Формирование единого киберпространства ЕАЭС: проблемы и перспективы

Лабоськин Михаил Алексеевич
канд. юрид. наук, доцент, доцент кафедры таможенного администрирования, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, laboskin-ma@ranepa.ru

В статье представлен анализ процесса формирования единого киберпространства Евразийского экономического союза (ЕАЭС) в контексте истечения срока действия цифровой повестки до 2025 года. На основе анализа нормативно-правовых актов, статистических данных и научной литературы выявлены основные проблемы институционально-правового, технологического и кибербезопасностного характера, препятствующие созданию единого цифрового пространства. Установлено, что отсутствие наднациональных полномочий в сфере цифровой экономики, несинхронизированность национальных стратегий цифровизации, незавершённость работы над Соглашением об обороте данных и отстающее от требований настоящего момента законодательство государств-членов ЕАЭС о киберпреступности являются структурными барьерами интеграции. Предложены направления решения указанных проблем, включая подписание в дополнение к Договору о ЕАЭС Протокола о формировании единого цифрового пространства, Соглашения об обороте данных, Стратегии информационной безопасности ЕАЭС и гармонизацию уголовного законодательства государств-членов.

Ключевые слова: ЕАЭС, киберпространство, цифровая повестка, кибербезопасность, трансграничный оборот данных, электронная подпись, киберпреступность, цифровая интеграция, регулятивные песочницы, информационная безопасность.

Введение

Формирование цифровой повестки и единого цифрового киберпространства ЕАЭС является стратегическим приоритетом интеграционного объединения. В октябре 2017 года Высший Евразийский экономический совет утвердил Основные направления реализации цифровой повестки ЕАЭС до 2025 года (Цифровая повестка-2025), определив три ключевых этапа: моделирование процессов цифровой трансформации (до 2019 года), формирование институтов цифровой экономики (до 2022 года) и реализацию проектов цифровых экосистем (до 2025 года) [1].

Ожидаемый экономический эффект от реализации Цифровой повестки-2025 оценивался как прирост совокупного ВВП государств-членов на 11 % от общего ожидаемого роста к 2025 году, рост занятости в отрасли информационно-коммуникационных технологий (ИКТ) на 66,4 % и дополнительный прирост экспорта ИКТ-услуг до 74 % [1][2]. Однако к моменту завершения срока действия Цифровой повестки-2025 сформировалась существенная диспропорция между стратегическими целями и фактическими результатами. Доля цифровой экономики в совокупном ВВП ЕАЭС по данным на 2020-2024 гг. не достигла целевых 20 %: в Беларуси она составила 7,0 %, в России − около 3,6 %, в Армении – 3,8%, в Казахстане − 0,3 %, в Кыргызстане − 0,0026% [3][4].

Необходимость обеспечения кибербезопасности актуализирует размер совокупного ущерба от киберпреступностьи мировой экономике, который в 2025 году мог достичь 10,5 трлн долл. США [5].

Целью настоящей статьи является систематизация основных проблем формирования единого киберпространства ЕАЭС и разработка предложений по их решению.

Материалы и методы

Исследование опирается на комплекс источников, включающий:

– нормативно-правовые акты ЕАЭС: Договор о ЕАЭС от 29 мая 2014 г., Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12, Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках ЕАЭС, Решение Коллегии ЕЭК от 22 августа 2023 г. № 120, Рекомендация Коллегии ЕЭК от 12 марта 2019 г. № 9 [1][6][7];

– статистические данные Евразийской экономической комиссии, Всемирного банка, правоохранительных органов государств-членов ЕАЭС [2][4][8][9];

– научные публикации в рецензируемых журналах, аналитические доклады и научно-исследовательские работы [3][5][10][11][12].

Методологическую основу составили сравнительно-правовой анализ законодательства государств-членов ЕАЭС в сфере кибербезопасности и цифрового регулирования, системный подход к оценке интеграционных процессов, контент-анализ нормативных документов и статистический анализ данных о киберпреступности и цифровом развитии.

Литературный обзор

Проблематика цифрового пространства ЕАЭС активно исследуется с момента провозглашения Цифровой повестки-2025.

