

Научная статья
УДК/UDC 342
DOI: 10.21779/2224-0241-2024-49-1-41-49

Некоторые проблемы совершенствования нормативной правовой регламентации вопросов информационной безопасности в Российской Федерации

С.М. Ильясов

Дагестанский государственный университет, г. Махачкала, Российская Федерация, *kafedraconst@mail.ru*

Аннотация. В статье рассматриваются некоторые проблемы нормативной правовой регламентации обеспечения информационной безопасности в России. Определены отдельные пробелы в правовом регулировании данной сферы, вызванные отставанием правовой регламентации от происходящих в реальной жизни изменений в информационной сфере. Проведен анализ отдельных нормативных правовых актов в сфере правового регулирования информационной безопасности, сделана попытка их группирования по уровням и содержанию. Отмечается, что принятие унифицированного конвенционального международного правового акта способствовало бы формированию у государств единого подхода к предотвращению конфликтов в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий на основе равноправного сотрудничества, а также предоставило бы возможность использовать во внутригосударственном законодательстве единую терминологическую базу. При рассмотрении внутригосударственного уровня делается вывод о том, что нормативное правовое регулирование информационной безопасности в Российском государстве отстает от развития информационно-коммуникационных технологий, что влечет за собой возникновение угроз информационной безопасности государства. Для их устранения необходимо создать целостную нормативную правовую базу, основанную на соблюдении баланса между информационной открытостью и обеспечением информационной безопасности.

Ключевые слова: нормативное правовое регулирование, информационно-коммуникационные технологии, информационная безопасность, киберугрозы, информационная среда

Для цитирования: Ильясов С.М. Некоторые проблемы совершенствования нормативно-правовой регламентации вопросов информационной безопасности в Российской Федерации // Юридический вестник ДГУ. 2024. Т. 49, № 1 (69). С. 41–49. DOI: 10.21779/2224-0241-2024-49-1-41-49

Original article

Some problems of improving the legal regulation of information security issues in the Russian Federation

Said M. Ilyasov

Dagestan State University, Makhachkala, Russian Federation, *kafedraconst@mail.ru*

Abstract. Some problems of regulatory legal regulation of information security in Russia are discussed in the article. Certain gaps in the legal regulation of this sphere have been identified, caused by the lag in legal regulation from the changes in the information sphere taking place in real life. The analysis of individual normative legal acts in the field of legal regulation of information security is carried out, an attempt is made to group them by levels and content. It is noted that the adoption of a unified conventional international legal act would contribute to the formation of a unified approach among States to conflict prevention in the field of information and communication technologies and information and communication technologies themselves on the basis of equal cooperation, and would also provide an opportunity to use a single terminology base in domestic legislation. When considering the domestic level, it is concluded that the normative legal regulation of information security in the Russian state lags behind the development of information and communication technologies, which entails the emergence of threats to the information security of the state. To eliminate them, it is necessary to create a holistic regulatory framework based on maintaining a balance between information openness and ensuring information security.

Keywords: regulatory legal regulation, information and communication technologies, information security, cyber threats, information environment

For citation: Ilyasov S.M. Some problems of improving the legal regulation of information security issues in the Russian Federation. *Yuridicheskii vestnik DGU = Law Herald of DSU*, 2024, vol. 49, no. 1 (69), pp. 41–49. DOI: 10.21779/2224-0241-2024-49-1-41-49 (In Russ.).

Стремительное развитие компьютеризации национальной безопасности в информационной обусловило необходимость создания системы сфере, поскольку влияние информационно-

коммуникационных технологий (ИКТ) усиливается и затрагивает наиболее значимые сферы деятельности Российского государства, граждан и организаций. В настоящее время большое влияние на развитие российской экономики оказывает такой элемент кибернетического пространства (киберпространства), как информационно-коммуникационная сеть Интернет, повсеместно внедренная в сектор (процесс) государственного управления и являющаяся одним из ключевых факторов построения эффективного и социально ответственного демократического государства в XXI веке. Соответственно возрастает и необходимость переосмысления и совершенствования нормативно-правового регулирования этой сферы деятельности, включая ее конституционную составляющую.

