ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ И ГОСУДАРСТВА В СОВРЕМЕННОМ МЕЖДУНАРОДНОМ ПРАВЕ

Материалы круглого стола кафедры государственного управления юридического факультета Белорусского государственного университета

Минск, 12 апреля 2022 г.

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ И ГОСУДАРСТВА В СОВРЕМЕННОМ МЕЖДУНАРОДНОМ ПРАВЕ

**Материалы круглого стола
кафедры государственного управления
юридического факультета
Белорусского государственного университета**

Минск, 12 апреля 2022 г.

Минск
БГУ
2022

УДК 341:002(06)
ББК 67.911.16я431
И74

Информационная безопасность личности и государства в совре-
И74 менном международном праве : материалы круглого стола каф. гос. упр. юрид. фак. Белорус. гос. ун-та, Минск, 12 апр. 2022 г. / Белорус. гос. ун-т ; редкол.: В. С. Михайловский (гл. ред.), Е. Ф. Довгань, Н. О. Мороз. – Минск : БГУ, 2022. – 298 с.
ISBN 978-985-881-434-2.

Представлены материалы круглого стола, посвященные различным аспектам обеспечения информационной безопасности в контексте международного, конституционного, административного, финансового, экологического, информационного и уголовного права. Издание приурочено к 7-летию кафедры государственного управления юридического факультета БГУ.

УДК 341:002(06)
ББК 67.911.16я431

ISBN 978-985-881-434-2

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Кафедра государственного управления как самостоятельное научно-педагогическое подразделение Белорусского государственного университета создана приказом ректора № 185-ОД от 10 апреля 2015 года. В год своего семилетнего юбилея кафедра государственного управления организовала научный круглый стол «Информационная безопасность личности и государства в современном международном праве». Мероприятие было реализовано при поддержке Белорусского государственного университета.

Для вузовского сообщества и научной общественности Беларуси были и остаются актуальными глубокий интерес к обеспечению международной безопасности, пристальное внимание к успехам и проблемам национального и международного правового обеспечения безопасного существования человека и государства. В ходе мероприятия обсудили современные угрозы информационной безопасности, уголовно-правовые аспекты охраны интересов личности, общества и государства в сфере использования информационных технологий, правила ответственного поведения государств в киберпространстве, правовую квалификацию киберсанкций и другие актуальные вопросы.

В круглом столе приняли участие представители кафедр Белорусского государственного университета, а также представители органов государственного управления Республики Беларусь, что придало мероприятию не только научно-аналитическое, но и практическое измерение. Для того чтобы представление о работе круглого стола было полным, материалы публикуются в авторской редакции с незначительными стилистическими правками.

Заведующий кафедрой государственного управления
юридического факультета БГУ,
кандидат политических наук, доцент
В.С. Михайловский

ВВЕДЕНИЕ

Современные информационные технологии существенным образом изменили мир как на межличностном, так и на межгосударственном уровнях. Злонамеренное использование информационных технологий государствами, физическими и юридическими лицами все чаще признается в качестве угрозы любым субъектам: государствам, международным организациям, индивидам и компаниям, как в резолюциях Совета Безопасности ООН, так и на региональном и национальном уровнях.

Все более острыми становятся для государств и компаний проблемы поддержания информационной безопасности, защиты государственных секретов и личных данных, противодействия трансграничной и национальной преступности с использованием информационных технологий, распространения враждебной пропаганды и ложных сведений как в мирное, так и в военное время, применения информационных технологий в качестве средств и методов ведения войны, обращения криптовалют, использования информационных технологий для организации, совершения и финансирования террористических актов, введения односторонних санкций со ссылкой на злонамеренную деятельность в киберпространстве, путем предотвращения использования софта, доступа к онлайн платформам, обеспечения доступа к Интернету, реализации иных прав физических лиц в Интернете и ряда других.

