Г. Г. Камалова,
доктор юридических наук, доцент,
заведующий кафедрой информационной безопасности в управлении,
Удмуртский государственный университет

ИНФОРМАЦИОННО-ПРАВОВЫЕ РИСКИ

Аннотация. Целью исследования является определение сущности и особенностей информационно-правовых рисков в условиях цифровой трансформации, геополитических изменений и противодействия пандемии COVID-19, определяющих основные современные векторы дальнейшего развития информационного права. Наиболее существенное внимание в работе уделено вопросам применения в информационном праве методологии рискориентированного подхода. На основе проведенного исследования автором сделан вывод о необходимости закрепления понятия «информационный риск» в законодательстве, определения порядка и критериев категорирования и оценки рисков в сфере обеспечения информационной безопасности, а также развития правовых механизмов преодоления и минимизации рисков, что позволит усилить уровень защищенности организаций и государства.

Ключевые слова: право, цифровые технологии, информационная безопасность, информационные риски, правовые риски, информационное право, публично-правовые отрасли, методология права

INFORMATION AND LEGAL RISKS

Abstract. The aim of the study is to determine the nature and characteristics of information and legal risks in the context of digital transformation, geopolitical changes and countering the COVID-19 pandemic, which determine the main modern vectors for the further development of information law. The most significant attention in the work is paid to the application of the risk-based approach methodology in information law. Based on the study, the author concluded that it is necessary to consolidate the concept of “information risk” in the legislation, determine the procedure and criteria for categorizing and assessing risks in the field of information security, as well as developing legal mechanisms for overcoming and minimizing risks, which will increase the level of security of organizations and the state.

Keywords: Law, Digital technologies, Information security, Information risks, Legal risks, Information law, Public law branches, Methodology of law

Современный мир характеризуется активной цифровизацией всех сфер жизни человека и общества. В указанных условиях государства ставят себе целью выход на передовые рубежи посредством построения национального сектора глобальной цифровой экономики и, соответственно, задачи разработки, внедрения и коммерциализации инновационных цифровых решений в интересах обеспечения национальных интересов. При этом стремительная динамика цифровых технологических решений, которая вызывает колоссальные практически революци-

онные изменения общественных отношений, формирует новые вызовы и риски в информационной сфере, что не могло не затронуть право как универсальный регулятор социальной действительности. Трансформация права происходит как в аспекте развития и совершенствования законодательства, так и правовой науки. Закономерно флагманом выступает информационное право, что детерминировано его предметной областью. Исследователи обращаются к различным сторонам правового регулирования цифровых технологий и обеспечения информационной безопасности [16, 19].

В современной цифровой правовой реальности стало фактически обычным обсуждение любых вопросов, связанных с общественными отношениями в информационной сфере, в русле преодоления или минимизации больших вызовов, рисков и угроз. Это представляется закономерным последствием современной ситуации развития регуляторных механизмов. Указанное имеет особое значение для сферы правового обеспечения информационной безопасности, которое продолжает активно эволюционировать в условиях влияния факторов цифровой трансформации, геополитических изменений и формирования многополярного мира, преодоления пандемии COVID-19. Сегодня правовое обеспечение информационной безопасности уже является не только отдельным направлением правовых исследований. Взаимосвязанные вопросы стали неотъемлемой стороной обсуждения любых проблем правового обеспечения развития цифровых технологий.

При этом приведенные термины «вызовы», «риски» и «угрозы», безусловно, обозначают хотя и взаимосвязанные, вместе с тем отнюдь не равноценные понятия. И если анализ информационных угроз является закономерной частью практической деятельности в сфере обеспечения информационной безопасности, где выявление актуальных информационных угроз для организации и для государства в целом на практике выступает первым этапом построения любой системы защиты информации, что нашло свое закономерное отражение в документах стратегического планирования и актах федеральных органов власти, то ситуация с рисками в информационной сфере видится в настоящее время несколько иной. Указанное и обусловило авторский интерес к исследованию вопросов, связанных с информационными и правовыми рисками.

