Анатолий А. Малюк[1], Андрей В. Морозов[2]
[1]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
[2]Всероссийский государственный университет юстиции (РПА Минюста России),
Азовская ул., 2, корп. 1, г. Москва, 117638, Россия
[1]e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508
[2]e-mail: av_morozov@list.ru, https://orcid.org/0000-0002-5016-0833

ФОРМИРОВАНИЕ ЦИФРОВОЙ ЭКОНОМИКИ И ПРОБЛЕМЫ СОВЕРШЕНСТВОВАНИЯ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

DOI: http://dx.doi.org/10.26583/bit.2019.4.02

Аннотация. Нормативно-правовое регулирование является одним из трех основных «китов», на которых покоится область обеспечения информационной безопасности личности, общества и государства. Недаром, начиная с 1992 года, этим вопросам уделяется пристальное внимание на всех уровнях федеральной и региональной власти Российской Федерации. Им посвящено значительное количество научных публикаций таких отечественных авторов, как И.Л. Бачило, А.А. Стрельцов, Ю.М. Батурин, Т.А. Полякова и др. Ключевым моментом в решении указанных вопросов, очевидно, является формирование целостной концепции построения законодательства в сфере обеспечения информационной безопасности, учитывающей динамический характер изменений, происходящих в других «китах» отрасли, а именно, в области технологии и гуманитарных аспектов (формирования в обществе культуры информационной безопасности). Таким образом, концепция нормативно-правового обеспечения должна быть увязана с политикой информационной безопасности как важнейшим элементом стратегии национальной безопасности государства. Рассмотрению подходов к формированию такой концепции и посвящена данная статья. В статье последовательно рассматриваются проблемы структуризации предметной области обеспечения информационной безопасности, направления правового регулирования деятельности в этой сфере, уровни соответствующего правового обеспечения. В заключение формулируются самые острые на сегодняшний день проблемы, требующие безотлагательного решения.

Ключевые слова: информационная безопасность, нормативно-правовое регулирование, политика информационной безопасности, структура правового обеспечения информационной безопасности.

Для цитирования: МАЛЮК, Анатолий А.; МОРОЗОВ, Андрей В. ФОРМИРОВАНИЕ ЦИФРОВОЙ ЭКОНОМИКИ И ПРОБЛЕМЫ СОВЕРШЕНСТВОВАНИЯ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 26, n. 4, p. 21–36, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1228>. Дата доступа: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.02.

***Благодарности.** Светлой памяти доктора юридических наук, профессора, одного из основателей информационного права Илларии Лаврентьевны Бачило посвящается.*

Anatoly A. Malyuk[1], Andrey V. Morozov[2]
[1]National Nuclear Research University MEPHI,
Kashirskoe shosse, 31, Moscow, 115409, Russia
[2]The All-Russian State University of Justice (RLA of the Ministry of Justice of Russia)
ul. Azov, 2, cor. 1, Moscow, 17638, Russia
[1]e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508
[2]e-mail: av_morozov@list.ru, https://orcid.org/0000-0002-5016-0833

The formation of the digital economy and the problems of improving legal regulation in the field of information security*

DOI: http://dx.doi.org/10.26583/bit.2019.4.02

Abstract. Legal regulation is one of the three pillars on which rests the field of information security of the individuals, society and the state. Not without reason, since 1992, these issues have received close attention at all levels of the Federal and regional authorities of the Russian Federation. A significant number of scientific publications of Russian authors such as I. L. Bachilo, A. A. Streltsov, Yu. M. Baturin, T. A. Polyakova, etc. are devoted to these issues. The key point in addressing these issues is a holistic concept of building legislation in the sphere of information security, taking into account the dynamic nature of changes in other pillars of the industry, namely, technology and human aspects (the formation a culture of information security in society). Thus, the concept of regulatory support should be linked to the information security policy as an essential element of the national security strategy of the state. This paper deals with the approaches to formation of such a concept. It consistently considers the problems of structuring the subject area of information security, the directions of legal regulation of activities in this area, the levels of appropriate legal support. In conclusion, the most acute problems to date that require urgent solutions are formulated.

Keywords: information security, legal regulation, information security policy, structure of legal support of information security.

For citation: MALYUK, Anatoly A.; MOROZOV, Andrey V. The formation of the digital economy and the problems of improving legal regulation in the field of information security. IT Security (Russia), [S.l.], v. 26, n. 4, p. 21–36, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1228>. Date accessed: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.02.

***Acknowledgements.** The bright memory of doctor of law, Professor, one of the founders of information law Illaria Bachilo dedicated.*

Введение

Ориентация на последовательное решение задач формирования в Российской Федерации цифровой экономики, утверждение Президентом страны новой редакции Доктрины информационной безопасности Российской Федерации (указ Президента от 5.12.2016 г. № 646) заставляют нас снова вернуться к вопросам нормативно-правового регулирования в этой области с учетом современных особенностей развивающихся здесь процессов.

Отметим, что Доктрина информационной безопасности, принятая в 2000 г., определила основные направления обеспечения информационной безопасности и наметила пути к созданию идеологии правового регулирования в данной области. В последнее десятилетие в нашей стране наблюдается существенная активность законодательной деятельности в информационной сфере. Подробный анализ результатов правоприменения Федеральных законов «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи», «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», «Об организации предоставления государственных и муниципальных услуг», «О защите детей от информации, причиняющей вред их здоровью и развитию», «О связи», «О коммерческой тайне», «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», «О безопасности критической информационной инфраструктуры Российской Федерации» и других показывает, что идет бурное развитие информационного законодательства, реализующего информационные права и свободы граждан. Однако сегодня проблема реального правового регулирования отношений в сфере обеспечения информационной безопасности (ИБ) зависит от ряда новых условий, учет которых должен способствовать

формулированию внятной методологии применения правовых средств и определению задач нормативно-правового регулирования [1].