Например, развитие информационных технологий значительным образом влияет на функционирование универсальной системы поддержания международного мира и безопасности. Так, Совет Безопасности ООН неоднократно признавал, что деятельность частных лиц и организаций в этой сфере может создавать угрозу международному миру и безопасности, как в результате непосредственных атак (например, использование дронов и удаленно управляемых лодок повстанческими группами в Йемене против Саудовской Аравии и Объединенных Арабских Эмиратов), так и путем финансирования, организации, планирования, совершения террористических актов, вовлечения в террористическую деятельность либо в результате обхода санкций Совета Безопасности ООН с использованием информационных технологий (Северная Корея).

Не меньше проблем вызывает противодействие трансграничной организованной преступности с использованием информационных технологий. Последние в этой связи используются не только в качестве механизма коммуникации и обмена информацией, но также для организации и совершения преступлений, отмывания преступных доходов, включая такие преступления как совершение террористических актов, финансирование терроризма, хищения и мошенничество с использованием кибер-ресурсов, программ и

методов, подрыв функционирования критической инфраструктуры государства и проч., что создает необходимость осуществления достоверной атрибутивности деяний, совершенствования национального законодательства, механизмов оказания правовой помощи, создания систем взаимодействия с онлайн платформами и провайдерами, проведения экспертизы и ряда иных для обеспечения соблюдения стандартов доказывания и должного процесса, презумпции невиновности.

Целый ряд государств и международных организаций, включая США, Европейский союз (далее – ЕС), Великобританию, Австралию разработали национальное законодательство, предусматривающее введение санкций без полномочий, полученных от Совета Безопасности ООН, в отношении государств, физических и юридических лиц, в том числе третьих стран за «злонамеренную» деятельность с использованием информационных технологий; закрытие вещания и отзыв лицензий СМИ, введение ограничений на торговлю софтом, предотвращения доступа к онлайн платформам, базам данных, предоставили онлайн платформам право осуществлять квалификацию тех или иных действий/ информации в качестве пропаганды и дефамации, принимать решение об удалении аккаунтов, наделив их фактически квази-судебными функциями. При этом правовая оценка предпринимаемых мер обычно не осуществляется.

Международный Комитет Красного Креста неоднократно отмечал активизацию применения киберсредств в период вооруженного конфликта (дронов, роботов, автоматизированных механизмов и иных), что влечет необходимость пересмотра положений действующего международного гуманитарного права для его адаптации к кибервызовам и угрозам.

Развитие информационных технологий непосредственного затрагивает и информационные права личности, включая реализацию таких прав как доступ к информации, свободу вероисповедания, защиту личной и семейной жизни, право на свободу выражения мнения, право быть забытым, право на образование, право получать выгоды от результатов научного прогресса и реализацию иных прав человека в Интернете

При этом, несмотря на возрастающий интерес к проблеме информационной безопасности личности и государства, действующие в настоящее время правовые нормы не в полной мере позволяют квалифицировать и урегулировать соответствующие общественные отношения, а доктринальная проработка многих аспектов проблемы недостаточна.

Как следствие, в настоящее время существует острая необходимость детальной правовой оценки принимаемых мер как на национальном, так и на международном уровнях, разработки правового регулирования, соответствующего современным вызовам в сфере информационной безопасности, обеспечения функционирования действующих механизмов права

международной безопасности, национального и международного уголовного права, законодательства в области обеспечения прав личности и финансовых отношений.

Специальный докладчик ООН по негативному влиянию односторонних принудительных мер на реализацию прав человека, профессор кафедры международного права факультета международных отношений БГУ, доктор юридических наук, профессор
Е.Ф. Довгань

ЧАСТЬ I. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ И ГОСУДАРСТВА В СОВРЕМЕННОМ МЕЖДУНАРОДНОМ ПРАВЕ

УДК 342

ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ В ОБЛАСТИ СВЯЗИ И ИНФОРМАТИЗАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

В.С. Михайловский

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В настоящей статье актуализируется вопрос об уточнении объекта государственного управления в области связи и информатизации в условиях развития информационного общества и процесса цифровизации. Автор анализирует компетенцию ряда республиканских органов государственного управления в сфере связи, информатизации, массовой информации, развития и обеспечения функционирования национального сегмента сети Интернет. В результате делается вывод о широком и многоаспектном объекте государственного управления в области связи и информатизации на основе легального понимания информатизации и развития информационных отношений в Республике Беларусь.