Т.С. Саркисяном отмечается, что цифровая повестка ЕАЭС была «лучшей интеграционной практикой» и отличалась от ограничивающего подхода ЕС и фактического отсутствия общей повестки в АСЕАН или Меркосур, однако 2025 год существенно отличается от 2017 года – года её утверждения, прежде всего из-за рывка искусственного интеллекта (ИИ) [3]. Автор подчёркивает, что отсутствие реакции на новую технологическую реальность ведёт к риску дезинтеграции: «разрозненные стандарты ИИ могут перестать функционировать» как элемент общего рынка [3].

Е.В. Коровникова рассматривает формирование цифрового пространства ЕАЭС в контексте геополитической и геоэкономической напряжённости, выделяя такие препятствия, как отсутствие вопросов цифровой повестки в Договоре о ЕАЭС, разный уровень цифрового развития и недостаточное регулирование в области персональных данных и цифровых финансовых услуг [5]. Автор отмечает, что «процесс цифровизации в рамках Союза в настоящее

время существенно затормозился» вследствие санкционного давления и геополитических факторов.

В работе О.В. Москаленко и М.С. Абрашкина систематизированы национальные стратегии цифровой трансформации и выявлены различия в уровне цифровизации: Россия и Беларусь демонстрируют более высокий уровень цифровой готовности, тогда как Казахстан и Кыргызстан сталкиваются с «недостаточной вовлечённостью профильных министерств в мероприятия по цифровой интеграции ЕАЭС», а Армения – с проблемами синхронизации национальной стратегии с общими целями Союза [10].

Проблемы кибербезопасности исследуются в ряде работ. Анализ законодательства государств-членов ЕАЭС в области борьбы с киберпреступностью показал, что «уголовные кодексы не охватывают все виды киберпреступлений» – в частности, не учитываются криптовалютные мошенничества и атаки на критическую инфраструктуру [6]. Базовым нормативным актом остаётся Соглашение государств-участников Содружества Независимых Государств о сотрудничестве в области обеспечения информационной безопасности от 20 ноября 2013 г. [6].

А.Г. Белобородко подчёркивает, что «около 70 % киберпреступлений во всём мире направлено против кредитно-финансовых организаций», что делает киберпреступность одним из ключевых операционных рисков для интеграции финансовых рынков ЕАЭС [7].

Отчёт Positive Technologies за 2024-2025 гг. фиксирует, что на организации государств-участников СНГ пришлось 14-18 % всех успешных кибератак в мире, при этом на долю Российской Федерации пришлось 72 % всех успешных атак в регионе, в Республики Беларусь − 9 %, Республики Казахстан − 7 % [9].

В Республике Беларусь зафиксирована высокая доля атак на государственные учреждения (18 %), в Республике Казахстан в 52 % случаев атаки приводили к утечке конфиденциальной информации [9].

В исследовании персональных данных в государствах-членах ЕАЭС указывается, что «в странах ЕАЭС отсутствует единый региональный документ, регламентирующий вопросы использования персональных данных», а регулирование находится в ведении национального законодателя [11].

И.П. Коцюрко, исследуя проблему «регулятивных песочниц» как инструмента тестирования цифровых инноваций в рамках ЕАЭС, отмечает, что «концепция применения специальных режимов («регулятивных песочниц») была утверждена Распоряжением Евразийского межправительственного совета от 27 ноября 2018 г. № 17, однако практическая реализация задержалась: разработанные проекты соглашений остались на стадии НИР [13].

Таким образом, анализ литературы показывает, что формирование единого киберпространства ЕАЭС исследуется преимущественно фрагментарно – в разрезе отдельных проблем (кебербезопасность, оборот данных, электронная подпись), тогда как комплексная оценка состояния киберпространства на момент истечения срока Цифровой повестки-2025 года требует систематизации.

