DOI: 10.17803/1729-5920.2022.184.3.119-127

И. А. Трофимец*

К вопросу о понятийном аппарате правового института информационной безопасности в Испании

Аннотация. Статья посвящена понятийному аппарату в связи с важностью его предметной системообразующей роли в праве. Автор обращает внимание на то, что в специальной терминологии проявляется функциональная обособленность отраслей права и правовых институтов. В поле зрения автора — особый институт информационного права информационная безопасность (кибербезопасность). Объектом исследования является глоссарий терминов кибербезопасности, представленный в ст. 3 Королевского указа-закона 12/2018 от 7 сентября «О безопасности сетей и информационных систем» и достижения доктрины по этому вопросу. Предпринята попытка доказать, что законодательное дефинирование нуждается в научном комментировании и толковании, что значительно облегчает правоприменительную деятельность, но никоим образом не подменяет нормотворчество. Собственная терминологическая база отрасли права и правового института способствует эффективному правовому регулированию общественных отношений, составляющих их предмет. Сделан вывод, что информационная безопасность охватывает защиту как информационных систем, так сетей и устройств (компьютеров), представляя собой синтез организационных, технических и юридических мер. В статье подчеркивается, что использование информационно-коммуникационных технологий (ИКТ) способствует беспрецедентному развитию обмена информацией, которое наряду с удобствами несет в себе серьезные риски и угрозы для глобализованного мира. И именно институт кибербезопасности призван защитить информационное общество от разного рода правонарушений в Интернете. В заключение указывается, что, хотя понятийный аппарат института информационной безопасности сформирован, по-прежнему остро стоит проблема денотации и коннотации правовых понятий, связанная с правильным использованием специальных юридических (или ставших юридическими) терминов, требующая решения на законодательном уровне.

Ключевые слова: кибербезопасность; информационная безопасность; безопасность информационных систем и сетей; организационные меры; юридические меры; технические меры; понятийный аппарат; правовой институт; юридические термины; технические термины.

Для цитирования: *Трофимец И. А.* К вопросу о понятийном аппарате правового института информационной безопасности в Испании // Lex russica. — 2022. — Т. 75. — № 3. — С. 119–127. — DOI: 10.17803/1729-5920.2022.184.3.119-127.

On Conceptual Apparatus of the Legal Institute of Information Security in Spain

Irina A. Trofimets, Cand. Sci. (Law), Associate Professor, Embassy of the Russian Federation in the Kingdom of Spain
Velasquez Street, 155, Madrid, Kingdom of Spain, 28002
kosareva-khv@mail.ru

Abstract. The paper is devoted to the conceptual apparatus in connection with the importance of its subject system-forming role in law. The author draws attention to the fact that the functional isolation of branches of law and legal institutions is manifested in special terminology. The author considers a special institute of

* *Трофимец Ирина Александровна,* кандидат юридических наук, доцент, Посольство Российской Федерации в Королевстве Испания
Ул. Веласкеса, д. 155, г. Мадрид, Королевство Испания, 28002
kosareva-khv@mail.ru

information law, namely information security (cybersecurity). The object of the study is a glossary of cybersecurity terms, presented in Article 3 of the Royal Decree-Law 12/2018 of September 7 «On the security of networks and information systems» and the achievements of the doctrine on this issue. An attempt has been made to prove that legislative definition needs scientific commentary and interpretation, which greatly facilitates law enforcement activities, but in no way replaces rulemaking. The proprietary terminology base of the branch of law and the legal institute contributes to the effective legal regulation of public relations that make up their subject. It is concluded that information security covers the protection of both information systems and networks and devices (computers), representing a synthesis of organizational, technical and legal measures. The paper emphasizes that the use of information and communication technologies (ICT) contributes to the unprecedented development of information exchange, which, along with convenience, carries serious risks and threats to the globalized world. It is the cybersecurity institute that is designed to protect the information society from various kinds of offenses on the Internet. In conclusion, it is indicated that, although the conceptual apparatus of the Institute of Information Security has been formed, there is still an acute problem of denotation and connotation of legal concepts associated with the correct use of special legal (or legal) terms that require solutions at the legislative level.

Keywords: cybersecurity; information security; security of information systems and networks; organizational measures; legal measures; technical measures; conceptual apparatus; legal institution; legal terms; technical terms.

