Журнал Белорусского государственного университета. Право. 2019;3:22–31
Journal of the Belarusian State University. Law. 2019;3:22–31

УДК 349

О ТЕОРЕТИКО-ПРИКЛАДНЫХ ПОДХОДАХ К ПРАВОВОМУ РЕГУЛИРОВАНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

В. Ю. АРЧАКОВ[1)]

[1)]*Государственный секретариат Совета Безопасности Республики Беларусь, ул. К. Маркса, 38, 220016, г. Минск, Беларусь*

Обосновывается актуальность научных исследований в области правового обеспечения информационной безопасности, важное значение четкого и полного понимания ее сущности. Раскрываются различные точки зрения на содержание понятия «информационная безопасность», аргументируется необходимость его комплексного рассмотрения в гуманитарном и технологическом аспектах. На основе национальных концептуальных подходов к информационной безопасности и существующих практик утверждается, что в Беларуси в данное понятие закладывается весь спектр отношений, присущих информационной сфере. Вместе с тем фрагментарное исследование комплексных проблем ее безопасности влечет неопределенность теоретических подходов и некоторые недостатки в правовом обеспечении. Предлагается принятие комплексного нормативного правового акта, регулирующего правовые отношения в сфере обеспечения информационной безопасности.

Ключевые слова: информационная безопасность; законодательство; правовое обеспечение информационной безопасности; нормативные правовые акты в информационной сфере; преступления против информационной безопасности.

THEORETICAL AND APPLIED APPROACHES TO THE LEGAL REGULATION OF INFORMATION SECURITY IN THE REPUBLIC OF BELARUS

V. Yu. ARCHAKOV[a]

[a]*State Secretariat of the Security Council of the Republic of Belarus, 38 K. Marx Street, Minsk 220016, Belarus*

The article substantiates the relevance of scientific research in the field of legal support of information security, the importance of a clear and complete understanding of its essence. Various points of view on the content of the concept of «information security» are revealed, the need for a comprehensive consideration in the humanitarian and technological aspects is argued. Based on national conceptual approaches to information security and existing practices, it is substantiated that in Belarus this concept lays the whole spectrum of relations inherent in the information sphere. At the same time, a fragmented study of the complex problems of its security entails the uncertainty of theoretical approaches and some shortcomings in legal support. The adoption of a comprehensive regulatory legal act regulating legal relations in the field of ensuring information security is proposed.

Keywords: information security; legislation; legal support of information security; information regulatory legal acts; crimes against information security.

Образец цитирования:
Арчаков ВЮ. О теоретико-прикладных подходах к правовому регулированию информационной безопасности в Республике Беларусь. *Журнал Белорусского государственного университета. Право.* 2019;3:22–31.

For citation:
Archakov VYu. Theoretical and applied approaches to the legal regulation of information security in the Republic of Belarus. *Journal of the Belarusian State University. Law.* 2019;3:22–31. Russian.

Автор:
Владимир Юрьевич Арчаков – заместитель Государственного секретаря Совета Безопасности Республики Беларусь.

Author:
Vladimir Yu. Archakov, deputy State Secretary of the Security Council of the Republic of Belarus.
iau@sssc.gov.by

Введение

Проблемы правового обеспечения информационной безопасности и возникающих отношений в социуме в последние два десятилетия интенсивно исследуются учеными-правоведами, которые в силу сравнительной новизны данной темы отмечают определенное отставание темпов разработки необходимых теоретических моделей и научных подходов от скорости развития информационного общества. Новые отношения объективно появляются и развиваются в самых различных сферах жизнедеятельности государств, социальных групп и каждого человека, однако они неизбежно находят свое отражение в информационной сфере, требуют всесторонней оценки и сбалансированного нормативного регулирования.

В свою очередь, информационная сфера оказывает все большее влияние на жизнедеятельность общества. Эта характерная тенденция общественного развития второй половины XX и начала XXI в., по мнению А. А. Стрельцова, обусловлена, во-первых, качественно новыми достижениями научно-технической революции в области вычислительной техники и телекоммуникаций, которые существенно повышают эффективность связанной с информацией деятельности, а во-вторых, признанием прав и свобод человека в области информационной деятельности базовыми ценностями современной цивилизации [1, с. 8]. Именно прогресс информационно-коммуникационных технологий (ИКТ), повлекший за собой многообразие информационных процессов и развитие информационных отношений современного общества, как отмечают И. Л. Бачило, О. С. Макаров и другие исследователи в данной области, обусловил потребность введения в юридический оборот понятия «информационная безопасность» [2, с. 32].

Основная часть

Необходимо особо подчеркнуть важное значение четкого и полного понимания сущности феномена информационной безопасности. На наш взгляд, следует согласиться с Е. Е. Перчук в том, что информатизация общества и имманентно связанная с ней информационная безопасность обрели глобальные масштабы и превратились в фактор, влияющий на выживание человечества в условиях формирования единого мирового информационного пространства [3, с. 8]. Как полагает Б. В. Вербенко, на постиндустриальном этапе развития информационная безопасность приобретает первостепенное значение в политической, социально-экономической, военно-технической и иных сферах жизни общества и ее необходимо считать системообразующей компонентой национальной безопасности в целом [4, с. 14]. Т. Л. Партыка, И. И. Попов указывают целый ряд факторов, которые в настоящее время выводят вопросы информационной безопасности на первый план в системе обеспечения национальной безопасности:

- национальные интересы, угрозы им и обеспечение защиты от этих угроз выражаются, реализуются и осуществляются через информацию и информационную сферу;
- человек и его права, информация и информационные системы и права на них – это основные объекты не только информационной безопасности, но и важнейшие элементы всех объектов безопасности во всех ее областях;
- решение задач национальной безопасности связано с использованием информационного подхода как основного научно-практического метода;
- проблема национальной безопасности имеет ярко выраженный информационный характер [5, с. 29–30].