Результаты

1. Достигнутый уровень цифрового пространства ЕАЭС

К 2025 году в рамках ЕАЭС реализован ряд институциональных и технологических инициатив:

– взаимное признание электронной подписи. Федеральным законом от 27 ноября 2023 г. № 552-ФЗ ратифицирован Протокол о внесении изменений в Договор о ЕАЭС, устанавливающий взаимное признание электронных подписей для участия в госзакупках на пространстве ЕАЭС [14];

– решением Коллегии ЕЭК от 22 августа 2023 г. № 120 утверждены Правила признания электронной подписи в трансграничном электронном документообороте с использованием службы доверенной третьей стороны [6];

− в Российской Федерации в соответствии с Постановлениями Правительства РФ от 24 июля 2025 № 1092 и от 31 июля 2025 г. № 1139 разворачиваются государственные информационные системы «Интеграционный шлюз» и «Доверенная третья сторона» для обеспечения межгосударственного информационного обмена [14];

– стандартизация информационной безопасности. Рекомендацией Коллегии ЕЭК от 12 марта 2019 г. № 9 утверждён перечень из 107 стандартов и рекомендаций в области информационной безопасности, применяемых в рамках цифровой повестки ЕАЭС, охватывающих разработку средств защиты информации, криптографическую защиту, сетевую безопасность и идентификацию субъектов [15];

– цифровая прослеживаемость товаров и механизмы маркировки внедряются на пространстве ЕАЭС, обеспечивая контроль за движением продукции [1][10];

– интегрированная информационная система (ИИС) ЕАЭС обеспечивает обмен сведениями в сфере таможенного регулирования, ветеринарного и фитосанитарного контроля, обращения лекарственных средств [14].

2. Нереализованные инициативы

Ряд основных элементов архитектуры единого киберпространства к концу 2025 года не был завершён:

– Соглашение об обороте данных в ЕАЭС не принято, хотя проект документа, включающий 7 разделов и 36 статей, был разработан ЕЭК [12]. Соглашение должно было закрепить свободу оборота данных наряду со свободой движения товаров, услуг, капитала и рабочей силы [12][11];

– система «регулятивных песочниц» ЕАЭС не создана в полноценном трансграничном формате. Концепция применения специальных режимов была утверждена в 2018 году, однако «разработанные проекты правовых актов, включая проект Соглашения о применении специальных режимов и проект Протокола о внесении изменений в Договор о ЕАЭС, остались на стадии научно-исследовательских работ» [13];

– протокол о внесении изменений в Договор о ЕАЭС в части цифрового пространства не принят, что сохраняет структурное ограничение − цифровая экономика и информационная безопасность не входят в компетенцию ЕАЭС по Договору о ЕАЭС [5][10].

3. Состояние кибербезопасности

По данным Positive Technologies, в первой половине 2025 года количество успешных кибератак на организации в странах-участницах СНГ превысило показатель за аналогичный период 2024 года на 20 %. Максимальному числу атак подверглись промышленность (15 %), государственные учреждения (13 %), IT-компании и телекоммуникации (по 7%) [9]. Доля успешных атак с применением вредоносного программного обеспечения выросла с 54 % до 67 %, с использованием социальной инженерии – с 48 % до 59 % [9].

Законодательство о киберпреступности в государствах-членах ЕАЭС характеризуется несинхронизированностью и устареванием. Уголовный кодекс Республики Беларусь «не содержит достаточного количества статей, охватывающих все виды киберпреступлений» и не учитывает криптовалютные мошенничества и атаки на критическую инфраструктуру [6]. Базовым документом остаётся Соглашение СНГ от 20 ноября 2013 г., которое «страны-участницы ЕАЭС всё ещё руководствуются при составлении новых актов» [6].

4. Различия в уровне цифрового развития. Сохраняющиеся диспропорции в вкладе цифровой экономики в ВВП государств-членов ЕАЭС создают фундаментальные трудности для гармонизации цифрового регулирования и интеграции цифровых сервисов.

Обсуждение

Полученные результаты позволяют выделить четыре блока основных проблем формирования единого киберпространства ЕАЭС:

– *институционально-правовые барьеры*. Отсутствие наднациональных полномочий ЕЭК в сфере цифровой экономики и информационной безопасности является корневым ограничением. Евразийская экономическая комиссия де-юре не может принимать обязательные решения в этих сферах, а государства-члены самостоятельно разрабатывают национальные стратегии [5][10]. Национальные законы о локализации персональных данных (в РФ, Республике Беларусь) жёстко ограничивают трансграничную передачу данных, блокируя межгосударственные проекты [11][12]. Это превращает регулятивные «песочницы» из инструмента интеграции в инструмент конкуренции юрисдикций;