Cite as: Trofimets IA. K voprosu o ponyatiynom apparate pravovogo instituta informatsionnoy bezopasnosti v Ispanii [On Conceptual Apparatus of the Legal Institute of Information Security in Spain]. *Lex russica*. 2022;75(3):119-127. DOI: 10.17803/1729-5920.2022.184.3.119-127. (In Russ., abstract in Eng.).

Становление глобального информационного общества и переход к обществу знаний требует соответствующего правового регулирования новых общественных отношений. Информационное право призвано решить эту проблему. Как любая отрасль права, информационное право представляет собой упорядоченную систему правовых норм, сформированных в правовые институты. Немаловажное место в системе информационного права занимает институт *безопасности сетей и информационных систем (информационная безопасность, кибербезопасность)*. Безопасность сетей и информационных систем является серьезной и общей проблемой как на международном, так и национальном уровне и предполагает интегральный подход к ее решению[1]. Так, например, имплементация в информационное право Испании Директивы (ЕС) 2016/1148 Европейского парламента и Совета от 06.07.2016[2] способствует применению мер, направленных на обеспечение высокого общего уровня безопасности сетей и информационных систем. Но особую роль в правовой системе играет терминологическая база, а именно нормы-дефиниции, содержащиеся в нормативных правовых актах, и определения, сформулированные учеными. Правильная концепция понятийного аппарата является первой ступенью в эффективном правовом регулировании. Информационное право — это молодая отрасль права, объективно имеет место необходимость обозначить и объяснить новые общественные отношения, являющиеся ее предметом. Понятийный аппарат отрасли информационного права и ее правовых институтов — явление динамическое, изменяющееся параллельно с юридической и технической лексикой, призванное материально и функционально обеспечить защиту информационных систем, сетей и специального оборудования (компьютеров) и гарантировать цифровые права гражданам и иным субъектам правоотношений. По мнению И. Л. Бачило, «упорядочение понятийного аппарата как связующего и вместе с тем дифференцирующего механизма в структуре правовой системы и практики применения актов и норм законодательства в современных условиях не только

[1] *Robles Carrillo M.* Seguridad de redes y sistemas de información en la Unión Europea: ¿un enfoque integral? // Revista de Derecho Comunitario Europeo 2018. № 22 (60). Págs. 563–600. ISSN 1138-4026.

[2] Директива № 2016/1148 Европейского парламента и Совета Европейского Союза «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» [рус., англ.] (вместе с Требованиями к группам реагирования на инциденты, связанные с компьютерной безопасностью (CSIRTs) и их задачами, Типами предприятий и цифровых услуг) (принята в г. Страсбурге 06.07.2016).

имеет технико-технологическое значение, но и является предметом внимания информационной безопасности, а в целом определяет эффективность и культуру правовой науки и законодательства»[3].

Большой вклад в теоретическую разработку понятийного аппарата института кибербезопасности внесли испанские ученые Р. Барзаналлана, М. Х. Карасо Либана, А. Х. Кастро, Д. Фернандес Бермехо, Г. Мартинес Атьенс, Х. Лосано Мираллес, Н. Марилена Алина, А. Мартин Ромеро, М. Роблес Каррильо, Х. Салгейру, Х. Тобал[4] и др., уделявшие внимание дефинированию специальных юридических терминов, логико-лингвистической процедуре раскрытия содержания через выделение существенных характерных признаков новых правовых категорий.

Безусловно, прогрессивные достижения ученых-юристов законодатели используют в своей нормотворческой деятельности. Ярким примером является испанская правовая система, где доктрина может служить источником права для регулирования общественных отношений. Представляется, что доктрина может быть отнесена к косвенным источникам права, поскольку основывается на действующих правовых нормах. Аргументы юристов-ученых правоприменитель может использовать для правильного толкования правовых норм, значение которых неоднозначно или входит в противоречие с другими правовыми нормами и требует дополнительного разъяснения, а также в случае отсылки к спорному юридическому понятию и отсутствия в законе его определения. Для внесения ясности и разрешения правовых коллизий возможно обратиться к системе знаний, разработанной авторитетными учеными-юристами.

