

УДК 351

ББК 67.401.11

DOI 10.22394/1682-2358-2017-5-68-75

O.V. Bryantseva, *Candidate of Science (Physics and Mathematics), Docent, Professor of the Informatics Department, Saratov State Academy of Law*

I.I. Bryantsev, *Candidate of Sciences (Sociology), Docent of the Public Administration Department, Povolzhsky Institute of Management named after P.A. Stolypin, Branch of the Russian Presidential Academy of National Economy and Public Administration*

THE DEVELOPMENT OF LEGISLATION ON THE PROTECTION OF INFORMATION AS AN ELEMENT OF NATIONAL SECURITY SYSTEM

The changes in legislation for the protection of information caused by the development of information technology and changes in the world and society are considered. Changes in legislation are analyzed from the point of view of strengthening national security. The discreet role of the state in the security system of cultural-historical and democratic values of the society is postulated.

Key words and word-combinations: national security, information security, telecommunication network.

О.В. Брянцева, *кандидат физико-математических наук, доцент, профессор кафедры информатики Саратовской государственной юридической академии (email: obryantseva@yandex.ru)*

И.И. Брянцев, *кандидат социологических наук, доцент кафедры государственного и муниципального управления Поволжского института управления имени П.А. Столыпина — филиала Российской академии народного хозяйства и государственной службы при Президенте РФ (email: ibry@yandex.ru)*

РАЗВИТИЕ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ИНФОРМАЦИИ КАК ЭЛЕМЕНТ СИСТЕМЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Аннотация. Рассматриваются изменения в законодательстве по защите информации, вызванные развитием информационных технологий и трансформациями в мире и обществе. Изменения в законодательстве проанализированы с точки зрения усиления национальной безопасности. Постулируется особая роль государства в системе защиты культурно-исторических и демократических ценностей общества.

Ключевые слова и словосочетания: национальная безопасность, информационная безопасность, информационно-телекоммуникационные сети.

Национальная безопасность государства — важный аспект его функционирования. Кроме обороны страны, для обеспечения национальной безопасности необходимы государственная, общественная, информационная, экологическая,

экономическая, транспортная, энергетическая безопасность, безопасность личности [1]. События последних лет, проявившиеся в глобальном геополитическом пространстве и непосредственно связанные с формированием информационной составляющей, весьма наглядно свидетельствуют о возрастании роли информационной компоненты в системе национальной безопасности. К наиболее ярким примерам можно отнести политические спекуляции вокруг обвинения России в ее якобы вмешательстве в выборы президента США и хакерские атаки, приписываемые северокорейскому киберсообществу. Национальная безопасность как система формируется на базе сложных многоуровневых структур взаимосвязанных между собой элементов. Одним из существенных компонентов этой системы следует рассматривать информационные технологии, развитие которых, как справедливо отмечают исследователи, является неотъемлемой частью построения информационного общества, на основе доступности различных информационных ресурсов, что и актуализирует значимость информационной безопасности [2; 3].

Информационные технологии формируют технологическую базу для реализации управленческих решений в разных сферах деятельности как внутри государства, так и на международном уровне с учетом принятой и реализуемой государственной политики. Российская Федерация является одним из основных геополитических субъектов современного глобального информационного общества и приверженцем международных принципов и подходов его формирования, определенных Окинавской хартией глобального информационного общества (2000), Декларацией принципов «Построение информационного общества — глобальная задача в новом тысячелетии» (2003) Планом действий Тунисского обязательства (2005), что обозначено в Указе Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы» [4].

В связи с этим особую актуальность приобретают вопросы, связанные с законодательным регулированием данной сферы с целью обеспечения защиты интересов общества и государства. Движущей силой, которая может обеспечить динамическое развитие социума и конкурентоспособность государства, выступает его способность производить, потреблять, распределять и обменивать информацию и таким образом формировать базу для современной постиндустриальной экономики. Создание необходимых условий для этого — насущная задача органов власти различных уровней, которые реализуют их через определение как внешних геополитических, так и внутренних приоритетов для обеспечения суверенитета и национальной безопасности.

