Научная статья
УДК 349
DOI 10.33184/pravgos-2022.2.12

ПОЛЯКОВА Татьяна Анатольевна[1], **КАМАЛОВА Гульфия Гафиятовна**[2]
[1]Институт государства и права РАН, Москва, Россия, Polyakova_ta@mail.ru
[2]Удмуртский государственный университет, Ижевск, Россия, gulfia.kamalova@gmail.com

НОВЫЕ ВЕКТОРЫ РАЗВИТИЯ СИСТЕМЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОДНОГО ИЗ ПРИОРИТЕТОВ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ (К 30-ЛЕТИЮ ПРИНЯТИЯ ЗАКОНА РОССИЙСКОЙ ФЕДЕРАЦИИ «О БЕЗОПАСНОСТИ»)

Аннотация. Статья посвящена актуальным вопросам развития российского законодательства об информационной безопасности в целях обеспечения национальной безопасности Российской Федерации. *Цель:* научное осмысление динамики и приоритетных векторов правового регулирования информационной безопасности в современных условиях цифровизации и геополитических рисков. *Методы:* исследование выполнено на основе применения системного подхода и комплекса общенаучных и специальных правовых методов. *Результаты:* авторы обосновывают необходимость разработки и принятия в России специального федерального закона, направленного на обеспечение информационной безопасности в условиях деструктивного воздействия западных государств на информационное пространство в целях дестабилизации геополитической обстановки. В фокусе внимания также развитие ключевых направлений правового обеспечения информационной безопасности за прошедшие тридцать лет с момента принятия Закона РФ «О безопасности». Среди наиболее проблемных вопросов, требующих организационно-правовых решений для обеспечения информационной безопасности, в настоящее время особенно выделяются: защита информационных прав и свобод гражданина, обеспечение достоверности общественно значимой информации и противодействие распространению фейковой информации, защита русского языка и культуры, усиление правовых требований к защите конфиденциальности цифровых данных, охрана цифрового суверенитета, противодействие кибератакам и киберпреступности, цифровому давлению глобальных IT-корпораций и др.

Ключевые слова: национальная безопасность, правовое обеспечение, информационная безопасность, цифровая эпоха, система информационного права, правовые риски, цифровой суверенитет, технологический суверенитет

Финансирование. Статья написана в рамках Государственного задания № 0136-2021-0042 «Правовое регулирование цифровой экономики, искусственного интеллекта, информационной безопасности».

Для цитирования: Полякова Т.А. Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов национальной безопасности (к 30-летию принятия Закона Российской Федерации «О безопасности») / Т.А. Полякова, Г.Г. Камалова // Правовое государство: теория и практика. – 2022. – № 2. – С. 112–121. DOI 10.33184/pravgos-2022.2.12.

Original article

POLYAKOVA Tatiana Anatolievna[1], **KAMALOVA Gulfiya Gafiyatovna**[2]
[1]Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia, Polyakova_ta@mail.ru
[2]Udmurt State University, Izhevsk, Russia, gulfia.kamalova@gmail.com

NEW VECTORS FOR DEVELOPMENT OF THE SYSTEM OF LEGAL SUPPORT OF INFORMATION SECURITY AS ONE OF THE PRIORITIES OF NATIONAL SECURITY (TO THE 30TH ANNIVERSARY OF THE ADOPTION OF THE LAW OF THE RUSSIAN FEDERATION «ON SECURITY»)

Abstract. The article is devoted to topical issues of development of legislation on information security in the context of ensuring the national security of the Russian Federation. The *purpose* of the study is to scientifically comprehend the dynamics and priority vectors of legal regulation of information security in the current conditions of digitalization and geopolitical risks. *Methods:* the study is carried out on the basis of a systematic approach and a complex of general scientific and special legal methods. *Results:* the authors justify the need to develop and adopt a special federal law in Russia, aimed at ensuring information security in the context of the destructive influence of western states on the information space in order to destabilize the geopolitical situation. The authors' attention is also focused on the development of key areas of legal support of information security for the past thirty years since the adoption of the Law of the Russian Federation «On Security». The most problematic issues requiring organizational and legal solutions to ensure information security currently include the protection of information rights and freedoms of citizens, ensuring the reliability of socially significant information and counteracting the dissemination of fake information, protecting the Russian language and culture, strengthening legal requirements to protect the confidentiality of digital data, protecting digital sovereignty, counteracting cyberattacks and cybercrime, digital pressure of global IT-corporations and others.