Национальная стратегия кибербезопасности в Испании[5] согласована со Стратегией национальной безопасности, в которой определяются цели и меры по достижению и поддержанию высокого уровня защиты сетей и информационных систем. Базовым нормативным правовым актом института информационной безопасности является упомянутый ранее Королевский указ-закон 12/2018 от 7 сентября «О безопасности сетей и информационных систем», в ст. 3 которого определены следующие важные юридические термины: основные услуги, цифровые услуги, операторы основных услуг, поставщики цифровых услуг, сети, информационные системы, цифровые данные и другие, которые составляют понятийный аппарат правового института информационной безопасности. Законодательно в терминологическую основу включены более 20 дефиниций, позволяющих гармонизировать правовые нормы и унифицировать правоприменительную деятельность. Как общая тенденция отмечается слияние в законодательстве юридических и технических терминов. Вместе с тем некоторые категории настолько сложные для понимания, что выразить их через дефиниции просто невозможно, требуется особое разъяснение, толкование специальных слов, словосочетаний, объясняющих их, другими словами, не исключаются ситуации, когда одно неизвестное выражается через другое, которому также необходимо дать понятие, и нередко на уровне закона, для того чтобы избежать терминологической путаницы. Неко-

---

[3] *Бачило И. Л.* Понятийный аппарат информационного права и система обеспечения информационной безопасности // Труды Института государства и права РАН. 2016. № 3. С. 8.

[4] *Barzanallana R.* Introducción a la Seguridad Informática. Murcia, 2021. 65 p. ; *Caraso Liebana M. J.* El Derecho de la protección de datos. Madrid, 2021. 169 p. ; *Castro J. A.* Opinión: La ciberseguridad: el reto de la transformación digital // URL: https://www.america-retail.com/opinion/opinion-la-ciberseguridad-el-reto-de-la-transformacion-digital/ (дата обращения: 22.12.2021) ; *Fernández Bermejo D., Martínez Atienza G.* Ciberseguridad, Ciberespacio y Ciberdelincuencia. Pamplona, 2018. 236 p. ; *Lozano Miralles J.* La lucha contra el terrorismo en el marco del sistema de seguridad nacional. Pamplona, 2021. 411 p. ; *Marilena Alina N.* Análisis a la Ley de Ciberseguridad ¿Qué supone su aplicación? // URL: https://www.dpoitlaw.com/analisis-a-la-ley-de-ciberseguridad-que-supone-su-aplicacion/ (дата обращения: 22.12.2021) ; *Martín Romero A.* Seguridad Informática y Alta Disponibilidad. Zaragoza, 2021. 403 p. ; *Robles Carrillo M.* Op. cit. ; *Salgueiro J.* Comentarios sobre la ciberseguridad en la seguridad privada // URL: https://www.interempresas.net/Ciberseguridad/Articulos/240015-Comentarios-sobre-la-ciberseguridad-en-la-seguridad-privada.html (дата обращения: 22.12.2021) ; *Tobal J.* Ciberseguridad. Madrid, 2020. 258 p.

[5] Официально используемый термин *кибербезопасность* — полисемичный термин, обозначающий правовой институт отрасли права (информационного права) и элемент особых публичных общественных отношений (национальной безопасности).

торые понятия не истолковываются законодателем ввиду их общепринятой коннотации.

Представляется, что изучение понятийного аппарата правового института *безопасность сетей и информационных систем* следует начать с разъяснения категорий «*безопасность сетей и информационных систем*», «*информационная безопасность*» и «*кибербезопасность*»[6]. Испанский законодатель использует терминологию *безопасность сетей и информационных систем* и детерминирует эту категорию как способность сетей и информационных систем противостоять с определенным уровнем надежности любым действиям, которые ставят под угрозу доступность, подлинность, целостность или конфиденциальность данных, хранящихся, передаваемых или обрабатываемых, а также соответствующих услуг, предлагаемых такими сетями и информационными системами или доступных через них (п. «в» ст. 3 Королевского указа-закона 12/2018 от 7 сентября «О безопасности сетей и информационных систем»)[7]. С точки зрения Н. Марилены Алины[8], категории «*безопасность сетей и информационных систем*», «*кибербезопасность*», *а также* «*информационная безопасность*» являются идентичными и представляют собой набор правил, процедур и инструментов, цель которых гарантировать доступность, целостность, конфиденциальность, а также правильное использование информации, содержащейся в информационных системах, и защиту сетей. По мнению А. Х. Кастро, следует применять исключительно термин «*кибербезопасность*». Кроме того, ученый отмечает, что сегодня именно *кибербезопасность* является одним из краеугольных камней процесса цифровой трансформации, в котором находятся государства, общество и граждане, и решение этих вопросов должно быть совместным[9]. Особенно обострились проблемы *кибербезопасности* в период пандемии COVID-19, когда ИКТ, обеспечивая социальные связи во время массовых ограничений и изоляции по мотивам здравоохранения, стали наиболее подвержены новым вызовам и угрозам, увеличивается число инцидентов[10].