В то же время нельзя не согласиться с И. М. Рассоловым, С. Г. Чубуковой в том, что в настоящее время в информационном праве не существует устоявшегося определения информационной безопасности. Это связано с тем, что многие авторы в своих определениях сосредоточены исключительно на законодательных дефинициях и конструкциях [6, с. 178]. Использование данного понятия наглядно иллюстрирует проблемы и трудности юридической техники, выразившиеся в формировании неоднозначных подходов к его толкованию, а также в отсутствии единой исчерпывающей трактовки, отражающей феноменологическую сущность такого явления, как информационная безопасность. Само же понятие «информационная безопасность» является достаточно широким и в разных контекстах отличается своим наполнением. Вкладываемое в него содержание зачастую сужает понимание информационной безопасности до технических аспектов защиты информации, при этом опускаются социально-гуманитарные аспекты межличностной коммуникации [2, с. 32, 39]. На эту же проблему указывает В. Г. Гавриленко, отмечая, что и в повседневной жизни информационная безопасность понимается лишь как необходимость борьбы с утечкой закрытой (секретной) информации, а также с распространением ложных и враждебных сведений [7, с. 10].

Как отмечают А. В. Федоров и Е. С. Зиновьева, в начале 1990-х гг., когда термин «информационная безопасность» только начал использоваться, обозначаемая им сфера отношений понималась как антипод информационной войне. Причем сама информационная война определялась не иначе как в стилистике межгосударственного силового противоборства. Тогда такие противоборства называли

конфликтами, не относимыми к войне, зачастую имея в виду гражданские войны, борьбу за национальную независимость и автономию и т. п. [8, с. 5–6]. Например, в тот период экспертами несколько завуалированно отмечалось, что содержание понятия «информационная безопасность» включает «вопросы компьютерной безопасности, безопасности информационных систем и процессов в обществе, а также создания необходимой социальной среды для гуманистической ориентации информационных процессов» [9, с. 1]. Надо сказать, что и в дальнейшем информационная безопасность часто увязывалась и до настоящего времени увязывается с противодействием информационным войнам и защитой от информационного оружия, хотя трактовки этих понятий до сих пор носят неконкретный характер и в них вкладывается самое разнообразное содержание – от компьютерных вирусов, радиоэлектронной борьбы и похищения секретов спецслужбами до массовой информации.

Позже, по мере активной и всеобщей компьютеризации, понятие «информационная безопасность» стало приобретать все более отчетливую техническую коннотацию. Под ним понималась защищенность информационной среды, которая, в свою очередь, трактовалась как совокупность информационных ресурсов, систем распространения, формирования и использования информации и информационной инфраструктуры [10, с. 33–34]. В. И. Ярочкин, рассматривая информационные ресурсы в первую очередь как материальный продукт, указывал, что ценность информации определяется прежде всего приносимыми доходами. Понимая под информационной безопасностью состояние жизненно важных интересов личности, предприятия, государства, зависящее от внутренних и внешних угроз, исследователь выделял такие ее компоненты, как персонал, материальные и финансовые средства, собственно информацию [11, с. 3, 7]. В. А. Семененко, также рассматривая информацию в качестве важнейшего стратегического ресурса, отмечал, что наряду с термином «защита информации» широко используется термин «информационная безопасность», и если защита информации характеризует процесс создания условий ее защищенности, то информационная безопасность отражает достигнутое состояние этой защищенности [12, с. 23–24], т. е. по своему смысловому наполнению это один и тот же в основном технический аспект. П. Н. Башлы, говоря о том, что информационная безопасность является одной из главных проблем современного общества, причиной ее обострения называет широкомасштабное использование автоматизированных средств накопления, хранения, обработки и передачи информации, а решение данного проблемного вопроса связывает только с обеспечением ее доступности, целостности и конфиденциальности [13, с. 3–4]. Превалирование технического аспекта наблюдалось в подходах и других авторов [14–17]. При этом в данном случае речь идет о взглядах исследователей на всю область информационной безопасности, а не на ее сугубо технический аспект, которому совершенно справедливо постоянно посвящается большой объем научных исследований.

Также следует отметить, что учеными, разрабатывавшими проблемы информационной безопасности, все же упоминался в той или иной степени ее нематериальный аспект – массовое сознание, воздействие на психику людей, обеспечение их прав в информационной сфере и т. д. Однако, во-первых, этот аспект, особенно что касается массового сознания и воздействия на психику, исследовался значительно менее интенсивно и даже несколько отделялся от понятия информационной безопасности. Например, С. А. Филин, который определял информационную безопасность как состояние защищенности информационной среды общества, одновременно применял и понятие «энергоинформационная безопасность» как защищенность психофизиологического состояния людей от внешних энергоинформационных угроз искусственного и естественного происхождения [18, с. 7]. Во-вторых, нематериальный аспект почти не находил своего отражения и развития в концептуальных и регулирующих актах.

