УДК 34

Эволюция правового регулирования защиты персональных данных в деятельности международных организаций в условиях цифровой трансформации

Бесчастнова Ольга Валерьевна

Кандидат юридических наук, доцент;
заведующий кафедрой уголовного права и правоохранительной деятельности,
Астраханский государственный университет,
414056, Российская Федерация, Астрахань, ул. Татищева. 20-а;
e-mail: beschastnova_ol@mail.ru

Слабкая Диана Николаевна

Старший научный сотрудник,
Научно-исследовательский институт Федеральной службы исполнения наказаний России,
125130, Российская Федерация, Москва, ул. Нарвская, 15-а;
e-mail: sdn10.70@mail.ru

Аннотация

В статье исследуется эволюция правового регулирования защиты персональных данных в деятельности международных организаций в условиях цифровой трансформации. Анализируются исторические предпосылки формирования международных стандартов, включая Конвенцию Совета Европы и Общий регламент по защите данных, а также их влияние на внутреннюю политику международных организаций. Особое внимание уделяется правовым коллизиям, связанным с иммунитетом организаций, трансграничными передачами данных и юрисдикционной подведомственностью споров. Рассматриваются современные вызовы сохранения и передачи личных данных, включая использование искусственного интеллекта, биометрических технологий и блокчейна, а также этические аспекты обработки персональных данных в гражданско-правовом обороте. Выделяются ключевые тенденции развития регулирования, подчеркивая необходимость баланса между эффективностью международного сотрудничества и защитой фундаментальных прав человека и гражданина.

Для цитирования в научных исследованиях

Бесчастнова О.В., Слабкая Д.Н. Эволюция правового регулирования защиты персональных данных в деятельности международных организаций в условиях цифровой трансформации // Вопросы российского и международного права. 2025. Том 15. № 5А. С. 245-254.

Ключевые слова

Защита персональных данных, международные организации, GDPR, цифровые технологии, трансграничная передача данных, правовые стандарты, конфиденциальность, искусственный интеллект, биометрические данные, блокчейн, этика обработки данных, кибербезопасность.

Введение

Современное право на защиту персональных данных формировалось как ответ на вызовы цифровой эпохи, когда стремительное развитие технологий обработки информации создало принципиально новые угрозы конфиденциальности и автономии личности.

Исторически этот правовой институт зародился в 1970-х годах как реакция на компьютеризацию государственного управления в западноевропейских странах, где впервые осознали необходимость правовых гарантий против потенциальных злоупотреблений при автоматизированной обработке личной информации. Первые национальные законы о защите данных в Швеции в 1973 году, в Германии в 1977 году и во Франции в 1978 году заложили основы для последующего международного регулирования, кульминацией которого стало принятие Конвенции Совета Европы №108 «О защите физических лиц при автоматизированной обработке персональных данных» в 1981 году [Оганесян, 2020].

Основная часть

Конвенция № 108, оставаясь единственным имеющим обязательную силу международным договором в этой сфере, создала универсальные стандарты защиты персональных данных, основанные на принципах законности и справедливости обработки, целевого использования, минимизации данных, их точности, ограниченного хранения и конфиденциальности [www]. Модернизация Конвенции в 2018 году (далее – Конвенция 108+) позволила адаптировать эти принципы к вызовам цифровой экономики, добавив требования прозрачности обработки, учета рисков, обязательного уведомления о нарушениях и усилив защиту особых категорий данных. Важно отметить, что Конвенция 108+ сохранила гибкий подход, позволяющий учитывать особенности различных правовых систем, что способствовало ее ратификации не только европейскими странами, но и другими государствами.

Параллельно с развитием международных стандартов происходило формирование региональных систем защиты персональных данных, наиболее развитой из которых стало европейское регулирование. Директива 95/46/ЕС заложила основы гармонизации национальных законодательств стран ЕС, а принятый в 2016 году Общий регламент по защите данных (GDPR) создал единое правовое пространство в этой сфере. GDPR детализировал и усилил принципы защиты данных, а также ввел новые права для субъектов данных (такие как право на переносимость данных и «право на забвение»), установил строгие требования к трансграничным передачам и ввел значительные штрафные санкции за нарушения установленных правил. Влияние GDPR вышло далеко за пределы ЕС, став de facto глобальным стандартом и образцом для законодателей многих стран [Бесчастнова, 2025].