Ключевые слова: информатизация; массовая информация; информация; национальный сегмент сети интернет; национальная доменная зона; цифровизация; связь.

THEORETICAL AND LEGAL FOUNDATIONS OF STATE MANAGEMENT IN THE FIELD OF COMMUNICATIONS AND INFORMATIZATION IN THE REPUBLIC OF BELARUS

V.S. Mikhailovsky

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

This article updates the clarification of the object of public administration in the field of communications and informatization in the context of the development of the information society and the process of digitalization. The author analyzes the competence of a number of republican bodies of public administration in the field of communications, informatization, mass information, development and maintenance of the national segment of the Internet. As a result, a conclusion is made about a broad and multifaceted object of public administration in the field of communications and informatization based on the legal understanding of informatization and the development of information relations in the Republic of Belarus.

***Keywords*:** informatization; mass information; information; national segment of the Internet; national domain zone; digitalization; connection.

Государственное управление в области связи и информатизации является важным направлением публично-правовой деятельности государственных органов и должностных лиц, особенно в эпоху стремительного развития информационно-коммуникационных и цифровых технологий. По мнению профессора О. И. Чуприс, современные ИТ «не только открывают безграничные возможности, но и порождают проблемы», а также потребность в совершенствовании организационных механизмов и правового регулирования в информационном пространстве [1, с. 151]. Объект управленческой деятельности в области связи и информатизации является достаточно широким, развивающимся и дополняющимся под влиянием процесса цифровизации экономики, общества и государства. Здесь возникают вопросы относительно «пересечения» государственного управления в области связи и информатизации с цифровизацией.

В. А. Шаршун отмечает, что цифровизация выступает в качестве преобразования информации в цифровую форму, что «в большинстве случаев ведет к снижению издержек, появлению новых возможностей и т. д.»; цифровизация – это современный общемировой тренд развития экономики и общества, приводящий к повышению эффективности экономики и улучшению качества жизни [2, с. 7]. По вопросу отличий цифровизации от информатизации ученый пишет, что процесс цифровизации предполагает следующие требования к цифровому преобразованию информации: реализация цифровой трансформации в абсолютном большинстве сфер общественной жизни; эффективность использования результатов данной трансформации, которыми пользуются пользователи цифровой информации, специалисты и граждане. Информатизация – это процесс построения и развития телекоммуникационной инфраструктуры с территориально распределенными информационными ресурсами [2, с. 10].

Таким образом, цифровизация является следующим этапом информационного развития общества, пришедшим вследствие результатов информатизации. Поскольку суть цифровизации заключается в преобразовании информации в цифровую форму, то государственное управление в области связи и информатизации охватывает и цифровизацию.

В Декрете Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» не содержится определение понятия «цифровизация» [3]. Однако в контексте административно-правового регулирования отношений в области связи и информатизации представляется обоснованным рассматривать цифровизацию как сопутствующий объект управленческой деятельности при внедрении цифровых технологий в

информационную сферу и сферу связи, в том числе при цифровом преобразовании информации в рамках управляемой информационной деятельности.

В свою очередь, понятие информатизации раскрывается в Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» и включает в себя организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования информационных ресурсов и реализации информационных отношений [4]. Однако несмотря на законодательное уточнение объекта управленческой деятельности (информатизации) в теории административно-правового регулирования отношений в области связи и информатизации могут возникнуть вопросы с определением государственных органов, компетенция которых соотносится с государственным управлением в данной области. Речь идет о деятельности Министерства связи и информатизации Республики Беларусь и Министерства информации Республики Беларусь.