Стратегия национальной безопасности РФ определяет угрозы национальной безопасности через совокупность условий и факторов, которые создают возможность ущерба национальным интересам [4], а Доктрина информационной безопасности РФ угрозы информационной безопасности, в свою очередь, характеризует на основе совокупности действий и факторов, создающих опасность ущерба в информационной сфере [5]. При этом обращает внимание, что в первом акте указаны условия и факторы, а во втором – действия и факторы. Отмеченные различия представляются неслучайными. Они определяются деятельностным характером обеспечения информационной безопасности, детерминированным динамикой общественных отношений в этой сфере. Сходное определение понятия угрозы информационной безопасности содержится в документах технического регулирования.

Правовое регулирование должно ориентироваться на теорию и практику обеспечения информационной безопасности, методические документы в этой сфе-

ре и акты технического регулирования в этой сфере, в которых выявление и минимизация актуальных информационных угроз являются неотъемлемой частью соответствующей деятельности. В связи с этим понятие информационных угроз сегодня в достаточной мере проработано. Определен порядок оценки информационных угроз и особенности формирования комплекса мер по защите информации на уровне как государства в целом, так и отдельных организаций.

Если обратиться к рискам в сфере обеспечения информационной безопасности, то следует отметить, что пока, с одной стороны, они сегодня являются общим моментом рассуждений о существующих проблемах в данной сфере, позволяющим акцентировать внимание на остроте современной ситуации и специфике регулируемых общественных отношений, а с другой – в указанной сфере все более широко применяется рискориентированный подход. Это закономерно находит свое отражение в научных исследованиях. Вместе с тем сегодня представляется важным провести определенный анализ сущности тех взаимосвязанных рисков, которые актуальны как для информационной сферы, так и правовой.

В связи с этим категорию риска в праве А. В. Остроушко предлагает рассматривать как юридико-техническое средство для обозначения ситуации, в отношении которой сложно прогнозировать результат [15]. Это позволяет связывать правовой риск с понятием правовых ситуаций, которые, по С. С. Алексееву, являются сложными жизненными обстоятельствами, требующими правового решения [7]. При этом для правовой ситуации традиционно характерны конфликтность, противоборство, противостояние и конкуренция. Правовое обеспечение информационной безопасности на различных уровнях в национальных интересах сегодня фактически осуществляется в ситуации ведущейся против Российской Федерации информационной войны, что определяет особенности современной повестки.

Интерес, на наш взгляд, представляет также позиция Ю. А. Тихомирова, который «правовой риск» рассматривает как элемент юридического прогнозирования, отмечая, что он «позволяет предвидеть как повторяющиеся, так и возможные и неожиданные отклонения от правовых моделей регуляторов» [18]. Совершенствование правового обеспечения в информационной сфере закономерно требует научного осмысления революционных изменений, происходящих под воздействием развития цифровых технологий и прогнозирования последствий их внедрения. Вместе с тем следует отметить, что большинство исследователей традиционно пишут об информационных рисках или рисках в информационной сфере, связывая их с возможными негативными последствиями развития цифровых технологий в рамках разработки и внедрения прорывных цифровых технологий, а также с вероятным ущербом их применения. Хотя прогнозирование правовых рисков позволяет выделять и положительные эффекты в этой области.

В настоящее время категория рисков и применение рискориентированного подхода получили свое закрепление в законодательстве о контрольно-надзорной деятельности государственных органов власти, где под рисками понимается возможность наступления события причинения ущерба охраняемым интересам, что также акцентирует внимание на возможных негативных последствиях реализации рисков. В последнее время все чаще понятие риска и рискориентированный под-

ход применяются при регулировании общественных отношений в финансово-кредитной сфере. В иных областях законодательства обязанность применения риск-ориентированного подхода в положениях нормативных правовых актов в явном виде пока не получила своего сколь-нибудь широкого закрепления.

Вместе с тем информационному законодательству данная категория тоже не чужда. Процесс преодоления риска нашел свое отражение в Федеральном законе «О защите детей от информации, причиняющей вред их здоровью и развитию» [2], который определяет информационную безопасность детей через состояние их защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) развитию. Хотя применение термина «информационный риск» в большей мере характерно для подзаконных актов, вместе с тем пп. 1 ч. 2 ст. 13 Федерального закона «Об электронной подписи» [1] устанавливает обязанность информирования о рисках, связанных с применением электронных подписей, а п. 21 ст. 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации» – уведомления о рисках, предоставления биометрических данных и рисках отказа от криптографических средств защиты [3]. Это закономерно отражает взаимосвязь процессов минимизации информационных рисков с деятельностью в сфере обеспечения информационной безопасности.