Keywords: national security, legal support, information security, digital age, information law system, legal risks, digital sovereignty, technological sovereignty

Financing. The article is written within the framework of State Task No. 0136-2021-0042 «Legal regulation of digital economy, artificial intelligence, information security».

For citation: Polyakova T.A., Kamalova G.G. New vectors for development of the system of legal support of information security as one of the priorities of national security (to the 30th anniversary of the adoption of the law of the Russian Federation «On Security»). *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice,* 2022, no. 2, pp. 112-121. DOI 10.33184/pravgos-2022.2.12 (In Russian).

Введение. Обеспечение национальной безопасности посредством охраны и защиты прав, свобод и законных интересов граждан, различных социальных групп и общества является стратегической, приоритетной задачей любого государства. Несомненно, это детерминирует формирование государственной политики в публично-правовой сфере, трансформацию правовой системы, включая систему правового регулирования отношений, связанных с обеспечением информационной безопасности, развитие ее принципов, категориально-понятийного аппарата и институционализации, вопросов ответственности.

В современной России первым законодательным актом, направленным на решение

задач правового обеспечения национальной безопасности, стал Закон РФ 1992 г. «О безопасности»[1], что позволяет сегодня констатировать преодоление тридцатилетнего рубежа развития правовых средств регулирования общественных отношений в данной сфере. В связи с этим нельзя не отметить роль указанного закона не только в становлении российского законодательства о безопасности, но и, по сути, в закреплении организационно-правовых основ безопасности, ее системы и порядка обеспечения, а также функциональных и методологических особенностей. Результаты научных исследований свидетельствуют о том, что Законом РФ «О безопасности» были созданы базовые законодательные основания для теоретических исследований правоотношений и совершенствования нормативно-правовой основы обеспечения национальной безопасности, а в дальнейшем – информационной безопасности как одного из ключевых направлений. Не останавливаясь в рамках данной статьи подробно на положениях указанного закона, важным представляется обратить внимание на то, что в нем были закреплены принципы обеспечения безопасности, такие как законность, баланс жизненно важных интересов личности, общества и государства, взаимная ответственность субъектов, интеграция с международными системами безопасности.

Однако в 2010 г. в связи с определением в условиях XXI в. новых стратегических задач был принят новый Федеральный закон «О безопасности»[2], в котором, безусловно, нашло отражение изменение официальных взглядов на обеспечение национальной безопасности под воздействием новых вызовов и угроз, а также развитие теоретических правовых концепций, связанных с безопасностью личности, общества и государства. Так, согласно ст. 4 данного федерального закона государственная политика в области обеспечения национальной безопасности охватывает взаимосвязанный массив политических, социально-экономических, организационно-правовых, информационных, военных, специальных и иных мер, что определяет комплексный характер регулирования данной сферы.

Современное состояние законодательства в сфере обеспечения информационной безопасности. Следует признать, что за прошедшие с 1992 г. три десятилетия наблюдается значительный прогресс в создании и совершенствовании правовых механизмов обеспечения как национальной безопасности в целом, так и отдельных ее направлений. В настоящее время действует целый ряд федеральных законов, регулирующих совокупность взаимосвязанных общественных отношений, включая вопросы обеспечения пожарной, промышленной, биологической, радиационной, транспортной и пищевой безопасности, безопасности дорожного движения и др., а также безопасности отдельных объектов инфраструктуры Российской Федерации и дружественных государств, в том числе объектов топливно-энергетического, оборонно-промышленного комплексов и космической отрасли. Это позволяет констатировать существенное расширение рамок и векторов обеспечения национальной безопасности в российском законодательстве. Одновременно обращает на себя внимание ситуация, связанная с отсутствием в системе правового регулирования в области безопасности специального федерального закона, направленного на обеспечение информационной безопасности, несмотря на различные дискуссионные предложения, обосновывающие необходимость его принятия. Такой позиции придерживаются и авторы настоящей статьи.