Министерство связи и информатизации Республики Беларусь – республиканский орган государственного управления, осуществляющий государственное регулирование и управление деятельностью в области связи и информатизации. Среди главных задач указанного Министерства выделяются: организация разработки и реализации программ развития связи и информатизации; координация деятельности юридических лиц и индивидуальных предпринимателей в области связи и информатизации в целях удовлетворения потребностей государственных органов, юридических и физических лиц в услугах связи, создания условий для обеспечения информационных потребностей государственных органов, юридических и физических лиц на основе создания информационных систем и (или) сетей, обеспечивающих формирование и обработку информационных ресурсов и предоставление пользователям документированной информации; разработка и реализация политики в области планирования, распределения и эффективного использования радиочастотного спектра радиоэлектронных средств гражданского назначения и др. [5]. Следовательно, Министерство связи и информатизации Республики Беларусь осуществляет государственное управление в области связи и информатизации в части создания условий в пределах своей компетенции для обеспечения услуг связи, формирования и функционирования информационных систем, сетей и ресурсов, а также для обеспечения распределения и эффективного использования радиочастотного спектра радиоэлектронных средств гражданского назначения. Иными словами, Министерство связи и информатизации Республики Беларусь осуществляет государственное управление в области связи и информатизации, связанное с техническими средствами связи, почтовой связью, электросвязью, а также с

созданием информационных систем, сетей, формированием информационных ресурсов.

Основными задачами Министерства информации Республики Беларусь являются: реализация государственной политики в сфере массовой информации, издательской и полиграфической деятельности, деятельности по распространению печатных изданий и продукции средств массовой информации; разработка и осуществление мероприятий, направленных на динамичное развитие экономики в сфере массовой информации, издательской, полиграфической деятельности, деятельности по распространению печатных изданий и продукции средств массовой информации; формирование культуры массовой информации, укрепление правовых и профессиональных основ деятельности средств массовой информации, организаций и индивидуальных предпринимателей, осуществляющих издательскую и полиграфическую деятельность и др. [6]. Таким образом, Министерство информации Республики Беларусь осуществляет государственное управление в сфере массовой информации, издательской и полиграфической деятельности, деятельности по распространению печатных изданий и продукции средств массовой информации. Объекты государственного управления Министерства связи и информатизации и Министерства информации Республики Беларусь отличаются согласно их компетенции, установленной нормативными правовыми актами о статусе указанных органов. Однако в широком смысле такого феномена, как информатизация, в том числе в легальном значении данного понятия, оба рассматриваемых министерства могут быть отнесены к государственным органам, осуществляющим государственное управление в области связи и информатизации. Ведь, как указано в Законе Республики Беларусь «Об информации, информатизации и защите информации», информатизация является социально-экономическим и научно-техническим процессом, обеспечивающим, в частности, условия для реализации информационных отношений [4].

Исходя из широкого понимания информатизации, развивающей информационные отношения, в объект государственного управления в области связи и информатизации закономерно включается и национальный сегмент сети Интернет. С национальным сегментом сети Интернет в Республике Беларусь связана деятельность целого ряда государственных органов и подведомственных организаций, в частности Оперативно-аналитического центра при Президенте Республики Беларусь, Министерства связи и информатизации Республики Беларусь, Министерства информации Республики Беларусь, Национального центра обмена трафиком, РУП «БелГИЭ» и др.

Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ) является специально уполномоченным

государственным органом в сфере безопасности использования национального сегмента сети Интернет, а также администратором национальной доменной зоны [7; 8]. При этом национальная доменная зона во многом обеспечивает формирование национального сегмента сети Интернета, поскольку его составляют информационные сети, системы и ресурсы, имеющие подключение к сети Интернет, размещенные на территории Республики Беларусь и (или) использующие доменные имена в национальной доменной зоне («.by», «.бел») [7]. ОАЦ, в частности, определяет порядок регистрации доменных имен в национальной доменной зоне, которая осуществляется в целях дальнейшего использования доменных имен для поименованного обращения к интернет-ресурсу владельца домена [7; 8]. ОАЦ также определяет уполномоченных поставщиков интернет-услуг, которые оказывают интернет-услуги государственным органам и иным государственным организациям (согласно Указу Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»); организациям, подчиненным (входящим в состав, систему) указанным государственным органам и иным государственным организациям; а также иным государственным организациям, определяемым ОАЦ [7].

Министерство информации Республики Беларусь осуществляет государственную регистрацию средств массовой информации, в том числе сетевых изданий (интернет-ресурсов, посредством которых распространяется массовая информация), а также выполняет функцию контроля в сфере массовой информации, в том числе в сети Интернет [9; 10]. Государственная регистрация информационных сетей, систем и ресурсов национального сегмента сети Интернет, размещенных на территории Республики Беларусь, осуществляется по заявительному принципу на основании соответствующего обращения поставщиков интернет-услуг уполномоченной Министерством связи и информатизации организацией – Республиканским унитарным предприятием по надзору за электросвязью «БелГИЭ» (Государственной инспекцией Республики Беларусь по электросвязи Министерства связи и информатизации) [7; 11].