Кроме того, поскольку развитие науки и техники продолжается, обращение к исследованию конституционно-правовых основ информационной безопасности в России обусловлено и существующими пробелами в правовом регулировании данной сферы, вызванными отставанием правовой регламентации от происходящих в реальной жизни изменений. Причем по некоторым направлениям это отставание выражается даже в отсутствии единых подходов к правовому пониманию ключевых категорий. Так, все еще не находят конкретного юридического закрепления такие дефиниции, как «киберпространство», «киберугрозы», единое толкование которых непосредственно влияет на реализацию информационной безопасности в стране, усложняет процесс противодействия киберугрозам и киберпреступности. Среди угроз информационной безопасности России, занимающих ведущее место и наносящих значительный урон, следует назвать угрозы, связанные с передачей, обработкой, хранением, защитой информации, приводящей к ее утечке в различных сферах деятельности государства. В свою очередь, недостаточное организационно-правовое обеспечение усугубляет развитие угроз, исходящих из информационного пространства, что увеличивает масштабы ущерба от их воздействия на системы обеспечения информационной безопасности.

Особого внимания заслуживают проблемы нормативного регулирования вопросов, связанных с применением искусственного интеллекта, поскольку, с одной стороны, его разработка обладает огромным потенциалом в противодействии информационной безопасности на различных уровнях, а с другой - искусственный интеллект инициирует появление новых видов угроз, связанных с его применением (например, дип-фейков). Здесь можно согласиться с А.В. Минбалеевым, который отмечает, что исследования «подтверждают важность развития правовых механизмов внедрения и использования искусственного интеллекта и других цифровых технологий в систему обеспечения кибербезопасности в России» [1, с. 155].

Однако само определение «информационная безопасность» можно толковать как более широкое по отношению к термину «кибербезопасность», не являющемуся самостоятельной дефиницией и не используемому в российских законодательных актах официально. При этом следует отметить, что в большинстве зарубежных стран она выделена в самостоятельную дефиницию. Также важно иметь в виду, что регулирование киберпространства исключительно в территориальных границах стран невозможно в силу его трансграничности [2, с. 80]. Поэтому в процессе правовой регламентации неизбежны процессы взаимовлияния.

Таким образом, следует констатировать, что активное развитие IT-сферы и, соответственно, увеличение киберугроз опережает нормативное правовое регулирование киберпространства и, соответственно, информационной безопасности, которое не достигает необходимого уровня, в том числе из-за отсутствия легальных определений и единого понимания терминологической базы среди ученых и практиков, что в целом существенно снижает информационную безопасность страны.

Поэтому в условиях повсеместной цифровизации крайне актуальной становится не только проблема противодействия угрозам в информационном пространстве, поскольку угрозы, возникающие в нем, оказывают негативное влияние на национальную безопасность Российского государства в целом, но и обеспечение информационной безопасности как одной из основных ее составляющих, в частности. Это подтверждается Стратегией национальной безопасности Российской Федерации, в соответствии с которой рост числа преступлений, совершаемых с использованием информационно-коммуникационных технологий, рассматривается как одна из угроз национальной безопасности, а их предупреждение, выявление, пресечение является стратегическим национальным приоритетом (п. 42)¹.

Проблемам правового обеспечения информационной безопасности и противодействия угрозам в киберпространстве посвящены научные труды многих отечественных и зарубежных ученых. Наиболее существенный вклад в развитие научных представлений в этой сфере внесли: С.А. Авакьян, И.Л. Бачило, Н.С. Бондарь, Е.О.Елизарова, М.В. Иванов, М.С. Кобышева, Н.Н. Ковалева, В.Н. Лопатин, А.С. Макарян, М.М. Путято, А.А. Снытникови др., работы которых посвящены развитию законодательной базы и совершенствованию правоприменительной практики в области информации, информационных технологий и защиты информации.

В связи с этим обращение к тематике исследования правовых основ информационной безопасности

¹ О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 2 июля 2021 г. № 400. URL: http://www.consultant.ru/document/cons_doc_LAW_389_271/ (дата обращения: 05.03.2022).

является актуальным, поскольку современное развитие информационных цифровых сред и информационного пространства обуславливает необходимость обеспечения информационной безопасности России, прежде всего, посредством его своевременного нормативного правового регулирования.

Как известно, текущая система нормативных правовых актов, регламентирующих сферу противодействия угрозам в киберпространстве и обеспечения информационной безопасности в Российской Федерации, включает международный и внутригосударственный уровни.

На международном уровне такими актами являются правовые акты, систему которых в сфере информационной безопасности составляют документы Генеральной Ассамблеи ООН, различные двусторонние, многосторонние и межправительственные соглашения государств, принятые на высшем уровне, а также заключенные в рамках различных международных организаций (БРИКС, ШОС, ОДКБ и др.). Кроме того, применительно к организациям действуют специальные отраслевые международные стандарты, примером могут служить стандарты серии ISO¹, разработанные с целью создания системы управления информационной безопасностью, защиты информационных ресурсов и услуг.

