Трансграничная передача персональных данных: коллизии российского и международного регулирования

Дзюнковский Ярослав Олегович
студент, Дальневосточный Федеральный Университет, dzyunkovskii.yo@yandex.ru

Панков Вячеслав Андреевич
студент, Дальневосточный Федеральный Университет, mr.pankov.slava@mail.ru

Статья посвящена правовым противоречиям, возникающим при трансграничной передаче персональных данных в точке пересечения российского режима охраны данных, европейских моделей контроля трансграничных потоков, региональных интеграционных решений и новых подходов к управлению данными в цифровой среде. Актуальность исследования связана с усилением регуляторной фрагментации, ростом требований к локализации, расширением экстерриториального действия отдельных правопорядков и ужесточением процедур допуска передачи данных за рубеж. Научная новизна состоит в систематизации коллизий между территориальным принципом действия национального права, наднациональными механизмами оценки допустимости передачи и функциональными потребностями цифровой экономики. Цель работы – выявить основные линии нормативного расхождения и определить направления согласования правовых режимов. В исследовании применены сравнительно-правовой, формально-юридический, логико-аналитический методы, обобщение и классификация. Источниковую базу составили русскоязычные научные публикации 2022–2025 гг., посвященные российскому регулированию, опыту ЕС, стран БРИКС, АТЭС, КНР и межрегиональным механизмам защиты данных. В аналитической части раскрыты коллизии критериев адекватности защиты, проблемы соотношения локализации и трансграничного обмена, расхождения в моделях цифрового суверенитета и дефицит унифицированных процедур признания эквивалентности защитных гарантий. Практическая полезность полученных результатов связана с их применением при подготовке локальных актов операторов, правовой экспертизе трансграничных потоков данных и разработке предложений по гармонизации регулирования.

Ключевые слова: трансграничная передача персональных данных, персональные данные, коллизии правового регулирования, локализация данных, цифровой суверенитет, GDPR, Data Governance Act, международное частное право, адекватный уровень защиты, гармонизация регулирования.

Введение

Наиболее острые противоречия возникают там, где национальное законодательство исходит из территориального контроля над данными, а цифровая инфраструктура строится по логике распределенной обработки и удаленного доступа. Российская модель после реформы трансграничной передачи стала заметно строже, тогда как международная практика сохраняет множественность подходов: от режима адекватности и договорных гарантий до секторального регулирования, локализационных барьеров и инструментов взаимного признания. В этой связи научный интерес смещается от простого описания норм к анализу коллизий между конкурирующими регуляторными логиками.

Цель исследования – выявить и систематизировать правовые коллизии, возникающие при трансграничной передаче персональных данных в точке соприкосновения российского и международного регулирования, а затем определить направления их doctринального и прикладного согласования.

Для достижения поставленной цели решаются три задачи:

1) раскрыть, как в современной литературе описываются модели трансграничного оборота данных и какие критерии положены в основу разграничения допустимых и ограниченных режимов передачи;

2) установить, в каких узлах российского регулирования проявляются расхождения с международными и региональными подходами к защите данных;

3) предложить аналитическую схему согласования правовых режимов, пригодную для правоприменения и внутреннего комплаенса операторов.

Научная новизна работы состоит в том, что коллизии трансграничной передачи персональных данных рассмотрены как результат наложения четырех регуляторных векторов: суверенизационного, интеграционного, рыночно-функционального и правозащитного. Такой ракурс позволяет точнее увидеть, почему формальное совпадение терминов в разных правопорядках не устраняет расхождения в допуске передачи, в оценке достаточности гарантий и в распределении ответственности между участниками цифровой цепочки.

Материалы и методы

Материальную базу исследования образовали работы, в которых проблема трансграничной передачи данных раскрыта с разных уровней правового анализа. А.Г. Абрамова [1] обобщает международные договоры и региональные механизмы защиты данных, что дает опору для сопоставления наднациональных моделей. А.Н. Артемова [2] рассматривает российские новеллы регулирования трансграничной передачи персональных данных и фиксирует изменения в конструкции допуска такой передачи; на основе сравнительно-правового исследования автор приходит к выводу о том, что придание российскому закону о персональных данных экстерриториального характера соответствует новейшей тенденции, сложившейся в других правопорядках (ЕС, США, Китая). Д.В. Бахтеев, А.М. Сосновикова, Е.В. Казенас [3] сосредоточены на незаконной трансграничной передаче и предлагают юридико-технологическую логику управления рисками. В работе Г. Болатбеккызы [4] внимание перенесено на связь трансграничных потоков данных с цифровизацией государственного управления, суверенитетом и пространством доверия. У. Г. Восс [5] показывает, как ограничения