К числу таких исходных условий, или как их называют в ряде публикаций, например [2], базовых принципов, можно отнести следующие:

1. Ориентация на общие цели формирования в стране информационного общества, адекватного целям обеспечения национальной безопасности страны в целом.
2. Ориентация деятельности по обеспечению ИБ на специфику информационной среды соответствующей социальной структуры (экономической, политической, управленческой, культурной и т.п.), что позволяет выявить особенности информационной инфраструктуры, определить специфику потребляемого и производимого информационного ресурса и параметры профиля защиты информационной среды.
3. В центре внимания всех мероприятий по обеспечению ИБ, прежде всего, должна находиться информационная среда системы органов государственной власти. Это объясняется тем, что их деятельность по управлению государством и обществом обеспечивает создание реальных гарантий свобод и прав человека, защиту интересов граждан страны и их социально значимых ассоциаций.
4. Признание системной связи процессов обеспечения ИБ с общими процессами информатизации обязывает рассматривать задачи в области их нормативно-правового регулирования в качестве составной части государственной политики в области информатизации, с одной стороны, и обеспечения национальной безопасности, с другой. Это определяет включение мер по обеспечению ИБ в структуру практически всех программ по реализации экономических, политических, административных правовых реформ и иных шагов по развитию Российской Федерации.
5. Рассмотрение задач правового регулирования в области обеспечения ИБ в контексте процессов глобализации требует постоянного анализа изменений политики и законодательства других стран. Это важная часть учета внешних факторов в процессе расширения и упрочения правовых гарантий России в мировом информационном пространстве, включая сотрудничество в рамках СНГ, ЕАЭС, ОДКБ и ШОС.
6. Постоянное отслеживание состояния информационного воздействия на идеологическую и морально-нравственную основу формирования личности, общественного мнения и правосознания населения страны, как важнейших элементов, составляющих обеспечение ИБ.

С учетом отмеченных базовых принципов первоочередными задачами дальнейшего совершенствования правового обеспечения ИБ представляется:

- уяснение предметной области ИБ на основе координации с общим правовым регулированием развития информатизации;
- тщательное исследование индикаторов безопасности;
- изучение природы угроз и рисков, а также чрезвычайных ситуаций, требующих реакции структур, непосредственно отвечающих за обеспечение ИБ.

Ниже данные задачи рассматриваются более подробно.

1. Структуризация предметной области обеспечения ИБ

Прежде чем двигаться дальше в намеченном рассмотрении обозначенных выше задач, необходимо внести некоторую ясность в используемую сегодня терминологию (или хотя бы сформулировать «информацию для размышления» в этом направлении). Дело в большом количестве споров, которые ученые правоведы ведут в настоящее время по поводу терминологических особенностей понятий «информационная безопасность», «кибербезопасность» и «безопасность информации». Последний термин, как и «защита

информации» как правило, используется помнящими еще закон 1995 года «Об информации, информатизации и защите информации». В то же время современная мода предпочитает все, что начинается с приставки «кибер». Хотя, например, термин «кибер», по мнению многих специалистов, разделяемому и авторами, слишком узко определяет правоотношения в глобальном информационном обществе.

Другой тип терминов связан с понятиями, определяющими применение аппаратно-программных средств и телекоммуникационных сетей передачи данных при реализации государственных задач и ведении бизнеса, таких как «информационный», «компьютерный», «цифровой», «электронный» и т.д. У каждого определения есть свои преимущества и недостатки. Очевидно, время расставит все по своим местам. Но сегодня мы вынуждены с сожалением констатировать катастрофическую нехватку точных законодательно закрепленных терминов и правовых норм, регулирующих правоотношения в глобальном информационном обществе.

Возвращаемся к проблеме структуризации предметной области правового обеспечения ИБ, за основу которой целесообразно принять понятие «политики информационной безопасности». Ведь политика определяется как «образ действий, направленных на достижение чего-нибудь, определяющих отношения с людьми» [3]. Посмотрим, как сегодня определяют политику информационной безопасности различные источники. Среди этих определений мы видим следующие.

«Под политикой безопасности организации понимают совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности является тем средством, с помощью которого реализуется деятельность в компьютерной информационной системе организации. Вообще политики безопасности определяются используемой компьютерной средой и отражают специфические потребности организации» [4].

«В современном мире понятие «политика информационной безопасности» может трактоваться как в широком, так и в узком смысле. Что касается первого, более широкого значения, она обозначает комплексную систему решений, которые приняты некоторой организацией, документированы официально и направлены на обеспечение безопасности предприятия. В узком понимании под этим понятием кроется документ местного значения, в котором оговорены требования безопасности, система проводимых мер, ответственность сотрудников и механизм контроля» [5].

«Под «политикой информационной безопасности» понимается совокупность документированных методологий и управленческих решений, а также распределение ролей и ответственности, направленных на защиту информации, информационных систем и ассоциированных с ними ресурсов» [6].

«Политика информационной безопасности Банка определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется организация банковской системы Российской Федерации в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в Банке» [7].

Анализ приведенных и других определений политики информационной безопасности приводит нас к представлению ее как совокупности «стратегии защиты информации» и «концепции защиты информации». Такой подход неоднократно использовался в различных работах, например в [8, 9].

В известных словарях стратегия определяется как «искусство планирования руководства, основанного на правильных и далеко идущих прогнозах» [10]. Перефразируя это определение, можно сказать, что стратегия – это общая, рассчитанная на перспективу, руководящая установка при организации и обеспечении соответствующего вида деятельности, направленная на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов.

Если говорить о стратегии обеспечения ИБ, то в зависимости от преследуемых целей можно выделить три базовых стратегии – оборонительную (защита от всех известных угроз), наступательную (защита от наиболее опасных потенциально возможных угроз) и упреждающую (защита от всех потенциальных угроз). Очевидно, что каждая из этих базовых стратегий может быть реализована при принятии определенных концептуальных решений, в совокупности образующих концепцию защиты информации.