Одновременно с развитием нормативной правовой базы происходило технологическое преобразование деятельности международных организаций, которые стали активно внедрять цифровые инструменты для повышения эффективности своей работы. Международные

гуманитарные организации стали осуществлять биометрическую идентификацию бенефициаров, системы электронных платежей и ваучеров, использовать анализ больших данных для прогнозирования кризисов и оптимизации помощи субъекту гражданско-правового оборота. Международные правоохранительные структуры создали сложные системы обмена информацией, финансовые институты – платформы для мониторинга экономических показателей [Курьянова, 2019]. Эти инновации, с одной стороны, значительно повысили оперативность и адресность международной деятельности, а с другой – создали беспрецедентные риски для прав и свобод индивидов, чьи персональные данные оказались в распоряжении международных структур.

Международные организации как особые субъекты международного права обладают уникальным правовым статусом, который формировался на протяжении XX века. Их ключевой характеристикой является производность от воли государств-учредителей, выраженной в учредительном договоре, который определяет цели, структуру и полномочия организации. Однако, будучи созданными государствами, международные организации обладают собственной правосубъектностью, позволяющей им независимо участвовать в международных отношениях. Эта независимость обеспечивается системой привилегий и иммунитетов, которые варьируются в зависимости от функций конкретной организации, но обычно включают иммунитет от юрисдикции национальных судов, неприкосновенность помещений и архивов, фискальные привилегии [Туманов, 2016].

Особенность правового положения международных организаций в сфере защиты персональных данных проявляется в нескольких аспектах.

Во-первых, их деятельность по определению носит трансграничный характер, что делает практически невозможным применение национальных законодательств о защите данных, которые территориально ограничены.

Во-вторых, будучи созданными множеством государств, они не могут быть подчинены правовой системе только одной страны, даже страны пребывания их штаб-квартиры.

В-третьих, контрольные и надзорные механизмы, предусмотренные национальными законами о защите данных (такие как деятельность уполномоченных органов по защите данных), вступают в противоречие с иммунитетами международных организаций и принципом их функциональной независимости.

Практика международных организаций в ЕС выработала несколько моделей регулирования защиты персональных данных. Наиболее распространенной стала разработка внутренних нормативных актов (правил, протоколов, регламентов), устанавливающих стандарты обработки данных, сопоставимые с международными и национальными требованиями. Например, ООН приняла Политику защиты персональных данных в 2018 году, Международный комитет Красного Креста – Правила защиты персональных данных в 2015, Европейский союз – Регламент 2018/1725, специально регулирующий обработку данных институтами ЕС. Эти документы обычно предусматривают создание специализированных подразделений по защите данных и механизмы внутреннего контроля.

Особый интерес представляет вопрос о юрисдикционной подведомственности споров, связанных с обработкой данных международными организациями. Доктрина иммунитета предполагает, что такие споры должны разрешаться внутренними механизмами организаций, а не национальными судами. Однако это требует от организаций создания эффективных процедур рассмотрения жалоб и предоставления средств правовой защиты. Так, например, Европейский суд по правам человека в решении по делу Waite and Kennedy v. Germany (1999) установил, что

иммунитет международных организаций от национальной юрисдикции допустим только при условии наличия разумных альтернативных средств защиты прав [Постановление ЕСПЧ]. Этот подход стимулировал многие организации к развитию внутренних механизмов обжалования, хотя их эффективность и независимость постоянно подвергаются критике.

Проблема трансграничных передач данных в контексте деятельности международных организаций имеет особую специфику. С одной стороны, такие организации по своей природе нуждаются в свободном обмене информацией между своими отделениями в разных странах. С другой стороны, национальные законодательства (особенно GDPR) устанавливают строгие ограничения на передачу данных за пределы своей юрисдикции. Разрешением данной дилеммы стало признание того, что передача данных международной организации не является «трансграничной передачей» в классическом понимании, поскольку организация представляет собой отдельный субъект в правовом пространстве. Однако это требует от организаций демонстрации того, что их внутренние стандарты защиты данных обеспечивают уровень защиты, сопоставимый (аутентичный в т.ч.) с национальными требованиями.