В числе основных факторов риска традиционно указывают наличие неопределенности ситуации, возможности причинения ущерба и его практической значимости. Кроме того, необходимо отметить определенную субъективность ситуации с риском в рамках рефлексии субъекта о предполагаемом риске и его оценке как существенного и актуального для соответствующей системы. При этом, анализируя информационные и правовые риски, следует признать справедливым мнение исследователей, полагающих, что риск на онтологическом уровне всегда является информационным, так как источник любого риска – неопределенность информации [17]. Хотя информационные риски, влияя на общественные отношения и трансформируя их, представляются для права несомненно важными, вместе с тем следует особое внимание уделить собственно правовым рискам в информационной сфере.

Классификация информационно-правовых рисков в самом общем виде в качестве оснований должна включать субъекта риска, объект риска и его последствия. Таким образом, правовые риски в информационной сфере целесообразно рассматривать в контексте рисков для личности, организации, общества и государства, а также применительно к развитию определенных цифровых технологий. Именно в этом ключе сегодня развивается информационное законодательство Российской Федерации, для которого важнейшими являются риски нарушения прав и свобод граждан, риски для обеспечения национальных интересов, риски в рамках достижения технологического и цифрового суверенитета и ряд иных.

При анализе информационных рисков с позиции права в самом общем виде следует выделять риски:

– связанные с недочетами в достижении современной повестки информационно-правовой политики;

– несовершенства законодательства, включая его несистемность, пробелы и коллизии;

– обусловленные сложностями и недостатками правоприменительной практики, включая проблемы расследования киберпреступлений;

– связанные с правосознанием и информационно-правовой грамотностью населения.

В условиях построения национального сектора цифровой экономики и соответственно развития сквозных цифровых технологий особую значимость приобретают связанные с ними риски. Так, на высокие риски обращения криптовалюты не единожды указывал Центральный банк РФ. Одной из проблем в информационной сфере является нарастание рисков распространения информации, связанное с фейковой информацией, что приобрело особую актуальность в условиях формирования многополярного мира и взаимосвязанного с этим противостояния цивилизаций.

В сфере развития цифровых технологий и их использования, полагаем, наиболее существенны риски неопределенности правового режима таких технологий и объектов, функционирующих на их основе. Цифровая революция трансформирует общество с беспрецедентным размахом, формирует колоссальные перспективы и трудности. Сегодня продвижение искусственного интеллекта, технологий больших данных (big data), виртуальной и дополненной реальности, распределенного реестра и иных сквозных цифровых технологий создают новые вопросы в праве, требующие междисциплинарного и межотраслевого решения. При этом раскрытие социально-экономического потенциала новейших технологий немыслимо без формирования и совершенствования правовой основы их разработки, производства и использования, включая международно-правовые аспекты. Формирование специальных правовых режимов указанных технологий и иных цифровых инноваций позволит снизить неопределенность в соответствующей сфере и соответственно минимизировать риски. Однако существующая правовая неопределенность сегодня вынужденно преодолевается посредством введения их экспериментальных правовых режимов.

Ряд информационно-правовых рисков сегодня связывают с профилированием, цифровыми двойниками и возможностью манипулирования цифровой личностью. Применение цифровых технологий может способствовать дискриминации лица по признакам пола, расы, успешности и многим иным, являясь, например, инструментом нарушения прав при решении вопроса о трудоустройстве лица, выдаче кредита, условно-досрочном освобождении и иных ситуациях. Показательной в этом смысле является также система социальных кредитов Китая. Учитывая, что уже сегодня машинный код порой выступает регулирующим фактором при принятии многих решений, игнорирование проблем обеспечения равенства людей может привести к социальной нестабильности и потрясениям в обществе, что определяет существующие риски в данной области.