– *технологические зависимости*. Высокая зависимость всех государств-членов ЕАЭС от иностранных цифровых платформ и технологий создаёт риски для стабильности цифровой инфраструктуры [10]. Неравномерное развитие национальной цифровой инфраструктуры (широкополосные сети, дата-центры, облачные платформы) усугубляется различиями в уровнях цифрового развития. Отсутствие совместимых национальных стандартов ИИ грозит дезинтеграцией общих рынков: «разрозненные стандарты ИИ могут перестать функционировать» [3];

– *кибербезопасность и киберугрозы.* Рост киберпреступности в государствах-членах ЕАЭС принимает угрожающие масштабы. Ущерб мировой экономике от киберпреступности оценивается от 0,7 до 3 трлн долл. США [16], при этом около 70% киберпреступлений направлено против кредитно-финансовых организаций [7]. Законодательство о киберпреступности устарело и не синхронизировано между странами: уголовные кодексы не охватывают криптовалютные мошенничества, атаки на критическую инфраструктуру [6]. Отсутствует единый координирующий орган и мониторинговый центр по кибербезопасности ЕАЭС [5][6];

– *управленческие и координационные проблемы*. Недостаточная вовлечённость профильных министерств Казахстана и Кыргызстана, проблемы синхронизации стратегии Армении и неполное использование ИИС ЕАЭС замедляют реализацию цифровых инициатив [10].

Для решения выявленных проблем предлагаются следующие направления:

- принятие Протокола о формировании единого цифрового пространства к Договору о ЕАЭС − закрепление наднациональных полномочий в сфере оборота данных, цифровых сервисов и информационной безопасности [5][10][12].

Принятие Соглашения об обороте данных в ЕАЭС – единые правила трансграничной передачи персональных и неперсональных данных с балансом суверенитета и свободы движения, с категоризацией данных на свободные, государственные и требующие обезличивания [12][11];

- создание системы «регулятивных песочниц» ЕАЭС – наднациональный режим тестирования цифровых технологий с трансграничным статусом, как предусмотрено Концепцией 2018 года [13];

- разработка Стратегии информационной безопасности ЕАЭС – на основе цифровой повестки с закреплением общих правил и стандартов, а также созданием единого координирующего органа и мониторингового центра [5][6];

- гармонизация уголовного законодательства о киберпреступности – приведение к современным вызовам (криптомошенничество, атаки на критическую инфраструктуру) с обновлением Соглашения СНГ от 20 ноября 2013 года [6][16];

- совместимые (не единые) национальные стандарты ИИ – обеспечение интероперабельности без ущерба суверенитету, как предлагает Саркисян: «не общие стандарты, а схожие, сообщающиеся друг с другом» [3];

Заключение

Единое киберпространство ЕАЭС – объективная необходимость сохранения субъектности государств-членов ЕАЭС в условиях глобальной цифровой конкуренции. Опыт реализации цифровой повестки 2017-2025 годов показал, что проектный подход без институциональной базы приводит к фрагментации: «регулятивные песочницы» очерчиваются национальными границами, данные не пересекают пределов государств-членов, а национальные законы становятся барьером для интеграции.

Новый цикл планирования (до 2030 года) требует следующих фундаментальных шагов: принятия Протокола о едином цифровом пространстве к Договору о ЕАЭС, Соглашения об обороте данных и Стратегии информационной безопасности ЕАЭС. Без этого любые цифровые инициативы будут точечными проектами, а не элементами единого пространства. Параллельно необходимо решить задачу гармонизации уголовного законодательства в сфере киберпреступности и создания совместимых стандартов ИИ, без чего единое киберпространство останется уязвимым как перед внешними киберугрозами, так и перед внутренней технологической дезинтеграцией.

Литература

1. Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года» [Электронный ресурс]. – URL: // https://docs.cntd.ru/document/555625953 (дата обращения: 27.08.2026).

2. World Bank. EAEU Overview. Цифровая повестка Евразийского экономического союза до 2025 года: перспективы и рекомендации.

3. Саркисян Т.С. Вне времени, хотя в пространстве // Россия в глобальной политике. - 2025. - Т. 23. - № 1. - С. 73-86.