Значительно более емкое и точное понимание информационной безопасности, нежели только как защиты информации, высказывала И. Л. Бачило, определившая ее как состояние всех компонентов ИКТ – информационных ресурсов, технологий и коммуникаций, позволяющее осуществлять их формирование и использование в интересах общества, государства и человека при минимизации отрицательных последствий для создателей, держателей и пользователей этих ресурсов, возникающих под влиянием внутренних и внешних угроз [19, с. 357]. П. У. Кузнецов указывал, что в системе правового обеспечения информационной безопасности основным элементом является комплекс информационных благ как объект воздействия (обеспечения), в котором выделяются доступ к информации, сфера духовной жизни, информационные ресурсы, информационная инфраструктура, программно-технические средства автоматизированных и автоматических систем управления, права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, защиту персональных данных и др. [20, с. 275]. Ряд авторов, определяя информационную безопасность как защиту от влияния вредоносных воздействий и информационных потоков, в качестве объектов защиты рассматривали личные интересы и развитие (в разрезе интересов личности), общественные отношения, историческое наследие, культурные традиции, обычаи, религию,

духовную жизнь (интересы общества), официальную информацию в экономике, политике, науке, технике, в сфере обороны, правопорядка и при чрезвычайных ситуациях (интересы государства) [21, с. 8]. Хотя представляется, что в данном случае существенно упускается как раз технологический аспект, по крайней мере в его нынешнем понимании.

Наряду с этим даже с наполнением понятия информационной безопасности всевозможными, в том числе нематериальными, аспектами оно продолжало определяться различно. К примеру, если в общем и целом безопасность практически всегда определялась через состояние защищенности, то некоторые эксперты высказывали понимание информационной безопасности личности, общества, государства как их способности обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы, продукты и услуги для поддержания своей жизнедеятельности, жизнеспособности, устойчивого функционирования и развития в условиях противодействия воздействиям внешних и внутренних угроз на индивидуальное, общественное сознание и телекоммуникационные системы [22, с. 15].

Существенную роль во всестороннем и упорядоченном понимании данных проблем сыграла Доктрина информационной безопасности Российской Федерации, впервые принятая на пространстве СНГ в 2000 г. как документ стратегического планирования в данной области. В одном акте были органично соединены и в нем же четко разделены по смыслу четыре составляющие национальных интересов в информационной сфере как объекты защиты (которые затем нашли отражение и в обновленной Доктрине информационной безопасности Российской Федерации 2016 г., где к национальным интересам добавилось формирование системы международной информационной безопасности):

- соблюдение конституционных прав и свобод человека, обеспечение духовного обновления страны, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;
- информационное обеспечение государственной политики;
- развитие современных информационных технологий;
- защита информационных ресурсов.

Обозначенные процессы информатизации и необходимость обеспечения их безопасности в полной мере характерны для Республики Беларусь. Так, вхождение нашей страны в информационное общество рассматривается Г. А. Василевичем, Д. А. Плетнёвым, М. С. Абламейко в качестве существенного условия ее социально-экономического развития. Значение информационной сферы как системообразующего фактора жизни белорусского общества постоянно увеличивается, в том числе в обеспечении национальной безопасности [23, с. 316; 24].

Наиболее полно, на наш взгляд, феномен информационной безопасности раскрывает О. С. Макаров, выделяя следующие его признаки:

- информационная безопасность характеризует защищенность определенной совокупности прав и интересов субъектов отношений;
- субъектами отношений выступают личность, общество и государство;
- объектами защиты являются права и интересы субъектов;
- указанные права и интересы возникают по поводу информации;
- рассматриваемые права и интересы объективно подвергаются деструктивному воздействию со стороны определенных факторов (угроз), среди которых отдельные выступают доминирующими;
- защищаемые права и интересы представляют собой динамично развивающуюся систему;
- технологической основой развития прав и интересов являются процессы информатизации;
- результат обеспечения информационной безопасности – создание таких условий, при которых на заданный вектор и темп развития информационных отношений не оказывают деструктивного влияния никакие внешние и внутренние факторы [2, с. 37–38].

Наряду с этим научных исследований по комплексным проблемам информационной безопасности в республике проводилось очень мало, хотя и российский опыт, и имеющиеся национальные разработки, и практический опыт субъектов отношений в информационной сфере позволили в целом сформировать контур отечественного понимания существующих в ней проблем и создать основу их решения.

Так, необходимое и современное понимание сущности информационной безопасности закреплено в 2011 г. Концепцией национальной безопасности Республики Беларусь, особая роль которой, по оценке М. В. Мясниковича, заключается в том, что она создает для законодательных актов и иных базовых документов стратегического планирования своего рода единую систему координат реализации стратегии развития конкретной сферы в увязке с национальными интересами [25, с. 546]. Отметим, что схожее по смыслу понятие «жизненно важные интересы Республики Беларусь» применялось и в предыдущей Концепции национальной безопасности Республики Беларусь (2001), однако именно в новом документе не только преемственно дано определение понятия «информационная безопасность» (состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере), но и более широко указаны основные национальные интересы Беларуси в информационной сфере, а также они всесторонне отражены в плоскости угроз и их источников. Важно, что в оборот введено понятие

«деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам».

Таким образом, подход к пониманию информационной безопасности в Беларуси на данный момент носит не «традиционно-технократический» характер, как его справедливо называли некоторые ученые [2, с. 34]. В него закладывается не только задача защиты информации, но и весь спектр отношений, присущих информационной сфере, включая гуманитарный, духовный, т. е. нематериальный, аспект. При этом принципиально важно, что именно гуманитарный аспект информационной сферы, упускаемый в иных или прежних подходах, объективно приобретает сегодня особое значение. Это воздействие на население различных стран и общественное сознание в целом становится одним из основных средств подготовки и развязывания военно-политических конфликтов и эффективным инструментом политической экспансии развитых стран.