В свое время впервые на проблему роста киберугроз по инициативе Российской Федерации обратила внимание ООН, принявшая Резолюцию о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности², ставшую импульсом к формированию современной системы регулирования вопросов международной информационной безопасности в рамках ООН, развитию российских инициатив и международного сотрудничества в этой сфере. Позднее было принято еще несколько резолюций³, направлен-

ных на необходимость для государств выполнять свои международные обязательства и в сфере использования информационно-коммуникационных технологий.

Т.Ю. Сидорова, проводя корреляцию положений резолюции с принципами Устава ООН, отмечает, что «в резолюции в полной мере нашли свое отражение принцип суверенного равенства государств, невмешательства во внутренние дела, сотрудничества, добросовестного исполнения обязательств ..., положение о защите прав человека, в частности неприкосновенности личной жизни. Вместе с тем в резолюции есть два момента, которые выходят за рамки исключительно межгосударственных обязательств. Первый момент связан с п. 1.9 резолюции о каналах поставок, обеспечивающих безопасность продуктов ИКТ, а второй – это п. 1.13, призывающий сотрудничать государства, частный сектор и гражданское общество в области производства и сбыта информационных товаров и информационно-технических услуг» [3, с. 105].

Однако в основном документы ООН отличаются своей мягкостью. В них нет провозглашения каких-либо принципов или норм, конкретизирующих правила поведения государств при возникновении угроз в киберпространстве, а также применения мер противодействия им. Из-за отсутствия общепризнанных международных правовых норм, касающихся кибербезопасности в информационной сфере, оценка применимости действующего законодательства к данной сфере осуществляется региональными организациями (например, НАТО), чьи программные документы («Таллинское руководство по применению юридических норм международного права к военным действиям в киберпространстве» (Tallinn manual on the international law applicable to cyber warfare)) содержат рекомендации к применению военных действий в качестве ответа на киберугрозы в киберпространстве. Как отмечает С. Гриняев, «ключевым тезисом Руководства является тезис о том, что применение средств информационного воздействия есть применение силы, соответствующее таковому понятию в Уставе ООН и общепринятом международном праве» [4, с. 18].

В целом следует констатировать, что на международном уровне отсутствует единый нормативный правовой акт, позволяющий обеспечить информационную безопасность государств, хотя проект Конвенции об обеспечении международной информационной безопасности разрабатывается на базе ООН, начиная с 2011 года⁴. Представляется,

¹ ISO/IEC 27001 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования». Доступ из справ.-правовой системы «КонсультантПлюс».

² Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН 53/70 от 04.01.1999 // Организация Объединенных Наций. Официальный сайт. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения: 10.12.2023).

³ Резолюция Генеральной Ассамблеи ООН 73/27 от 5 декабря 2018 года «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // Организация Объединенных Наций. Официальный сайт. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27&Lang=R (дата обращения: 10.12.2023); Резолюция Генеральной Ассамблеи ООН 73/264 от 22 декабря 2018 года «Advancing responsible State behaviour in cyberspace in the context of international security» // Организация Объединенных Наций. Официальный сайт. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/264&Lang=R (дата обращения: 10.12.2023).

⁴ Конвенция об обеспечении международной информационной безопасности (концепция). URL: http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOA_AcATW2Rwa3yNK1bNAW19.pdf (дата обращения: 10.12.2023).

что это обусловлено неоднородностью развития внутригосударственного правового регулирования вопросов информационной безопасности в разных странах: если в одних государствах (таких как США, Великобритания, Польша и др.) этому направлению уделяется значительное внимание, то в других (некоторые страны Азиатского региона и Центральной Африки) оно развито слабо. Такая неоднородность обусловлена различной интенсивностью внешнего информационного воздействия, сказывающейся на последующем создании национальных систем информационной защиты [5, с. 5], а также тенденциями правового регулирования распространения информации в различных странах и регионах мира, отличающихся по географическим, социальным, политическим и религиозным признакам¹. Отсутствие единого понимания самого информационного пространства также оказывает существенное влияние на выстраивание межгосударственных взаимоотношений. Как верно говорит Р.П. Борисов, «отсутствие общего подхода в значительной степени осложняет взаимодействие государств в контексте обеспечения безопасности на международном уровне, так как разные подходы к определению безопасности влекут за собой также постановку разных задач и целей в этой сфере» [6, с. 95].