Кибербезопасность может быть определена как защита *информации в цифровом формате (цифровой информации)* за счет комплекса организационных, технических и юридических мер. За миром Интернета стоят люди и (или) их объединения, и право призвано регулировать отношения между ними, имеющими доступ к ИКТ. Это особые субъекты правоотношений, чей юридический статус отличается многообразием (государство, муниципальные образования и частные лица). Искусственный интеллект субъектом правоотношений пока не признается, отнесен к категории объектов.

Дискуссионным с научной точки зрения остается вопрос об объектах правоотношений. Думается, что объектом защиты являются сама *информация,* а также *информационные системы и сети.* Термин «информация» не нашел на территории Испании прямого законодательного дефинирования, он отождествлен с категорией «цифровые данные», которая также не имеет формального закрепления, поскольку считается общепринятой и устоявшейся, представляя собой сведения, получаемые, хранимые, передаваемые с помощью ИКТ. Р. Барзаналлана, рассуждая об этимологии слова «информация» (от лат. *informatio* — «формировать ум», «дисциплинировать», «инструктировать», «учить»), выражает сомнения в тождественности его происхождения и современной интерпретации[11]. Вместе с тем многие понятия, сопутствующие *информации, информационным системам и сетям* как объектам информационной безопасности, официально определены, что позволяет правильно применять эти правовые категории.

Наиболее связаны с объектом информационной безопасности понятия, закрепленные в законе, — это *основные услуги* и *цифровые услуги,* которые можно определить как особый вид деятельности специальных субъектов, связанный со сбором, обработкой, хранением, передачей и распространением информации

---

6 Дискуссию по вопросу тождественности категорий «информационная безопасность» и «кибербезопасность» см.: *Трофимец И. А.* Информационная безопасность в информационной сфере записей актов гражданского состояния // Вестник ВГУ. Серия «Право». 2021. № 3 (46).

7 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información // BOE. Núm. 218. 08.09.2018. Pág. 87675–87696.

8 *Nastasache Marilena Alina*. Op. cit.

9 *Castro J. A.* Op. cit.

10 *Tobal J.* Op. cit.

11 *Barzanallana R.* Op. cit. P. 1.

с применением ИКТ, требующий правовой охраны. *Основные услуги* включены в стратегические секторы, относящиеся к критическим инфраструктурам, это те услуги, которые необходимы для поддержания первоочередных социальных функций, связанных с охраной здоровья, личной безопасностью, экономическим благополучием граждан и эффективным функционированием государственных органов власти; их предоставление зависит от сетей и информационных систем. С точки зрения информационного права *основные услуги* также являются цифровыми (электронными) по своему формату.

Цифровые услуги представляют собой онлайн-рынки, онлайн-поисковые системы и сервисы облачных вычислений. В отношении видов цифровых услуг содержится отсылочная норма, их перечень закреплен в приложении «а» к Закону 34/2002 от 11 июля «Об услугах информационного общества и электронной коммерции»[12]. В качестве разновидности испанский законодатель выделяет *услугу облачных вычислений,* под которой понимается цифровая услуга, обеспечивающая доступ к модульному и гибкому набору вычислительных ресурсов, используемых совместно.

Технологические достижения в области информации привели к появлению новых объектов, ценностей и активов, подлежащих дефинированию и нуждающихся в правовом регулировании и защите[13]. Категории, имеющие прямое отношение к информационным системам и сетям, широко представлены в Королевском указе-законе, что облегчает задачу правоприменительных органов при рассмотрении вопросов информационной безопасности. Многие специальные понятия получили разъяснение. *Сети электронных коммуникаций* или *информационные сети* — это техническое устройство или группа устройств, взаимосвязанных друг с другом, одно или несколько из которых выполняют с помощью программ автоматическую обработку *цифровых данных*, то есть сведений (*информации*), хранящихся, обрабатываемых, восстанавливающихся или передающихся с помощью технических устройств (машин).