Необходимо оговориться: это отнюдь не означает, что возможно пренебрегать техническим аспектом информационной безопасности. Глобальной проблемой остается защита критической информационной инфраструктуры государств [26]: только в России в текущем 2019 г. предотвращено внедрение вредоносного программного обеспечения на более чем 7 тыс. объектах критической информационной инфраструктуры [27]. Число кибервоздействий на финансовые организации во всем мире увеличивается примерно на 30 % ежемесячно, количество киберпреступников составляет не менее 40 млн человек, а нанесенный ущерб оценивается в 500 млрд долл. США и, по разным оценкам, к 2021 г. составит от 1 до 6 трлн. долл. США. По некоторым данным, только во второй половине 2018 г. зафиксировано 2,39 млрд утечек конфиденциальной информации, а через два года от утечек персональных и корпоративных данных пострадает более 1,5 млрд человек[1] [28, с. 3]. Что касается киберпреступности в нашем государстве, она также неуклонно возрастает: в 2016 г. зарегистрировано 2471 преступление в сфере высоких технологий, в 2017 г. – 3099, в 2018 г. – 4741 [29, с. 15]. По информации Следственного комитета Республики Беларусь, в 2018 г. количество поступивших заявлений о совершении киберпреступлений в нашей стране в сравнении с 2013 г. возросло в пять раз[2].

Об этих разных по сути составляющих – материальной и нематериальной – прямо упоминают и разработчики Концепции национальной безопасности Республики Беларусь, хотя в самом документе такого разделения нет. В частности, указывается, что информационная безопасность имеет два основных аспекта: содержательный (духовная сфера) и технический (материальная сфера). К первому разработчики документа относят содержание и направленность всей циркулирующей информации, ко второму – совокупность информационно-телекоммуникационных средств, технологий, систем, ресурсов, предназначенных для создания, хранения, распространения, передачи и обработки информации. В целом соглашаясь с таким подходом, возможно, на наш взгляд, предложить, исходя из приведенного содержания данных аспектов, относить эти составляющие (аспекты, области) не к информационной безопасности, а ко всей информационной сфере. Хотя подходить к рассмотрению сущности и содержания информационной безопасности необходимо именно через эти два аспекта данной сферы, которые возможно определить как «гуманитарный» и «технологический». Такой подход, в частности, применяется в принятой в 2019 г. Концепции информационной безопасности Республики Беларусь (далее – Концепция), которая через описание гуманитарного и технологического аспектов информационной сферы определяет и предметные области, в отношении которых реализуется понимание информационной безопасности:

1) информационное пространство как область деятельности, связанная с созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание и собственно на информацию. В данном определении разработчики Концепции преднамеренно ушли от упоминания воздействий на информационную инфраструктуру, как это сделано в некоторых международных актах[3], тем самым обозначая информационное пространство как исключительно

[1]Инструменты для противодействия киберпреступлениям нужно постоянно совершенствовать [Электронный ресурс] // БЕЛТА. 2019. 14 мая. URL: https://www.belta.by/tech/view/instrumenty-dlja-protivodejstvija-kiberprestuplenijam-nuzhno-postojanno-sovershenstvovat-347226-2019/ (дата обращения: 20.05.2019).

[2]Инструменты для противодействия киберпреступлениям нужно постоянно совершенствовать [Электронный ресурс] // БЕЛТА. 2019. 14 мая. URL: https://www.belta.by/tech/view/instrumenty-dlja-protivodejstvija-kiberprestuplenijam-nuzhno-postojanno-sovershenstvovat-347226-2019/ (дата обращения: 20.05.2019).

[3]Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности [Электронный ресурс] : [заключ. в г. Санкт-Петербурге, 20.11.2013 г.] // КонсультантПлюс : Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2019; Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] : [заключ. в г. Москве, 25.12.2013 г.] // КонсультантПлюс : Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2019; Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] : [заключ. в г. Екатеринбурге, 16.06.2009 г.] // КонсультантПлюс : Россия / ЗАО «КонсультантПлюс». М., 2019.

нематериальную область. В свою очередь, именно конкретизацией этого понятия оно разграничивается с более общим понятием «информационная сфера». О необходимости такого разграничения, на наш взгляд, весьма метко высказался А. В. Нестеров, назвав эти два понятия неопределенными и неконкретными метафорами [30, с. 61];

2) информационная инфраструктура как совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации. Немаловажно, что в новой Концепции впервые официально применен термин «кибербезопасность», а также производные от него понятия, и это новшество автоматически определяет ориентирование государства на уже устоявшиеся в мире основные стандарты, подходы, формы и способы противодействия компьютерным инцидентам, компьютерным преступлениям и иным воздействиям на информационно-коммуникационную инфраструктуру. Дальнейшим практическим шагом в развитии института кибербезопасности будет имплементация этого понятия в национальное законодательство, что окончательно определит точки его соприкосновения с правовыми нормами и подходами других стран и иных субъектов международных отношений;

3) информационные ресурсы как накопленная и используемая информация всех видов с сохранением ее доступности, целостности и конфиденциальности. Тема их защищенности в общем контексте информационной безопасности намного шире, нежели понятие безопасности компьютерной информации. Для выстраивания последовательной государственной политики в этой области устанавливается всеобъемлющая связь между общедоступной информацией, государственными информационными ресурсами, информацией ограниченного распространения всевозможных видов, персональными данными граждан. На основании этого в каждом из данных сегментов выделяются главенствующие приоритеты – баланс свободы информации и права на тайну, гарантированность государством распространения или предоставления общедоступной информации, безопасный доступ к информационным ресурсам добросовестных пользователей, целесообразность и соразмерность реализации защитных мер.

Как представляется, конкретизация содержания понятия информационной безопасности позволит более углубленно и специфично подходить к ее исследованию с точки зрения достижения состояния защищенности, выявлять и прогнозировать существующие и потенциальные риски, предпринимать необходимые меры по их предупреждению и совершенствованию правового обеспечения.