В этой связи принятие унифицированного международного правового акта на уровне ООН способствовало бы формированию у государств единого подхода к предотвращению конфликтов в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий на основе равноправного сотрудничества, а также предоставило бы возможность использовать во внутригосударственном законодательстве единую терминологическую базу. Здесь следует отметить, что Россия выступает инициатором многих предложений по совершенствованию международной информационной безопасности в рамках ООН, например, по существенному расширению спектра угроз информационной безопасности, по созданию на платформе ООН международно-правовых механизмов, направленных на предотвращение и урегулирование межгосударственных конфликтов в информационном пространстве, организацию межведомственного взаимодействия².

Однако в связи с существующей в настоящее время общественно-политической обстановкой

происходит трансформация международной информационной безопасности, связанная «с переговорным процессом в рамках ООН, который в условиях нарастания политического антагонизма между ключевыми субъектами диалога становится все более политизированным и начинает испытывать некоторые трудности» [7, с. 170].

Представляется, что конфронтации государств, возникающие из-за происходящих политических процессов, не должны затруднять переговорный процесс, осуществляемый под эгидой ООН. Выходом из сложившейся ситуации может стать взаимодействие стран на основе заключения двусторонних договоров и соглашений.

Внутригосударственный (национальный) уровень нормативно-правового регулирования включает нормативные правовые акты федерального, регионального, муниципального значения. Считаем также, что законодательство Российской Федерации в сфере информационной безопасности можно условно разделить по содержанию на нормативные правовые акты общего и специального правового регулирования.

На федеральном уровне к первой группе, прежде всего, следует отнести Конституцию РФ, так как она является базовым основным документом, содержащим положения, формирующие основу правовой защиты информации, и основным источником права в области обеспечения информационной безопасности в России.

Так, Основной закон закрепляет право, направленное на защиту частной жизни (ст. 23), недопущение использования информации о частной жизни лица без его согласия (ст. 24), свободный поиск, получение и распространение информации любым законным способом (ст. 29), право каждого на достоверную информацию о состоянии окружающей среды (ст. 42), а также иные положения, касающиеся обеспечения информационной безопасности. Особое значение имеет статья 15 Конституции, регламентирующая порядок применения международно-правовых договоров.

К этой же группе следует отнести кодифицированные нормативные правовые акты, положения которых направлены на регулирование вопросов, связанных с охраной нематериальных благ (ст. 150 ГК), защитой чести, достоинства и деловой репутации от недостоверной информации (ст. 152 ГК), защитой информации ограниченного доступа (например, тайны усыновления) (ст. 273 ГПК), основаниями применения ограничений неприкосновенности частной жизни (ст. 13 УПК), пресечением неправомерных действий в сфере информационной безопасности (ст. 159.3 УК РФ), компьютерной информации (ст. 159.6 УК РФ), применением уголовной ответственности за неправомерный доступ к охраняемой законом компьютерной информации и т.д. (ст. 272-274 УК РФ).

¹ Отчет о мониторинге правоприменения регулирования информационного пространства в странах мира в 2020 году. URL: <https://rdc.grfc.ru/2021/02/enforcement-of-information-space/?ysclid=lvass0zq5wt69648971> (дата обращения: 10.12.2023).

² Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности: указ Президента РФ от 12 апреля 2021 г. № 213. Доступ из справ.-правовой системы «КонсультантПлюс».

Конкретизация названных выше конституционных положений осуществляется в федеральном законодательстве. Одним из основных нормативных правовых актов, регулирующих отношения, связанные с информационной безопасностью, является Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ. Данный акт содержит несколько положений, включающих информацию о безопасности данных в сети Интернет, в первую очередь, о защите информации от уничтожения, распространения, копирования и т.д. (ч. 4 ст. 6, ч. 1 ст. 16) и реализации права на доступ к ней. Кроме того, Законом определена «ответственность за правонарушения в сфере информации, информационных технологий и защиты информации, а также установлены правила ограничения доступа к информации в сети Интернет, включая распространение информации с нарушением исключительных прав на фильмы, в том числе кинофильмы, телефильмы. Предусмотрен в Законе и порядок ограничения доступа в информационно-коммуникационных сетях (включая Интернет) к информации, распространяемой с нарушением закона, в которой содержатся призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях» [8, с. 44].

Схожие законодательные акты существуют в зарубежных странах, например, в Китае, который в Законе «Об интернет-безопасности» закрепил вопросы обеспечения национальной и сетевой безопасности, защиту национального «киберсуверенитета» Китая, прав и интересов государства, граждан, юридических лиц и других субъектов публичных правоотношений [9, с. 21].