Перспективы развития правового регулирования защиты персональных данных в деятельности международных организаций связаны с несколькими тенденциями.

Во-первых, это дальнейшая гармонизация стандартов посредством присоединения организаций к Конвенции № 108+ и принятие ими обязательств по приведению своих правил в соответствие с международными нормами.

Во-вторых, развитие механизмов сотрудничества между национальными органами по защите данных и внутренними аудиторами международных организаций.

В-третьих, совершенствование внутренних средств правовой защиты в организациях для соответствия критериям «разумной альтернативы».

В-четвертых, выработка специальных правил для трансграничных потоков данных в гуманитарной и правоохранительной сферах, учитывающих их специфику.

Современный этап развития цифровых технологий ставит перед системой защиты персональных данных в международных организациях новые вызовы. Использование искусственного интеллекта для анализа данных, внедрение распределенных реестров, развитие прогнозной аналитики – все эти инновации требуют переосмысления традиционных принципов защиты данных. Особую остроту приобретают вопросы совместимости новых технологий с принципами минимизации данных, целевого использования и ограничения хранения. В этом контексте международные организации могут стать площадками для выработки новых подходов к защите приватности в цифровую эпоху.

Роль международных организаций в формировании глобальных стандартов защиты персональных данных продолжает расти. Такие структуры, как ООН посредством Группы по цифровому сотрудничеству, Совет Европы через Консультативный комитет Конвенции 108+, ОЭСР (англ. Organisation for Economic Co-operation and Development, OECD) – международная экономическая организация развитых стран) с помощью деятельности своего Комитета по цифровой экономике, активно участвуют в разработке принципов и рекомендаций по регулированию обработки данных. Взаимодействие между международными и национальными системами защиты персональных данных постепенно эволюционирует от конфронтации к поиску баланса. На смену спорам о юрисдикции приходят механизмы взаимного признания стандартов и сертификации систем защиты данных. Все большее распространение получают совместные инициативы, такие как создание «зон доверия» для трансграничного обмена данными между национальными органами и международными организациями. Это позволяет

сочетать уважение к суверенитету государств в определении уровня защиты данных с необходимостью обеспечения эффективного международного сотрудничества.

Особого внимания заслуживает вопрос об ответственности международных организаций за нарушения в сфере защиты персональных данных. Традиционный иммунитет от судебных исков ставит проблему обеспечения доступа пострадавших к средствам правовой защиты. Решением проблемы становится развитие внутренних механизмов рассмотрения жалоб и возмещения ущерба, а также заключение специальных соглашений со странами пребывания о частичном отказе от иммунитета в рассматриваемой сфере [Yeung K., Bygrave L. A., 2022].

Этические аспекты обработки персональных данных приобретают особое значение для международных организаций, особенно работающих в гуманитарной сфере [Михайлов, 2022]. Использование биометрических данных беженцев, обработка информации о жертвах конфликтов, применение алгоритмов для распределения помощи – все эти действия требуют не только юридического, но и этического обоснования.

Пандемия COVID-19 продемонстрировала как важность международного обмена данными для противодействия глобальным угрозам, так и связанные с этим риски для неотъемлемых прав человека и гражданина. Международные организации, участвовавшие в разработке и внедрении цифровых инструментов отслеживания контактов, оказались перед дилеммой между эффективностью мер и защитой конфиденциальности [Исмагилова, 2020]. Этот опыт подчеркивает необходимость разработки специальных протоколов обработки данных в чрезвычайных ситуациях, сочетающих оперативность реагирования с гарантиями прав личности.

Финансовые аспекты защиты данных также приобретают особое значение для международных организаций. Внедрение комплексных систем защиты информации требует значительных ресурсов, что создает проблемы для организаций с ограниченным бюджетом. В то же время последствия утечек данных могут нанести существенный репутационный ущерб и снизить доверие к организации. В этой связи все большее значение приобретает дифференцированный подход, который позволяет сосредоточить усилия и ресурсы на защите наиболее чувствительных категорий данных в зависимости от степени их уязвимости и потенциальных последствий нарушения.