Концепция – это «определенный способ понимания, трактовки каких-либо явлений, ведущий замысел, конструктивный принцип различных видов деятельности» [11]. Таким образом, концепция обеспечения ИБ может быть представлена последовательностью следующих действий:

- определение функций защиты, реализация которых позволит обеспечить достижение определенной стратегической цели;
- формирование набора задач защиты, решение которых обеспечивает реализацию необходимых функций;
- выбор необходимых средств защиты, которые обеспечивают решение сформированного набора задач;
- создание оптимальной системы защиты, объединяющей все необходимые средства;
- реализация макропроцессов управления защитой (планирование, оперативно-диспетчерское управление, календарно-плановое руководство и обеспечение повседневной деятельности).

Приняв за основу приведенную структуру политики информационной безопасности, необходимо далее при формировании концепции правового обеспечения ИБ структурировать информационное пространство, в котором будут реализовываться элементы этой политики. Структура информационного пространства, в котором государство через систему субъектов национального и международного права осуществляет свое присутствие и активную деятельность по обеспечению ИБ, в наиболее общем виде может быть представлена совокупностью пяти системно связанных зон:

1. Регулирование правового режима элементов информационно-коммуникационных технологий.
2. Регулирование правового статуса субъектов информационных процессов.
3. Регулирование использования информационных ресурсов.
4. Формирование и гармонизация международных правовых актов.
5. Регулирование отношений в глобальном информационном пространстве, включая Интернет.

Подобная структуризация использовалась разными авторами при исследовании концептуальных проблем правового обеспечения ИБ. В частности здесь могут быть приведены работы А.А. Стрельцова [12] и И.Л. Бачило [13]. При этом необходимо отметить специфику двух методов правового регулирования по группам указанных зон. В первой группе методов, ориентированных на первую и вторую зоны, реализуются методы как бы центростремительного свойства. Здесь можно отметить, что регулирование режима элементов информационно-коммуникационных технологий (ИКТ) часто слабо связано со

спецификой предметных областей их применения. Внимание в большей мере сосредоточено здесь на мерах защиты от проникновения, внешнего влияния, и меньше на обеспечении позитивного воздействия на безопасное использование. Это можно наблюдать на примере распределения частот, формирования режима локальных и корпоративных сетей, криптографии, режимов электронной подписи и т.п.

Методы центробежного свойства действуют в среде, охватывающей три последние зоны. Здесь превалирует нормативно-правовое регулирование, ориентированное на специфику пользователей информационных ресурсов. Необходимо отметить, что именно эта часть регулируется сегодня в меньшей степени. Естественно, что риски и угрозы возникают при активном использовании всех зон информационной инфраструктуры, особенно в процессе организации и потребления информации как ограниченного, так и открытого доступа.

Вывод, который можно сформулировать на основе приведенного общего представления политики и предметных областей обеспечения ИБ, сводится к тому, что деятельность органов государственной власти, других субъектов, участвующих в этом процессе, должна осуществляться во всех предметных и функциональных зонах информационного пространства и быть ориентированной на предотвращение, пресечение угроз, а также на ликвидацию последствий конфликтов, правонарушений в информационной среде, влекущих материальный, моральный, политический ущерб, наносимый государству, обществу, человеку.

Что касается правового регулирования отношений в сфере ИБ, связанных с созданием и использованием ИКТ, то необходимо отметить, что по задачам, целям и средствам оно шире, нежели правовое регулирование деятельности и отношений по обеспечению ИБ. Это обстоятельство требует более точного определения соответствующей предметной области, а также методов и средств нормативного оформления специфики форм и методов реализации соответствующей деятельности.

Методологически важно в связи с этим различать здесь два объекта правового регулирования:

- ИКТ-комплекс как совокупность элементов инфраструктуры, на основе которых формируется технологическая база информационных систем различного уровня;
- ИКТ-систему, или организационно-технологическую систему, реализующую определенные информационные задачи и функции конкретных субъектов, участников информационных процессов.

Далее заметим еще, что конкретизация правового регулирования обеспечения ИБ целесообразна по трем основным объектам, формирующим отношения в данной области и реализующимся во всех упомянутых предметных зонах информационного пространства. Эти объекты охватывают:

- правовой режим элементов ИКТ на основе выделения специфики каждого элемента (ресурса, технологии, коммуникации), что образует как бы нулевой цикл правового регулирования, на основе которого формируются дальнейшие правоотношения в информационной сфере;
- правовую основу обеспечения ИБ с учетом специфики определенного субъекта, включаемого в соответствующую функциональную среду через информационную систему этого субъекта;
- правовое обеспечение специализации субъекта, осуществляющего деятельность в области обеспечения ИБ, его профессионального интереса, полномочий и ответственности.

Решение обозначенных задач требует соблюдения ряда условий. Главное здесь – это ориентация на социально значимые задачи пользователя и понимание специфики его предметной и функциональной деятельности. Для выстраивания систем информационного обеспечения потребностей пользователя необходимо знать параметры инфраструктуры и характер информационного ресурса. Это позволит осуществлять эффективный контроль соблюдения правового режима технологии, коммуникации и ресурса в целях более корректного их интегрирования при создании информационных систем, программного обеспечения и организации сетей. Если известно, для чего и какая необходима информация, в какой форме, каком количестве и когда, то, исходя из характеристики ее правового режима в сфере деятельности субъекта, наиболее точно могут быть установлены обязанности в области обеспечения ИБ и необходимые параметры правового регулирования. При этом следует иметь в виду, что обычно информационная среда пользователя страдает как от недостатка, так и от избытка информации. Это связано с плохой организацией структуры информации, что существенно влияет на многие параметры безопасности.

Следует также отметить, что обеспечение данного условия находится за пределами собственно ИКТ. Оно определяется состоянием практики организации систем государственного и местного управления, механизмов их взаимодействия между собой и с другими социальными структурами. Вопрос упирается в недостатки (а в ряде случаев просто в отсутствие) нормативно-правовых актов, устанавливающих правовой статус субъектов государственного, корпоративного, частного секторов экономики, правового оформления структуры экономики страны независимо от форм собственности, ведения необходимой системы статистики и учета с ориентацией на классификаторы Российской Федерации, гармонизированные с классификаторами ООН, ЕС, ВТО и т.д. Упорядочение этой деятельности позволит поставить вопрос и об упорядочении информационного обеспечения управления, включая, естественно, и деятельность по обеспечению ИБ.