Начиная с 2010 года, российским законодателем, ориентирующимся на общемировые тенденции развития информационно-телекоммуникационных технологий и информационного пространства, в базовый Закон «Об информации, информационных технологиях и о защите информации» было внесено более 67 поправок. На сегодняшний день также разработан проект закона о внесении изменений в данный нормативный правовой акт, касающихся регулирования обращения с большими пользовательскими данными (big data), представляющими собой совокупность информации из Интернета и иных источников о физических лицах и их поведении (без персональных данных)¹, не позволяющей без использования дополнительной информации или обработки определить конкретное физическое лицо. Однако, несмотря на актуальность проблемы правового регулирования big data, заключающейся

в необходимости не только понимания того, какую информацию следует относить к большим данным, но и возможности разграничения массивов данных, их обработки и анализа, законопроект, позволяющий запретить операторам обрабатывать такие данные для идентификации конкретного физического лица, кроме как по запросам органов власти, осуществляющих оперативно-разыскную деятельность, до сих пор не принят. Вероятно, это сопряжено с оценкой законодателем рисков, связанных с поиском баланса между необходимостью нивелировать угрозы, связанные со сбором, хранением, обработкой и передачей прав на большие данные, и необходимостью избежать чрезмерного регулирования правил доступа и обработки общедоступных данных в целях устранения возможного ущерба инновационной активности.

Официальная позиция на обеспечение национальной безопасности Российской Федерации в информационной сфере закреплена в Доктрине информационной безопасности РФ². Данный нормативный правовой акт развивает положения Стратегии национальной безопасности в информационной сфере и служит основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

Важная роль в нормативном правовом регулировании вопросов информационной безопасности отводится, согласно конституционным положениям ст. 80, Президенту РФ, выступающему инициатором последующей разработки правовых механизмов обеспечения информационной безопасности на всех уровнях государственной власти. В частности, им утверждены Основы государственной политики Российской Федерации в области международной информационной безопасности³.

Стратегия развития информационного общества в РФ⁴ предусматривает национальные стратегические направления развития информационного пространства, учитывающего потребности общества в сфере получения качественных и достоверных сведений, развитие информационной инфраструктуры, применение информационных техноло-

¹ О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»: проект Федерального закона № 571124-7. Доступ из справ.-правовой системы «КонсультантПлюс».

² Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 г. № 646. Доступ из справ.-правовой системы «КонсультантПлюс».

³ Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности: Указ Президента Российской Федерации от 12.04.2021 № 213. Доступ из справ.-правовой системы «КонсультантПлюс».

⁴ О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09.05.2017 № 203. Доступ из справ.-правовой системы «КонсультантПлюс».

гий, таких как платформы онлайн-образования, онлайн-медицины, единая инфраструктура электронного правительства, Национальная электронная библиотека и, соответственно, противодействия угрозам в данной сфере.

Существенную группу нормативных правовых актов в сфере правового регулирования информационно-безопасности России составляют акты Правительства РФ, определяющие направления деятельности в данной сфере. Так, согласно Концепции технологического развития на период до 2030 года¹ Правительством определены основные вызовы, принципы и цели технологического развития на период до 2030 года, основные направления «для разработки (корректировки) и реализации государственных программ (подпрограмм) Российской Федерации, региональных программ (подпрограмм) субъектов Российской Федерации, схем территориального планирования Российской Федерации, а также плановых и программно-целевых документов государственных корпораций, государственных компаний и акционерных обществ с государственным участием». В соответствии с Концепцией информационной безопасности в сфере здравоохранения², направленной на расширение области применения информационных технологий в сфере здравоохранения, определяются цели и задачи, позволяющие обеспечить построение единой системы обеспечения информационной безопасности в сфере здравоохранения, защиту информации в информационных системах в области здравоохранения и т.д.

Ко второй группе нормативных правовых актов специального правового регулирования следует отнести законодательство, регламентирующее обеспечение особых правовых режимов в информационной сфере.

Расширение спектра киберугроз обусловило необходимость обеспечения сохранности персональных данных и защиты частной жизни. Особый правовой режим установлен Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»³, предусматривающим порядок получения и обработки персональных данных и биометрических данных физических лиц.

¹ Об утверждении Концепции технологического развития на период до 2030 года: распоряжение Правительства РФ от 20.05.2023 № 1315-р. Доступ из справ.-правовой системы «КонсультантПлюс».