Таким образом, государственное управление в области связи и информатизации в части национального сегмента сети Интернет охватывает обеспечение безопасности его использования, регистрацию доменных имен в национальной доменной зоне, регулирование оказания интернет-услуг, государственную регистрацию сетевых изданий, информационных сетей, систем и ресурсов национального сегмента сети Интернет, осуществление контрольных полномочий, в частности, в сфере распространения массовой информации в сети Интернет и др. Как отмечает В. В. Архипов, «рассматривая специальные случаи участия государственных органов в правовом

регулировании отношений в сети Интернет, <…> круг таких органов определяется особенностями конкретного правоотношения» [12, с. 156]. Полагаем, данное положение характерно и в рамках рассмотрения административно-правовых отношений в области связи и информатизации, в том числе в части национального сегмента сети Интернет. Ведь информационная составляющая пронизывает множество сфер современной общественной жизни [13, с. 3], а, значит, и государственное управление в области связи и информатизации основывается на широком и многоаспектном объекте управления. Резюмируя вышеизложенное, отметим, что государственное управление в области связи и информатизации охватывает процессы информатизации и цифровизации в рамках их связи с информационной сферой, в том числе сети Интернет, и сферой связи, информационными сетями, системами и ресурсами. Таким образом, информатизация, ИТ, массмедийное пространство, цифровизация включаются в объект государственного управления в области связи и информатизации.

Библиографический список

1. Чуприс, О.И. Правовое обеспечение безопасности информационного пространства в Союзном государстве и государствах–участниках: задачи выработки общих подходов и стандартов / О.И. Чуприс // Материалы постоянно действующего семинара при Парламентском Собрании Союза Беларуси и России (засед. 24-ое, г. Гродно, 17-19 мая 2011 г.) / Под ред. С.Г. Стрельченко. – Секретариат Парламент. Собрания Союза Беларуси и России, 2011. – С. 151–153.

2. Шаршун, В.А. Цифровизация права : электронный учеб.-метод. комплекс для специальности: 1-24 80 01 «Юриспруденция» «Правовое обеспечение публичной власти» / В.А. Шаршун ; БГУ, Юрид. фак-т, каф. конституционного права. – Минск : БГУ, 2021. – 207 с.

3. О развитии цифровой экономики [Электронный ресурс] : Декрет Президента Респ. Беларусь, 21 дек. 2017 г., № 8 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

4. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь, 10 нояб. 2008 г., № 455-З : в ред. Закона Респ. Беларусь от 24.05.2021 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

5. Функции и главные задачи Министерства связи и информатизации Республики Беларусь [Электронный ресурс] // Министерство связи и информатизации Республики Беларусь. – Режим доступа : https://www.mpt.gov.by/ru/funkcii-i-glavnye-zadachi. – Дата доступа : 01.09.2022.

6. Положение о Министерстве информации Республики Беларусь [Электронный ресурс] : утв. постановлением Совета Министров Респ. Беларусь, 26 окт. 2001 г., № 1545 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

7. О мерах по совершенствованию использования национального сегмента сети Интернет [Электронный ресурс] : Указ Президента Респ. Беларусь, 1 февр. 2010 г., № 60

: в ред. Указа Президента Респ. Беларусь от 18.09.2019 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

8. Инструкция о регистрации доменных имен в национальной доменной зоне [Электронный ресурс] : утв. приказом Оперативно-аналитического центра при Президенте Республики Беларусь, 18 июня 2010 г., № 47 : в ред. приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 25.08.2021 г. № 138 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

9. О средствах массовой информации [Электронный ресурс] : Закон Респ. Беларусь, 17 июл. 2008 г., № 427-З : в ред. Закона Респ. Беларусь от 24.05.2021 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

10. О мерах по совершенствованию контрольной (надзорной) деятельности [Электронный ресурс] : Указ Президента Респ. Беларусь, 16 окт. 2017 г., № 376 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

11. Административные процедуры, совершаемые в отношении юридических лиц и индивидуальных предпринимателей [Электронный ресурс] // БелГИЭ. Республиканское унитарное предприятие по надзору за электросвязью. – Режим доступа : https://www.belgie.by/ru/ap_u. – Дата доступа : 01.09.2022.