Взаимодействие международных организаций с частным сектором в сфере защиты данных создает новые правовые вопросы. При передаче обработки данных на аутсорсинг или использовании облачных сервисов организации должны обеспечивать соблюдение своих стандартов защиты данных подрядчиками [Ioannidou I., Sklavos N., 2021]. Это требует разработки сложных договорных механизмов и систем контроля, особенно когда подрядчики находятся в разных юрисдикциях.

Региональные особенности регулирования защиты данных создают дополнительные сложности для международных организаций. Различия между подходами ЕС, США, Китая и других стран вынуждают организации разрабатывать гибкие системы соответствия, способные адаптироваться к юрисдикционным требованиям разных государств. В то же время это стимулирует выработку универсальных стандартов, которые могли бы стать мостом между различными правовыми юрисдикциями.

Роль международного права в регулировании защиты персональных данных продолжает усиливаться. Помимо Конвенции 108+, значительное влияние оказывают руководящие принципы ООН по ведению бизнеса и неотъемлемым правам человека, рекомендации ОЭСР,

документы ISO (международная организация, занимающаяся выпуском стандартов). Формируется многоуровневая система регулирования, сочетающая обязательные и частно-правовые нормы.

Международные организации играют ключевую роль в этом процессе как разработчики стандартов и площадки для согласования позиций разных стран.

Перспективным направлением развития является использование технологий блокчейн для защиты персональных данных в деятельности международных организаций. Децентрализованный характер хранения информации, возможность точного контроля доступа и прозрачность изменений соответствуют основным принципам защиты данных [Дерюгина, 2020]. Пилотные проекты в этой области уже реализуются некоторыми организациями в сфере гуманитарной помощи.

Особую актуальность как уже отмечалось выше приобретает вопрос о защите персональных данных уязвимых групп, с которыми работают международные организации. Беженцы, жертвы конфликтов, перемещенные лица часто не имеют возможности эффективно контролировать свою персональную информацию. Это требует от организаций принятия дополнительных гарантий и специальных процедур защиты данных таких категорий.

Защита персональных данных в деятельности международных организаций превратилась в сложную, многогранную систему, сочетающую элементы международного и внутреннего права, технические и организационные меры, правовые и этические стандарты. Поиск баланса между эффективностью международного сотрудничества и защитой фундаментальных прав личности остается динамичным процессом, требующим постоянного диалога между государствами, международными организациями и институтом гражданского общества. Дальнейшее развитие этой системы будет определяться способностью адаптироваться к технологическим изменениям, сохраняя при этом верность основополагающим принципам уважения человеческого достоинства и автономии личности в цифровую эпоху.

Заключение

Современное регулирование защиты персональных данных в деятельности международных организаций представляет собой динамично развивающийся правовой механизм, формирующийся под влиянием технологических вызовов, международных стандартов и национальных законодательств. Исторически сложившиеся принципы защиты данных, закрепленные в Конвенции 108+ и GDPR, стали основой для разработки внутренних политик международных организаций, которые вынуждены балансировать между необходимостью эффективного трансграничного обмена информацией и соблюдением неотъемлемых прав личности.

Ключевой проблемой остается вопрос юрисдикции и иммунитета: традиционные привилегии международных организаций зачастую ограничивают возможность применения национальных законов о защите данных, что требует создания эффективных внутренних механизмов контроля и обжалования. Перспективы развития этой сферы связаны с дальнейшей гармонизацией стандартов, внедрением риск-ориентированного подхода, совершенствованием технологических мер защиты и укреплением сотрудничества между международными и национальными регуляторами. Особое значение приобретают этические аспекты обработки данных, особенно в гуманитарной сфере, где на кону стоят права уязвимых групп.

В условиях стремительной цифровизации международные организации становятся не только объектами регулирования, но и активными участниками формирования глобальных стандартов защиты данных. Их опыт в поиске баланса между инновациями и конфиденциальностью может послужить моделью для государств и корпораций. Однако успех этого процесса зависит от способности организаций адаптироваться к новым технологическим реалиям, сохраняя приверженность фундаментальным принципам уважения прав человека в цифровую эпоху.

Сублимируем, защита персональных данных в международных организациях – это непрерывный поиск компромисса между эффективностью глобального сотрудничества и незыблемостью прав личности, требующий гибкости, прозрачности и постоянного диалога между всеми заинтересованными сторонами.