² Концепция информационной безопасности в сфере здравоохранения: утв. протоколом президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 10.03.2022 № 7. Доступ из справ.-правовой системы «КонсультантПлюс».

³ О персональных данных: федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023). Доступ из справ.-правовой системы «КонсультантПлюс».

Обеспечение правового режима государственной тайны в России осуществляется Законом «О государственной тайне»⁴, согласно которому регулируются отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации, в деятельности органов государственной власти и местного самоуправления, а также различных организаций и учреждений.

В настоящее время особое внимание законодателей обращено к проблемам социально-экономического развития страны в рамках цифровой экономики. В связи с этим был принят Закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», которым регулируется «создание правовых условий для ускоренной разработки и внедрения новых продуктов и услуг в сферах применения цифровых инноваций по всем сферам экономики России, в том числе в части развития технологий сетей пятого поколения».

1 января 2021 года вступил в силу Закон «О цифровых финансовых активах», положениями которого предусматривается определение криптовалюты, но запрещается ее использование в России для оплаты товаров и услуг. Также под запрет попадает реклама платежей цифровыми деньгами.

Значимым событием являются разработка и принятие так называемого закона о цифровом рубле⁵, которым были внесены изменения в ряд законодательных актов, регулирующих банковскую деятельность, исполнительное производство, национальную платежную систему, взыскание таможенных платежей, гражданские правоотношения. Прежде всего, усилия законодателя направлены на поддержку российской экономики и ограничение оттока денежных средств в иные иностранные цифровые валюты, повышение доступности, удобства, скорости и безопасности расчетов при применении цифровых технологий. Цифровой рубль является видом безналичных денежных средств и представляет собой уникальный цифровой код, хранящийся в цифровых кошельках на специальной платформе Центрального банка. Благодаря блокчейн-технологии, транзакции с использованием цифровых рублей смогут проводиться даже в условиях временной недоступности интернета (т.н. «холодный кошелек»).

⁴ О государственной тайне: закон РФ от 21.07.1993 № 5485-1 (ред. от 05.12.2022). Доступ из справ.-правовой системы «КонсультантПлюс».

⁵ О внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 24 июля 2023 г. №340-ФЗ; О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации: федеральный закон от 24 июля 2023 г. №339-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Однако на сегодняшний день ни один нормативный правовой акт не содержит легального определения цифрового рубля. В связи с этим представляется, что легальное определение цифрового рубля следует закрепить в Федеральном законе «О национальной платежной системе».

На противодействие угрозам в киберпространстве направлен ряд указов Главы государства. Так, Указом от 6 марта 1997 года № 188¹ был закреплён перечень сведений конфиденциального характера, таких как персональные данные, тайна судопроизводства, коммерческая тайна и т.д., что позволило сформировать основные правила, направленные на защиту интересов в информационной сфере.

К законодательным актам специального правового регулирования, на наш взгляд, стоит отнести и Указ Главы государства «О развитии искусственного интеллекта в РФ»², который определяет вектор развития России в сфере разработки и внедрения в сферы экономики искусственного интеллекта.

Относительно регионального и муниципального уровня правового регулирования следует отметить весьма незначительное их наполнение, обусловленное, рядом факторов, включая остаточный принцип правовой регламентации на региональном и местном уровне и преимущественно федеральный уровень регулирования данной сферы, невысокий уровень цифровых компетенций должностных лиц и пр. При этом следует отметить важность особого внимания со стороны институтов государственной власти регионального уровня и органом местного самоуправления к проблемам кибербезопасности, о чем свидетельствует проблема обеспечения информационной безопасности органов государственной власти субъектов РФ и органов местного самоуправления, проявившаяся с момента усиления кибератак на региональные и местные сайты органов власти, начиная с 2022 года.

Следует отметить, что обеспечение информационной безопасности осложняется недостатком компетентных специалистов на рынке труда, чья востребованность очень высока. Кроме того, еще острее стоит проблема расследования правонарушений. Профессиональное образование

только встает на путь подготовки юристов в IT-сфере.