12. Архипов, В.В. Интернет-право : учебник и практикум для бакалавриата и магистратуры / В.В. Архипов. – М. : Юрайт, 2016. – 249 с.

13. Ловцов, Д.А. Информационные правоотношения: особенности и продуктивная классификация / Д.А. Ловцов // Информац. право. – 2009. – № 1 (16). – С. 3–6.

УДК 351.746.1

О ПРОБЛЕМНЫХ АСПЕКТАХ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

А.Л. Баньковский

Государственный секретариат
Совета Безопасности Республики Беларусь,
ул. К. Маркса 38, Минск, 220016, Беларусь

В статье рассматриваются адресно-целевые и практикоориентированные вопросы совершенствования и прогрессивного развития информационно-аналитической деятельности уполномоченных субъектов в сфере обеспечения национальной безопасности. Автором предлагаются соответствующие обоснованные и систематизированные меры по достижению цели и решению поставленных задач в рамках данной работы и дальнейших профильных перспективных разработок.

***Ключевые слова*:** информационно-аналитическая деятельность, национальная безопасность, обеспечение национальной безопасности.

ON THE TOPICAL ASPECTS OF INFORMATION AND ANALYTICAL ACTIVITIES IN THE SPHERE OF NATIONAL SECURITY

A.L. Bankovsky

State Secretariat of the
Security Council of the Republic of Belarus,
38 K. Marksa street, Minsk, 220016, Belarus

The article deals with targeted and practice-oriented issues of improving and progressive development of information and analytical activities of authorized entities in the field of ensuring national security. The author proposes applicable reasonable and systematic measures to achieve the goal and solve the tasks set within the framework of this work and further specialized perspective developments.

Keywords: information and analytical activities, national security, ensuring national security.

В современных условиях аномального роста постпандемийной и конфликтогенной неопределенности во всех сферах жизнедеятельности, которую ученые и практики пытаются объяснить через категорию, так называемой, новой нормальности [1], а в научно-популярной публицистике с подачи Н.Талеба, описывать с помощью феномена «черных лебедей» [2]

потребность в четком и профессиональном стратегическом анализе происходящих событий значительно возрастает.

Дополнительными факторами, осложняющими решение данной задачи, остаются продолжение скачкообразного развития информационно-коммуникационных технологий, экспоненциальный рост объемов информации (прежде всего «больших данных»), которую необходимо учитывать при выработке, обосновании и принятии управленческих решений. В контексте массового тиражирования всевозможных симулякров в понимании Ж.Бодрийяра [3] в условиях навязываемой извне гиперреальности объективный и беспристрастный анализ реальной обстановки в сфере национальной безопасности, а также релевантный прогноз ее развития представляется все более трудновыполнимой задачей.

Учитывая нехватку ресурсов, некоторое отставание уполномоченных государственных органов от бизнес-сообщества в рамках разработки и внедрения различных ноу-хау, одним из важнейших направлений повышения качества управленческого процесса является совершенствование ИАД. В то же время, исходя из анализа доступных источников и литературы, а также практики современной информационно-аналитической деятельности можно говорить о наличии ряда взаимосвязанных и взаимообусловленных проблем, которые в силу различных факторов формируют проблемное поле и затрудняют дальнейшее развитие ИАД.