передачи данных переплетаются с экстерриториальностью GDPR, американскими механизмами обмена и локализационными режимами. С.-У. С.-А. Возкаев [6] анализирует последствия реформы 2025 г. для правового режима защиты персональных данных. С. П. Саяпин [7] раскрывает содержание Data Governance Act и тем самым позволяет отделить режимы персональных данных от более широкого регулирования оборота данных. Е. А. Свиридова [8] анализирует модели правового регулирования защиты персональных данных, сложившиеся в ЕС и странах азиатско-тихоокеанского региона. Чжао Лэй [9] сопоставляет режимы ЕС, США и КНР, выявляя их ценностные и институциональные расхождения. А. В. Шелепов [10] исследует подходы стран БРИКС к регулированию данных и подчеркивает значение взаимного признания защитных мер для трансграничного обмена.

В работе использованы анализ научных публикаций, сравнительный правовой анализ, формально-юридический метод, классификация, обобщение, логико-аналитический анализ и синтез. Перечисленные методы применены для разграничения моделей трансграничной передачи, выявления точек нормативного несовпадения между российским и зарубежным регулированием, а затем для выработки схемы интерпретации обнаруженных коллизий.

Результаты

Анализ литературы позволяет выделить несколько конкурирующих моделей регулирования трансграничной передачи персональных данных. Первая строится вокруг идеи адекватности правовой защиты и развита прежде всего в европейской правовой традиции; в ней допустимость передачи зависит от сопоставимости гарантий принимающей юрисдикции, набора договорных и организационных механизмов, а затем – от надзорной оценки рисков [1; 5; 8; 9]. Вторая модель опирается на более децентрализованное и фрагментарное регулирование, где единый универсальный критерий отсутствует, а правовой режим формируется через сочетание отраслевых правил, договорных механизмов и судебной практики; подобная логика отчетливо прослеживается при сравнении американского подхода с европейским [5; 9]. Третья модель исходит из приоритета цифрового суверенитета, локализации и усиленного государственного контроля над потоками данных; ее признаки заметны в китайском регулировании и в ряде суверенизационных тенденций иных правопорядков [4; 9]. Четвертая модель ориентирована на региональное координирование и взаимное признание сопоставимых мер защиты, что видно в исследованиях по ЕС, АТЭС и БРИКС [1; 8; 10].

Российский режим трансграничной передачи после последних изменений в научной литературе описывается как переход от сравнительно формального допуска передачи к более насыщенной процедуре предварительной оценки, документирования и возможного ограничения потока данных. В теоретико-правовом ключе уточняются пределы информационного самоопределения личности, критерии соразмерности ограничений частной жизни и требования к необратимости обезличивания при публичном доступе к агрегированным массивам. В этой конструкции усиливается значение статуса принимающей юрисдикции, внутренней проверки гарантий иностранного получателя и надзорного компонента [2; 3; 6]. При этом коллизия возникает уже на исходном уровне: международный цифровой оборот строится на постоянной распределенной обработке и множественности технических посредников, тогда как российский режим тяготеет к модели заранее очерченной, проверяемой и юридически локализуемой передачи [2; 4; 6]. Чем сложнее фактическая архитектура обмена данными, тем труднее оператору уложить ее в линейную правовую схему «передающий субъект – принимающая сторона – территория передачи».

Первая группа коллизий связана с различием критериев допустимости передачи. В европейской конструкции центральное место занимает эквивалентность защитных гарантий, причем оценка строится вокруг прав субъекта данных, механизмов контроля, объема доступных средств правовой защиты и общего режима обращения данных [1; 5; 8]. В российской конструкции, судя по рассмотренным публикациям, наряду с защитой прав субъекта существенно возрастает значение административно-процедурной проверяемости передачи и возможности публичного контроля за ее параметрами [2; 6]. На практике расхождение проявляется в том, что одна и та же трансграничная операция способна восприниматься как приемлемая по логике договорных и организационных гарантий в одном режиме, но как недостаточно определенная и недостаточно прозрачная – в другом.