Библиография

1. «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» (Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999): https://www.consultant.ru/document/cons_doc_LAW_121499/
2. Бесчастнова О.В., Слабкая Д.Н. Противоречия в реализации принципов Общего регламента по защите данных в правовой системе ЕС: аспекты защиты персональных данных // Вопросы российского и международного права. 2025. Том 15. № 4-1А. С.
3. Дерюгина, Т. В. Блокчейн, смарт-контракты и управление незарегистрированными правами интеллектуальной собственности / Т. В. Дерюгина, А. Е. Пономарченко // Парадигмы управления, экономики и права. – 2020. – № 2. – С. 163-169.
4. Исмагилова, О. Мировой опыт регулирования защиты, передачи и хранения данных / О. Исмагилова, К. Хаджи // Экономическая политика. – 2020. – Т. 15, № 3. – С. 152-175. – DOI 10.18288/1994-5124-2020-3-152-175.
5. Жуматаева, М. Т. Правовая основа информационной безопасности: теоретический аспект / М. Т. Жуматаева, Н. Чыныбаева // Вестник Международного Университета Кыргызстана. – 2023. – № 3(51). – С. 162-167. – DOI 10.53473/16946324_2023_3_162. – EDN QHXRCC.
6. Новиков, А. В. Результаты реализации инициатив глобальной политики «Образование для всех» 1990-х на примере Индии / А. В. Новиков, Д. Н. Слабкая, И. М. Шипорин // Теории и проблемы политических исследований. – 2023. – Т. 12, № 12А. – С. 58-64. – DOI 10.34670/AR.2023.60.13.009.
7. Постановление ЕСПЧ 18.02.1999 "Дело "Уэйт и Кеннеди (Waite and Kennedy) против Германии" (жалоба N 26083/94) [рус., англ.] https://e-ecolog.ru/docs/XGUK-FJPNd6Yhiw7-dBUl?utm_referrer=https%3A%2F%2Fyandex.ru%2F
8. Курьянова, С. Л. Биометрическая идентификация клиентов в банковской сфере: отечественный и зарубежный опыт / С. Л. Курьянова, О. С. Цвигунова // Азимут научных исследований: экономика и управление. – 2019. – Т. 8, № 4(29). – С. 238-241. – DOI 10.26140/anie-2019-0804-0051. – EDN ZRPHIU.
9. Михайлов, М. А. Организационные, правовые и этические аспекты получения, хранения и использования биометрической информации в целях всеобщей регистрации населения / М. А. Михайлов, Т. А. Кокодей // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2022. – Т. 8 (74), № 4. – С. 345-353.
10. Оганесян Т. Д. Право на защиту персональных данных: исторический аспект и современная концептуализация в эпоху Big Data // Журнал зарубежного законодательства и сравнительного правоведения. 2020. № 2. С. 48-63. DOI: 10.12737/jflcl.2020.010
11. Туманов С.Н. Международные межправительственные организации: понятие и функциональная характеристика // Вопросы российского и международного права. 2016. Том 6. № 11А. С. 3-16.
12. Шебанова Н.А. Охрана персональных данных: опыт международного регионального сотрудничества // Международное право и международные организации / InternationalLawand InternationalOrganizations. – 2020. – № 2. DOI: 10.7256/2454-0633.2020.2.32597 URL: https://nbpublish.com/library_read_article.php?id=32597
13. Andrew J., Baker M. The general data protection regulation in the age of surveillance capitalism //Journal of Business Ethics. – 2021. – С. 565-578.
14. Bayamlıoğlu E. The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called “right to explanation” //Regulation & Governance. – 2022. – Т. 16. – №. 4. – С. 1058-1078.