В условиях дальнейшего развития информационного общества и цифровизации всех сфер решение задач обеспечения национальной безопасности требует разработки теоретико-методологических вопросов информационной безопасности, которые справедливо определены как приоритетные в целях решения стратегических задач Рос-

[1] О безопасности : закон РФ от 05.03.1992 № 2446-1 (ред. от 26.06.2008) // Ведомости СНД и ВС РФ. 1992. № 15, ст. 769.

[2] О безопасности : федер. закон от 28.12.2010 № 390-ФЗ // Собрание законодательства РФ. 2011. № 1, ст. 2.

сийской Федерации[1]. Однако по прошествии времени генезис государственной политики и выделение приоритетов в этой области показывают переход не только от концептуальных документов к стратегическим, утверждаемым указами Президента РФ, то есть приобретающим нормативно-правовой характер, но также к основам стратегического планирования в области национальной безопасности[2]. В этой связи представляется, что в рамках данной статьи нельзя обойти вниманием развитие системы документов стратегического планирования в области информационной безопасности, несомненно связанных с общей системой правового обеспечения национальной безопасности.

Полагаем, что определенной точкой бифуркации можно считать утверждение Президентом РФ 2 июля 2021 г. Стратегии национальной безопасности РФ. Следует отметить, что в данном новом документе стратегического планирования проблемам информационной безопасности впервые посвящен целый раздел, в котором обращается внимание на повышение угроз безопасности граждан, общества и государства, в том числе расширение применения цифровых технологий для вмешательства во внутренние дела государства и подрыва его суверенитета (включая информационный, цифровой, сетевой, технологический и др.).

Сегодня государственную правовую политику России в области информационной безопасности отражает Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ в декабре 2016 г., которая, на наш взгляд, с учетом новой Стратегии национальной безопасности требует существенной корректировки. Следует отметить, что выделение обеспечения информационной безопасности в качестве стратегического приоритета связано с развитием российского информационного пространства, укреплением национальной информационной инфраструктуры и одновременно существующими проблемами безопасности. Вместе с тем, как было отмечено ранее, в российском законодательстве отсутствует специальный федеральный закон, регулирующий сферу обеспечения информационной безопасности, и нормы, связанные с этими вопросами, сосредоточены в основном в общем акте, направленном на регламентацию информационной сферы в целом[3], что, как представляется, не в полной мере отвечает новым вызовам, угрозам и рискам современного этапа развития общественных отношений. По сути, единственным законодательным актом, напрямую связанным с информационной безопасностью, является Федеральный закон, направленный на обеспечение безопасности критической информационной инфраструктуры России[4].

Кроме того, следует отметить, что отдельные нормы в рассматриваемой сфере рассредоточены по значительному числу нормативных правовых актов. Исследование

[1] О Стратегии национальной безопасности Российской Федерации : указ Президента РФ от 02.07.2021 № 400 // Собрание законодательства РФ. 2021. № 27 (ч. II), ст. 5351 ; Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50, ст. 7074 ; О Стратегии научно-технологического развития Российской Федерации : указ Президента РФ от 01.12.2016 № 642 // Собрание законодательства РФ. 2016. № 49, ст. 6887 ; О развитии искусственного интеллекта в Российской Федерации : указ Президента РФ от 10.10.2019 № 490 // Собрание законодательства РФ. 2019. № 41, ст. 5700 ; О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента РФ от 09.05.2017 № 203 // Собрание законодательства РФ. 2017. № 20, ст. 2901 и др.