Однако не все технические термины, встречающиеся в юридической практике, получили официальное детерминирование. *Точка обмена интернет-трафиком (Internet Exchange Point — IXP)* — сетевая установка, соединяющая более двух независимых автономных систем, в основном для облегчения обмена интернет-трафиком. *IXP* позволяет автономным системам подключаться друг к другу, не требуя прохождения интернет-трафика между любой парой участвующих автономных систем через третью автономную систему, а также без изменения или иного вмешательства в такой трафик. *Система доменных имен (Domain Name System — DNS)* — иерархически распределенная система, которая отвечает на запросы, предоставляя информацию, связанную с доменными именами, в частности относящуюся к идентификаторам, используемым для поиска и адресации компьютеров в Интернете. *Реестр доменных имен* — организация, которая управляет и направляет реестр доменных имен Интернета в конкретном домене. *Интернет-рынок* — это спрос-предложения цифровых услуг, которые позволяют потребителям и предпринимателям (поставщикам-исполнителям) заключать договоры о продаже или предоставлении онлайн-услуг либо на определенном веб-сайте рыночной онлайн-услуги, либо на веб-сайте предпринимателя (поставщика-исполнителя). *Интернет-поисковая система* — цифровая служба (сервис), позволяющая пользователям выполнять поиск, в принципе, на всех веб-сайтах с помощью запроса по теме в форме ключевого слова, фразы или другого типа записи, результатом запроса является указание ссылок, по которым можно найти информацию, относящуюся к запрашиваемому контенту. Как видно из приведенных определений, правовые категории являются по происхождению техническими. На юридические проблемы, возникающие при администрировании сетевых информационных систем, обращал внимание А. Мартин Ромеро в работе «Безопасность и высокая доступность», подчеркивая важность официального разъяснения технических понятий[14]. В отношении таких терминов, как «*технический стандарт*» и «*техническая спецификация*»,

[12] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico // BOE. Núm. 166. 12.07.2002.

[13] *Fernández Bermejo D., Martínez Atienza G.* Op. cit. P. 36.

[14] *Martín Romero A.* Op. cit.

используются международные определения, закрепленные соответственно в ст. 2.1 и 2.4 Регламента (ЕС) № 1025/2012 Европейского парламента и Совета от 25.10.2012 «О европейской стандартизации»[15].

Как отмечалось, круг лиц, в отношении которых обеспечивается информационная безопасность, — это специальные субъекты, имеющие доступ к ИКТ. *Оператор основных услуг* имеет принадлежность к Испании, когда его резиденция или зарегистрированный офис находится на национальной территории, при условии что они совпадают с местом, где административное управление его деятельностью централизовано. Аналогичным образом Королевский указ-закон должен применяться к основным услугам, которые операторы-резиденты или операторы-нерезиденты предлагают через постоянное представительство, расположенное в Испании. Операторы сетей и услуг цифровых (электронных) коммуникаций и доверенные поставщики цифровых (электронных) услуг, которые не определены в качестве критических операторов, не подпадают под юрисдикцию этого законодательного акта. Закон 8/2011 от 28 апреля[16], устанавливающий меры по защите критически важных инфраструктур, содержит критерии отнесения субъекта к категории «*оператор основных услуг*». Список основных услуг и операторов этих услуг обновляется для каждого сектора раз в два года согласно отраслевым стратегическим планам. Когда оператор основных услуг предлагает услуги в других странах Европейского Союза, он обязан проинформировать о своем намерении единые контактные пункты этих государств. В случае если операторы основных услуг обозначены как критически важные операторы независимо от стратегического сектора, в котором сделано такое назначение, то контролирующими и надзорными органами выступают Секретариат государственной безопасности, Министерство внутренних дел через Национальный центр защиты инфраструктуры и кибербезопасности (*CNPIC*). Другими координирующими органами являются Национальный криптологический центр (*CCN-CERT*) и Национальный институт кибербезопасности Испании (*INCIBE-CERT).* Особую компетенцию имеет Министерство обороны Испании в лице специализированной структуры реагирования *(ESPDEF-CERT).* В случае если оператор основных услуг не является критически важным оператором, то координирующим и контролирующим выступает соответствующий отраслевой орган государственной власти. Компетентные структуры должны координировать свои действия друг с другом и с различными отраслевыми органами, чтобы избежать дублирования требуемых обязательств и облегчить их выполнение операторами основных услуг. В качестве тождественного термина «*оператор основных услуг*» используется «*критический оператор*». Частным случаем является «*критически важный оператор*». Думается, что такой подход оправдан, поскольку характеризует сферу деятельности *оператора основных услуг* — это критическая инфраструктура, что позволяет избегать ошибок с квалификацией этих субъектов, а выделение внутри нее *важной критической инфраструктуры* указывает на особую значимость отдельных сфер государственной деятельности. Представляется, что организация деятельности субъектов ИКТ в режиме благоприятствования имеет важное значение для информационного общества, в том числе за счет надежной системы безопасности, наделением органов власти определенными полномочиями в сфере цифровизации.