В целом проведенный анализ правовых основ информационной безопасности в Беларуси [31] позволяет говорить о том, что они развиваются поступательно и в основном синхронно с процессами информатизации. Принимаются новые нормативные правовые акты, нарабатывается правоприменительная практика противодействия вызовам и угрозам информационной безопасности. В республике действуют основные правовые режимы обеспечения информационной безопасности. Законодательно закреплены задачи и функции ряда государственных органов по обеспечению информационной безопасности. Судебные инстанции активно нарабатывают практику решения споров и рассмотрения дел, связанных с причинением вреда информационной безопасности. Качественно нормативное обеспечение информационной безопасности в Республике Беларусь не уступает зарубежным аналогам. Законодательно закреплены защита информационных ресурсов, обеспечение государственной политики в информационной сфере, а также безопасности критически важных объектов информационно-телекоммуникационной инфраструктуры, противодействие преступлениям в информационной сфере, обеспечение безопасности международного информационного обмена. Основные национальные интересы в информационной сфере (свобода информации, право на тайну личной жизни, запрет цензуры и т. д.), а также гарантии их защищенности закреплены конституционно.

Классическим способом правового обеспечения информационной безопасности, в том числе в Беларуси, является введение необходимых ограничений (запретов) и предписаний (мер позитивного обязывания). Система предписаний и запретов в белорусском законодательстве соответствует общемировому уровню, а по некоторым параметрам она более прогрессивна. Например, такое деяние, как склонение к самоубийству, в белорусском законодательстве криминализировано в 1999 г., в то время как в российском – только в 2017 г.

В целом же развитость национальной правовой мысли в области обеспечения информационной безопасности, судя, например, по анализу подходов в государствах – участниках СНГ, может характеризоваться конкретными параметрами, среди которых выделяются[4]:

• наличие комплекса концептуальных взглядов на систему информационной безопасности, реализованных в документе стратегического планирования, определяющего цель, задачи, направления и механизмы защиты национальных интересов в информационной сфере;

• наличие минимально необходимого для комплексного правового обеспечения информационной

[4]О принятии Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности [Электронный ресурс] : постановление МПА СНГ, 23 нояб. 2012 г., № 38-20 // КонсультантПлюс : Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.

безопасности научно обоснованного и непротиворечивого понятийного аппарата;

• достаточная степень сформированности системы правовых предписаний и запретов, определяющих правила поведения в информационной сфере (это, в свою очередь, предполагает готовность общества к криминализации деяний, посягающих на права и интересы субъектов информационной сферы);

• наличие правовых режимов, эффективность которых достаточна для обеспечения информационной безопасности;

• выстроенность системы субъектов обеспечения безопасности в информационной сфере и разработанности организационно-правовых механизмов их деятельности;

• наличие системы правосудия, эффективно действующей в специфических условиях информационных отношений.

Вместе с тем надо признать, что, во-первых, эти параметры являются в большей степени формальными, т. е. позволяют определить необходимую конфигурацию национального правового обеспечения информационной безопасности, но не его эффективность. Во-вторых, не все эти параметры в Беларуси реализованы.

Так, правовое обеспечение информационной безопасности Республики Беларусь концептуально не определено, и даже с принятием Концепции преждевременно говорить о ее свершившейся реализации по предназначению как регулирующего инструмента в этой сфере. В отечественной правовой науке отсутствует четкая система взглядов на развитие правоотношений в данной области. Не сформулированы стратегические цели правового обеспечения информационной безопасности, принципы и пределы регулирования [32, с. 91]. Понятие «информационная безопасность» на законодательном уровне не закреплено, тема информационной безопасности в законодательстве практически не просматривается, а задекларированная в Концепции национальной безопасности Республики Беларусь обобщающая категория «информационная безопасность» закреплена только в Уголовном кодексе Республики Беларусь, где она фактически подменяет более узкое понятие «компьютерная безопасность». Единственными законодательными актами, регламентирующими отношения в области обеспечения информационной безопасности, выступают законы Республики Беларусь о ратификации соответствующих международных соглашений в форматах СНГ и Союзного государства Беларуси и России. Специальные законодательные акты, регулирующие вопросы информационной безопасности, отсутствуют. Те направления, по которым законодательство в информационной сфере развивается наиболее динамично (закрепление прав, деятельность в СМИ и интернете, цифровая экономика, информационно-психологическая безопасность, институты тайн, безопасность систем связи, техническая защита информации, архивное дело и делопроизводство), зачастую располагают собственными системами законодательства от законов до подзаконных актов. Каждая из систем имеет оригинальный понятийный аппарат и собственную теоретическую основу.

Кроме этого, в белорусском законодательстве в области информационной безопасности смешаны позитивные и охранительные нормы. Каждый законодательный акт (например, об информатизации, СМИ, связи) содержит элементы правового регулирования безопасности без выделения специальных субъектов и особых мер («своими силами»), раздельного регулирования отношений информационного развития и обеспечения безопасности. Множество норм, касающихся ответственности за совершение преступных деяний в информационной сфере, не обеспечены позитивными нормами, определяющими правила поведения, в том числе запреты.

В целом же нормативное обеспечение информационной безопасности в Республике Беларусь осуществляется только как реагирование на элементы развития информатизации и цифровизации, в связи с чем оно изобилует несистемными актами. Из-за отсутствия базового нормативного акта, регулирующего отношения информационной безопасности, автономно развиваются правоотношения в области безопасности информационных ресурсов, защиты коммуникаций, охраны человека и общества от деструктивного информационного воздействия. С учетом этого видимой проблемой нормативного обеспечения информационной безопасности в Республике Беларусь на сегодня является то, что в этой сфере не проводилась систематизация законодательства [32, с. 91].

Заключение

Многообразие теоретических взглядов на рассмотренные темы позволяет обоснованно классифицировать их, например, по объекту (предмету) правового регулирования. Так, можно выделить: закрепление прав в информационной сфере; регулирование безопасности цифровой экономики; обеспечение информационной безопасности в СМИ; обеспечение информационной безопасности в сети Интернет; обеспечение информационно-психологической безопасности; регулирование защиты информационных ресурсов; регулирование института тайн; регулирование безопасности информационных систем; противодействие преступлениям против информационной безопасности; обеспечение международной информационной безопасности.