15. Calzada I. Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL) //Smart Cities. – 2022. – Т. 5. – №. 3. – С. 1129-1150.
16. Goyal N., Howlett M., Taeihagh A. Why and how does the regulation of emerging technologies occur? Explaining the adoption of the EU General Data Protection Regulation using the multiple streams framework //Regulation & Governance. – 2021. – Т. 15. – №. 4. – С. 1020-1034.
17. Ioannidou I., Sklavos N. On general data protection regulation vulnerabilities and privacy issues, for wearable devices and fitness tracking applications //Cryptography. – 2021. – Т. 5. – №. 4. – С. 29.
18. Labadie C., Legner C. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR //Journal of Information Technology. – 2023. – Т. 38. – №. 1. – С. 16-44.
19. Team I. T. G. P. et al. EU general data protection regulation (GDPR): an implementation and compliance guide. – Packt Publishing Ltd, 2025.
20. Vlahou A. et al. Data sharing under the General Data Protection Regulation: time to harmonize law and research ethics? //Hypertension. – 2021. – Т. 77. – №. 4. – С. 1029-1035.
21. Yeung K., Bygrave L. A. Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship //Regulation & Governance. – 2022. – Т. 16. – №. 1. – С. 137-155.

The Evolution of Legal Regulation of Personal Data Protection in the Activities of International Organizations in the Context of Digital Transformation

Ol'ga V. Beschastnova

PhD in Law, Associate Professor;
Head of the Department of Criminal Law and Law Enforcement Activities,
Astrakhan State University,
414056, 20-a, Tatishcheva str., Astrakhan, Russian Federation;
e-mail: beschastnova_ol@mail.ru

Diana N. Slabkaya

Senior Researcher,
Scientific-Research Institute of the Federal Penitentiary Service of the Russian Federation,
125130, 15-a, Narvskaya str., Moscow, Russian Federation;
e-mail: sdn10.70@mail.ru

Abstract

The article examines the evolution of legal regulation of personal data protection in the activities of international organizations in the context of digital transformation. The authors analyze the historical prerequisites for the formation of international standards, including the Council of Europe Convention and the General Data Protection Regulation (GDPR), as well as their impact on the internal policies of international organizations. Special attention is paid to legal conflicts related to organizational immunity, cross-border data transfers, and jurisdictional jurisdiction of disputes. The study explores contemporary challenges in the storage and transfer of personal data, including the use of artificial intelligence, biometric technologies, and blockchain, as well as ethical aspects of personal data processing in civil transactions. Key trends in regulatory development are identified, emphasizing the need to strike a balance between the efficiency of international cooperation and the protection of fundamental human and civil rights.

For citation

Beschastnova O.V., Slabkaya D.N. (2025) Evolyutsiya pravovogo regulirovaniya zashchity personal'nykh dannykh v deyatel'nosti mezhdunarodnykh organizatsiy v usloviyakh tsifrovoy transformatsii [The Evolution of Legal Regulation of Personal Data Protection in the Activities of International Organizations in the Context of Digital Transformation]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (5A), pp. 245-254.

Keywords

Personal data protection, international organizations, GDPR, digital technologies, cross-border data transfer, legal standards, confidentiality, artificial intelligence, biometric data, blockchain, data processing ethics, cybersecurity.