4. Евразийская экономическая комиссия. Цифровая экономика. Статистика Евразийского экономического союза 2020-2024. [Электронный ресурс]. – URL: https://eec.eaeunion.org/comission/department/dep_stat/union_stat/current_stat/digital/statistical_compilations/digital_economy.php (дата обращения: 27.08.2026)

5. Коровникова Н.А. Особенности формирования цифрового пространства (опыт ЕАЭС) // Социальные новации и социальные науки: [электронный журнал]. - 2022. - № 2.- С. 155-169.

6. 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.

7. Белобородко А.Г. Кибербезопасность как один из ключевых факторов интеграции фондового рынка ЕАЭС // Научные труды Белорусского государственного экономического университета. Сборник научных трудов. Вып. 15. - Минск. - 2022. - С. 23-29.

8. Смирнова И. Цифровая интеграция: как в Евразийском союзе борются с киберпреступностью [Электронный ресурс]. – URL: // https://eurasia.expert/kak-v-evraziyskom-soyuze-boryutsya-s-kiberprestupnostyu/ (дата обращения: 25.08.2026).

9. Positive Technologies. Ландшафт киберугроз СНГ: H2 2024 − Q3 2025. [Электронный ресурс]. – URL: https://ptsecurity.com/research/analytics/cis-cyberthreat-landscape-h2-2024-q3-2025/ (дата обращения: 25.08.2026).

10. Москаленко О.В., Абрашкин М.С. Цифровая интеграция стран ЕАЭС: проблемы и направления развития // Ученые записки Санкт-Петербургского филиала имени В.Б. Бобкова филиала Российской таможенной академии. – 2025. – № 2(94). – С. 84-87.

11. Шебанова Н.А. Охрана персональных данных в государствах-членах ЕАЭС [Электронный ресурс]. – URL: https://ipcmagazine.ru/articles/1729251/ (дата обращения: 25.08.2026)

12. Евразийская экономическая комиссия. Аннотация НИР по разработке механизма трансграничного оборота данных в ЕАЭС. 2023.

13. Коцюрко И.П. Экспериментальные правовые режимы как инструмент модернизации регулирования цифровых инноваций в условиях евразийской интеграции // European and Asian Law Review. – 2025. – Т. 8. – № 2. – С. 31-40. DOI: 10.34076/27821668_2025_8_2_31.

14. Электронные подписи к документам стран ЕАЭС получат официальный статус [Электронный ресурс]. – URL: https: //www.vedomosti.ru/economics/articles/2025/03/10/1096924-elektronnie-podpisi-k-dokumentam-stran-eaes-poluchat-ofitsialnii-status (дата обращения: 25.08.2026)

15. Рекомендация Коллегии Евразийской экономической комиссии от 12.03.2019 № 9 «О перечне стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза» [Электронный ресурс]. – URL: https://docs.cntd.ru/document/553889469 (дата обращения: 25.08.2026)

16. Бушуев А.Л. Киберпреступность и преступления в сфере информационных технологий как угроза экономической безопасности стран-членов ЕАЭС // Актуальные проблемы развития ЕАЭС в условиях современных глобальных изменений. Материалы Всероссийской научно-практической конференции. – Иркутск. – 2021. – С. 81-86.

Formation of a unified cyberspace of the eaeu: problems and prospects

Laboskin M.A.
Russian Presidential Academy of National Economy and Public Administration

The article presents an analysis of the process of forming a unified cyberspace for the Eurasian Economic Union (EAEU) in the context of the expiration of the digital agenda until 2025. Based on an analysis of regulatory legal acts, statistical data, and scientific literature, the main problems of an institutional, legal, technological, and cybersecurity nature that hinder the creation of a unified digital space have been identified. It has been established that the lack of supranational powers in the field of the digital economy, the lack of synchronization between national digitalization strategies, the incomplete work on the Agreement on Data Circulation, and the legislation of EAEU member states on cybercrime that lags behind current requirements are structural barriers to integration. Directions for addressing these problems have been proposed, including the signing of a Protocol on the Formation of a Unified Digital Space, an Agreement on Data Circulation, and an Information Security Strategy in addition to the EAEU Treaty.

Keywords: EAEU, cyberspace, digital agenda, cybersecurity, cross-border data circulation, electronic signature, cybercrime, digital integration, regulatory sandboxes, information security.