[2] Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности : указ Президента РФ от 12.04.2021 № 213 // Собрание законодательства РФ. 2021. № 16 (ч. 1), ст. 2746.

[3] Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (ч. 1), ст. 3448.

[4] О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26.07.2017 № 187-ФЗ // Собрание законодательства РФ. 2017. № 31 (ч. 1), ст. 4736.

позволяет утверждать, что отмеченные тенденции, с одной стороны, свидетельствуют о необходимости специального законодательного регулирования в области информационной безопасности Российской Федерации, с другой стороны, в свете исторической и перспективной динамики развития ИКТ-среды и обеспечения ее безопасности подтверждают потребность в научном переосмыслении роли и места правового обеспечения информационной безопасности в системе национальной безопасности, а также в правовой системе.

Не останавливаясь в данной статье подробно на дискуссии о проблемах дефинирования понятия «информационная безопасность», нельзя не отметить, что оно имеет системообразующий характер, определяющий саму возможность жизни и функционирования любого субъекта. Неслучайно вопросы правового обеспечения информационной безопасности занимают одно из ключевых мест в системе информационного права и совокупность правовых норм и доктринальных положений традиционно характеризуется как подотрасль этой комплексной отрасли права [1]. Вместе с тем сегодня роль правовых вопросов информационной безопасности является ключевой, стала приоритетом в системе правового регулирования информационной сферы, буквально пронизывая ее. Полагаем, что это является еще одним подтверждением неразрывной связи информационного права и правового обеспечения информационной безопасности, а также ставит под сомнение вопрос о том, что правовое обеспечение информационной безопасности остается лишь подотраслью в системе информационного права, учитывая ее значение в системе права в условиях ее трансформации.

Приоритеты и векторы развития правового регулирования в сфере информационной безопасности. Обратившись к предметной сфере регулирования, следует отметить рост информационных угроз и рисков, а также вовлечение в эту сферу разнообразных проблем, детерминированных вызовами современности. В прогнозах по результатам экспертного исследования на 2022 г. (сделанных до событий февраля – марта этого года) отмечались следующие актуальные тренды развития киберугроз и средств обеспечения информационной безопасности: рост использования программ-вымогателей, шифровальщиков и иных способов кибермошенничества, совершенствование технического регулирования и усиление требований регуляторов, дальнейшее развитие сертификации средств информационной безопасности и необходимости импортозамещения. Кроме того, важное место в прогнозах заняли вопросы идентификации, аутентификации и управления доступом, а также сетевого доступа с «нулевым доверием», еще более актуализировавшиеся в условиях распространения коронавирусной инфекции COVID-19 и широкомасштабных западных санкций[1].

При этом цифровизация, усугубленная общемировым кризисом и начавшимися глобальными тектоническими процессами, в настоящее время усиливает не только роль достоверной информации и знаний, активизирует динамику появления новых субъектов и объектов правоотношений, новых способов осуществления деятельности в информационной сфере, но и оказывает значительное влияние на развитие системы правового регулирования, что детерминировано логикой экспоненциальной динамики цифровых и квантовых технологий, а также глобальной конкуренцией национальных экономик и государственного управления, порой переходящей в конфронтацию. При этом цифровые технологии сегодня выступают драйвером развития различных сфер, определяя их перспективы и в значительной мере позволяя выиграть в обострившейся конкурентной борьбе.

Непреходящую роль для обеспечения информационной безопасности имеет развитие ее конституционно-правовых основ, определивших сферу обороны и безопасно-

[1] Прогноз развития киберугроз и средств защиты информации. 2022 [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/2022-Cyber-Threats-and-Information-Security-Forecast (дата обращения: 20.03.2022).