Сфера развития законодательства в области обеспечения информационной безопасности, выявление складывающихся тенденций и основных проблем стало предметом исследования многих российских ученых [5—7]. В частности, процесс формирования правовой системы обеспечения международной информационной безопасности, а также системы информационной безопас-

ности в рамках законодательства Российской Федерации рассматривается в работах Т.А. Поляковой и других авторов [8].

В контексте проводимых в этой сфере исследований целесообразным представляется подход, позволяющий изучать компонент информационной безопасности в общей структуре национальной безопасности через анализ вносимых в соответствующие законодательные акты изменений, что позволяет выявлять формирующиеся приоритеты и направления в реализуемой политике.

Первый закон по защите информации был принят в 1995 г. [9], Доктрина информационной безопасности — в 2000 г. [10], а в 2006 г. вступил в силу Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [11], который действует и сегодня.

За прошедшие годы произошли большие изменения в информационной сфере, в применении информационных технологий, в развитии электронного правительства [12], что усилило значимость информационной безопасности. Все изменения отражались в нормативно-правовых актах по защите информации, в частности, в Законе № 149-ФЗ. На начало 2017 г. принято двадцать его редакций. С начала 2017 г. принято еще шесть редакций, действующая (на 1 октября) — 24-я, а остальные вступают в силу с 1 ноября 2017 г. и 1 января 2018 г. соответственно. В декабре 2016 г. Указом Президента РФ была утверждена новая Доктрина информационной безопасности [13], одной из правовых основ которой является Закон № 149-ФЗ.

Рассмотрим изменения в данном Законе, произошедшие более чем за десять лет с точки зрения национальной (информационной) безопасности. Этот Закон по-прежнему регламентирует отношения, возникающие при использовании информационных технологий, при осуществлении поиска, хранения, производства, передачи и защиты информации.

Первые изменения были внесены в 2010 г., — через четыре года после его принятия. Введено понятие электронного документа, в связи с чем изменена ст. 11 «Документирование информации». Усилена роль электронного документа, подписанного электронной цифровой подписью. Ее законодательное закрепление как основного и практически единственного IT-решения по обеспечению подлинности позволяет сделать электронные документы равнозначными документам на бумажном носителе, если иное не предусмотрено федеральным законодательством.

Государственным органам и органам местного самоуправления теперь вменяется в обязанность обеспечение доступа к информации о своей деятельности и с использованием информационно-телекоммуникационных сетей, в частности Интернета (ст. 8). Изменена ст. 14 «Государственные информационные системы». Содержащаяся в сетях информация признается официальной, а соответствующие государственные органы должны обеспечить ее достоверность и актуальность, а также доступ к ней и ее защиту. Указанные поправки направлены на дальнейшее развитие Доктрины информационной безопасности Российской Федерации, закрепляющей при-

оритеты по правовому обеспечению информационной безопасности Российской Федерации на принципах законности, баланса интересов граждан, общества и государства в информационной сфере и обеспечении гарантий конституционных прав и свобод человека и гражданина на доступ к информации и предоставление полноценных возможностей для деятельности в информационной сфере.

Дальнейшие изменения были внесены Федеральным законом от 21 июля 2011 г. № 252-ФЗ. В ст. 12 о государственном регулировании применения информационных технологий был добавлен п. 4 об обеспечении информационной безопасности детей, что, несомненно, является актуальным компонентом в системе национальной безопасности, отвечающим за информационно-психологическую безопасность и создающим правовую основу для развития и реализации мер, направленных на поддержание и укрепление здоровья нации и защиту индивидуальной психики и общественного сознания.