References

1. Decision of the Supreme Eurasian Economic Council dated October 11, 2017, No. 12 «On the Main Directions for Implementing the Digital Agenda of the Eurasian Economic Union until 2025» [Electronic resource]. — URL: https://docs.cntd.ru/document/555625953 (accessed: August 27, 2026).
2. World Bank. EAEU Overview. The Digital Agenda of the Eurasian Economic Union until 2025: Prospects and Recommendations.
3. Sarkisyan T. S. Beyond Time, Yet Within Space // Russia in Global Affairs. — 2025. — Vol. 23, No. 1. — Pp. 73–86.
4. Eurasian Economic Commission. Digital Economy. Statistics of the Eurasian Economic Union, 2020–2024 [Electronic resource]. — URL: https://eec.eaeunion.org/comission/department/dep_stat/union_stat/current_stat/digital/statistical_compilations/digital_economy.php (accessed: August 27, 2026).
5. Korovnikova N. A. Specifics of Forming the Digital Space (The EAEU Experience) // Social Innovations and Social Sciences: [electronic journal]. — 2022. — No. 2. — Pp. 155–169.
6. Klyukanova T. M., Vinichenko A. T., Khristinchenko K. Yu. Analysis of the Legislation of the EAEU Countries in the Field of Combating Cybercrime // Eurasian Integration: Economics, Law, Politics. — 2024. — Vol. 18, No. 3. — Pp. 83–90.
7. Beloborodko A. G. Cybersecurity as a Key Factor in the Integration of the EAEU Stock Market // Scientific Works of the Belarusian State Economic University. Collection of Scientific Papers. Issue 15. — Minsk. — 2022. — Pp. 23–29.
8. Smirnova I. Digital Integration: How the Eurasian Union Combats Cybercrime [Electronic resource]. — URL: https://eurasia.expert/kak-v-evraziyskom-soyuze-boryutsya-s-kiberprestupnostyu/ (accessed: August 25, 2026).
9. Positive Technologies. CIS Cyber Threat Landscape: H2 2024 − Q3 2025 [Electronic resource]. — URL: https://ptsecurity.com/research/analytics/cis-cyberthreat-landscape-h2-2024-q3-2025/ (accessed: August 25, 2026).
10. Moskalenko O. V., Abrashkin M. S. Digital Integration of the EAEU Countries: Problems and Development Directions // Scientific Notes of the St. Petersburg Branch named after V. B. Bobkov of the Russian Customs Academy. — 2025. — No. 2(94). — Pp. 84–87.
11. Shebanova N. A. Protection of Personal Data in the EAEU Member States [Electronic resource]. — URL: https://ipcmagazine.ru/articles/1729251/ (accessed: August 25, 2026).
12. Eurasian Economic Commission. Abstract of the Research Project on the Development of a Mechanism for Cross-Border Data Flow in the EAEU. 2023.
13. Kotsyurko I. P. Experimental Legal Regimes as a Tool for Modernizing the Regulation of Digital Innovations in the Context of Eurasian Integration // European and Asian Law Review. — 2025. — Vol. 8, No. 2. — Pp. 31–40. DOI: 10.34076/27821668_2025_8_2_31.
14. Electronic Signatures for Documents in the EAEU Countries Will Receive Official Status [Electronic resource]. — URL: https://www.vedomosti.ru/economics/articles/2025/03/10/1096924-elektronnie-podpisi-k-dokumentam-stran-eaes-poluchat-ofitsialnii-status (accessed: August 25, 2026).
15. Recommendation of the Board of the Eurasian Economic Commission dated March 12, 2019, No. 9 «On the List of Standards and Recommendations in the Field of Information Security Used in the Implementation of the Digital Agenda of the Eurasian Economic Union» [Electronic resource]. — URL: https://docs.cntd.ru/document/553889469 (accessed: August 25, 2026).
16. Bushuev A. L. Cybercrime and Crimes in the Field of Information Technology as a Threat to the Economic Security of the EAEU Member States // Current Problems of the EAEU Development in the Context of Modern Global Changes. Proceedings of the All-Russian Scientific and Practical Conference. — Irkutsk. — 2021. — Pp. 81–86.