Поставщики цифровых услуг — это организации, которые учреждены в Европейском Союзе и имеют зарегистрированный офис в Испании, а также те, которые не созданы в Европейском Союзе, но назначают в Испании своего представителя для соблюдения Директивы (ЕС) 2016/1148 Европейского парламента и Совета от 06.07.2016, за исключением постав-

[15] Регламент № 1025/2012 Европейского парламента и Совета Европейского Союза «О европейской стандартизации, изменении Директив 89/686/ЕЭС и 93/15/ЕЭС Совета ЕС и Директив 94/9/ЕС, 94/25/ЕС, 95/16/ЕС, 97/23/ЕС, 98/34/ЕС, 2004/22/ЕС, 2007/23/ЕС, 2009/23/ЕС и 2009/105/ЕС Европейского парламента и Совета ЕС и отмене Решения 87/95/ЕЭС Совета ЕС и Решения 1673/2006/ЕС Европейского парламента и Совета ЕС» [рус., англ.] (вместе с Европейскими организациями..., Требованиями к идентификации технических условий в области информационных и коммуникационных технологий, Заинтересованными организациями, имеющими право на финансирование, Корреляционной таблицей) (принят в г. Страсбурге 25.10.2012).

[16] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas // BOE. Núm. 102. 29.04.2011.

щиков цифровых услуг, относящихся к категории «малый бизнес». Поставщики цифровых услуг должны сообщать о своей деятельности компетентному органу в течение трех месяцев с момента ее начала. *Представитель* — это физическое или юридическое лицо, учрежденное в Европейском Союзе, которое уполномочено действовать от имени поставщика цифровых услуг, нерезидента Европейского Союза, и которому национальный компетентный орган или *CSIRT* предъявляет требования в отношении обязательств, возлагаемых на поставщика цифровых услуг.

Цифровые права и цифровые данные (цифровая информация) — сравнительно новые правовые категории, недавно получившие официальное разъяснение. Особое место в институте кибербезопасности занимает сегмент защиты *персональных данных граждан*. Определение *персональных данных граждан* относится к категории т.н. «резиновых», поскольку невозможно исчерпывающе обозначить, какие сведения их составляют. Любая информация личного характера, затрагивающая частную или семейную жизнь гражданина, является его персональными данными. Согласно ст. 18.4 Конституции Испании[17], «закон должен ограничивать использование информационных технологий, чтобы гарантировать честь, личную и семейную тайну граждан и полное осуществление права». С точки зрения Х. Сальгейру, «...эволюция информационных и коммуникационных технологий, особенно с развитием Интернета, означает, что сети и информационные системы в настоящее время играют решающую роль в обществе, что не исключает обеспечение кибербезопасности граждан, их данных»[18]. М. Х. Карасо Либана предлагает уделять особое внимание при оказании цифровых услуг защите персональных данных, что, по его мнению, приобретает актуальность в период расширения рынка таких услуг[19]. И действительно, в рамках института кибербезопасности в Испании уделено много внимания защите *персональных граждан* как особого объекта правовой охраны и предмета Органического закона 3/2018 от 5 декабря «О защите персональных данных и гарантии цифровых прав»[20]. Данный нормативный правовой акт призван адаптировать правовую систему Испании к Регламенту (ЕС) 2016/679 Европейского парламента и Совета от 27.04.2016[21], касающемуся защиты физических лиц в отношении обработки их персональных данных и свободного обращения этих данных. К сожалению, в данном нормативном правовом акте отсутствуют нормы-дефиниции, которые можно было бы имплементировать в национальную правовую систему Испании.