References

1. "Convention for the Protection of Natural Persons with regard to Automated Processing of Personal Data" (Concluded in Strasbourg on 28.01.1981) (together with Amendments to the Convention for the Protection of Natural Persons with regard to Automated Processing of Personal Data (CTS No. 108), allowing the accession of the European Communities, adopted by the Committee of Ministers in Strasbourg on 15.06.1999): https://www.consultant.ru/document/cons_doc_LAW_121499/
2. Beschastnova O.V., Slabkaya D.N. Contradictions in the implementation of the principles of the General Data Protection Regulation in the EU legal system: aspects of personal data protection // Issues of Russian and international law. 2025. Volume 15. No. 4-1A. P.
3. Deryugina, T. V. Blockchain, smart contracts and management of unregistered intellectual property rights / T. V. Deryugina, A. E. Ponomarchenko // Paradigms of management, economics and law. - 2020. – No. 2. – pp. 163-169.
4. Ismagilova, O. World experience in regulating data protection, transmission and storage / O. Ismagilova, K. Hadji // Economic policy. – 2020. – Vol. 15, No. 3. – pp. 152-175. – DOI 10.18288/1994-5124-2020-3-152-175.
5. Zhumatayeva, M. T. The legal basis of information security: a theoretical aspect / M. T. Zhumatayeva, N. Chynybayeva // Bulletin of the International University of Kyrgyzstan. – 2023. – № 3(51). – PP. 162-167. – DOI 10.53473/16946324_2023_3_162. – QHXRCC EMAIL ADDRESS.
6. Novikov, A.V. The results of the implementation of the global policy initiatives "Education for all" in the 1990s on the example of India / A.V. Novikov, D. N. Slabkaya, I. M. Shiplorin // Theories and problems of political research. – 2023. Vol. 12, No. 12a. – pp. 58-64. – DOI 10.34670/AR.2023.60.13.009.
7. Statement dated 02/18/1999 "The case of Whit and Kennedy (Waite and Kennedy) v. Germany" (complaint No. 26083/94) [rus., eng.] https://e-ecolog.ru/docs/XGUK-FJPNd6Yhiw7-dBUl?utm_referrer=https%3A%2F%2Fyandex.ru%2F
8. Kuryanova, S. L. Biometric identification of clients in the banking sector: domestic and foreign experience / S. L. Kuryanova, O. S. Tsvigunova // Azimuth of scientific research: economics and management. – 2019. – Vol. 8, No. 4(29). – pp. 238-241. – DOI 10.26140/anie-2019-0804-0051 . – PUBLISHING HOUSE of ZRFIU.
9. Mikhailov, M. A. Organizational, legal and ethical aspects of obtaining, storing and using biometric information for the purpose of universal population registration / M. A. Mikhailov, T. A. Kokodey // Scientific Notes of the V.I. Vernadsky Crimean Federal University. Legal sciences. – 2022. – Vol. 8 (74), No. 4. – pp. 345-353.
10. Oganesyan T. D. The right to personal data protection: historical aspect and modern conceptualization in the era of big data // Journal of Foreign Legislation and Comparative Jurisprudence. 2020. No. 2. pp. 48-63. DOI: 10.12737/jflcl.2020.010
11. Tumanov S.N. International intergovernmental organizations: concept and functional characteristics // Issues of Russian and international law. 2016. Volume 6. No. 11A. pp. 3-16.
12. Ebanova N.A. Orana The personalized tribute: the experience of an international state // The international State and international relations. organization / International law and international organizations. – 2020. – № 2. DOI: 10.7256/2454-0633.2020.2.32597 URL: https://nbpublish.com/library_read_article.php?id=32597
13. Andrew J., Baker M. General provisions on data protection in the era of surveillance capitalism //Journal of Business Ethics. 2021. pp. 565-578.
14. Bayamlioglu E. The right to challenge automated decisions in accordance with the General Data Protection Regulation: in addition to the so–called “right to explanation” //Regulation and management. – 2022. – Vol. 16. – No. 4. – pp. 1058-1078.
15. Kalzada I. Privacy of citizens' data in China: the current state of the Law on the Protection of Personal Information (PIPL) //Smart cities. – 2022. – Vol. 5. – No. 3. – pp. 1129-1150.

16. Goyal N., Howlett M., Teihag A. Why and how is the regulation of new technologies? Explanation of the adoption of the EU General Data Protection Regulation using the concept of multiple flows //Regulation and management. – 2021. Vol. 15. – No. 4. – pp. 1020-1034.
17. Ioannidou I., Sklavos N. On the general regulation of data protection, vulnerabilities and privacy issues for wearable devices and fitness tracking applications // Cryptography. – 2021. – Vol. 5. – No. 4. – p. 29.
18. Labadi S., Legner S. Creating data management capabilities in accordance with the requirements of data protection legislation: lessons from the EU GDPR //Journal of Information Technology. – 2023. – Vol. 38. – No. 1. – pp. 16-44.
19. The I. T. G. P. team and others. EU General Data Protection Regulations (GDPR): Guidelines for implementation and compliance. – Packt Publishing Ltd, 2025.20.
Vlahou A. et al. Data exchange in accordance with the General Data Protection Regulation: is it time to bring legislation in line with the ethics of scientific research? //Hypertension. – 2021. – Vol. 77. – No. 4. – pp. 1029-1035.
21. Jung K., Bygrave L. A. Demystification of the modernized European data protection regime: Interdisciplinary conclusions of scientists in the field of legal and regulatory management //Regulation and Governance. – 2022. – Vol. 16. – No. 1. – pp. 137-155.