Вторая группа коллизий касается соотношения локализации и трансграничности. В ряде работ локализация рассматривается как самостоятельный слой суверенного контроля, обеспечивающий удержание первичной базы данных, юрисдикционную досягаемость и доказуемость правомерной обработки [4; 5; 9; 10]. Вместе с тем международные и региональные режимы, ориентированные на торговый оборот и цифровые услуги, трактуют чрезмерную локализацию как барьер для трансграничных сервисов и как фактор роста регуляторных издержек [5; 8; 10]. Отсюда возникает структурное противоречие: для одного правопорядка локализация выступает гарантийным механизмом, для другого – ограничением экономически оправданного движения данных. В российском праве данный узел обостряется из-за сочетания охранительной логики и требований к доказуемости соблюдения условий передачи [2; 6].

Отдельный пласт противоречий затрагивает вопрос о субъекте ответственности. Европейская литература и ее русскоязычное осмысление показывают тенденцию к распределенной ответственности по всей цепочке обработки, где контролер данных отвечает за дальнейшую судьбу информации в инфраструктуре глобальных сервисов [5; 7]. Российские исследования, напротив, концентрируют внимание прежде всего на операторе, инициирующем передачу, и на его обязанности проверить получателя, оформить основания передачи и принять меры предосторожности [2; 3]. В транснациональной цифровой среде такая разница осложняет распределение рисков между российским оператором, иностранным облачным провайдером, субподрядчиками и иными посредниками. Юридическая конструкция ответственности оказывается несимметричной: один правопорядок разворачивает ее по всей сети обработки, другой – стягивает к инициатору передачи.

Заметный исследовательский интерес вызывает расхождение между персональными данными и более широким массивом данных как объектом регулирования. За последние несколько лет информационные технологии существенным образом преобразовали межгосударственные и внутригосударственные социально-экономические отношения, а цифровая трансформация глубоко затронула важнейшие сферы общественной жизни. Основная особенность всех цифровых преобразований последних лет заключается в том, что в их основе неизменно лежат данные.[7, с. 153], поэтому регулирование data governance нельзя сводить к классической модели охраны персональных данных. В работах последних лет подчеркивается, что европейское нормотворчество в сфере data governance строится шире классического режима защиты персональных данных и формирует особые правила повторного использования защищенных наборов данных,

посредничества и дата-альтруизма [7]. Российская правовая доктрина при анализе трансграничной передачи чаще сосредоточена именно на персональных данных и на рисках утраты контроля над ними [2; 3; 6]. Коллизия здесь выражена в смешении режимов: трансграничные цифровые сервисы обрабатывают смешанные массивы, где персональные данные сосуществуют с промышленными, статистическими и поведенческими данными, а правовые режимы их обращения различаются. При отсутствии четкого разграничения оператору трудно выбрать надлежащий правовой режим всей трансграничной операции.

Сравнение региональных и межгосударственных моделей показывает, что унификация в данной сфере развивается через набор частичных механизмов согласования. Различия в подходах между крупнейшими игроками создают проблемы для других стран, усиливают фрагментированность глобальной регуляторной среды, создают неопределенность и повышают издержки исполнения требований для бизнеса. А.Г. Абрамова [1] фиксирует значение международных договоров и региональных инициатив, Е.А. Свиридова [8] показывает различие между европейской и азиатско-тихоокеанской логикой, а А.В. Шелепов [10] указывает на перспективность взаимного признания мер защиты в рамках БРИКС. Несмотря на то, что за последнее время имел место заметный прогресс с сфере защиты данных, в частности, GDPR устанавил высокие стандарты защиты данных, а региональные структуры, такие как АТЭС и ASEAN, обеспечили гибкость и сотрудничество, правовые пробелы и неясности, тем не менее, сохранились, включая согласование региональных и международных стандартов, решение проблемы трансграничной передачи данных и обеспечение эффективного правоприменения [1, с. 45], поэтому согласование режимов защиты данных не сводится к формальному сближению терминологии.