Следующее условие вытекает из первого. Оно касается выделения индикаторов (показателей, измерителей состояния процесса) эффективности обеспечения ИБ. Данные индикаторы весьма разнообразны и касаются технических, технологических, организационных, социальных параметров. С правовой точки зрения классификация индикаторов существенно важна по двум направлениям. Первое включает оценку состояния элементов обеспечения безопасности информационной инфраструктуры – наличие, работоспособность всех составляющих. Это как бы обеспечение внутрисистемного поля безопасности. Второе направление имеет более широкий фронт измерения и касается индикаторов эффективности использования мощностей, потенциала ИКТ в конкретных предметно-функциональных секторах (зонах) информатизации – экономики, культуры, управления, экологии, обороны и т.д. Именно здесь, в зоне обеспечения потребностей пользователя ИКТ, наибольшее значение приобретают социальные индикаторы обеспечения ИБ. Они тесно связаны с оценкой состояния информационного обеспечения основной профильной деятельности различных субъектов.

В этой связи возникает вопрос о двух сторонах правового регулирования. Первая – это информационно-коммуникационный комплекс (технологический аспект) и вторая – информационно-коммуникационная система. Очевидно, здесь должен быть разный набор индикаторов эффективности обеспечения ИБ.

К индикаторам, характеризующим эффективность отрасли ИКТ в целом, можно отнести и показатели использования ресурсов в качестве продукции для товарно-рыночного обмена. Проблемы обеспечения ИБ в этой части касаются отслеживания состояния производства, качества продукции, импорта, рынка в целом (баланса

внутреннего и внешнего рынков, соблюдения при этом правового режима продукции), а также степени безопасности включения российской информационной инфраструктуры в глобальные сети.

На основе выявленных признаков обеспечения безопасности на уровне элементов ИКТ-комплекса выстраивается система индикаторов обеспечения ИБ для каждой информационной среды конкретного субъекта в сфере информатизации (определенного класса или вида субъектов). При этом учитывается, что общеобязательные нормы законов, обращенных ко всем или конкретным видам субъектов информационного права, приобретают значение реализации субъективных прав и обязанностей в каждой конкретной области функциональной деятельности субъектов, в процессе их взаимодействия с другими информационными системами. Это означает, что все отношения ориентированы на правовой статус конкретного субъекта и его функциональную сферу деятельности.

Следующим шагом работы в поле индикаторов обеспечения ИБ является суммарная, а там где возможно, интегрированная оценка состояния этого обеспечения ИБ применительно к сферам национальной безопасности – оборонной, экономической, политической, экологической, идеологической, нравственной и т.д. Здесь индикаторы должны быть ориентированы на ИКТ-системы определенных субъектов (структур).

2. Направления правового регулирования деятельности по обеспечению ИБ

В условиях широкомасштабного внедрения цифровой экономики необходимо четко определить те направления правового регулирования, которые оказывают существенное влияние на обеспечение ИБ. В качестве объектов правового регулирования здесь могут быть выбраны параметры каждого из выбранных индикаторов безопасности для элементов ИКТ. Это обосновывается следующим. Во-первых, каждый из них (технология, коммуникация, ресурс) имеет существенные связи с организационно-техническими методами защиты и организационно-экономическими методами их оформления. Во-вторых, это специфические объекты области обеспечения ИБ, которые, как следует из анализа имеющейся на сегодня правовой базы, до сих пор не получили однозначной правовой квалификации и скорее всего являются объектами комплексного правового регулирования.

Проблемы обеспечения ИБ для информационных технологий концентрируются вокруг выбора методов их защиты. В одних случаях, технология выступает как готовый рыночный продукт, требующий сертификации, в других – это объект интеллектуальной собственности и требует иных, скорее всего, комплексных методов правовой защиты и порядка использования. С областью технологии связаны также вопросы безопасности импорта, адаптации приобретенного продукта к условиям определенной информационной среды и многие другие.

Не менее сложные вопросы встают и при правовой квалификации отношений, связанных с созданием и применением средств коммуникации. Здесь безопасность сконцентрирована вокруг проблем выделения и использования частот, защиты различных каналов связи и сетей, вокруг определения и обеспечения соблюдения норм, регулирующих деятельность провайдеров связи, установление порядка и пределов их ответственности за контент при должном оформлении самого содержания ресурса. Проблемы безопасности касаются и объединения сетей с разным уровнем защиты.

Наибольшего внимания требуют вопросы безопасности самой информации (информационного ресурса). Наиболее продвинутыми здесь оказываются вопросы защиты государственной тайны, хотя и здесь еще достаточно нерешенных проблем.

Но совершенно очевидна нормативно-правовая лакуна в регулировании режима информации других категорий ограниченного доступа. Отметим также, что безопасность касается не только информации ограниченного доступа. Открытая, особенно массовая информация, также является объектом заботы соответствующего правового регулирования, так как своевременность, достоверность, адресность официальной информации – неотъемлемая часть обеспечения ИБ.

Как уже упоминали выше, к настоящему времени в отечественном законодательстве имеется довольно развитый блок законов, регулирующих процесс информатизации и обеспечения ИБ. При этом, однако, необходимо отметить, что, например, норма Гражданского кодекса Российской Федерации о коммерческой и служебной тайне является неудачной по причине смешения информации частного и публичного свойства. И это не единственный пример. Фактически, налицо ситуация, когда отсутствие многих законов, регулирующих порядок установления правового режима в совокупности его признаков (категория по доступу, условия определения права собственности или исключительных прав, порядка документирования и защиты, порядка учета) создает на сегодня значительное поле риска и влечет возникновение угроз и реальных конфликтов.