Вопросы нарушения информационной безопасности раскрываются через специальную терминологию. *Риск* — любые идентифицируемые обстоятельства или факты, которые могут отрицательно повлиять на безопасность сетей и информационных систем. Риск можно количественно оценить как вероятность материализации угрозы, оказывающей воздействие с точки зрения работоспособности, физической целостности субъектов и объектов. *Инцидент* — неожиданное или нежелательное событие с последствиями в виде ущерба безопасности сетей и информационных систем. Обязательна оценка воздействия инцидента на предоставление основной услуги и (или) цифровой услуги на протяженность пространства (территории), на которое он может повлиять, выявление зависимости других стратегических секторов от основных услуг и влияние с точки зрения степени его продолжительности на экономическую и социальную деятельность, а также государственную и общественную безопасность. *Управление инцидентами* — процедуры, применяемые для обнаружения, анализа и ограничения инцидента, а также реагирования на него. Создаются специальные группы реагирования на инциденты компьютерной безопасности (*CSIRT*).

---

17 Constitución Española // BOE. Núm. 311. 29.12.1978.

18 *Salgueiro J.* Op. cit.

19 См.: Caraso *Liebana M. J.* Op. cit.

20 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales // BOE. Núm. 294. 06.12.2018. Pág. 119788–119857.

21 Регламент Европейского парламента и Совета Европейского Союза 2016/679 от 27.04.2016 о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных) // URL: http://www.eurasiancommission.org/ru/act/texnreg/depsanmer/consumer_rights/Documents/pdf (дата обращения: 22.01.2022).

Все законодательные дефиниции можно разделить условно на группы. Первую группу представляют определения объектов и связанных с ними категорий (цифровые данные, основные услуги, цифровые услуги, информационные системы, сети и др.). Ко второй относятся дефиниции субъектов информационной безопасности (оператор основных услуг, поставщик цифровых услуг, контрольно-надзорные органы и организации и др.). Третью группу составляют технические термины, которые получили юридическое признание (доменные имена, реестр доменных имен, точка обмена интернет-трафиком и др.). Особое место занимают понятия, разъясняющие нарушение кибербезопасности (риск, угроза, инцидент, управление инцидентами и др.). Понятийный аппарат, сформированный из легальных дефиниций или т.н. норм-определений, тем не менее в ряде случаев нуждается в расширительном толковании. По этой причине наиболее сложные и важные термины, а также отношения, связанные с ними, детально регламентируются в других законодательных актах или научных работах. Это касается таких категорий, как основные услуги, цифровые услуги, оператор основных услуг, поставщик цифровых услуг. Испанский законодатель использует именно такой прием юридической техники — дает дополнительное объяснение ранее детерминированным категориям. В качестве недостатка можно отметить, что такой подход усложняет содержание нормативного правового акта и его применение на практике.