Параллельно литература демонстрирует, что дискуссия о трансграничной передаче уже не сводится к классической оппозиции «приватность против свободного обмена». В статье Г. Болатбеккызы [4] трансграничная передача рассматривается через призму цифровизации государственного управления, где перемещение данных соприкасается с вопросами суверенитета, безопасности и административной эффективности. В работах Д.В. Бахтеева, А.М. Сосновиковой, Е.В. Казенаса [3] в центр поставлены незаконные формы вывода данных за рубеж и управленческие механизмы снижения таких рисков. С.-У. С.-А. Возкаев [6], анализируя реформу 2025 г., показывает укрепление превентивной и риск-ориентированной линии защиты. Д. В. Бахтеев, А. М. Сосновикова и Е. В. Казенас предлагают не столько усилить санкцию за нарушение законодательства в рассматриваемой сфере, сколько обеспечить наказание лиц, совершающих кибератаки, и вооружить операторов персональных данных действенным инструментом минимизации рисков утечки информации [3, с. 943]. В сумме названные подходы позволяют заключить, что современная коллизия затрагивает уже многослойную систему публичных и частных интересов, где регулятор одновременно решает задачу охраны прав субъекта, обеспечения цифровой устойчивости и сохранения юрисдикционного контроля над чувствительными потоками данных.

Отдельного внимания заслуживает сравнительная линия ЕС – США – КНР. Чжао Лэй [9] показывает, что режим трансграничной передачи данных в ЕС является наиболее полным и эффективным, обладая демонстрационным эффектом. Китайская система в настоящее время имеет серьезные недостатки. А закон США в последние годы все больше ориентирован на служение интересам геополитики. Законы о трансграничной передаче данных демонстрируют тенденции политической инструментализации. Балканизация Интернета становится все более очевидной. Работа У. Г. Восса [5] дополняет этот вывод анализом экстерриториальности GDPR и влияния международных соглашений на фактическую осуществимость потоков данных. Для российского правопорядка названное сопоставление значимо по двум причинам. Во-первых, российская модель не совпадает полностью ни с европейской, ни с китайской, хотя отдельные черты суверенизационного подхода в ней выражены отчетливо. Во-вторых, любая попытка механически заимствовать внешнюю модель сталкивается с внутренним противоречием между конституционно-правовой охраной частной жизни, отраслевым регулированием персональных данных и государственным интересом к контролю цифровой инфраструктуры.

На основании проведенного анализа коллизии российского и международного регулирования трансграничной передачи персональных данных группируются по четырем направлениям: коллизии критериев допустимости передачи; коллизии между локализацией и экономикой распределенной обработки; коллизии в распределении ответственности по цепочке участников; коллизии между режимом персональных данных и более широким регулированием оборота данных. Такая классификация позволяет перейти от разрозненного описания норм к более строгой картине правоприменительных рисков и служит опорой для последующей интерпретации полученных положений.

Обсуждение

Полученные результаты показывают, что источник основных противоречий лежит глубже уровня отдельных запретов и разрешений. Российское регулирование стремится придать трансграничной передаче персональных данных режим повышенной юридической определенности, где передача поддается предварительной верификации, формальному описанию и административному контролю. Международные и региональные модели, напротив, чаще исходят из иной логики: допустимость передачи связывается с достаточностью гарантий, функциональной необходимостью цифрового обмена и возможностью компенсировать различия правопорядков договорными и организационными средствами. Отсюда вытекает принципиальное расхождение в самой конструкции правового риска. В российской модели риск чаще понимается как недостаточная контролируемость передачи, в европейской – как недостаточность защиты прав субъекта после передачи, в азиатско-тихоокеанских и межрегиональных режимах – как отсутствие процедур согласования между юрисдикциями.

Сопоставление работ из корпуса литературы позволяет заметить и более тонкое расхождение. Исследования, посвященные цифровому суверенитету, локализации и государственному управлению, исходят из того, что правовой контроль над местом нахождения данных и каналами их перемещения укрепляет безопасность и снижает зависимость от внешней инфраструктуры. Работы, ориентированные на международный обмен данными и цифровую торговлю, оценивают те же меры иначе: как регуляторное утяжеление, осложняющее услуги, трансграничные платформенные модели и взаимодействие между операторами. Ни одна из названных позиций не сводится к простой ошибке второй стороны. Они отражают разные функции права: охранительную, интеграционную и инфраструктурную. Коллизия возникает потому, что современная трансграничная передача персональных данных одновременно затрагивает все три.

Важный вывод касается неполной применимости классического коллизионного инструментария международного частного права к цифровым потокам персональных данных. В традиционной конструкции достаточным не-

редко считалось определение применимого права или выявление юрисдикционно значимой связи. Для трансграничной передачи данных одного такого шага уже недостаточно. Данные циркулируют через множество посредников, перераспределяются автоматически, реплицируются в резервных контурах, а обработка нередко продолжается в смешанной цифровой экосистеме. По этой причине коллизия в данной сфере принимает сетевой характер: она затрагивает несколько правопорядков одновременно и не устраняется простым выбором одной применимой системы. Именно здесь особенно заметна ограниченность традиционного правового мышления, ориентированного на двусторонний трансграничный контакт.