сти, оборота цифровых данных в качестве предмета ведения Российской Федерации, что детерминируется их стратегической значимостью [2]. Конституционными нормами закреплены информационные права и свободы, основы права на информационную безопасность личности, а также их пределы и основания ограничений. В современных условиях противостояния западных государств с Российской Федерацией и исключения нашего государства из ряда международных организаций конституционные положения определяют меру прав и свобод человека и гражданина, их незыблемость.

Вместе с тем отмечается, что информационные права и свободы не безграничны: существуют конституционно установленные границы их реализации, определяющие модель правомерного поведения субъекта в информационной сфере [3]. Однако научных исследований правовых проблем в данной сфере пока явно недостаточно. Так, в целях правового обеспечения информационной безопасности государственного управления сегодня как никогда актуально изучение информационно-правовых пределов принятия юридически значимых решений искусственным интеллектом [4].

Исследования показывают, что развитие цифровых технологий актуализирует значение правовых вопросов защиты охраняемых законом тайн и иной информации ограниченного доступа как в связи с необходимостью защиты конфиденциальности в цифровой среде и противодействия несанкционированному доступу к цифровым данным, так и, например, в связи с расширением состава и характера информации ограниченного доступа (тайн). Сегодня исследователи предлагают расширить систему охраняемых законом тайн путем включения в них тайны идентификации, телемедицинской тайны и др. [5; 6, с. 11]. Полагаем, что с такой позицией следует согласиться, но в связи с этим остается не в полной мере ясным место конфиденциальности электронных сообщений и иных цифровых данных. Кроме того, с увеличением в настоящее время кибератак и ростом киберпреступности целесообразным видится усиление законодательных требований к защите конфиденциальности цифровых данных.

В условиях перехода к полицентризму одним из негативных результатов цифровизации явилось создание и распространение в цифровой среде недостоверной (фейковой) информации, что стало острой проблемой. Идут процессы совершенствования технологий воздействия на личное и массовое сознание, дестабилизации общества, что детерминирует необходимость развития организационно-правовых механизмов обеспечения информационно-психологической безопасности личности и общества, а также противодействия правовыми средствами распространению недостоверной общественно значимой информации.

Беспрецедентное распространение фейковой информации сегодня сочетается со стремлением глобальных транснациональных IT-корпораций, демонстрирующих право сильного, контролировать характер распространяемой в сети Интернет информации, что породило переосмысление феномена интернет-цензуры [7]. При этом необходимость ограничения влияния на цифровое пространство IT-гигантов отмечается и в западных государствах, обеспокоенных применением антиконкурентных практик[1]. Исследователями также отмечается скоординированная политика транснациональных IT-корпораций, фактически сформировавших олигополию и обеспечивающих доминирование в мире прозападной точки зрения и информационного давления на страны[2].

[1] В Евросоюзе ограничат цифровые гиганты [Электронный ресурс]. URL: https://news.rambler.ru/internet/48374307/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 27.03.2022).

[2] В ОП РФ винят американских ИТ-гигантов в трудностях отношений между РФ и Европой [Электронный ресурс]. URL: https://news.rambler.ru/ weapon/48366300/?utm_content=news _media&utm_medium =read_more&utm_source=copylink (дата обращения: 25.03.2022).

Все эти процессы затрудняют донесение до мировой общественности позиции России по стратегически значимым для нее вопросам и позволяют представлять в искаженном свете многие современные процессы и смыслы. Указанное требует развития правовых механизмов обеспечения национальных интересов в цифровом пространстве, в том числе посредством пресечения незаконного ограничения конституционно закрепленных информационных прав и свобод на доступ к информации, а также защиты русского языка и российской культуры в контексте обеспечения национальной безопасности. В связи с этим исследователями отмечается, что защита русского языка является компонентом национальной безопасности, однако мероприятия, проводимые в данном направлении, сегодня носят не подкрепленный необходимыми правовыми нормами характер [8, с. 62–63].

