УДК 349

ОТДЕЛЬНЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ*

Т. А. Бражник

Национальный исследовательский университет «Высшая школа экономики»

Поступила в редакцию 3 октября 2018 г.

Аннотация: *рассматриваются проблемы соотношения информационной безопасности и информационной безопасности личности в российском и зарубежном законодательстве и документах стратегического планирования Российской Федерации. Многочисленные нормативные акты регулируют различные аспекты в данной сфере, однако на международном и национальном уровне не хватает унификации в терминологии и базовых принципах обеспечения информационной безопасности. Анализируется круг отношений, который включается исследователями в сферу информационной безопасности личности. Делается вывод, что для гармоничного развития института информационной безопасности личности необходимо усиление внетехнических, социально направленных мер и стимулов.*
Ключевые слова: *информационная безопасность, информационная безопасность личности, национальная безопасность, идентификация, защита информации, доктрина информационной безопасности, кибербезопасность, критическая информационная инфраструктура, право на информацию, информационные правоотношения, конфиденциальность, персональные данные, цифровая экономика, информационное право.*

Abstract: *the article analyses certain problems of correlation between information security and information security of a person in the Russian and foreign legislation, documents of strategic planning. Numerous normative acts regulate various aspects in matter at hand, however, international and national legal sourser face a lack of unification in the terminology and basic principles of information security development. The bundle of relations traditionally included into the sphere of information security of the person is analyzed. The author highlights that further development of the institute of information security of a person crucially depends on strengthening of non-technical, socially oriented measures and incentives.*
Key words: *information security, information security of the person, national security, identification, information protection, information security doctrine, cybersecurity, critical information infrastructure, the right to information, legal relations, confidentiality, personal data, data economy, information law.*

Развитие и совершенствование информационно-коммуникационных технологий, в частности повсеместное использование сети «Интернет»,

* Статья подготовлена в ходе проведения исследования в рамках Программы фундаментальных исследований Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ) и с использованием средств субсидии в рамках государственной поддержки ведущих университетов Российской Федерации «5–100».

существенным образом влияет на взаимоотношения личности, общества и государства в самых различных сферах, что находит отражение в текущем законодательстве. Технологии способствуют расширению связей, ускорению совершения транзакций, распространению информации, однако создают также предпосылки для появления новых угроз защищаемым правам и законным интересам, поэтому обеспечение информационной безопасности становится все более актуальным для различных правоотношений. Так, информатизация и, соответственно, необходимость обеспечения информационной безопасности, коснулась сфер государственного управления[1], таможенного обеспечения[2] , здравоохранения[3], социальной защиты[4], построения информационного общества знаний[5], отрасли гражданско-правовых отношений[6], а также различных аспектов защиты прав граждан в информационной сфере.

Очевидно, что обеспечение информационной безопасности – сфера, в которой частные и публично-правовые интересы весьма тесно взаимосвязаны[7], в связи с чем информационная безопасность личности, гарантии прав граждан в информационных отношениях выступают как основа для нормального функционирования всех отраслей права, особенно информационного. Можно также отметить, что текущее нормативное правовое регулирование идет в направлении защиты целостности, стабильности и устойчивости национального сегмента сети «Интернет», унификации правил идентификации, импортозамещения аппаратных и программных средств, обеспечения цифрового суверенитета и безопасности критической информационной инфраструктуры[8]. Регламентации данных вопросов посвящены многочисленные документы стратегического пла-

[1] См.: *Терещенко Л. К., Тиунов О. И.* Информационная безопасность органов исполнительной власти на современном этапе // Журнал рос. права. 2015. № 8. С. 100–109.

[2] См.: *Недосекова Е. С.* Информационная безопасность таможенных органов в системе национальной безопасности России : административно-правовые аспекты // Вестник Рос. таможенной академии. 2011. № 3.

[3] См.: *Журавлев М. С.* Правовое обеспечение электронного документооборота в телемедицине // Информационное право. 2017. № 4.

[4] См.: *Худойкина Т. В., Толкунова Н. А.* Информационные аспекты систематизации законодательства в сфере социальной защиты населения // Информационное право. 2010. № 3. С. 10–14.

[5] См.: *Пашнина Т. В., Минбалеев А. В.* Развитие права на информацию в свете стратегических документов Российской Федерации // Законы России : опыт, анализ, практика. 2018. № 3.

[6] См.: *Косовец А. А.* Информационная безопасность в системе обеспечения экономической и национальной безопасности России // Вестник Академии экономической безопасности МВД России. 2011. № 2.

[7] Eric Diehl, Ten Laws for Security. Springer International Publishing Switzerland 2016.

[8] О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26 июля 2017 г. № 187-ФЗ // Собр. законодательства Рос. Федерации. 2017. № 31 (ч. 1). Ст. 4736.