Исследовательская лакуна просматривается в слабой разработанности механизмов взаимного признания гарантий между правопорядками, которые не состоят в тесной интеграционной связи. Именно данный пробел превращает множество трансграничных операций в зону высокой неопределенности. Научная литература сравнительно подробно описывает модели ЕС, АТЭС, БРИКС и отдельных национальных режимов, но значительно реже отвечает на прикладной вопрос: по каким критериям оператору и надзорному органу устанавливать сопоставимость правовой защиты в конкретной трансграничной цепочке обработки. Без разработки таких критериев любой режим остается либо избыточно закрытым, либо чрезмерно зависимым от индивидуальной оценки каждого кейса.

Ограничение проведенного анализа связано с характером источниковой базы. Работа опирается на научные публикации, посвященные главным образом нормативным конструкциям и компаративным моделям. Судебная практика, внутренние комплаенс-протоколы операторов, технические архитектуры облачной обработки и транснациональные договорные механизмы затронуты в изученной литературе неравномерно. По этой причине сделанные выводы точнее всего работают на уровне правовой доктрины и общего проектирования режима передачи данных. Для более узких прикладных задач – например, для оценки конкретной сервисной архитектуры или конкретного облачного контракта – потребовалось бы дополнительное исследование специальной практики.

Заключение

Первая задача решена через выделение основных моделей трансграничного оборота данных – модели адекватности, фрагментарно-договорной модели, суверенизационной модели и модели регионального координирования.

Вторая задача привела к выявлению основных узлов расхождения между российским и международным регулированием. Наиболее заметные противоречия проявляются в критериях допустимости передачи, в соотношении локализации и распределенной обработки, в распределении ответственности между участниками цифровой цепочки и в разграничении режима персональных данных с более широким регулированием данных как ресурса цифровой экономики.

Третья задача решена посредством аналитической классификации коллизий по четырем направлениям, пригодной для правовой экспертизы трансграничных потоков данных. Такая схема дает возможность точнее оценивать правовой риск конкретной операции передачи и формировать более дифференцированные решения при разработке внутренних политик оператора, договорных условий и предложений по совершенствованию законодательства.

Литература

1. Абрамова А. Г. Ключевые международные договоры и региональные подходы к вопросу защиты персональных данных // Регион и мир. 2023. Т. XIV, № 6 (49). С. 43–46. DOI: 10.58587/18292437-2023.6-43.
2. Артемова А. Н. Правовое регулирование трансграничной передачи персональных данных // Юридическая наука и практика. 2023. Т. 19, № 3. С. 9–16. DOI: 10.25205/2542-0410-2023-19-3-9-16.
3. Бахтеев Д. В., Сосновикова А. М., Казенас Е. В. Преодоление нелегальной трансграничной передачи персональных данных // Journal of Digital Technologies and Law. 2024. Vol. 2, no. 4. P. 943–972. DOI: 10.21202/jdtl.2024.45.
4. Гульбакыт Болатбеккызы. Правовые проблемы трансграничной передачи данных в эпоху цифровизации государственного управления // Journal of Digital Technologies and Law. 2024. Vol. 2, no. 2. P. 286–307. DOI: 10.21202/jdtl.2024.15.
5. Восс У. Г. Трансграничные потоки данных, общий регламент защиты персональных данных и управление данными // Вестник международных организаций. 2022. Т. 17, № 1. С. 56–95. DOI: 10.17323/1996-7845-2022-01-03.
6. Возкаев С.-У. С.-А. Защита персональных данных после реформы 2025 года // Аграрное и земельное право. 2025. № 9. С. 297–300. DOI: 10.47643/1815-1329_2025_9_297.
7. Саяпин С. П. Европейский закон об управлении данными (Data Governance Act): общие аспекты правового регулирования и основные выводы // Образование и право. 2024. № 5. С. 153–159.
8. Свиридова Е. А. Региональные модели правового регулирования защиты данных в странах ЕС и АТЭС // Проблемы экономики и юридической практики. 2024. Т. 20, № 2. С. 81–88.
9. Чжао Л. Основные модели режимов трансграничной передачи данных: ЕС, США и КНР // Право и политика. 2024. № 4. С. 50–60. DOI: 10.7256/2454-0706.2024.4.70797. EDN: WNDYGF.
10. Шелепов А. В. Подходы стран БРИКС к регулированию данных // Вестник международных организаций: образование, наука, новая экономика. 2022. Т. 17, № 3. С. 212–234.