Тотальная цифровизация всех сфер жизни ведет к рискам несанкционированного вмешательства в экономическую сферу и личную жизнь граждан. Это требует принять меры, направленные на построение открытой и безопасной ин-

тернет-среды при обеспечении защиты персональных данных в цифровом пространстве. Указанное актуализирует исследования в области правового обеспечения цифровой среды доверия.

Наибольшие риски для жизни граждан, предпринимательской деятельности и сферы государственного управления влечет киберпреступность. В последние месяцы компьютерные атаки приобрели особую остроту в свете противостояния и противоборствования в информационной среде. Не всегда таким кибератакам удается противостоять, несмотря на все принимаемые меры. Так, в середине сентября 2022 г. в своем телеграм-канале о проведенных DDoS-атаках и взломе официального сайта заявила Организация Договора о коллективной безопасности, что повлекло нарушение работоспособности ресурса, попытки внесения изменений в цифровые данные и их утрату [10]. Указанное демонстрирует уровень существующих информационных рисков.

Хотя информационная сфера по своей сути трансгранична, сегодня специалистами отмечаются риски балконизации Интернета. Не ставя в настоящем научном исследовании цель подробно рассмотреть существующие в этой сфере проблемы, в то же время следует отметить, что это не единственный риск и интернет-пространство сегодня контролируется не только государствами в целях обеспечения национальной безопасности, но и глобальными IT-корпорациями. В настоящее время сложилась ситуация фильтрации информации, распространяемой в информационно-коммуникационной сети Интернет, ведущими мировыми IT-компаниями, что нарушает права и свободы граждан Российской Федерации и требования российского законодательства [13]. В этом свете изменения российского информационного законодательства декабря 2020 г. следует оценивать как компонент механизма предупреждения рисков нарушения прав человека.

Исследование показывает, что для эффективного развития правовых средств обеспечения информационной безопасности важное значение имеет развитие правовых механизмов рискориентированного подхода в информационном праве, в том числе закрепление понятия «информационный риск» в законодательстве, определение совокупности категорий риска и критериев их оценки в данной сфере применительно к основным видам цифровых технологий, формирование правовых средств категорирования и оценивания информационных рисков, а также правовых средств их минимизации и преодоления.

В связи с вышерассмотренным интересным также представляется обсуждение вопросов страхования рисков информационной безопасности. Следует отметить, что План мероприятий по обеспечению информационной безопасности в рамках реализации программы «Цифровая экономика РФ» ставит задачи разработки нормативных документов по страхованию информационных рисков (киберрисков) и введению при этом налоговых льгот. В связи с этим нельзя обойти вниманием тот факт, что исторически риски в праве наиболее связаны с общественными отношениями в сфере страхования. Вопросы необходимости закрепления в законодательстве возможности страхования рисков в области информационной безопасности поднимают специалисты по защите информации [11]. Страховые компании сегодня уже предлагают соответствующие продукты [14].

Вместе с тем представляется необходимым исследование возможности введения обязательного страхования таких рисков.

Нельзя обойти вниманием также существующие сегодня информационно-правовые риски в научной сфере. Информационное право, как сравнительно молодая отраслевая юридическая наука, прошедшая этап первоначального становления, в настоящее время переживает очередной виток своего развития. В связи с этим следует отметить определенные проблемы информационного права по развитию его понятийного аппарата как языка соответствующей науки, системы ее подотраслей, институтов и подинститутов, общей теории и методологии, что неоднократно отмечалось исследователями.

В последние годы при правовом регулировании общественных отношений в информационной сфере возрастает роль технического регулирования. Современное развитие технического регулирования детерминировано научно-техническим прогрессом, процессами интеграции и глобализации, потребностями обеспечения качества товаров, процессов, работ и услуг, а также обеспечения их конкурентоспособности на национальном, региональном и мировом уровне.