Следующим шагом по усилению информационной безопасности стало введение Федеральным законом от 28 июля 2012 г. № 139-ФЗ ст. 15.1. «Единый реестр доменных имен, указателей страниц сайтов в сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты, содержащие информацию, распространение которой в Российской Федерации запрещено». В ней говорится о создании автоматизированной информационной системы с включением в нее доменных имен и сетевых адресов соответствующих сайтов, определены органы, осуществляющие создание, формирование и ведение такого реестра — это федеральные органы исполнительной власти, контролирующие средства массовой информации, массовых коммуникаций, информационных технологий и связи. Прописаны основания для включения в реестр. Это порнографические материалы, связанные с несовершеннолетними, информация, касающаяся наркотических и психотропных средств (способы и методы изготовления, использования и распространения), а также призывы к самоубийству и способы его совершения.

С изменением в обществе и развитием информационных технологий эта статья менялась, в частности, добавлялись следующие основания для включения в реестр: информация о пострадавшем от противоправных действий несовершеннолетнем, распространение которой запрещено федеральным законодательством; информация, нарушающая требования федерального законодательства по государственному регулированию организации и проведения азартных игр, о запрете проведения азартных игр с использованием Интернета; информация о способах, методах разработки, изготовления и использования различных наркотических средств; информация о розничной продаже дистанционным способом алкогольной, различной спиртосодержащей продукции, розничная продажа которой ограничена или запрещена законодательством.

Федеральным законом от 7 июня 2013 г. № 112-ФЗ введено понятие информации в форме открытых данных — это общедоступная в Интернете информация, допускающая автоматизированную обработку для ее повторного использования, регламентировано ее размещение. В связи с этим изменены ст. 13

«Информационные системы» и ст. 14 «Государственные информационные системы». Оператор информационных систем должен обеспечить возможность размещения информации в форме открытых данных. Доступ к информации из государственных информационных систем дается только тем, кто прошел авторизацию в единой системе идентификации и аутентификации, тем самым повышается ответственность пользователей.

В Федеральный закон от 2 июля 2013 г. № 187-ФЗ добавлена ст. 15.2, регламентирующая порядок ограничений на доступ к информации, распространяемой с нарушениями исключительных прав на фильмы. Соответственно, это введено в сферу деятельности Законом № 149-ФЗ (ч. 2, ст. 1). Правообладатель при обнаружении в сети фильмов, распространяемых без его разрешения или при нарушении законодательства, вправе обратиться в соответствующие органы с заявлением о принятии мер по ограничению доступа к данным информационным ресурсам. В статье прописаны сроки и порядок мер по ограничению доступа к данной информации и об отмене ограничений. В связи с принятием новой ст. 17 об ответственности за нарушение в сфере информационных технологий и защиты информации введена ч. 4 о том, что владельцы сайта и провайдеры хостинга не несут ответственности перед правообладателями и пользователями за ограничения доступа к информации.

В 2014 г. законодатель изменил ст. 15.2, расширив ее применение на авторские и (или) смежные права, заменив нарушения исключительных прав на фильмы на нарушение авторских и (или) смежных прав.

В декабре 2013 г. были внесены изменения в статью о государственных информационных системах (ст. 14). Согласно этим изменениям государственные информационные системы создаются и эксплуатируются в соответствии с законодательством о контрактной системе в сфере закупок. Введена ст. 15.3 «Порядок ограничений доступа к информации, распространяемой с нарушением закона» напрямую связанная с обеспечением национальной безопасности. Имеется ввиду информация, размещаемая в информационно-коммуникационных сетях, о призывах к массовым беспорядкам, экстремистской деятельности, участию в массовых мероприятиях, проводимых с нарушением закона.

С развитием информационно-коммуникационных технологий и Интернета появилась необходимость регламентирования информации, размещенной в сети и в информационных системах. В связи с этим в Закон № 149-ФЗ были внесены изменения Федеральным законом от 5 мая 2014 г. № 97-ФЗ, в частности, добавлена ст. 10.1 «Об обязанностях организатора распространения информации в сети Интернет». Дано определение организатора информации как лица, обеспечивающего работу информационных систем и программ, предназначенных для приема, передачи, обработки электронных сообщений пользователей в Интернете. О начале своей деятельности он должен уведомить соответствующий орган. Информацию о фактах таких действий и информацию о пользователях он обязан хранить в течение шести месяцев с момента окончания их и предоставлять

соответствующим органам в целях безопасности Российской Федерации или для оперативно-розыскной деятельности, исполнять требования к оборудованию и программам. Прописано, на кого положения данной статьи не распространяются.