Применение западными государствами экономических и иных санкций актуализировало дальнейшее развитие правового регулирования цифровых технологий, включая совершенствование правовых механизмов создания и оборота цифровых валют как направления обеспечения экономической безопасности России. Необходимо отметить, что правовой режим цифровых валют и цифровых финансовых активов является комплексным и лежит на стыке финансового и информационного права, что предопределяет необходимость усиления межотраслевых исследований публично-правовых вопросов цифровизации в интересах национальной безопасности. Хотя сегодня предпринимаются попытки создать препятствия использованию цифровой валюты для решения российских экономических задач[1], децентрализованная природа цифровых финансовых активов вряд ли позволит реализовать такой сценарий. Однако для обеспечения национальной безопасности стратегически важно формирование и дальнейшее создание правовых условий для оборота цифровых валют в интересах России.

Развитие цифровых инноваций является ключевым вектором экономического укрепления России. В связи с этим особое значение приобретает внедрение правовых механизмов обеспечения информационной безопасности, разработки и внедрения цифровых инноваций. Одним из основных способов формирования необходимых правовых механизмов для таких инноваций является развитие специальных правовых режимов. Наиболее существенные перспективы сегодня отмечаются у систем искусственного интеллекта и робототехники, скачок в развитии которых ожидается в 2022 г.[2] Вместе с тем устройства и программы на базе технологии искусственного интеллекта являются конвергентными и предполагают одновременное развитие больших данных, сетей и систем связи, облачных и других инновационных технологий. Кроме того, искусственные интеллектуальные системы несут не только риск, но и могут быть применены в составе инфраструктуры обеспечения информационной безопасности как подсистема, позволяющая анализировать большие данные о потенциальных рисках и аномальном поведении пользователей, что также требует научного осмысления с позиции права.

Указанные и многие иные факторы актуализируют развитие организационно-правовых аспектов деятельности в сфере защиты информации, включая инженерно-техническое, криптографическое и программно-аппаратные направления. Большое значение в этой сфере наряду с правовым регулированием имеет техническое регулирование, включая сертификацию и декларирование соответствия, а также саморегулирование и сорегулирование.

Широкое использование в России оборудования и программного обеспечения зарубежного производства повышает уязвимость

[1] США и Евросоюз обсудили обход антироссийских санкций. США и ЕС договорились не допустить использование Россией цифровых валют для обхода санкций [Электронный ресурс] // Известия. 2022. 25 марта. URL: https://iz.ru/1310369/2022-03-25/ssha-i-evrosoiuz-obsudili-obkhod-antirossiiskikh-sanktcii?utm_source=yxnews&utm_medium=desktop (дата обращения: 25.03.2022).

[2] Прогноз развития киберугроз и средств защиты ты информации. 2022.

российской информационной инфраструктуры и информационных ресурсов, что стало особенно явным в обстоятельствах так называемой Русской весны 2022 г., когда в результате санкционного давления оказались нарушены цепочки поставок и логика обслуживания информационных продуктов и компонентов цифровых технологий. Это усиливает вектор государственной политики на поддержку безопасных разработок цифровых устройств и программного обеспечения для продвижения отечественных продуктов. В связи с этим, полагаем, следует приветствовать введение налоговых и иных преференций для IT-сферы как отрасли инноваций и передовых технологий, а также исследования существующих правовых препятствий для цифровизации. В связи с существующими рисками и вызовами информационной сферы 1 мая 2022 г. Президентом РФ был издан специальный Указ, направленный на введение дополнительных мер по обеспечению информационной безопасности Российской Федерации[1] и развитие системы деятельности по защите информации посредством формирования в организациях специализированных структурных подразделений и выделения ответственных должностных лиц.

В современных условиях в целях достижения цифрового технологического суверенитета перспективным является развитие организационно-правовых механизмов анализа защищенности цифровых данных, формирования безопасной цифровой среды, обладающей необходимым уровнем цифровой зрелости [9]. Особое внимание при этом целесообразно уделять формированию организационно-правовых и экономических условий разработки и производства отечественной элементной базы, системного программного обеспечения, а также средств и систем защиты информации.