Сегодня государственная система технического регулирования, являясь важнейшей компонентой экономической и правовой системы России, претерпевает революционные изменения под влиянием новых вызов, рисков и угроз цифровизации. В современном мире правовое регулирование технической сферы в целом и сферы цифровых технологий приобретает огромное значение, и представители бизнес-сферы обоснованно ожидают от государства взвешенных решений стоящих задач. Государственная политика России в области технического регулирования цифровых технологий направлена на создание базовых защитных механизмов, направленных на охрану экономических интересов России, отечественных производителей и потребителей объектов стандартизации при продвижении высокоэффективных передовых технологических решений. Это приобретает особое значение в условиях, когда технически и программно сложные цифровые устройства и иные цифровые решения предполагают доверие со стороны их пользователей, а развитие цифровой экономики является условием динамичного формирования экономики уровня передовых государств как фактора преодоления сырьевой зависимости России в условиях жесткой внешнеэкономической конкуренции и санкционных рисков. При этом значимое место в процессе цифровизации нашей страны занимает формирование эффективного механизма технического регулирования, необходимость которого продиктована задачами максимально результативного использования интеллектуального потенциала, имеющегося в нашей стране. В этом аспекте следует отметить, что обеспечение безопасности в различных ее аспектах, включая информационную безопасность, является приоритетной целью технического регулирования, что ставит перед правом задачи осмысления происходящих в информационной сфере процессов, а также определения границ правового и технического регулирования в рамках междисциплинарных исследований.

Отмечая взаимосвязь развития технического и правового регулирования цифровых технологий, следует отметить, что они не конкурируют, а взаимодополняют друг друга. В связи с этим представляют интерес положения документов

стандартизации, включая ГОСТ Р 58771-2019 «Менеджмент риска. Технологии оценки риска» [6].

Существенное значение для информационного права сегодня, полагаем, имеет дальнейшее развитие его методологии, которой порой уделяется недостаточное внимание. Однако исследование методологии информационного права не раз привлекало внимание исследователей [9, 12]. Вместе с тем современные тренды развития ставят новые вопросы в этой области и формируют определенные риски.

Останавливаясь на научной методологии, следует отметить, что это не просто комплекс или совокупность методов. Методология науки предполагает наличие базовых идей, концептов и подходов, которые определяют общую направленность избираемых методов. Так, ранее действовавший паспорт научной специальности 12.00.13 «Информационное право» в составе методологии информационно-правового научного исследования указывал принципы развития предмета исследования, его логической определенности, исторической конкретности и диалектической связи между логическим и историческим способами познания, системности и всесторонности исследования. Важное место уделялось общенаучным подходам системного и деятельностного методов, теоретическому моделированию, юридической интерпретации и многим другим.

Исследователи также отмечали технологический метод в информационном праве как его специфику [8]. Вместе с тем представляется, что технологический подход в информационном праве пока не получил необходимого обоснования и его выделение в значительной мере лишь отражает связь информационного права и цифровых технологий.

В последнее время для исследований в области информационного права важную роль приобретают рискориентированный подход и его методология. Применение этого подхода все чаще прослеживается в рамках научных работ. Это свидетельствует как о его практической значимости, так и потенциале применения в научно-исследовательской деятельности.

Сегодня нельзя обойти вниманием публично-правовой аспект методологии. При этом следует отметить, что методология публично-правовых отраслей права в паспорте научной специальности 5.1.2 обозначена достаточно кратко как методы публичного права. Это, с одной стороны, повышает риски снижения внимания со стороны исследователей к вопросам научной методологии информационного права, а также сводит методологию лишь к совокупности методов, что представляется неверным и достаточно узким подходом к этим вопросам. В целом укрупнение научных специальностей в праве, полагаем, несет в себе риск утраты определенных достижений отраслевых юридических наук, включая комплексный характер информационного права в аспекте его методологии в результате неизбежного обобщения знания.

Список литературы

1. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 14.07.2022) // Собрание законодательства РФ. 2011. № 15. Ст. 2036.

2. О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.07.2021) // Собрание законодательства РФ. 2011. № 1. Ст. 48.

3. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 14.07.2022) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

4. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // Собрание законодательства РФ. 2021. № 27 (ч. II). Ст. 5351.

5. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

6. Национальный стандарт Российской Федерации ГОСТ Р 58771-2019 Менеджмент риска. Технологии оценки риска. Официальное издание. Москва: Стандартинформ, 2020. 90 с.

7. Алексеев С. С. Право на пороге нового тысячелетия: Некоторые тенденции мирового правового развития – надежда и драма современной эпохи. Москва, 2000. С. 25–26.

