты обеспечения экономической безопасности стран Евразийского экономического союза в условиях цифровизации // Вестник Екатерининского института. 2022. № 4 (60). С. 20–23. EDN: TEVLQE
2. *Белобородько А. М.* Кибербезопасность как один из ключевых факторов интеграции фондового рынка ЕАЭС // Научные труды Белорусского государственного экономического университета : сборник научных трудов. Вып. 15. Минск : Белорусский государственный экономический университет, 2022. С. 23–29. EDN: DMMXJE
3. *Клюканова Т. М.* Международно-правовое противодействие терроризму // Юридическая наука: история и современность. 2023. № 9. С. 145–151. EDN: OSSUXV
4. *Ковалев О. Г., Скипидаров А. А.* Нормативно-правовое регулирование реализации стратегии кибербезопасности в государствах Европейского союза // Столыпинский вестник. 2021. № 2. С. 39–50. EDN: BRDEFM
5. *Курбанов Р. К.* Евразийская интеграция и право. М. : Издательство «Юнити-Дана», 2016. 496 с. ISBN: 978-5-238-02835-4. EDN: WFTGV
6. *Мога И. С.* Цифровая трансформация технического регулирования в ЕАЭС // Научный альманах Центрального Черноземья. 2022. № 1–8. С. 24–28. EDN: ZKNXKV
7. *Tendulkar R.* Cyber-Crime, Securities Markets and Systemic Risk. Madrid : IOSCO. 2013. 59 p. URL: https://www.world-exchanges.org/storage/app/media/research/Studies_Reports/2013-cyber-crime-securities-markets-amp-systemic-risk.pdf (дата обращения: 23.05.2024).

Об авторах:

Клюканова Татьяна Михайловна, доцент кафедры правоведения Северо-Западного института управления РАНХиГС, кандидат юридических наук (Санкт-Петербург, Российская Федерация);
e-mail: tatianam1211@mail.ru

Виниченко Арина Теймуровна, магистрант Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация);
e-mail: vinichenkoarina@yandex.ru

Христинченко Кирилл Юрьевич, магистрант Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация);
e-mail: kirill-xxx-1234@yandex.ru

References

1. Babaeva Z. S. Actual Aspects of Ensuring Economic Security of the Countries of the Eurasian Economic Union in the Context of Digitalization // Bulletin of the Catherine Institute [Vestnik Ekaterininskogo instituta]. 2022. No. 4 (60). P. 20–23. (In Russ.) EDN: TEVLQE

2. Beloborodko A. M. Cyber Security as One of the Key Factors of Integration of the EAEU Stock Market // Scientific works of the Belarusian State University of Economics : collection of scientific papers. Issue 15. Minsk : Belarusian State University of Economics, 2022. P. 23–29. (In Russ.) EDN: DMMXJE
3. Klyukanova T. M. International Legal Counteraction to Terrorism // Legal Science: History and Present [Yuridicheskaya nauka: istoriya i sovremennost']. 2023. No. 9. P. 145–151. (In Russ.) EDN: OSSUXV
4. Kovalev O. G., Skipidarov A. A. Regulatory and Legal Regulation of the Implementation of the Cybersecurity Strategy in the States of the European Union // Stolypin Bulletin [Stolypinskii Vestnik]. 2021. No. 2. P. 39–50. (In Russ.) EDN: BRDEFM
5. Kurbanov R. A. Eurasian Integration and Law. Moscow : Publishing "Unity-Dana", 2016. 496 p. ISBN: 978-5-238-02835-4. (In Russ.) EDN: VWFTGV
6. Moga I. S. Digital Transformation of Technical Regulation in the EAEU // Scientific Almanac of the Central Chernozem Region [Nauchnyi al'manakh Tsentral'nogo Chernozem'ya]. 2022. No. 1–8. P. 24–28. (In Russ.) EDN: ZKNXKV
7. Tendulkar R. Cyber-Crime, *S*ecurities Markets and Systemic Risk. Madrid : IOSCO. 2013. 59 p. URL: https://www.world-exchanges.org/storage/app/media/research/Studies_Reports/2013-cyber-crime-securities-markets-amp-systemic-risk.pdf (accessed: 23.05.2024).

About the authors:

Tatyana M. Klyukanova, Associate Professor, Department of Law, North-West Institute of Management of RANEPA (Saint Petersburg, Russian Federation) PhD in Jurisprudence;
e-mail: tatianam1211@mail.ru

Arina T. Vinichenko, Master's Student, North-West Institute of Management of RANEPA (Saint Petersburg, Russian Federation);
e-mail: vinichenkoarina@yandex.ru

Kirill Yu. Khristinchenko, Master's Student, North-West Institute of Management of RANEPA (Saint Petersburg, Russian Federation);
e-mail: kirill-xxx-1234@yandex.ru