нирования, законы и подзаконные акты[9]. В связи с этим можно сделать вывод, что обеспечение должного уровня информационной безопасности личности является ключевой предпосылкой для развития иных аспектов национальной информационной безопасности в целом.

Необходимо отметить, что международное регулирование демонстрирует схожие тенденции. В ответ на возрастающие угрозы кибертерроризма, неправомерного использования персональных данных, использования информационных технологий в теневой экономике многие страны и международные организации разрабатывают нормативные акты, направленные на регламентацию отношений в информационной среде. Большая часть документов носит технический и методологический характер и имеет форму стандартов. Международная организация по стандартизации (ISO) разработала целый ряд стандартов в сфере информационной безопасности[10]. Например, стандарт ISO/IEC 27000 вводит общие принципы и терминологию по управлению информационной безопасностью систем. Существуют отдельные стандарты по кибербезопасности, которые, в свою очередь, содержат определение киберпространства, его пределов и элементов[11]. Однако данные стандарты в силу своей природы носят технический характер и недостаточно регламентируют информационную безопасность личности, отличную от безопасности пользовательской информации или оборудования.

Многосторонние международные правовые акты в сфере обеспечения информационной безопасности относятся к различным и нередко разрозненным институтам информационного права, таким как преступность в сфере компьютерной информации[12], обработка персональных данных[13] и т. д. В настоящее время, несмотря на предпринятые попытки создания, не существует единого международного соглашения в сфере информационной безопасности[14]. Законодательство отдельных стран показывает скачкообразный рост числа актов, принимаемых в рамках обеспечения

[9] См.: *Ефремов А. А.* Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. № 1.

[10] URL: https://www.iso.org/isoiec-27001-information-security.html (дата обращения: 20.09.2018).

[11] См.: *Марков А. С., Цирлов В. Л.* Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1 (2).

[12] Конвенция о преступности в сфере компьютерной информации (ETS No 185) : заключена в г. Будапеште 23.11.2001. Документ опубликован не был.

[13] Конвенция о защите физических лиц при автоматизированной обработке персональных данных : заключена в г. Страсбурге 28.01.1981 // Бюллетень международных договоров. 2014. № 4. Апрель.

[14] Конвенция об обеспечении международной информационной безопасности (концепция). URL: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU (дата обращения: 20.09.2018).

информационной безопасности и безопасности данных[15]. Отдельно стоит отметить Директиву Европейского союза о безопасности сетей и информационных систем[16], подчеркивающую особую роль информационных технологий для развития общества и защиты пользователей, закон Сингапура о кибербезопасности[17], проект закона Китайской Народной Республики[18]. Кроме отдельных отраслевых законов, зарубежные страны разрабатывают и принимают стратегические документы в сфере обеспечения информационной безопасности, например Стратегию национальной кибербезопасности Словении[19], регулирующую технические и внетехнические меры обеспечения безопасности государства, общества и личности. Необходимо отметить, что большая часть положений зарубежного законодательства обращена как раз к технической составляющей информационной безопасности личности.

Место информационной безопасности личности в системе информационной безопасности Российской Федерации определяется также целым рядом стратегических документов и отраслевых законов. Доктрина информационной безопасности Российской Федерации 2016 г. является, как указано в ст. 1, системой «официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере»[20], согласно которым, как представляется, впоследствии строится система нормативного правового регулирования информационной безопасности в России. Подобный базовый и основополагающий характер Доктрины может свидетельствовать о самостоятельном юридическом, а не сугубо политическом характере документа.

Кроме того, Доктрина, как указано в ст. 2, основывается на положениях Стратегии национальной безопасности Российской Федерации[21], а так-

[15] См.: *Maria Tzanou*. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right, International Data Privacy Law. 2013. Vol. 3, № 2. P. 88–99.

[16] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // OJ L 194, 19.7.2016. P. 1–30.

[17] Cybersecurity Act // Электронный доступ на сайте Министерства связи и информации Сингапура. URL: https://www.csa.gov.sg/legislation/cybersecurity-act (дата обращения: 20.09.2018).

[18] Ministry of Public Security of the People's Republic of China published the Draft Regulations on the Classified Protection of Cybersecurity. URL: https://www.huntonprivacyblog.com/2018/07/17/china-publishes-draft-regulations-classified-protection-cybersecurity/ (дата обращения: 20.09.2018).

[19] Slovenian National Cyber Security Strategy. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-in-slovenia (дата обращения: 20.09.2018).

[20] Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 5 декабря 2016 г. № 646 // Собр. законодательства Рос. Федерации. 2016. № 50. Ст. 7074.