В целом представляется, что имеющиеся упущения в национальном законодательстве вытекают из недостатка отечественной научной и теоретической базы. Однако, принимая во внимание вышеизложенное, возможно полагать, что оценка состояния существующего нормативного обеспечения информационной безопасности государства должна учитывать ряд других и уже понятных на сегодня параметров в дополнение к указанным выше. К их числу считаем возможным отнести:

• охват нормативного обеспечения всех сфер информационной безопасности, образующих интегрированное состояние информационной безопасности, таких как защита информационных ресурсов, обеспечение государственной политики в информационной сфере, обеспечение безопасности критически важных объектов информатизации, противодействие деструктивному информационному воздействию, противодействие преступлениям в информационной сфере, обеспечение безопасности международного информационного обмена;

• степень юридической силы нормативных актов, регулирующих отношения в сфере информационной безопасности (на современном этапе развития информационного законодательства минимально достаточным может быть признан подход, требующий, чтобы каждая из названных выше категорий информационных отношений была урегулирована законом);

• конституционная закрепленность отношений, возникающих по поводу защиты базовых прав и интересов взаимодействующих субъектов;

• правовая регламентация системы субъектов обеспечения информационной безопасности и нормативное закрепление их функций и полномочий;

• законодательное закрепление ответственности за нарушение норм, регулирующих отношения в области информационной безопасности.

Практическое применение сформированных выше конструкций позволит определить уровень нормативно-правового обеспечения информационной безопасности Республики Беларусь и готовность ее правовой системы к дальнейшему генезису информационных отношений.

Таким образом, неуклонное и динамичное возрастание роли информационной сферы обусловливает повышение значимости информационной безопасности, реализация которой отражается на всех сферах жизнедеятельности личности, общества и государства и становится важнейшим фактором социально-экономического развития. В Беларуси понимание феномена информационной безопасности сформировалось, научно обосновано и закреплено документами стратегического планирования в виде концептуальных взглядов на национальную безопасность и ее важную составляющую – информационную безопасность.

Защиту прав и интересов субъектов отношений в информационной сфере необходимо рассматривать в гуманитарном и технологическом аспектах, что позволяет максимально полно учитывать права и интересы всех субъектов отношений в информационной сфере, а также более четко определять конкретные предметные области защиты и дополнять их по мере дальнейшего формирования информационного общества и социально-экономического развития в целом. Рассмотрение феномена информационной безопасности, а также выработку соответствующих стратегических и тактических мер по достижению защищенности информационной сферы необходимо осуществлять, во-первых, в неизменной совокупности указанных аспектов, а во-вторых, с четким их разграничением как различных частных одного и того же общего.

Следующим эволюционным этапом нормативного регулирования отношений по обеспечению информационной безопасности представляются упорядочение и систематизация законодательства на основе базовых принципов, норм позитивного права, закрепленных в корневом нормативном правовом акте, объединенных единым предметом и сферой правового регулирования.

Вышеизложенное подвигает и к внесению предложений о разработке всеохватывающего законодательного акта, определяющего концептуальные направления и основные практические меры по защите национальных интересов в информационной сфере в среднесрочной перспективе, например специального закона «Об обеспечении информационной безопасности Республики Беларусь», интегрирующего правовое регулирование обеспечения информационной безопасности.

Библиографические ссылки

1. Стрельцов АА. *Правовое обеспечение информационной безопасности России: теоретические и методологические основы*. Минск: Беллітфонд; 2005. 304 с.

2. Бачило ИЛ, Бондуровский ВВ, Вус МА, Лепехин АН, Макаров ОС, Перевалов ДВ. *Парадигма правового регулирования обеспечения международной информационной безопасности на примере опыта СНГ и ОДКБ*. Макаров ОС, редактор. Минск: Институт национальной безопасности Республики Беларусь; 2016. 344 с.

3. Перчук ЕЕ. *Информатизация и информационная безопасность (философско-методологические аспекты)* [автореферат диссертации]. Москва: Российская академия государственной службы; 2002. 25 с.

4. Вербенко БВ. *Информационная безопасность России в контексте современного политического процесса: сущность, проблемы обеспечения* [автореферат диссертации]. Москва: Российская академия государственной службы; 2004. 25 с.

5. Партыка ТЛ, Попов ИИ. *Информационная безопасность.* 5-е издание. Москва: ФОРУМ; 2012. 432 с. (Профессиональное образование).

6. Рассолов ИМ, Агапов АБ, Протасов ВН, Шагиева РВ, Грищенко ГА, Чубукова СГ. *Информационные правоотношения: теоретические аспекты*. Рассолов ИМ, редактор. Москва: Проспект; 2017. 208 с.

7. Гавриленко ВГ. *Информация и информационная безопасность: правовой аспект*. Ядевич НИ, редактор. Минск: Право и экономика; 2014. 322 с. (Юридическое обозрение).

8. Федоров АВ, Зиновьева ЕС. *Информационная безопасность: политическая теория и дипломатическая практика*. Москва: МГИМО-Университет; 2017. 357 с.

9. Когдов НМ, Цевенков ЮМ, Булкин ОА. *Информатизация общества и информационная безопасность*. Москва: НИИВО; 1993. 39 с.

10. Приходько АЯ. *Словарь-справочник по информационной безопасности*. Москва: СИНТЕГ; 2001. 124 с. (Информационная безопасность).

11. Ярочкин ВИ. *Информационная безопасность*. Москва: Международные отношения; 2000. 400 с.

