УДК 004.056.5 Вестник УрФО № 3(33) / 2019, с. 64–68

Полякова Т. А., Минбалеев А. В., Бойченко И. С.

DOI: 10.14529/secur190307

КОНЦЕПТУАЛЬНЫЕ ПОДХОДЫ К ПРАВОВОМУ РЕГУЛИРОВАНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ И ТРАНСФОРМАЦИИ ПРАВА[1]

Статья посвящена анализу основных концептуальных подходов и проблем правового регулирования информационной безопасности в Российской Федерации, которое является стратегическим направлением в области обеспечения безопасности личности, общества и государства. Проанализированы актуальные вопросы реазации Федерального пректа «Информационная безопасность». Выделены основные ограничения, существующие в сфере правового обеспечения информационной безопасности в условиях цифровизации.

Обоснована необходимость применения междисциплинарного подхода к вопросам обеспечения информационной безопасности, а также формирования риск ориентированной модели управления в области информационной безопасности. Учитывая, что массив информационно-правовых отношений, рост информационного контента, а также рост киберпреступлений и инцидентов, выделен ряд новых рисков исполнения национальной программы «Цифровая экономика Российской Федерации».

Ключевые слова: *информационная безопасность, трансформация, среда доверия правовое обеспечение, цифровизация, цифровая экономика, национальный проект, правовое регулирование, вызовы и угрозы.*

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16013 «Исследование концептуальных подходов к формированию системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе». The study was supported by the RFBR within the framework of the research project № 18-29-16013 "Research of conceptual approaches to the formation of the system of legal regulation of information security in the conditions of great challenges in the global information society».

CONCEPTUAL APPROACHES TO THE LEGAL REGULATION OF INFORMATION SECURITY IN THE CONDITIONS OF DIGITALIZATION AND TRANSFORMATION OF LAW

The article is devoted to the analysis of the main conceptual approaches and problems of legal regulation of information security in the Russian Federation, which is a strategic direction in the field of security of the individual, society and the state. The topical issues of implementation of the Federal project "Information security"are analyzed. The main restrictions existing in the sphere of legal support of information security in the conditions of digitalization are allocated.

The necessity of an interdisciplinary approach to the issues of information security, as well as the formation of risk-oriented management model in the field of information security. Given that the array of information and legal relations, the growth of information content, as well as the growth of cybercrime and incidents, identified a number of new risks of execution of the national program "Digital economy of the Russian Federation".

Keywords: *information security, transformation, trust environment, legal support, digitalization, digital economy, national project, legal regulation, challenges and threats.*

Цифровизация общества – стратегическое направление реализации государственной политики, направленное на формирование конкурентно-способной экономики, развитие бизнеса, оптимизацию системы государственного и муниципального управления. Она оказывает свое воздействие на различные сферы общественной жизни. Не исключением является и сфера информационной безопасности.

Основополагающим началом в области обеспечения информационной безопасности сегодня является Федеральный проект «Информационная безопасность», являющийся составной частью Национального проекта «Цифровая экономика», содержит 56 мероприятий, как минимум 15, из которых касаются создания и совершенствования нормативного правового регулирования в сфере информационной безопасности и электронного взаимодействия. Важно учитывать, что указанные мероприятия, требуют не внесения точечных изменений, а направлены на системное и обоснованное формирование правовых и регуляторных условий для развития цифровой экономики, что требует фундаментальных правовых исследований, прежде всего в области правового обеспечения информационной безопасности. Проанализируем Федеральные проекты «Нормативное регулирование цифровой среды» и «Информационная безопасность». Из 18 блоков, направленных на принятие тех или иных федеральных законов, регулирующих отношения в области цифровой экономики, более половины из них косвенно касаются информационной безопасности. Однако в проекте «Информационная безопасность» разработка законов непосредственно касающихся регулирования отношений в области информационной безопасности не предусмотрена.

Сегодня приходится констатировать о

ряде проблем в реализации Федерального проекта «Информационная безопасность». Ряд мероприятий задерживаются, в отношении же реализованных есть много вопросов. Так, п. 1.8 Федерального проекта «Информационная безопасность», касающийся закрепления правового статуса российского сегмента сети «Интернет», его инфраструктуры, порядок ее функционирования» был реализован путем принятия Федерального закона от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» и вызвал дискуссии, как в профессиональной среде, так и обществе в целом по проблемам ограничений доступа к информации в сети Интернет.