[21] О Стратегии национальной безопасности Российской Федерации : указ Президента РФ от 31 декабря 2015 г. № 683 // Собр. законодательства Рос. Федерации. 2016. № 1 (ч. 2). Ст. 212.

же иных стратегических документах, к которым можно причислить также Стратегию научно-технологического развития Российской Федерации[22], многочисленные соглашения между Российской Федерацией и иными странами о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности[23], а также ряд указов Президента РФ[24]. Совокупность данных актов и соответствующих федеральных законов позволяет сделать вывод о существовании подробной регламентации института информационной безопасности личности, определении его взаимосвязи с информационной безопасностью государства и общества.

Однако более детальный анализ указанных источников позволяет сделать вывод об обратном. Так, Доктрина информационной безопасности Российской Федерации ставит потребности личности на первое место в перечислении национальных интересов Российской Федерации в информационной сфере, что позволяет говорить о первоочередном характере защиты прав и интересов личности. Кроме того, информационная безопасность Российской Федерации основывается, в первую очередь, на состоянии защищенности личности, «…при котором обеспечиваются конституционная реализация прав и свобод человека и гражданина, достойные качество и уровень жизни граждан…», что характеризует институт информационной безопасности как производный от информационной безопасности личности.

В то же время Стратегия национальной безопасности Российской Федерации содержит положения, противоречащие данному выводу. Например, ст. 6 Стратегии, перечисляя составляющие национальной безопасности, ставит иную приоритетность: «Национальная безопасность включает в себя оборону страны и все виды безопасности, пред-

[22] О Стратегии научно-технологического развития Российской Федерации : указ Президента РФ от 1 декабря 2016 г. № 642 // Собр. законодательства Рос. Федерации. 2016. № 49. Ст. 6887.

[23] О подписании Соглашения между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности см., например: Распоряжение Правительства РФ от 4 июля 2017 г. № 1424-р // Официальный интернет-портал правовой информации (www.pravo.gov.ru) ; О подписании Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности : распоряжение Правительства РФ от 15 ноября 2013 г. № 2120-р // Собр. законодательства Рос. Федерации. 2013. № 47. Ст. 6135 ; О подписании Соглашения между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности : распоряжение Правительства Рос. Федерации от 13 мая 2010 г. № 721-р // Там же. 2010. № 21. Ст. 2628 ; и др.

[24] О некоторых вопросах информационной безопасности Российской Федерации см., например: Указ Президента РФ от 22 мая 2015 г. № 260 // Собр. законодательства Рос. Федерации. 2015. № 21. Ст. 3092 ; О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена : указ Президента РФ от 17 марта 2008 г. № 351 // Там же. 2008. № 12. Ст. 1110.

усмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности».

Конечно, нельзя говорить о незначительности роли обеспечения безопасности личности в системе национальной безопасности, однако налицо некоторое противопоставление информационной безопасности государства и безопасности личности.

Подобные несоответствия встречаются также в положениях государственной программы Российской Федерации «Информационное общество (2011–2020 годы)»[25], толкующей Доктрину информационной безопасности Российской Федерации в качестве приоритетного документа о стратегическом сдерживании и предотвращении военных конфликтов, которые могут возникнуть в результате применения информационных технологий, вместо обеспечения защиты прав и интересов граждан в информационной сфере. Именно поэтому информационная безопасность рассматривается в рамках данной программы как качественная характеристика построения технологических систем и сетей, что представляется неверным и излишне узким толкованием данного института.

Представляется, что обеспечение безопасности функционирования информационно-телекоммуникационной инфраструктуры и телекоммуникационных систем хотя и является необходимым инструментарием для обеспечения информационной безопасности личности, общества и государства, однако не ему тождественным. Положения программы «Цифровая экономика Российской Федерации»[26] ориентированы также на техническую составляющую информационной безопасности: обеспечение единства, устойчивости и безопасности информационно-телекоммуникационной инфраструктуры, использование российских технологий обеспечения целостности, конфиденциальности, аутентификации и доступности передаваемой информации и процессов ее обработки и т. д. Очевидно, что интересы личности в информационной сфере, которые нуждаются в обеспечении и безопасности, шире, чем технические принципы работы оборудования и обработки данных.

Еще большие противоречия в определении содержания института информационной безопасности личности можно обнаружить при анализе более специальных нормативных документов. С одной стороны, Соглашение об обеспечении информационной безопасности в рамках общих таможенных процессов в государствах – членах Евразийского экономического сообщества не содержит отсылок или упоминаний прав и интересов личности или граждан. Данный документ регламентирует исклю-

[25] Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)» : постановление Правительства РФ от 15 апреля 2014 г. № 313 // Собр. законодательства Рос. Федерации. 2014. № 18 (ч. 2). Ст. 2159.