12. Семененко ВА. *Информационная безопасность*. Москва: МГИУ; 2005. 215 с.

13. Башлы ПН. *Информационная безопасность*. Ростов-на-Дону: Феникс; 2006. 253 с.

14. Леонов АП, редактор. *Компьютерная преступность и информационная безопасность*. Минск: АРИЛ; 2000. 552 с. (Библиотека журнала «Управление защитой информации»).

15. Копылов ВА. *Информационное право*. Москва: Юристъ; 1997. 472 с.

16. Казанцев СЯ, редактор. *Правовое обеспечение информационной безопасности*. Москва: Академия; 2005. 240 с.

17. Расторгуев СП. *Основы информационной безопасности*. Москва: Академия; 2007. 192 с.

18. Филин СА. *Информационная безопасность*. Москва: Альфа-Пресс; 2006. 412 с.

19. Бачило ИЛ. *Информационное право.* 3-е издание. Москва: Юрайт; 2013. 485 с.

20. Кузнецов ПУ. *Основы информационного права.* Москва: Проспект; 2016. 312 с.

21. Петров СВ, Слинькова ИП, Гафнер ВВ, Кисляков ПА. *Информационная безопасность.* Новосибирск: АРТА; 2012. 296 с.

22. Минаев ВА, редактор. *Правовое обеспечение информационной безопасности*. Москва: Маросейка; 2008. 368 с.

23. Василевич ГА, Плетнёв ДА, редакторы. *Информационное право.* Минск: Адукацыя і выхаванне; 2015. 392 с.

24. Абламейко МС. *Правовые проблемы построения информационного общества в Республике Беларусь: теория и практика* [диссертация]. Минск: Белорусский государственный университет; 2012. 129 с.

25. Зась СВ, Бурак КВ, Заборовский АМ, Марков МС, Миронова ТН, Рыженков МВ и др. *Национальная безопасность Республики Беларусь*. Мясникович МВ, Мальцев ЛС, редакторы. Минск: Беларуская навука; 2011. 557 с.

26. Вильданов М, Башкиров Н. Международно-правовые аспекты защиты инфраструктуры государств от киберугроз. *Зарубежное военное обозрение*. 2019;8:21–26.

27. Егоров И. Войны виртуальные и реальные. Совбез РФ: число опасных кибератак на критическую инфраструктуру страны выросло до 17 тысяч. *Российская газета* [Интернет]. 2019, 14 августа [процитировано 20 августа 2019 г.]. Доступно по: https://rg.ru/2019/08/14/chislo-opasnyh-kiberatak-na-obekty-v-rf-vyroslo-v-11-raz-za-tri-goda.html.

28. Пелевина Н. Конфиденциальная информация утекает через сотрудников. Флешка атакует. *Российская газета*. 2018, 18 апреля.

29. Михайловская С. Найти и обезопасить в интернет-пространстве. *Беларуская думка*. 2019;7:10–19.

30. Нестеров АВ. Кибербезопасность против информационной безопасности: юридический аспект. В: Полякова ТА, Бачило ИЛ, Наумов ВБ. *Новые вызовы и угрозы информационной безопасности: правовые проблемы*. Москва: Канон+; 2016. с. 60–65. Совместное издание с Институтом государства и права РАН.

31. Арчаков ВЮ, Макаров ОС. Нормативное регулирование информационной безопасности в Республике Беларусь. В: Вишневская ВП, Князев СН, редакторы. *Национальная безопасность: информационно-психологическая безопасность, образование*. Минск: Институт пограничной службы Республики Беларусь; 2018. с. 79–93.

32. Макаров ОС, Баньковский АЛ. Концептуальные направления правового регулирования в сфере информационной безопасности Республики Беларусь. *Право.by.* 2018;5;91–96.

References

1. Streltsov AA. *Pravovoe obespechenie informatsionnoi bezopasnosti Rossii: teoreticheskie i metodologicheskie osnovy* [Legal support of information security in Russia: theoretical and methodological foundations]. Minsk: Bellitfond; 2005. 304 p. Russian.

2. Bachilo IL, Bondurovskii VV, Vus MA, Lepekhin AN, Makarov OS, Perevalov DV. *Paradigma pravovogo regulirovaniya obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti na primere opyta SNG i ODKB* [The paradigm of legal regulation of ensuring international information security based on the experience of the CIS and CSTO]. Makarov OS, editor. Minsk: Institute of National Security of the Republic of Belarus; 2016. 344 p. Russian.

3. Perchuk EE. *Informatizatsiya i informatsionnaya bezopasnost' (filosofsko-metodologicheskie aspekty)* [Informatization and information security (philosophical and methodological aspects)] [dissertation abstract]. Moscow: Russian Academy of State Service; 2002. 25 p. Russian.

4. Verbenko BV. *Informatsionnaya bezopasnost' Rossii v kontekste sovremennogo politicheskogo protsessa: sushchnost', problemy obespecheniya* [Information security of Russia in the context of the modern political process: essence, problems of security] [dissertation abstract]. Moscow: Russian Academy of State Service; 2004. 25 p. Russian.

5. Partyka TL, Popov II. *Informatsionnaya bezopasnost'* [Information security]. 5th edition. Moscow: FORUM; 2012. 432 p. (Vocational education). Russian.

6. Rassolov IM, Agapov AB, Protasov VN, Shagieva RV, Grishchenko GA, Chubukova SG. *Informatsionnye pravootnosheniya: teoreticheskie aspekty* [Information legal relations: theoretical aspects]. Rassolov IM, editor. Moscow: Prospekt; 2017. 208 p. Russian.

7. Gavrilenko VG. *Informatsiya i informatsionnaya bezopasnost': pravovoi aspekt* [Information and information security: legal aspect]. Yadevich NI, editor. Minsk: Pravo i ekonomika; 2014. 322 p. (Legal review). Russian.