Невзирая на попытки рассмотрения отдельных вопросов ИАД применительно к теории и практике государственного управления [4, с.450-462], систематизации наработанных подходов к организации ИАД на ведомственном уровне, проведение отдельных диссертационных изысканий [5], издание монографических работ по использованию отдельных методов в ИАД [6] в отечественной научной и специальной литературе указанная проблема все еще не получила должного изучения. Не в полной мере сформирован заказ на проведение научно-прикладных исследований в рассматриваемой сфере на республиканском уровне. В то же время в Российской Федерации, Азербайджане [7], других странах СНГ за последние десятилетия отмечается активизация исследовательской работы по актуальным вопросам ИАД. Так, в комплексных трудах П.Конотопова и Ю.Курносова [8], иных авторов [9-12] рассматриваются различные аспекты данной проблемы, в том числе на уровне федеральных и региональных субъектов государственного управления, отдельных правоохранительных органов.

В западном научном и публицистическом дискурсе также важное значение уделяется рассмотрению вопросам ИАД в сфере национальной безопасности, разведывательной деятельности [13-14]. В частности, традиционной особенностью американских разработок в данной области является их высокая практикоориентированность. Так, бывший аналитик ЦРУ

Morgan D.Jones [15] предлагает широкому кругу читателей «14 мощных инструментов», которые, по его мнению, помогут решению конкретных бизнес и иных сложных и нестандартных проблем по методикам спецслужб. Это один из показательных примеров своего рода конверсии в сфере ИАД, когда отдельные методы и приемы, применяемые субъектами системы обеспечения национальной безопасности, могут успешно использоваться в иных сферах жизнедеятельности общества.

Применительно к внешнеэкономической сфере исследование модели функционирования германских торгово-промышленных палат [16] также позволяет сделать вывод, что, наряду с консультационной, их экспертно-аналитическая функция, является одним из ключевых видов деятельности этих структур.

Промежуточные результаты проводимого автором комплексного исследования ИАД применительно к теории и практике обеспечения национальной безопасности [17] позволили выявить ряд ключевых проблемных теоретико-прикладных аспектов.

Первое. Наличие методологической неопределенности в отношении структуры, сущности и содержания феномена современной ИАД, ее места и роли в системе обеспечения национальной безопасности, соответствующих отраслях гуманитарных и иных наук, особенностей правого регулирования, а также перспективных направлений ее дальнейшего развития.

Второе. Использование традиционных, в ряде случаев устаревших, методов ИАД на различных уровнях принятия управленческих решений (тактическом, оперативном, стратегическом) приводит к снижению эффективности данного вида деятельности, сохранению режима «ручного» управления. Недостаток адаптированных научно обоснованных методик организации и проведения аналитических исследований, практического применения новых форм, методов и приемов современной ИАД, прежде всего оценки состояния национальной безопасности.

Третье. Отсутствие единых стандартов в сфере осуществления ИАД как на ведомственном, так и на республиканском уровнях, что существенно затрудняет не только собственно проведение ИАД, но и выработку обоснованных квалификационных требований к профессиональным кадрам в данной сфере.

Четвертое. Наличие различных несистематизированных организационно-управленческих решений, а также противоречий в определении роли и места соответствующих информационно-аналитических подразделений (далее – ИАП) в структурно-функциональной системе органов государственного управления, организаций. Отсутствие в отдельных субъектах системы обеспечения национальной безопасности информационно-аналитических подразделений, а выполнение их функций различными, в том числе

непрофильными структурами и специалистами, может приводить в некоторых случаях к снижению качества информационно-аналитической продукции.

Пятое. Низкий, в ряде случаев фрагментарный, уровень регулирования в ведомственных нормативных правовых актах вопросов организации ИАД (либо отсутствие такого регулирования), что также затруднят выполнение возложенных на ИАП задач.

Шестое. Наличие комплекса вопросов в существующей системе ведомственной/межведомственной подготовки и переподготовки специалистов-аналитиков для решения задач ИАД в сфере обеспечения национальной безопасности. Отсутствие либо недостаток собственной научно-исследовательской и учебной базы для их обучения, переподготовки, повышения квалификации.

Седьмое. Недостаточно эффективная работа по формированию кадрового резерва аналитиков с учетом перспективной потребности в развитии отдельных узкопрофильных направлений ИАД. Нехватка либо отсутствие «обратной связи» с отдельными заказчиками данного вида образовательной услуги.

Восьмое. Неявное определение места и роли, организационно-правового статуса государственных и некоммерческих «фабрик мысли» в системе государственного управления.