[26] Об утверждении программы «Цифровая экономика Российской Федерации» : распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р // Собр. законодательства Рос. Федерации. 2017. № 32. Ст. 5138.

чительно аспекты определения режима передаваемой электронными сообщениями информации, такие как защиту от вирусов, от несанкционированного доступа к средствам вычислительной техники и телекоммуникационному оборудованию, обеспечение сетевой безопасности, анализ защищенности систем и т. д.

С другой стороны, Соглашения между Правительством Российской Федерации и Правительством Южно-Африканской Республики, Правительством Федеративной Республики Бразилии, Правительством Китайской Народной Республики, а также Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности прямо устанавливают в тексте, что международное сотрудничество между сторонами по вопросам обеспечения информационной безопасности строится на признании принципа баланса между обеспечением безопасности и соблюдением прав человека в области использования информационно-коммуникационных технологий, а также на признании роли информационной безопасности в обеспечении прав и основных свобод человека и гражданина.

Очевидно, что на уровне двустороннего международно-правового сотрудничества вопросы разграничения информационной безопасности в целом, информационной безопасности государства, а также информационной безопасности личности в частности решены недостаточно. Кроме того, проблемы детальной регламентации можно выявить при анализе текущего информационного законодательства. Так, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[27] (далее – Закон «Об информации»), являющийся базовым в информационно-правовой сфере, не содержит какой-либо регламентации информационной безопасности личности. Положения, касающиеся отдельных аспектов регулирования информационной безопасности, относятся к обеспечению безопасности Российской Федерации при создании и эксплуатации информационных систем, защите информации данных систем, выполнению организационных и технических мер по обеспечению безопасности персональных данных. Очевидно, что указанные положения имеют также сугубо технико-методологическую направленность и определяют меры по предоставлению или ограничению доступа к отдельным видам информации. Кроме того, в законе не содержится определения информационной безопасности или же отсылки к иным актам, содержащим такое определение. Однако, помимо указанных выше сфер технической регламентации информационной безопасности, законом проводится отсылка к отдельному институту информационной безопасности детей, имеющему уже более широкое социально-психологическое толкование, поскольку защита детей проводится в целях предотвращения вреда их здоровью и моральному развитию[28].

[27] Собр. законодательства Рос. Федерации. 2006. № 31 (ч. 1). Ст. 3448.

[28] О защите детей от информации, причиняющей вред их здоровью и развитию : федер. закон от 29 декабря 2010 г. № 436-ФЗ // Собр. законодательства Рос. Федерации. 2011. № 1. Ст. 48.

Будет справедливым вывод о том, что в текущих нормативных правовых актах не содержится достаточной регламентации института информационной безопасности личности, а также критериев его разграничения с информационной безопасностью в общем широком значении, употребляемом в основополагающих стратегических документах. Более того, некоторые российские исследователи толкуют такой стратегический документ как Доктрину в качестве инструмента для «незамедлительного и постоянного противодействия деструктивной деятельности иностранных элементов в информационной сфере»[29], что также не позволяет в полной мере определить место личности в системе мер обеспечения информационной безопасности.

Для развития института информационной безопасности личности необходимо исходить из принципа баланса интересов, поиска эффективных механизмов защиты прав и свобод личности в информационной сфере. Так как в сферу информационной безопасности личности входят также иные информационные права, такие как право на информацию, необходимо разрабатывать внетехнические меры обеспечения информационной безопасности личности. Так, при реализации права на информацию, граждане сталкиваются не только с угрозой недостаточной доступности информации, но и с проблемой качественного характера такой информации, отвечающей критериям безопасности, достоверности и т. д. Поэтому регулирование в данной сфере должно учитывать социальные реалии, национальные и культурные традиции России, а также отвечать целям защиты личности от существующих информационных угроз.

Можно также сделать вывод о том, что толкование информационной безопасности личности как состояние защищенности от внешних и внутренних угроз в текущих нормативных источниках неоднородно и поэтому используется преимущественно в технической сфере. Очевидно, что информационная безопасность личности предполагает также наличие определенной свободы личности в информационной среде, в том числе свободы на реализацию конституционных и информационных прав, однако обеспечение такой свободы должно гарантироваться правовыми и социальными методами.

[29] *Ищенко А. Н., Прокопенко А. Н., Страхов А. А.* Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере // Проблемы правоохранительной деятельности. 2017. № 2. С. 62.

Национальный исследовательский университет «Высшая школа экономики»

Бражник Т. А., младший научный сотрудник

E-mail: tbrazhnik@hse.ru

National Research University «Higher School of Economics»

Brazhnik T. A., Junior Research Assistant

E-mail: tbrazhnik@hse.ru