В июле 2016 г. Федеральным законом от 6 июля 2016 г. в Закон № 374-ФЗ были внесены изменения в ст. 10.1 об обязанностях организатора распространения информации. В ч. 3 ст. 10.1 введен п. 2, вступающий в силу с 1 июля 2018 г., обязывающий хранить электронные сообщения пользователей Интернета до шести месяцев после окончания их приема, передачи, доставки, обработки. При дополнительном кодировании сообщений организатор распространения информации обязан представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений.

В связи с введением ст. 10.1 в июле 2014 г. появилась ст. 15.4, регламентирующая порядок ограничения доступа к информационному ресурсу организатора распространения информации в Интернете.

Федеральный закон от 24 ноября 2014 г. № 364-ФЗ изменил ст. 10, обязав владельцев сайтов размещать на них информацию о своем местонахождении, адресе, наименованиях, адресе электронной почты для направления ему заявления о нарушении авторских и (или) смежных прав. Этот же закон ввел ст. 15.6 о порядке ограничения доступа к сайтам, где неоднократно размещалась информация, нарушающая авторские и (или) смежные права, ст. 15.7 — о внесудебных мерах по прекращению нарушения авторских прав в информационно-коммуникационных сетях, в которой прописаны меры и сроки, в которых их можно предпринимать.

В декабре 2014 г. внесены изменения в статьи, касающиеся информационных систем. В частности, информационные системы, используемые государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями, государственными и муниципальными учреждениями должны размещаться на территории Российской Федерации. Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации, вывода из эксплуатации государственных информационных систем утверждает Правительство Российской Федерации.

Защиту персональных данных регулирует новая ст. 15.5, ограничивающая доступ к информации, которая обработана с нарушением законодательства о персональных данных. Согласно этой статье должна быть создана информационная система «Реестр нарушителей прав субъектов персональных данных» и прописан порядок его ведения. В ч. 4 ст. 16 «Защита информации» введен пункт 7, обязывающий базы данных с персональными данными граждан Российской Федерации хранить на территории Российской Федерации.

В 2015 г. введены ст. 10.3 об обязанностях оператора поисковой системы, ст. 12.1, регламентирующая государственное регулирование в сфере использования российских программ для электронных вычислительных машин и баз

данных. В последней прописано создание единого реестра российского программного обеспечения, необходимое для расширения использования российских программ и баз данных и для оказания их владельцам (правообладателям) господдержки. Прописаны требования, которым должно удовлетворять программное обеспечение для включения в реестр. Реестр находится по адресу <https://reestr.minsvyaz.ru/>, и с конца января 2016 г. в него включено более 2800 программ и баз данных.

В 2017 г., данный Закон дополнен новыми статьями. Так, в ст. 10.4 дано определение новостного агрегатора (обработка и распространение новостной информации, доступ более миллиона пользователей Интернета в течение суток) и требования, которые они должны соблюдать. Нельзя допускать использование новостного агрегатора в целях разглашения государственной или иной охраняемой законом тайны, распространения публичных призывов к осуществлению террористической деятельности, экстремистских материалов, а также материалов, пропагандирующих порнографию, насилие и жестокость.

Статья 10.5 теперь содержит определение владельца аудиовизуального сервиса (распространения в Интернете совокупности аудиовизуальных произведений, находящихся на территории Российской Федерации, доступ более миллиона пользователей Интернета в течение суток) и требования, которые необходимо соблюдать. Нельзя допускать использование аудиовизуального сервиса для разглашения государственной или иной тайны, охраняемой законом, для призывов к террористической деятельности, распространения экстремистских материалов, материалов, пропагандирующих порнографию, насилие и жестокость, осуществлять классификацию аудиовизуальных произведений, чтобы не причинить вред детям.