При этом представляется целесообразным при подготовке нормативных правовых актов, необходимых для решения поставленных задач и выполнения предусмотренных мероприятий обратить внимание на неразработанность и необоснованность использования на уровня законопроектов ряда понятий, в том числе таких, как: антивирусный мультисканер, база знаний индикаторов вредоносной активности, киберкультура и ряда др. Все они отличаются признаком правовой неопределенности. В случае принятия соответствующих законопроектов, вызовут ряд проблем в сфере правоприменения.

При разработке программы «Цифровая экономика» и национальной программы «Цифровая экономика», впервые первоочередной задачей ставилось создание нормативного правового регулирования (регуляторной среды). Правовое обеспечение, как цифровой экономики в целом, так и федерального проекта «Информационная безопасность требует фундаментального, научного подхода, выражающееся в недостаточности внесения точечных изменений в законодательство Российской Федерации.

Анализируя положения федерального проекта «Информационная безопасность представляется важным отметить существенное уменьшение количества мероприятий по сравнению с ранее предусматриваемыми в планах развития цифровой экономики. С одной стороны, это связано с тем, что в программе мероприятия были датированы 2018 годом и выполнены.

С другой стороны, определенные положения, которыми была предусмотрена разработка стандартов в сфере информационной безопасности в рамках ЕАЭС и их гармонизация, проведение учений ЕАЭС в области информационной безопасности созданы и реализованы элементы инфраструктуры единого пространства доверия электронной подписи, обеспечивающего трансграничное информационное взаимодействие ЕАЭС в рамках национального проекта «Цифровая экономика» не нашли своего отражения.

Правовое обеспечение, исходя из анализа положений национального программы Цифровой экономики, многоуровневое, включает международное регулирование. В эпоху цифровизации формирование среды доверия, киберкультуры, правил поведениям в глобальном информационном обществе являются важными аспектами развития глобального информационно общества. Изменение парадигмы права в области обеспечения информационной безопасности происходит, прежде всего, в рамках региональных объединений: Евразийского экономического союза, союзного государства, Шанхайской организации сотрудничества, Содружества Независимых Государств, БРИКС и др.

К важнейшим направлениям в области информационной безопасности в национальном проекте «Цифровой экономики» относится обеспечение информационной безопасности в «Умном городе», которое также требует научных исследований как теоретического, так и практического характера в сфере информационного права.

Сформированная триада субъектов – личности, общества и государства, как важнейшие субъекты отношений в области обеспечения информационной безопасности в эпоху трансформации права также испытывает на себе последствия процессов цифровизации.

Процессы и проблемы цифровизации, требующие универсальных правовых средств, на основе междисциплинарных подходов организационно-правовых проблем в области информационной безопасности при формировании единой цифровой среды доверия, должны быть решены при помощи фундаментальной науки, формирования единого понятийного аппарата в рамках как национального, так и наднационального права. Кроме того, использование междисциплинарной прививки, в исследованиях, как прикладного, так и практического права в области права, информационных технологий,

управления, технологий безопасности, окажет положительное воздействие на формирование правовых средств, обеспечивающих информационную безопасность личности, общества и государства.

В этой связи предлагается предусмотреть в процессе разработки нормативных правовых и иных актов, связанных с цифровой экономикой и информационной безопасностью, гармонизацию понятийного аппарата, целью которой будет поиск механизмов единства понятий не в рамках одного и/или группы нормативных правовых актов, актов рекомендательного характера, стандартов, а через всю иерархию информационного законодательства, возможным решением, является кодификация информационного законодательства, которое будет включать в себя и часть «цифрового» законодательства.

Важной частью концептуального регулирования сферы информационной безопасности в условиях цифровизации является и формирование системы ограничений. Любая деятельность, протекающая в обществе, подвергаются ограничению, поскольку существует необходимость охраны прав, свобод и законных интересов субъектов. Ограничения в процессе правового регулирования обеспечения информационной безопасности прежде всего связываются с проблемами, которые могут мешать данному процессу, ограничивать его. Кроме того, необходимо ограничивать регулирование сферы информационной безопасности в тех случаях, когда есть опасность, что те или иные информационные процессы может привести к негативным последствиям. Сегодня важно выявить и те и другие ограничения, поскольку важно понять с какими сложностями сталкивается сегодня любое государство мира, а также важно предостеречь любое государство мира от возможных ошибок в построении системы правового обеспечения информационной безопасности .в условиях больших вызовов в глобальном информационном обществе, цифровизации и трансформации права.