В заключение следует отметить, что на сегодняшний день вопросам нормативного правового обеспечения информационной безопасности уделяется внимание на всех уровнях государственной власти. Однако развитие информационно-коммуникационных технологий значительно опережает правовое регулирование данной области, что влечет за собой возникновение угроз информационной безопасности Российского государства, для устранения которых необходима целостная нормативная база. В связи с этим необходимо совершенствовать законодательство и своевременно актуализировать принятые нормы. Для этого должны работать компетентные специалисты, способные реализовывать законодательную функцию на стыке двух профессий: юриста и IT-специалиста [10, с.378]. В свою очередь, органы государственной власти всех уровней должны направить свои усилия на разработку нормативной правовой базы, позволяющей применять информационно-коммуникационные технологии и гарантировать суверенитет, безопасность, а также соблюдать нормы о правах личности в информационной сфере, их защите и охране. В частности, целесообразно сосредоточить нормы о защите прав в информационном пространстве в одном законе, например, в Федеральном законе от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации». Важная роль в обеспечении информационной безопасности России отводится определению приоритетных направлений и механизмов реализации государственной политики Российской Федерации в области международной информационной безопасности в целях противодействия основным угрозам в этой области. Международное сотрудничество в сфере информационной безопасности сейчас развивается на двусторонней основе между Россией и другими государствами. Поэтому особенно важно результативно проводить активную работу по принятию международной конвенции по информационной безопасности в рамках ООН. Кроме того, следует изучать опыт зарубежных стран в сфере правового регулирования информационной безопасности с целью выявления новых угроз в информационном пространстве и противодействия им.

¹ Об утверждении Перечня сведений конфиденциального характера: указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015). Доступ из справ.-правовой системы «КонсультантПлюс».

² О развитии искусственного интеллекта в РФ (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»: указ Президента РФ от 10.10.2019 №490. Доступ из справ.-правовой системы «КонсультантПлюс».

Список источников

1. Минбалеев А.В. Проблемы цифрового права : учебное пособие / А.В. Минбалеев. Саратов : Амрит, 2022. 233 с.
2. Кобышева М.С., Иванов М.В., Кобышев К.И. Анализ сферы кибербезопасности в условиях цифровой трансформации экономики Российской Федерации // Цифровая экономика и индустрия 4.0: форсайт Россия: сборник трудов научно-практической конференции с зарубежным участием. Т. 1. Санкт-Петербург, 2020. С. 75-86.
3. Сидорова Т. Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН // Сибирский юридический вестник. 2020. № 3 (90). С. 103-108.
4. Гриняев С. «Таллинское руководство по применению юридических норм международного права к военным действиям в киберпространстве» в оценках западных экспертов // *Обзор.НЦПТИ*. 2013. №3. С. 18-22.
5. Бекмурзаев И. Д., Курбанов А. Х., Хажмурадова С. Д. Международный опыт обеспечения национальной информационной безопасности // Общество, экономика, управление. 2020. Т. 5, № 1. С. 5-11.
6. Борисов Р.П. Различия в терминологических и содержательных подходах субъектов международных отношений в области обеспечения информационной безопасности. Основные направления сотрудничества государств по созданию системы международных отношений в рамках обеспечения информационной безопасности // Юриспруденция в теории и на практике: актуальные вопросы и современные аспекты: сборник статей XV Международной научно-практической конференции. Пенза, 2023. С. 95-99.
7. Себекин С.А. Система международной информационной безопасности в условиях политической турбулентности // Вестник СПбГУ. Международные отношения. 2023. Т. 16, вып. 2.
8. Карихия А. А., Севостьянов В. Л. Информационная безопасность: правовые аспекты // Правовая информатика. 2018. №4.
9. Вологодина Е.С. О некоторых аспектах правового регулирования кибербезопасности в Китайской Народной Республике // Цифровой суверенитет и кибербезопасность: материалы Четвертого международного транспортно-правового форума / под редакцией А.А. Чеботаревой, В.Е. Чеботарева. М., 2022. С. 21-28.
10. Шкодина Е.С., Шиханова Е.Г. Правовое регулирование кибербезопасности: постановка проблемы // Онтологические и социокультурные основания альтернативного проекта глобализации: сборник материалов I международной научной онлайн-конференции. Екатеринбург, 2021. С. 378–381.