Далее отметим, что весьма ответственным в структуре предметной области правового регулирования обеспечения ИБ является участок, связанный с правовой характеристикой субъектов отношений в области информации и информатизации. Обеспечение ИБ здесь приобретает особую остроту, так как от правового статуса субъекта, его правоспособности, дееспособности, его компетенции (сферы деятельности, прав и обязанностей) зависит мера, формы и методы работы с ресурсом, технологией и коммуникацией. Именно в этой зоне правового регулирования должна происходить интеграция правового режима всех составляющих ИКТ и правомочий конкретного субъекта.

Не останавливаясь подробно на оценке сегодняшнего состояния правового регулирования в данной области, отметим только, что и здесь вопросы обеспечения безопасности находятся в некотором подвешенном состоянии. Затянувшиеся решения по разграничению предметов ведения и полномочий между органами управления федерального и регионального уровней, структурные изменения, частая смена руководства органов исполнительной власти не способствуют стабильности их правового статуса. Нет ясности в правовом положении и местного самоуправления. Это является одной из возможных объективных причин возникновения рисков и угроз в информационной сфере.

Следующая зона правового регулирования отражает область использования информационных ресурсов в соответствии с функциональными потребностями субъектов. Это области экономики, управления, отношения, связанные с реализацией прав граждан и юридических лиц. Иначе говоря, это все пространство социальной активности самых различных структур. Именно здесь позиции правового регулирования, сформулированные и оформленные нормативно на предыдущих уровнях, обретают активную жизнь и проявляются в самых сложных ситуациях. Проблемы обеспечения ИБ здесь тесно связаны с общегосударственными функциями учетно-регистрационного и контрольного характера. Соответствующие органы, организации и их подразделения призваны здесь обеспечивать безопасность информационных систем, соблюдение правил эксплуатации компьютерных систем и сетей, порядок лицензирования, сертификации, стандартизации, оформление государственных заказов на определенные работы, безопасность таможенного контроля в части информационных технологий и ресурсов. Чувствительной зоной для обеспечения

ИБ остается и область экологии, создания, сохранности, обнародования и защиты экологической информации.

Самостоятельным участком правового регулирования является собственно деятельность структур обеспечения ИБ. Важными проблемами здесь являются правовой статус и функции специализированных органов в области обеспечения ИБ государства и общества, формирование структур, привлекаемых к выполнению отдельных заданий в этой области, а также определение функций всех органов государственной власти и местного самоуправления по выполнению обязательных мер в области обеспечения ИБ государства, общества, граждан.

Формируя направления правового регулирования, важно также обратить внимание на критерии безопасности с точки зрения обеспечения непрерывности защищаемых процессов. В большинстве случаев в настоящее время деятельность по обеспечению безопасности направлена на установление разных видов ограничений, связанных с процедурами защиты непосредственно ресурсов и технологий, но при этом меньшее внимание уделяется обеспечению условий для того, чтобы данный продукт активно работал в интересах общества. Контрольно-учетные и регистрационные функции часто используют для обеспечения фискальных целей, что значительно снижает значение сертификации и лицензирования. Система защиты и охраны различных сведений опирается, в основном, на запреты, а не на процедуры создания, получения и использования этих данных. Процессуальная, процедурная сторона дела и в этой области требует особого правового внимания. Например, в такой области, как выявление угроз для программного обеспечения почти по каждому элементу технологического цикла (проектирование, кодирование, отладка, испытания, контроль), а впоследствии и в ходе наблюдения за соблюдением правил безопасности необходимы процедуры, обеспечиваемые нормативно-правовыми средствами. Многое пока разрешается на основе служебных традиций и субъективных решений.

Еще одно замечание (об этом было отмечено выше) – это вопрос об установлении режима служебной информации (служебной тайны) до сих пор остается на уровне дискуссий. Все это – проблемы упорядочения правового регулирования в области обеспечения ИБ.

Таким образом, ученым правоведам предстоит исследовать и нормативно закрепить в законопроектной деятельности огромное количество новелл, учитывающих, в том числе, международное сотрудничество России по гармонизации российского законодательства и законодательства других стран в области цифровой экономики, разработать правовые основы функционирования и развития перспективных цифровых рынков в стране. Существенному развитию должен подвергнуться институт электронной подписи и ее аналогов в плане широкого «бытового» (не корпоративного) применения с учетом решения вопросов применения, экспертизы и достоверности электронных документов в деятельности государственных органов, судов, прокуратуры, адвокатуры, нотариата и т.д. Необходимо создание и развитие электронных реестров и регистров, прежде всего населения, кадастра, прав на недвижимое имущество и сделок с ним, нормативных правовых актов и т.д. Наконец появляются совершенно новые направления правового регулирования, такие как регламентация деятельности систем искусственного интеллекта, рынка криптовалют и другие.

Все это, естественно, должно быть реализовано с соблюдением требований информационной безопасности и ставит насущную необходимость решения правовых вопросов защиты, безопасности и соблюдения авторских прав на объекты интеллектуальной собственности.

Наконец, по нашему мнению, к числу основных недостатков правового регулирования основ информационной безопасности следует отнести отсутствие федерального закона, если не систематизирующего (кодифицирующего) информационное законодательство Российской Федерации, то регулирующего правовые основы информационной безопасности, включая законодательное определение национальных интересов в информационной сфере, терминов «информационный суверенитет» и т.д., регулирование основ информационной безопасности в различных сферах общественной жизни, вопросов управления и защиты национального информационного пространства, информационной политики России в международном информационном пространстве. Такой закон позволит реализовать системный подход к правовому регулированию использования национальных информационных ресурсов, их защиты и управления ими, а также обеспечить совершенствование правового регулирования проблем функционирования и развития информационной инфраструктуры. Отметим, что указанная точка зрения авторов находит поддержку и научной общественности [14].

3. Уровни правового обеспечения информационной безопасности

Казалось бы, работа в области создания нормативно-правовых актов (в том числе законов) является предметом деятельности законодательной и исполнительной властей. Контроль ответственности в рамках законов – дело правоохранительных органов. При этом выделение участка сферы обеспечения ИБ в данной области нормативно зафиксировано как «участие». Но часто это «участие» остается неопределенным. Это связано с тем, что правовое пространство, как и информационное, имеет свойство расширения и усложнения. В этих условиях существенно возрастает роль в формировании правового базиса информационной безопасности служб обеспечения ИБ.