Cross-border transfer of personal data: collisions of russian and international regulation

Dzyunkovskii Ya.O., Pankov V.A.

Far Eastern Federal University

This article examines the legal contradictions arising during the cross-border transfer of personal data at the intersection of the Russian data protection regime, European models for controlling cross-border flows, regional integration solutions, and new approaches to data management in the digital environment. The relevance of this study is due to increasing regulatory fragmentation, growing localization requirements, the expansion of the extraterritorial scope of certain legal systems, and the tightening of procedures for authorizing the transfer of data abroad. The scientific novelty lies in the systematization of conflicts between the territorial principle of national law, supranational mechanisms for assessing the admissibility of transfer, and the functional needs of the digital economy. The aim of the work is to identify the main lines of regulatory divergence and determine areas for harmonizing legal regimes. The study employs comparative legal, formal legal, and logical-analytical methods, as well as generalization and classification. The source base consists of Russian-language scientific publications published between 2022 and 2025, devoted to Russian regulation, the experience of the EU, BRICS countries, APEC, China, and interregional data protection mechanisms. The analytical section reveals conflicting criteria for assessing protection adequacy, problems with the relationship between localization and cross-border exchange, discrepancies in digital sovereignty models, and the lack of unified procedures for recognizing the equivalence of protective guarantees. The practical utility of the obtained results lies in their application in the preparation of local acts of operators, legal assessments of cross-border data flows, and the development of proposals for regulatory harmonization.

Keywords: cross-border transfer of personal data, personal data, conflicts of law, data localization, digital sovereignty, GDPR, Data Governance Act,

international private law, adequate level of protection, regulatory harmonization.

References

1. Abramova A. G. Key International Treaties and Regional Approaches to the Protection of Personal Data // Region and the World. 2023. Vol. XIV, No. 6 (49). Pp. 43–46. DOI: 10.58587/18292437-2023.6-43.
2. Artemova A. N. Legal Regulation of Cross-Border Transfer of Personal Data // Legal Science and Practice. 2023. Vol. 19, No. 3. Pp. 9–16. DOI: 10.25205/2542-0410-2023-19-3-9-16.
3. Bakhteyev D. V., Sosnovikova A. M., Kazenas E. V. Overcoming Illegal Cross-Border Transfer of Personal Data // Journal of Digital Technologies and Law. 2024. Vol. 2, no. 4. P. 943–972. DOI: 10.21202/jdtl.2024.45.
4. Gulbaktyt Bolatbekkyzy. Legal Issues of Cross-Border Data Transfer in the Era of Digitalization of Public Administration // Journal of Digital Technologies and Law. 2024. Vol. 2, no. 2. P. 286–307. DOI: 10.21202/jdtl.2024.15.
5. Voss, W. G. Cross-Border Data Flows, General Data Protection Regulation, and Data Governance // Bulletin of International Organizations. 2022. Vol. 17, no. 1. P. 56–95. DOI: 10.17323/1996-7845-2022-01-03.
6. Vozkayev, S.-U. S.-A. Personal Data Protection after the 2025 Reform // Agrarian and Land Law. 2025. No. 9. pp. 297–300. DOI: 10.47643/1815-1329_2025_9_297.
7. Sayapin S. P. The European Data Governance Act: General Aspects of Legal Regulation and Key Conclusions // Education and Law. 2024. No. 5. pp. 153–159.
8. Sviridova E. A. Regional Models of Legal Regulation of Data Protection in the EU and APEC Countries // Problems of Economics and Legal Practice. 2024. Vol. 20, No. 2. pp. 81–88.
9. Zhao L. The Main Models of Cross-Border Data Transfer Regimes: the EU, the USA, and China // Law and Politics. 2024. No. 4. Pp. 50–60. DOI: 10.7256/2454-0706.2024.4.70797. EDN: WNDYGF.
10. Shelepov, A. V., “BRICS Countries’ Approaches to Data Regulation,” in: Bulletin of International Organizations: Education, Science, and the New Economy. 2022. Vol. 17, No. 3. Pp. 212–234.