References

1. Minbaleev A.V. Problemy tsifrovogo prava : uchebnoe posobie [Problems of digital law : a textbook], A.V. Minbaleev. Saratov : Amirit Publ., 2022, 233 p. (In Russ.).
2. Kobysheva M.S., Ivanov M.V., Kobyshev K.I. Analiz sfery kiberbezopasnosti v usloviyakh tsifrovoi transformatsiii ekonomiki Rossiiskoi Federatsii [Analysis of the sphere of cybersecurity in the conditions of digital transformation of the economy of the Russian Federation], *Tsifrovaya ekonomika i industriya 4.0: foresait Rossiya* [Digital economy and industry 4.0: foresight Russia]: proceedings of the scientific and practical conference with foreign participation. Volume 1. St. Petersburg, 2020, pp. 75-86. (In Russ.).
3. Sidorova T. Yu. Mezhdunarodnaya informatsionnaya bezopasnost': pravovye aspekty i deyatelnost' OON [International information security: legal aspects and activities of the United Nations], *Sibirskii yuridicheskii vestnik* [Siberian Legal Bulletin], 2020, no. 3 (90), pp. 103-108. (In Russ.).
4. Grinyaev S. «Tallinnskoe rukovodstvo po primeneniyu yuridicheskikh norm mezhdunarodnogo prava k voennym deistviyam v kiberprostranstve» v otsenkakh zapadnykh ekspertov ["Tallinn Manual on the application of legal norms of international law to military operations in cyberspace" in the assessments of Western experts], *Obzor.NTsPTI* [Review.NCPTI], 2013, no.3, pp. 18-22. (In Russ.).
5. Bekmurzaev I. D., Kurbanov A. X., Khazhmuradova S. D. Mezhdunarodnyi opyt obespecheniya natsional'noi informatsionnoi bezopasnosti [International experience in ensuring national information security], *Obshchestvo, ekonomika, upravlenie* [Society, economics, management], 2020, vol. 5, no. 1, pp. 5-11. (In Russ.).
6. Borisov R.P. Razlichiya v terminologicheskikh i sodержatel'nykh podkhodakh sub"ektov mezhdunarodnykh otnoshenii v oblasti obespecheniya informatsionnoi bezopasnosti. Osnovnye napravleniya sotrudnichestva gosudarstv po sozdaniyu sistemy mezhdunarodnykh otnoshenii v ramkakh obespecheniya informatsionnoi bezopasnosti [Differences in terminological and substantive approaches of subjects of international relations in the field of information security. The main directions of cooperation between states on the creation of a system of international relations within the framework of ensuring information security], *Yurisprudentsiya v teorii i na praktike: aktual'nye voprosy i sovremennye aspekty* [Jurisprudence in theory and in practice: topical issues and modern aspects]: collection of articles of the XV International Scientific and Practical Conference. Penza, 2023, pp. 95-99. (In Russ.).
7. Sebekin S.A. Sistema mezhdunarodnoi informatsionnoi bezopasnosti v usloviyakh politicheskoi turbulentsi [The system of international information security in the context of political turbulence], *Vestnik SPbGU*.

Mezhdunarodnye otnosheniya [Bulletin of St. Petersburg State University. International relations], 2023, vol. 16, issue 2. (In Russ.).

8. Kartskhiya A. A., Sevost'yanov V. L. Informatsionnaya bezopasnost': pravovye aspekty [Information security: legal aspects], *Pravovaya informatika [Legal informatics]*, 2018, no.4. (In Russ.).

9. Vologdina E.S. O nekotorykh aspektakh pravovogo regulirovaniya kiberbezopasnosti v Kitaiskoi Narodnoi Respublike [On some aspects of legal regulation of cybersecurity in the People's Republic of China], *Tsifrovoy suverenitet i kiberbezopasnost' [Digital sovereignty and cybersecurity]*: materials of the Fourth International Transport and Legal Forum, edited by A.A. Chebotareva, V.E. Chebotareva. Moscow, 2022, pp. 21–28. (In Russ.).

10. Shkodina E.S., Shikhanova E.G. Pravovoe regulirovanie kiberbezopasnosti: postanovka problemy [Legal regulation of cybersecurity: problem statement], *Ontologicheskie i sotsiokul'turnye osnovaniya al'ternativnogo proekta globalizatsii [Ontological and socio-cultural foundations of the alternative project of globalization]*: a collection of materials of the I international scientific online conference. Yekaterinburg, 2021, pp. 378–381. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Ильясов Санд Миравович, аспирант кафедры конституционного и международного права юридического института Дагестанского государственного университета, г. Махачкала, Российская Федерация. E-mail: kafedraconst@mail.ru

Поступила в редакцию 29.02.2024 г.; одобрена после рецензирования 03.03.2024 г.; принята к публикации 05.03.2024 г.

INFORMATION ABOUT THE AUTHOR

Ilyasov Said Miravovich, postgraduate student of the Department of Constitutional and International Law of the Law Institute of Dagestan State University, Makhachkala, Russian Federation. E-mail: kafedraconst@mail.ru

Received 29.02.2024; approved after reviewing 03.03.2024; accepted for publication 05.03.2024