8. Fedorov AV, Zinovieva ES. *Informatsionnaya bezopasnost'*: *politicheskaya teoriya i diplomaticheskaya praktika* [Information security: political theory and diplomatic practice]. Moscow: MGIMO-University; 2017. 357 p. Russian.

9. Kogdov NM, Tsevenkov YM, Bulkin OA. *Informatizatsiya obshchestva i informatsionnaya bezopasnost'* [Informatization of society and information security]. Moscow: NIIVO; 1993. 39 p. Russian.

10. Prikhodko AYa. *Slovar'-spravochnik po informatsionnoi bezopasnosti* [Dictionary-guide on information security]. Moscow: SINTEG; 2001. 124 p. (Information security). Russian.

11. Yarochkin VI. *Informatsionnaya bezopasnost'* [Information security]. Moscow: Mezhdunarodnye otnosheniya; 2000. 400 p. Russian.

12. Semenenko VA. *Informatsionnaya bezopasnost'* [Information security]. Moscow: MGIU; 2005. 215 p. Russian.

13. Bashly PN. *Informatsionnaya bezopasnost'* [Information security]. Rostov-on-Don: Feniks; 2006. 253 p. Russian.

14. Leonov AP, editor. *Komp'yuternaya prestupnost' i informatsionnaya bezopasnost'* [Computer crime and information security]. Minsk: ARIL; 2000. 552 p. (The library of the journal «Information Security Management»). Russian.

15. Kopylov VA. *Informatsionnoe pravo* [Information law]. Moscow: Yurist; 1997. 472 p. Russian.

16. Kazantsev SYa, editor. *Pravovoe obespechenie informatsionnoi bezopasnosti* [Legal support of information security]. Moscow: Akademiya; 2005. 240 p. Russian.

17. Rastorguev SP. *Osnovy informatsionnoi bezopasnosti* [Fundamentals of information security]. Moscow: Akademiya; 2007. 192 p. Russian.

18. Philin SA. *Informatsionnaya bezopasnost'* [Information security]. Moscow: Alfa-Press; 2006. 412 p. Russian.

19. Bachilo IL. *Informatsionnoe pravo* [Information law]. 3rd edition. Moscow: Yurait; 2013. 485 p. Russian.

20. Kuznetsov PU. *Osnovy informatsionnogo prava* [Fundamentals of information law]. Moscow: Prospekt; 2016. 312 p. Russian.

21. Petrov SV, Slinkova IP, Gafner VV, Kislyakov PA. *Informatsionnaya bezopasnost'* [Information security]. Novosibirsk: ARTA; 2012. 296 p. Russian.

22. Minaev VA, editor. *Pravovoe obespechenie informatsionnoi bezopasnosti* [Legal support of information security]. Moscow: Maroseika; 2008. 368 p. Russian.

23. Vasilevich GA, Pletnev DA, editors. *Informatsionnoe pravo* [Information law]. Minsk: Adukacyja i vyhavanne; 2015. 392 p. Russian.

24. Ablameyko MS. *Pravovye problemy postroeniya informatsionnogo obshchestva v Respublike Belarus'*: *teoriya i praktika* [Legal problems of building the information society in the Republic of Belarus: theory and practice] [dissertation]. Minsk: Belarusian State University; 2012. 129 p. Russian.

25. Zas SV, Burak KV, Zaborovskii AM, Markov MS, Mironova TN, Ryzhenkov MV, et al. *Natsional'naya bezopasnost' Respubliki Belarus'* [National Security of the Republic of Belarus]. Myasnikovich MV, Maltsev LS, editors. Minsk: Belaruskaja navuka; 2011. 557 p. Russian.

26. Vildanov M, Bashkirov N. [International legal aspects of protecting the infrastructure of states from cyber threats]. *Zarubezhnoe voennoe obozrenie*. 2019;8:21–26. Russian.

27. Egorov I. The wars are virtual and real. Security Council of the Russian Federation: the number of dangerous cyberattacks on the country's critical infrastructure has grown to 17 thousand. *Rossiyskaya gazeta* [Internet]. 2019 August 14 [cited 2019 August 20]. Available from: https://rg.ru/2019/08/14/chislo-opasnyh-kiberatak-na-obekty-v-rf-vyroslo-v-11-raz-za-tri-goda.html. Russian.

28. Pelevina N. [Confidential information leaks through employees. Flash drive attacks]. *Rossiiskaya gazeta*. 2018 April 18. Russian.

29. Mikhailovskaya S. [Find and secure in the Internet space]. *Belaruskaja dumka*. 2019;7:10–19. Russian.

30. Nesterov AV. [Cybersecurity versus information security: legal aspect]. In: Polyakova TA, Bachilo IL, Naumov VB, editors. *Novye vyzovy i ugrozy informatsionnoi bezopasnosti: pravovye problemy* [New challenges and threats to information security: legal problems]. Moscow: Canon+; 2016. p. 60–65. Co-published by the Institute of State and Law, Russian Academy of Sciences. Russian.

31. Archakov VYu, Makarov OS. [Normative regulation of information security in the Republic of Belarus]. In: Vishnevskaya VP, Knyazev SN, editors. *Natsional'naya bezopasnost': informatsionno-psikhologicheskaya bezopasnost', obrazovanie* [National security: information and psychological security, education]. Minsk: Institute of the Border Guard Service of the Republic of Belarus; 2018. p. 79–93. Russian.

32. Makarov OS, Bankovsky AL. Conceptual directions of legal regulation in the field of information security of the Republic of Belarus. *Pravo.by*. 2018;5:91–96. Russian.

Статья поступила в редколлегию 03.10.2019.
Received by editorial board 03.10.2019.