С октября 2017 г. начала действовать ст. 15.6-1 о порядке ограничения доступа к копиям заблокированных сайтов, а с 1 ноября — ст. 15.8, регламентирующая меры для противодействия использованию информационных ресурсов и сетей, через которые осуществляется доступ к ресурсам и сетям, ограничен на территории РФ.

Таким образом, изменения в Законе № 149-ФЗ направлены на усиление информационной безопасности, а следовательно, развитие и совершенствование всей системы национальной безопасности страны по таким направлениям, как защита каналов связи, сетевая и эксплуатационная безопасность, компьютерная безопасность, административная безопасность. Нормативно-правовое усиление по этим направлениям способно комплексно решать ключевые задачи по сохранению и защите информационных ресурсов России, укреплению ее международного авторитета, повышению эффективности работы по снижению криминальной напряженности, защите прав, свобод и безопасности российских граждан в системе их информационно-коммуникационных взаимодействий. В результате компонент информационной безопасности в системе национальной безопасности приобретает особый вес и актуальность по сравнению с другими ее элементами.

Главная тенденция, на которую следует обратить внимание в проведенном анализе, — это обозначение законодателем особой роли государства в системе защиты культурно-исторических и демократических ценностей общества. Данное обстоятельство во многом предопределяет и специфические требования, которые будет предъявлять общество к уровню компетентности и гражданской ответственности государственных служащих, руководящих реализацией политики и принимающих решения в сфере информационной безопасности России.

Библиографический список

1. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31 дек. 2015 г. № 683 // СЗ РФ. 2016. № 1 (ч. II). Ст. 212.
2. *Брянцева О.В., Филиппова Е.А.* Развитие электронного правительства в России и его представление в средствах массовой информации // Право, наука, образование: традиции и перспективы: сборник статей по материалам международной научно-практической конференции, посвященной 85-летию Саратовской государственной юридической академии (в рамках VII Саратовских правовых чтений, Саратов, 29–30 сентября 2016 г.) / отв. ред. Е.В. Вавилин [и др.]. Саратов, 2016. С. 174–175.
3. *Архангельская Е.В.* Представление и обработка данных о преступлениях с помощью компьютерной техники // Вестник Саратовской государственной юридической академии. 2016. № 1 (108). С. 235–241.
4. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203 // СЗ РФ. 2017. № 20. Ст. 2901.
5. Информационная безопасность систем организационного управления: Теоретические основы / под ред. Н. Кузнецова, В. Кульбы. М., 2006.
6. *Асланов Р.М.* Зарубежный опыт правового регулирования обеспечения информационной безопасности // Политика и общество. 2012. № 2 (86).
7. *Тереженко Л.К.* Модернизация информационных отношений и информационного законодательства. М., 2013.
8. *Полякова Т.А., Акулова Е.В.* Развитие законодательства в области обеспечения информационной безопасности: тенденции и основные проблемы // Право. Журнал Высшей школы экономики. 2015. № 3. С. 4–17.
9. Об информации, информатизации и защите информации: Федер. закон от 20 февр. 1995 г. № 24-ФЗ // СЗ РФ. 1995. № 8. Ст. 609.
10. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сент. 2000 г. № Пр-1895) // Российская газета. 2000. № 187, 28 сент.
11. Об информации, информационных технологиях и о защите информации: Федер. закон от 27 июля 2006 г. № 149-ФЗ (в ред. от 19 дек. 2016 г. с изм. и доп. от 1 янв. 2017 г.) // СЗ РФ. 2006 г. № 31 (ч. 1). Ст. 3448.
12. *Брянцева О.В., Филиппова Е.А.* Обзор нормативно-правовых актов, регулирующих электронное правительство // Современные тенденции развития науки и технологий: сборник по материалам XXIII международной научно-практической конференции, г. Белгород, 28 февраля 2017 г. Белгород, 2017. № 2-6. С. 22–28.
13. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 дек. 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074.