БИБЛИОГРАФИЯ

1. *Бачило И. Л.* Понятийный аппарат информационного права и система обеспечения информационной безопасности // Труды Института государства и права РАН. — 2016. — № 3. — С. 5–16.
2. Понятийный аппарат в информационном праве / отв. ред. И. Л. Бачило, В. Б. Наумов, Т. А. Полякова. — М., 2017. — 264 с.
3. *Трофимец И. А.* Информационная безопасность в информационной сфере записей актов гражданского состояния // Вестник ВГУ. Серия «Право». — 2021. — № 3 (46).
4. Цифровая трансформация: вызовы праву и векторы научных исследований : монография / под общ. ред. А. Н. Савенкова ; отв. ред. Т. А. Полякова, А. В. Минбалеев. — М. : РГ-Пресс, 2021. — 344 с.
5. *Barzanallana R.* Introducción a la Seguridad Informática. — Murcia, 2021. — 65 p.
6. *Caraso Liebana M. J.* El Derecho de la protección de datos. — Madrid, 2021. — 169 p.
7. *Castro Jose A.* Opinión: La ciberseguridad: el reto de la transformación digital // URL: https://www.america-retail.com/opinion/opinion-la-ciberseguridad-el-reto-de-la-transformacion-digital/ (дата обращения: 22.12.2021).
8. *Fernández Bermejo D., Martínez Atienza G.* Ciberseguridad, Ciberespacio y Ciberdelincuencia. — Pamplona, 2018. — 236 p.
9. *Lozano Miralles J.* La lucha contra el terrorismo en el marco del sistema de seguridad nacional. — Pamplona, 2021. — 411 p.
10. *Marilena Alina N.* Análisis a la Ley de Ciberseguridad ¿Qué supone su aplicación? // URL: https://www.dpoitlaw.com/analisis-a-la-ley-de-ciberseguridad-que-supone-su-aplicacion/ (дата обращения: 22.12.2021).
11. *Martín Romero A.* Seguridad Informática y Alta Disponibilidad. — Zaragoza, 2021. — 403 p.
12. *Robles Carrillo M.* Seguridad de redes y sistemas de información en la Unión Europea: ¿un enfoque integral? // Revista de Derecho Comunitario Europeo. — 2018. — № 22 (60). — P. 563–600. — ISSN 1138-4026.
13. *Salgueiro J.* Comentarios sobre la ciberseguridad en la seguridad privada // URL: https://www.interempresas.net/Ciberseguridad/Articulos/240015-Comentarios-sobre-la-ciberseguridad-en-la-seguridad-privada.html (дата обращения: 22.12.2021).
14. *Tobal J.* Ciberseguridad. — Madrid, 2020. — 258 p.

Материал поступил в редакцию 30 января 2022 г.

REFERENCES

1. Bachilo IL. Ponyatiynyy apparat informatsionnogo prava i sistema obespecheniya informatsionnoy bezopasnosti [Conceptual apparatus of information law and information security system]. *Trudy Instituta gosudarstva i prava RAN [Proceedings of the Institute of State and Law of the Russian Academy of Sciences].* 2016;3:5-16. (In Russ.)
2. Bachilo IL, Naumov VB, Polyakova TA. Ponyatiynyy apparat v informatsionnom prave [Conceptual apparatus in information law]. Moscow; 2017. (In Russ.)
3. Trofimets IA. Informatsionnaya bezopasnost v informatsionnoy sfere zapisey aktov grazhdanskogo sostoyaniya [Information security in the information sphere of civil status records]. *Vestnik VGU. Seriya «Pravo» [Proceedings of Voronezh State University. Series «Law»].* 2021;3(46). (In Russ.)
4. Savenkov AN, Polyakova TA, Minbaleev AV, editors. Tsifrovaya transformatsiya: vyzovy pravu i vektory nauchnykh issledovaniy: monografiya [Digital transformation: Challenges to law and vectors of scientific research. A monograph]. Moscow: RG-Press; 2021. (In Russ.)
5. Barzanallana R. Introducción a la Seguridad Informática. Murcia; 2021.
6. Caraso Liebana MJ. El Derecho de la protección de datos. Madrid; 2021.
7. Castro Jose A. Opinión: La ciberseguridad: el reto de la transformación digital. Available from: https://www.america-retail.com/opinion/opinion-la-ciberseguridad-el-reto-de-la-transformacion-digital [cited 2021 December 22].
8. Fernández Bermejo D, Martínez Atienza G. Ciberseguridad, Ciberespacio y Ciberdelincuencia. Pamplona; 2018.
9. Lozano Miralles J. La lucha contra el terrorismo en el marco del sistema de seguridad nacional. Pamplona; 2021.
10. Marilena Alina N. Análisis a la Ley de Ciberseguridad ¿Qué supone su aplicación? Available from: https://www.dpoitlaw.com/analisis-a-la-ley-de-ciberseguridad-que-supone-su-aplicacion [cited 2021 December 22].
11. Martín Romero A. Seguridad Informática y Alta Disponibilidad. Zaragosa; 2021.
12. Robles Carrillo M. Seguridad de redes y sistemas de información en la Unión Europea: ¿un enfoque integral? *Revista de Derecho Comunitario Europeo.* 2018;22(60);563-600. ISSN 1138-4026.
13. Salgueiro J. Comentarios sobre la ciberseguridad en la seguridad privada. Available from: https://www.interempresas.net/Ciberseguridad/Articulos/240015-Comentarios-sobre-la-ciberseguridad-en-la-seguridad-privada.html [cited 2021 December 22].
14. Tobal J. Ciberseguridad. Madrid; 2020.