Среди ограничений первого блока можно выделить следующие:

1. Понятийный аппарат. Основой для регулирования любых отношений является определение того, с чем законодатель и правоприменитель будут работать. В сфере информационной безопасности происходит стремительное развитие понятийного аппарата, о чем свидетельствует как Доктрина информационной безопасности РФ, так и новые принимаемые акты международного и национального уровней. Ряд ключевых новых понятий закреплено в Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы. Но законодатель не решил всех проблем, поскольку явно существует необходимость совершенствования имеющихся терминов, в том числе «информационная безопасность», «информационные угрозы», «информационные риски» и др. в связи с развитием международной информационной безопасности, появлением новых угроз, в том числе киберугроз, использованием цифровых технологий.

2. Ограничения в сфере моделей регулирования. Сегодня существует явная необходимость создания оптимальной модели правового регулирования обеспечения информационной безопасности. Однако отсутствие законодательной оценки возможностей технического регулирования, саморегулирования и сорегулирования, организационного регулирования в сфере информационной безопасности вызывают ряд ограничений на пути трансформации правового регулирования обеспечения информационной безопасности.

3. Технические ограничения. Сегодня явно необходимо констатировать неготовность большинства предприятий, ведущих хозяйственную деятельность в условиях активного развития цифровых технологий, внедрять и использовать новейшие средства информационной безопасности и создавать эффективную локальную правовую систему правового обеспечения информационной безопасности на локальном уровне.

Важным направление развития концептуальных подходов к правовому обеспечению информационной безопасности сегодня является и риск ориентированный подход к управлению в соответствующей сфере. В отношении риск ориентированного подхода к управлению в сфере информационной безопасности Положением о системе управления реализацией Национальной программы «Цифровая экономика Российской Федерации», утв. постановлением Правительства Российской Федерации от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» закреплены риски только в отношении неисполнения федерального проекта национальной программы

«Цифровая экономика Российской Федерации».

Учитывая, что массив информационно-правовых отношений, рост информационного контента, а также рост киберпреступлений и инцидентов, необходимо отнести к рискам исполнения национальной программы «Цифровая экономика Российской Федерации» такие ситуации, как: риск пробелов правового регулирования цифровых отношений (отсутствие единого понятийного аппарата в сфере цифровизации, отсутствие принципов, отсутствие нормативных правовых актов, регулирующих определенные общественные отношения), риск конкуренции норм между информационным, финансовым, гражданским и другими отраслями законодательства, риск невозможности технологического обеспечения национальной программы «Цифровая экономика Российской Федерации», риск кадрового дефицита, риск излишней регламентированности общественных отношений в области цифровой экономики в целом и информационной безопасности в частности, риск ошибок в рамках «регуляторной гильотины», риск невозможности поиска правовых решений и механизмов для регулирования новых общественных отношений и др. Сегодня явно существует необходимость систематизации таких рисков в рамках федеральных центров управления процессов в сфере цифровизации и развития цифровой экономики.

ПОЛЯКОВА Татьяна Анатольевна, доктор юридических наук, исполняющий обязанности заведующего сектором информационного права и международной информационной безопасности Института государства и права Российской академии наук. 119019, Москва, ул. Знаменка, 10. E-mail: Polyakova_ta@mail.ru

МИНБАЛЕЕВ Алексей Владимирович, доктор юридических наук, главный научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права Российской академии наук. 119019, Москва, ул. Знаменка, 10. E-mail: alexmin@bk.ru

БОЙЧЕНКО Игнат Сергеевич, кандидат юридических наук, научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права Российской академии наук. 119019, Москва, ул. Знаменка, 10. E-mail: 79154538848@yandex.ru

POLYAKOVA Tatiana Anatolievna, Doctor of Law, Acting Head of the Information Law and International Information Security Sector of the Institute of State and Law of the Russian Academy of Sciences. 119019, Moscow, st. Znamenka, 10. E-mail: Polyakova_ta@mail.ru

MINBALEEV Aleksey Vladimirovich, Doctor of Law, Chief Researcher of the Information Law and International information security Sector, Institute of State and Law of the Russian Academy of Sciences. 119019, Moscow, st. Znamenka, 10. E-mail: alexmin@bk.ru

BOYCHENKO Ignat Sergeevich, candidate of law, researcher in the information law sector and international information security, Institute of state and law of the Russian Academy of Sciences. 119019, Moscow, st. Znamenka, 10. E-mail: 79154538848@yandex.ru