Прежде всего, это относится к гармонизации законодательства в сфере обеспечения ИБ, причем не только национального, но и в области взаимодействия России с другими государствами. Хотя ратификация международных договоров и признание других актов международного сотрудничества в области информатизации – прерогатива законотворческих органов. Однако выработка, согласование условий международного сотрудничества и обеспечения интересов России с учетом требований национальной безопасности (включая и информационную) представляется сферой внимания органов обеспечения ИБ. Применение национального законодательства в процессах информационного обеспечения борьбы с коррупцией, терроризмом, другими преступлениями, в процессе снижения информационного неравенства и предотвращения информационных агрессий, войн и т.д. – непосредственная функция структур обеспечения ИБ, а проблема безопасности в сети Интернет – одна из форм реализации этой функции.

Отметим далее, что при любом построении методологии правового обеспечения ИБ его реальное состояние зависит от деятельности соответствующих органов и их персонала в этой области. Распределение предметов ведения и полномочий здесь, как и в любой другой сфере государственного управления, является определяющим фактором качества работы соответствующих субъектов. В этой связи важно более точно установить обязанности в рассматриваемой области на федеральном уровне, на уровне субъектов Российской Федерации, на уровнях отдельных юридических лиц, а также граждан.

На федеральном уровне определяющими направлениями, очевидно, являются законотворческая деятельность, решение задач организационно-правового характера (создание системы органов, ответственных за обеспечение ИБ на всех уровнях государственного аппарата, наделение их соответствующим правовым статусом, обеспечение координации их деятельности).

Непосредственным объектом внимания нормотворчества в области обеспечения ИБ для Государственной Думы являются законы Российской Федерации, касающиеся нулевого цикла регулирования элементов ИКТ (правового режима информации, программного обеспечения и иных составляющих технологии, правового статуса органов государственной власти и организаций, непосредственно задействованных в деятельности по обеспечению ИБ). При этом важно учитывать, что действующие законы принимались в разное время, согласованы между собой недостаточно, что очевидные пробелы в законодательстве сокращаются медленно. Все это не обеспечивает адекватности современному состоянию дел в области обеспечения национальной безопасности внутри страны и ее интересов в мире в целом. В этих условиях ближайшая задача может быть определена как системная оценка состояния нормативной базы и разработка конкретной программы правового обеспечения ИБ на федеральном уровне, включая законодательную и иную нормотворческую часть работы. Доктрина информационной безопасности, определяя основные направления правового обеспечения, все же в значительной мере оставляет размытыми конкретные задачи в данной области.

Не лишним в этой связи будет обратиться к опыту других стран и, в частности США, где достаточно оперативно решаются вопросы такого характера. За последнее время здесь сформированы службы внутренней национальной безопасности США при сохранении при этом, и ФБР, и ЦРУ. Сведение воедино всей информации, поступающей из всевозможных источников, рассчитано на координацию деятельности всех секретных служб и усиление борьбы с терроризмом. И не только. Следует учитывать, что в последние годы категория «национальной безопасности» приобретает более широкое понимание и применяется в США для обоснования и защиты действий правительства этой страны во внутренней и внешней политике с большей дозой агрессии и силы принуждения, чем прежде. Информационная сфера при этом используется как основное поле действий при переориентировке обеспечения безопасности от оборонной стратегии к наступательной, в том числе и в борьбе за мировое господство.

Возвращаясь к проблемам России, таким же, как и в Беларуси, что отмечено в [15, с. 82] «наряду с системной оценкой и упорядочением законодательства, его гармонизацией с международными актами важно установить правовые нормы, обязывающие соблюдать требования организационно-технических регуляторов и, прежде всего, стандартов всех уровней». Здесь следует отметить несоответствие необходимым требованиям многих документов, удостоверяющих сегодня техническую безопасность объектов, в первую очередь критической информационной инфраструктуры. Поправить положение призван принятый в 2017 году Закон «О безопасности критической информационной инфраструктуры Российской Федерации» (введен в действие с 1 января 2018 г.). Задачей теперь является безотлагательное формирование методик фиксации правонарушений и их расследования в информационной сфере. Процессуальное и процедурное законодательство в области обеспечения ИБ должно стать одним из центров внимания правотворческой работы.

Следующий элемент – организационное обеспечение деятельности в области ИБ. Очевидно, это сфера ведения специализированных федеральных органов исполнительной власти. Однако здесь проблемы сводятся не только к координации их статуса и функций, но и затрагивают важную область регулирования деятельности других органов исполнительной власти. К ним, например, относится организация подразделений информационной безопасности органов власти всех сфер и уровней. Эта проблема требует особого внимания. Ее нельзя сводить только к соблюдению режима сведений, относимых

к государственной тайне. Режим служебной информации (служебной тайны) сегодня фактически находится в бесхозном состоянии.

Особо отметим также вопрос о деятельности в этом направлении органов власти субъектов Российской Федерации и местного самоуправления. Не повторяя неоднократных выводов различных комиссий, подчеркнем, что острота установления прав и обязанностей этих органов исполнительной власти в области сертификации, лицензирования, стандартов, всех обязанностей по обеспечению ИБ в пределах их совместного с федеральными органами ведения, а также в пределах их собственной компетенции пока не снижается. В связи с этим возникает вопрос о координации деятельности всей системы органов управления в области обеспечения ИБ. Кто ответствен за проведение этой работы сегодня? Не ясно. Указанные проблемы должны быть заложены в основные позиции развития административной и правовой реформ. Эти вопросы, кстати, особо подчеркнуты в Доктрине информационной безопасности Российской Федерации 2016 года.