8. Амелин Р. В. О роли технологического метода в информационном праве // Информационное пространство: обеспечение информационной безопасности и право: сборник научных трудов. 2018. С. 148–155.

9. Бачило И. Л. О методах и методологии в информационном праве // Динамика институтов информационной безопасности. Правовые проблемы: сборник научных трудов / отв. ред. Т. А. Полякова, В. Б. Наумов, Э. В. Талапина. 2018. С. 20–28.

10. В ОДКБ заявили о взломе сайта организации // RT на русском. URL: https://russian.rt.com/tag/kiber-ataka (дата обращения: 15.09.2022).

11. Воеводин В. А., Ковалев И. С., Фоломеев Л. А. Страхование информационных рисков как экономический инструмент обеспечения информационной безопасности // Norwegian Journal of Development of the International Science. 2020. № 41-2. Pp. 14–17.

12. Камалова Г. Г. К вопросу о методологических основах формирования информационного права Российской Федерации // Информационное право. 2009. № 2. С. 38–43.

13. Камалова Г. Г. Цензура в цифровую эпоху: вопросы правового обеспечения национальной безопасности // Информационное право. 2021. № 2. С. 32–36.

14. Кибер-Инго. Страхование информационных рисков для юридических лиц // Ингосстрах. URL: https://new.ingos.ru/corporate/cyber-ingo (дата обращения: 16.09.2022).

15. Остроушко А. В. Правовые риски в информационной сфере // Актуальные вопросы публичного права. 2014. № 5 (29). С. 62–73.

16. Право и иные регуляторы в развитии цифровых технологий / А. В. Минбалеев, А. В. Мартынов, Г. Г. Камалова, С. Г. Чубукова, О. В. Сушкова, М. В. Бундин, В. М. Жернова, К. Ю. Никольская, И. С. Бойченко. Саратов, 2022. 338 с.

17. Рыбаков О. Ю., Тихонова С. В. Информационные риски и эффективность правовой политики // Журнал российского права. 2016. № 3. С. 88–95.

18. Тихомиров Ю. А. Прогнозы и риски в правовой сфере // Журнал российского права. 2014. № 3. С. 16.

19. Формирование системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе / Т. А. Полякова, А. В. Минбалеев, А. А. Чеботарева, В. Б. Наумов, И. С. Бойченко. Саратов, 2022. 332 с.

О. А. Кислый,
кандидат педагогических наук,
доцент кафедры правового обеспечения государственной
и муниципальной службы,
Институт государственной службы и управления Российской академии
народного хозяйства и государственной службы
при Президенте Российской Федерации
М. А. Исаева,
инспектор отделения по координации деятельности отдела по контролю
в сфере миграции Управления по вопросам миграции Главного управления
Министерства внутренних дел России по г. Москве

НЕКОТОРЫЕ ВОПРОСЫ РАССМОТРЕНИЯ ИНСТИТУТА ЭЛЕКТРОННЫХ ВИЗ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Российская Федерация окутана процессами международной миграции с 90-х гг. прошлого века. Предпосылками этих процессов стали эволюция деятельности внешней экономики, всемирных деловых контактов, «устремление» национального хозяйства в сторону иностранных инвестиций, снятие многих административных преград въезда и пребывания иностранных граждан и лиц без гражданства в Российской Федерации и выездом за рубеж своих граждан. Очевидно и доказано, что право (законодательство) «аутентично» и индивидуально: имеет собственную «природу» и закономерности своих «метаморфоз», но при этом находится в зависимости от окружающей среды социума. А потому содержание, сфера распространения, «темперамент» правового регулирования – это все поддается «огранке», претерпевая изменения в среде действия права. В связи с чем поговорим об институте электронных виз в Российской Федерации.

Ключевые слова: иностранные граждане, миграция, подразделения по вопросам миграции, миграционная политика, цифровизация, электронная виза, международные процессы

SOME ISSUES CONSIDERED BY THE INSTITUTE OF ELECTRONIC VISAS IN THE RUSSIAN FEDERATION

Abstract. The Russian Federation has been “shrouded” by the processes of international migration since the 90s of the last century. The prerequisites for these