Кроме того, одним из ключевых направлений правового обеспечения информационной безопасности является подготовка специалистов IT-отрасли, повышение цифровой и информационно-правовой грамотности населения, формирование условий для развития отечественных стартапов и повышения конкурентоспособности российских организаций, работающих в данной сфере.

В условиях отсутствия правового консенсуса по вопросам международной информационной безопасности важным представляется укрепление межгосударственного сотрудничества в рамках региональных интеграционных союзов в целях повышения развития рынка цифровых технологий и укрепления национального суверенитета в информационной сфере. В связи с этим целесообразно осуществлять межгосударственное взаимодействие при подготовке кадров, в ходе научно-исследовательской и опытно-конструкторской деятельности, в процессе технического регулирования цифровых технологий на взаимовыгодных условиях для расширения и укрепления экономического пространства и взаимовыгодного экономического сотрудничества в рамках ШОС, БРИКС и ЕАЭС [10].

Таким образом, проведенное исследование подтверждает вывод о том, что, несмотря на весьма широкий спектр различных аспектов и приоритетов национальной безопасности, на российское законодательство в последние три десятилетия значительно влияют новые вызовы и угрозы. В связи с этим сегодня необходимо принять специальный Федеральный закон «Об информационной безопасности Российской Федерации», в котором должно найти отражение системное регулирование широкого круга взаимосвязанных вопросов с учетом существующих вызовов праву и рисков современности.

[1] О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : указ Президента РФ от 01.05.2022 № 250 [Электронный ресурс] // Офиц. интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 01.05.2022).

Список источников

1. Полякова Т.А. Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы инфор-

мационного права (прошлое и будущее) / Т.А. Полякова, А.В. Минбалеев, Н.В. Кроткова // Государство и право. – 2021. – № 12. – С. 97–108.

2. Полякова Т.А. Развитие конституционно-правовых основ обеспечения информационной безопасности как составляющей национальной безопасности: векторы научных исследований в области информационного права / Т.А. Полякова, М.А. Шмаков // Военное право и современные информационные технологии правового обеспечения в сфере национальной безопасности и военно-технического сотрудничества : сборник докладов международной научно-практической конференции. – Москва, 2021. – С. 55–65.

3. Камалова Г.Г. Пределы и ограничения в информационном праве России / Г.Г. Камалова // Национальная безопасность/nota bene. – 2020. – № 2. – С. 11–30.

4. Архипов В.В. Пределы принятия юридически значимых решений с использованием искусственного интеллекта / В.В. Архипов, В.Б. Наумов, К.М. Смирнова // Вестник Санкт-Петербургского университета. Право. – 2021. – Т. 12, № 4. – С. 882–906.

5. Наумов В.Б. Задача обеспечения тайны идентификации в информационном праве / В.Б. Наумов // Мониторинг правоприменения. – 2019. – № 3 (32). – С. 70–75.

6. Буланова В.С. Информационно-правовое обеспечение оказания телемедицинских услуг в условиях цифровой трансформации : автореф. дис. … канд. юрид. наук : 12.00.13 / В.С. Буланова. – Москва, 2021. – 29 с.

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

8. Алексеев К.В. Проблемы правовой защиты русского языка в контексте национальной безопасности России / К.В. Алексеев, Н.Ф. Воробьев // Юридическая наука. – 2017. – № 4. – С. 62–66.

9. Полякова Т.А. Понятие и правовая природа «цифровой зрелости» / Т.А. Полякова, А.В. Минбалеев // Государство и право. – 2021. – № 9. – С. 107–116.

10. Камалова Г.Г. Межгосударственное сотрудничество в сфере технического регулирования цифровых технологий / Г.Г. Камалова // Сборник избранных статей по материалам научных конференций ГНИИ «Нацразвитие». – Санкт-Петербург, 2021. – С. 97–99.

References

1. Polyakova T.A., Minbaleev A.V., Krotkova N.V. Development of the science of information law and legal provision of information security: formation of the scientific school of information law (past and future). *Gosudarstvo i pravo = State and Law,* 2021, no. 12, pp. 97–108. (In Russian).