Здесь же надо обратить внимание на состояние информационной дисциплины в целом, в том числе на уровне корпоративных структур (холдинги, АО, фирмы и т.д.) независимо от формы их собственности. Это одна из важнейших составляющих обеспечения ИБ. Финансовая отчетность, бухгалтерский учет, установленная законом прозрачность в этой части зачастую находятся в состоянии бесконтрольном и слабоуправляемом. Установление водораздела между общим управлением в этой области и задачами обеспечения ИБ представляет определенную сложность. Однако она должна быть преодолена и обеспечена соответствующей правовой основой.

И еще один момент, напрямую связанный с Доктриной информационной безопасности Российской Федерации, где несколько раз обращается внимание на необходимость формирования культуры личной информационной безопасности. К сожалению, в плане правового регулирования сегодня необходимо признать, что вопросу об участии в обеспечении безопасности граждан уделяется минимум внимания. Фактически постоянно расширяется хакерство, мошенничество и т.п. Вместе с тем зона воспитания правосознания граждан в этой области оставляется на откуп СМИ, которые до сих пор делают упор на, как говорят, «клубничке», на сообщениях о потерях, преступлениях и катастрофах. Установки на активное участие человека в делах государства, а тем более в профилактике безопасности пока не ощущается. Более того, продолжает действовать модель противопоставления «государства» как института и личности, государства и других структур общества. Это активная зона создания опасности для общества. Формирование отчуждения личности от социальных проблем информационными средствами и есть прямой путь создания угроз для социума и его институтов.

Выводы

Итак, подведем некоторые итоги. В условиях активного формирования цифровой экономики реалии глобального информационного взаимодействия и одновременно противостояния требуют дальнейшего совершенствования, а в некоторых случаях и переработки нормативных правовых актов, обозначающих и предлагающих пути решения проблем обеспечения информационной безопасности.

Актуальность и приоритетность направления совершенствования нормативной правовой базы в области обеспечения информационной безопасности, с учетом соответствующих предложений и рекомендаций Совета Безопасности Российской Федерации, подтверждаются необходимостью создания структурно единой и

функционально взаимосвязанной системы обеспечения информационной безопасности на федеральном, региональном и муниципальном уровнях, что, в свою очередь, подчеркивает важность стратегического планирования и правового обеспечения в данной области, а главное, что именно право призвано не допустить состояния информационного хаоса.

Предварительный вывод по части дальнейших направлений и уровней правового обеспечения безопасности в информационной сфере сводится к тому, что по-прежнему остается актуальным комплексное решение ряда проблем. К таким проблемам сегодня можно отнести:

- ликвидацию пробелов в законодательстве по информатизации в целом и в части обеспечения ИБ;
- гармонизацию действующего законодательства в области обеспечения ИБ в рамках:

– отраслевых федеральных законов и законов субъектов Российской Федерации, а также действующих подзаконных нормативно-правовых актов в области обеспечения ИБ на этих уровнях,

– законодательства Российской Федерации, стран СНГ, ЕАЭС, ОДКБ и Союза Российской Федерации и Республики Беларусь,

– законов и стандартов России и других стран в области информационного сотрудничества, а также по использованию пространства и средств Интернета.

- развитие процессуального законодательства в области обеспечения ИБ, совершенствование законодательства об ответственности за правонарушения в информационной сфере;
- совершенствование нормативной основы в области координации деятельности всех государственных структур, задействованных в обеспечении ИБ, в целях реализации единой государственной политики в данной области и преодоления элементов «ведомственных суверенитетов».

СПИСОК ЛИТЕРАТУРЫ:

1. Стрельцов А.А. Новая Доктрина информационной безопасности Российской Федерации: информационно-правовые основы защиты от информационных угроз // Труды по интеллектуальной собственности, 2017, № 1. С. 119–123. URL: https://elibrary.ru/item.asp?id=30611967 (дата обращения: 20.04.2019).
2. Полякова Т.А. Базовые принципы как основные начала правового обеспечения информационной безопасности // Труды Института государства и права РАН, 2016, № 3. С. 17–40. URL: https://elibrary.ru/item.asp?id=26293251 (дата обращения: 20.04.2019).
3. Словарь русского языка: 70 000 слов / Под ред. Н.Ю. Шведовой. – 22-е изд., стер. – М.: Рус. Яз. ,1990. С. 552.
4. Лекции по курсу «Интернет-технологии». URL: https://studfiles.net/preview/5582384/page:33/ (дата обращения: 20.04.2019).
5. Мальцева И. Политика информационной безопасности и принципы ее организации. URL: http://fb.ru/article/43925/politika-informatsionnoy-bezopasnosti-i-printsipyi-ee-organizatsii (дата обращения: 24.09.2019).
6. Курс лекций «Безопасность информационных систем». Сайт Национального открытого университета «Интуит». URL: http://www.intuit.ru/studies/courses/13845/1242/lecture/27501?page=2 (дата обращения: 20.04.2019).
7. Шаблоны типовых документов по информационной безопасности. Политика информационной безопасности.
   URL: http://securitypolicy.ru/%D1%88%D0%B0%D0%B1%D0%BB%D0%BE%D0%BD%D1%8B (дата обращения: 20.04.2019).
8. Малюк А.А. Теория защиты информации. – М.: Горячая линия – Телеком, 2012. – 184 с. URL: https://www.twirpx.com/file/2294459/ (дата обращения: 20.04.2019).

9. Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. – М.: Горячая линия – Телеком, 2018. – 314 с. URL: http://www.techbook.ru/book.php?id_book=976 (дата обращения: 20.04.2019).
10. Словарь русского языка: 70 000 слов / Под ред. Н.Ю. Швецовой. – 22-е изд., стер. – М.: Рус. Яз., 1990. С. 770.
11. Большой энциклопедический словарь: в 2-х т. / Гл. ред. А.М. Прохоров. – М.: Сов. энциклопедия, 1991. Т. 1. С. 625.
12. Стрельцов А.А. Предмет правового обеспечения информационной безопасности // Российский юридический журнал, 2003, № 2. С. 24–35. URL: https://elibrary.ru/item.asp?id=18988734 (дата обращения: 20.04.2019).
13. Бачило И.Л. Правовое обеспечение информационной безопасности на новом этапе развития информационного общества. [Электронный ресурс] // Сайт Института государства и права РАН (статьи сотрудников института: 3503.21.01.2014. С. 1–6).
URL: http://igpran.ru/public/articles/BachiloIL.2014.1.pdf (дата обращения: 24.09.2019).
14. Иванцов С.В., Узембаева Г.И. Противодействие преступлениям экстремистской направленности, совершаемым с использованием средств массовой информации или информационно-телекоммуникационных сетей: уголовно-правовые и криминологические аспекты: монография. – М.: Юрлитинформ, 2018. – 144 с. URL: http://www.urlit.ru/Katalog/2133-Protivodejstvie-prestuplenijam-jekstremistskoj-napravlennosti-sovershaemim-s-ispolzovaniem-sredstv-massovoj-informacii-ili-informacionno-telekommunikacionnih-setej-ugolovno-pravovie-i-kriminologicheskie-aspekti.html (дата обращения: 20.04.2019).
15. Шалаева Т.З. Информационные ресурсы устойчивого развития республики Беларусь: правовые проблемы // Национальная государственность и европейские интеграционные процессы. Т. 2. Проблемы унификации законодательства в Содружестве Независимых Государств и Европейском Союзе: сб. науч. тр. / редкол.: С. А. Балашенко [и др.]. – Минск : Изд. центр БГУ, 2008. – 434 с. ISBN 978-985-476-684-3. С. 80–83 URL: http://elib.bsu.by/bitstream/123456789/5677/1/2008_2-2.pdf#4 (дата обращения: 20.04.2019).

REFERENCES:

[1] Streltsov A.A. New Doctrine of information security of the Russian Federation: information and legal bases of protection against information threats. Trudy po intellektual'noj sobstvennosti, 2017, №. 1. P. 119–123. URL: https://elibrary.ru/item.asp?id=30611967 (accessed: 20.04.2019) (in Russian).
[2] Polyakova T.A. Basic principles as the basic principles of legal information security. Trudy Instituta gosudarstva i prava RAN, 2016, № 3. P. 17–40. URL: https://elibrary.ru/item.asp?id=26293251 (accessed: 20.04.2019) (in Russian).
[3] Dictionary of the Russian language: 70 000 words ed. N.Yu. Shvedova. – 22nd ed., erased. – M.: Rus. Yaz., 1990. P. 552 (in Russian).
[4] Lectures on the course "Internet technologies". [Electronic resource.]. URL: https://studfiles.net/preview/5582384/page:33/ (accessed: 20.04.2019) (in Russian).
[5] Maltseva I. information security Policy and principles of its organization. URL: http://fb.ru/article/43925/politika-informatsionnoy-bezopasnosti-i-printsipyi-ee-organizatsii (accessed: 20.04.2019 (in Russian).
[6] Course of lectures "security of information systems". Website Of the national open University "Intuit". URL: http://www.intuit.ru/studies/courses/13845/1242/lecture/27501?page=2 (accessed: 20.04.2019) (in Russian).
[7] Templates of standard documents on information security. Information security policy. [Electronic resource.]URL: http://securitypolicy.ru/%D1%88%D0%B0%D0%B1%D0%BB%D0%BE%D0%BD%D1%8B (accessed: 20.04.2019) (in Russian).
[8] Malyuk A.A. Theory of information security. – M.: Goryachaya liniya – Telekom, 2012. – 184 p. URL: https://www.twirpx.com/file/2294459/ (accessed: 20.04.2019) (in Russian).
[9] Malyuk A. A. Fundamentals of security policy of critical information infrastructure systems. Course of lectures. – M.: Goryachaya liniya – Telekom, 2018. – 314 p. URL: http://www.techbook.ru/book.php?id_book=976. (accessed: 20.04.2019) (in Russian).
[10] Dictionary of the Russian language: 70 000 words ed. N.Yu. Shvedova. – 22nd ed., erased. – M.: Rus. Yaz., 1990. P. 770 (in Russian).
[11] Great encyclopedic dictionary: in 2 T. / Chief editor A. M. Prokhorov.– M.: Sov. enciklopediya, 1991. Vol. 1. P. 625 (in Russian).
[12] Streltsov A.A. Subject of legal provision of information security. Rossijskij yuridicheskij zhurnal, 2003, №. 2, C. 24–35. URL: https://elibrary.ru/item.asp?id=18988734 (accessed: 20.04.2019) (in Russian).

[13] Bachilo I.L. Legal provision of information security at the new stage of information society development. [Electronic resource]. Website Of the Institute of state and law RAS (articles of the Institute staff: 3503.21.01.2014. C. 1–6). URL: http://igpran.ru/public/articles/BachiloIL.2014.1.pdf (accessed: 20.04.2019) (in Russian).

[14] Ivantsov S.V., Usembaeva G.I. Countering extremist crimes committed with the use of the media or information and telecommunications networks: criminal-legal and criminological aspects].– M.: YUrlitinform, 2018. – 144 p. URL: http://www.urlit.ru/Katalog/2133-Protivodejstvie-prestuplenijam-jekstremistskoj-napravlennosti-sovershaemim-s-ispolzovaniem-sredstv-massovoj-informacii-ili-informacionno-telekommunikacionnih-setej-ugolovno-pravovie-i-kriminologicheskie-aspekti.html (accessed: 20.04.2019) (in Russian).

[15] Shalaeva T.Z. Information resources of sustainable development of the Republic of Belarus: legal problems. National statehood and European integration processes. In 2 vols. Problems of unification of legislation in the Commonwealth of Independent States and the European Union: collection of scientific works. Tr. / redkol.: S.A. Balashenko [et al.].– Minsk : Izd. centr BGU, 2008. – 434 p. ISBN 978-985-476-684-3. C. 80–83 URL: http://elib.bsu.by/bitstream/123456789/5677/1/2008_2-2.pdf#4 (accessed: 20.04.2019) (in Russian).

Поступила в редакцию – 23 апреля 2019 г. Окончательный вариант – 01 ноября 2019 г.
Received – April 23, 2019. The final version – November 01, 2019.