2. Polyakova T.A., Shmakov M.A. Development of the constitutional and legal foundations for ensuring information security as a component of national security: vectors of scientific research in the field of information law. *Voennoe pravo i sovremennye informacionnye tekhnologii pravovogo obespecheniya v sfere nacional'noj bezopasnosti i voenno-tekhnicheskogo sotrudnichestva. Sbornik dokladov mezhdunarodnoj nauchno-prakticheskoj konferencii* [Military law and modern information technologies of legal support in the field of national security and military-technical cooperation. Collection of reports of the International scientific-practical conference]. Moscow, 2021, pp. 55–65. (In Russian).

3. Kamalova G.G. Restrictions and boundaries in the Russian information law. *Nacional'naya bezopasnost' / nota bene = National Security / Nota Bene,* 2020, no. 2, pp. 11–30. (In Russian).

4. Arkhipov V.V., Naumov V.B., Smirnova K.M. The limits of automatic decision-making based on artificial intelligence in cases that have legal significance. *Vestnik Sankt-Peterburgskogo universiteta. Pravo = Vestnik of Saint Petersburg University. Law,* 2021, vol. 12, no. 4, pp. 882–906. (In Russian).

5. Naumov V.B. The task of ensuring the secrecy of identification in information technology law. *Monitoring pravoprimeneniya = Monitoring of Law Enforcement,* 2019, no. 3 (32), pp. 70–75. (In Russian).

6. Bulanova V.S. *Informacionno-pravovoe obespechenie okazaniya telemedicinskih uslug v usloviyah cifrovoj transformacii. Avtoref. Kand. Diss.* [Information and legal support for the provision of telemedicine services in the context of digital transformation. Cand. Diss. Thesis]. Moscow, 2021. 29 p.

7. Kamalova G.G. Censorship in the digital era: issues of legal regulation of national security. *Informacionnoe pravo = Information Law,* 2021, no. 2, pp. 32–36. (In Russian).

8. Alekseev K.V., Vorobyov N.F. Problems of legal protection of the Russian language in the context of Russia's national security. *Yuridicheskaya nauka = Legal Science,* 2017, no. 4, pp. 62–66. (In Russian).

9. Polyakova T.A., Minbaleev A.V. The concept and legal nature of digital maturity. *Gosudarstvo i pravo = State and Law,* 2021, no. 9, pp. 107–116. (In Russian).

10. Kamalova G.G. Interstate cooperation in the sphere of technical regulation of digital technologies. *Sbornik izbrannyh statej po materialam nauchnyh konferencij GNII «Nacrazvitie»* [Collection of selected articles on the materials of scientific conferences by SSRI «National development»]. Saint Petersburg, 2021, pp. 97–99. (In Russian).

Информация об авторах

Полякова Татьяна Анатольевна – доктор юридических наук, профессор, главный научный сотрудник, исполняющая обязанности заведующей сектором информационного права и международной информационной безопасности Института государства и права Российской академии наук, заслуженный юрист Российской Федерации;

Камалова Гульфия Гафиятовна – доктор юридических наук, доцент, заведующая кафедрой информационной безопасности в управлении Удмуртского государственного университета.

Information about the Authors

Polyakova Tatiana Anatolievna – Doctor of Law, Professor, Chief Researcher, Acting Head of the Information Law and International Information Security Sector of the Institute of State and Law, Russian Academy of Sciences, Honored Lawyer of the Russian Federation;

Kamalova Gulfiya Gafiyatovna – Doctor of Law, Associate Professor, Head of the Department of Information Security in Management, Udmurt State University.

Статья поступила в редакцию 04.03.2022; одобрена после рецензирования 12.05.2022; принята к публикации 13.05.2022.

The article was submitted 04.03.2022; approved after reviewing 12.05.2022; accepted for publication 13.05.2022.