Девятое. Недостаточная определенность (либо отсутствие) этических основ ИАД, включая морально-этическую ответственность аналитиков за подготовленную ими информационно-аналитическую продукцию (оценки, выводы, прогнозы, обоснование альтернатив управленческих решений и т.п.). В первую очередь, это касается так называемых псевдоаналитиков, которые всегда «знают» точные ответы на все вопросы (что произойдет, как, почему и что это значит). Определяющее значение в данном контексте имеет патриотизм аналитика, его «государственный образ мышления», направленность на формирование условий и поиск направлений для устойчивого прогрессивного развития.

Кроме того, отсутствие в Республике Беларусь комплексного научно-прикладного исследования ИАД в системе обеспечения национальной безопасности, прежде всего в контексте определения научно обоснованной практикоориентированной методологии мониторинга рисков, вызов, угроз, их оценки, прогноза, обоснования и подготовки выверенных альтернатив для принятия наиболее эффективных управленческих решений.

В контексте рассмотрения направлений дальнейшего совершенствования ИАД, исходя из указанных и иных проблемных аспектов, одним из них является разработка и унификация системы оценки эффективности

информационно-аналитической деятельности органа государственного управления, организации.

Несмотря на сугубо индивидуальный и специфический характер подобной системы оценки эффективности применительно к каждому органу государственного управления возможна разработка и унификация базовых критериев оценки ИАД со стороны руководства ведомства, вышестоящего органа государственного управления (областного исполнительного комитета, министерства, концерна, Правительства, и т.д.).

В основу такой оценки целесообразно закладывать взаимосвязанный и взаимообусловленный комплекс объективных количественных и качественных показателей ИАД, отдавая при этом предпочтение второй группе, поскольку в данной сфере интеллектуальной деятельности приоритет остается именно за качеством подготовки управленческих решений, их эффективности и достаточности, своевременности выявленных проблемных аспектов, полноты предложенных мер реагирования, точностью прогнозов, выявленных тенденций и т.д.

При таком общем методологическом подходе более высокой оценке будет полежать качественно подготовленное комплексное аналитическое исследование, содержащее «добавленную аналитическую стоимость», прежде всего в виде обоснованных оценок и выводов, целевого прогноза развития ситуации, аргументированных научно обоснованных предложений по минимизации выявленных рисков и принятию исчерпывающих мер реагирования, чем, например, в срок подготовленные формализованные отчеты о работе, но без какой-либо аналитической и прогностической части.

В то же время данный процесс подлежит нормативному регулированию путем определения и согласования формы и видов информационно-аналитической продукции, ее структуры и содержания, аналитического и прогнозного наполнения, сроков подготовки и направления соответствующих материалов. В противном случае уровень субъективизма в оценках будет оставаться высоким, что затруднит эффективную организацию ИАД.

Таким образом, анализ зарубежных научных и иных источников свидетельствует, что недостаток исследований и научно обоснованных методических разработок в отношении ИАД в нашей стране повышает вероятность отставания даже от наших партнеров по СНГ, которые уделяют данным вопросам самое пристальное внимание.

Указанные обстоятельства обуславливают необходимость разработки научно обоснованных предложений по методологическому совершенствованию ИАД, комплексному анализу данного феномена в системе обеспечения национальной безопасности.

Представляется, что успешному разрешению выявленных и иных проблемных аспектов, с которыми в той или иной степени сталкиваются в

повседневной деятельности сотрудники ИАП, во многом может способствовать разработка теоретико-прикладных основ современной ИАД, ее стройной научно обоснованной практикоориентированной модели, понятийно-категориального аппарата, применительно к целям и задачам субъектов системы обеспечения национальной безопасности.

В качестве стратегической цели в данной области выступает формирование национальной аналитической школы, фундаментом которой должна стать система профессиональной подготовки и переподготовки аналитиков в системе субъектов обеспечения национальной безопасности на базе ведущих республиканских и ведомственных вузов. Реализация указанных мер будет способствовать формированию основы для повышения качества подготовки управленческих решений с целью дальнейшего устойчивого развития.

Библиографический список

1. Глобальная система на переломе: пути к новой нормальности. Совместное исследование ИМЭМО РАН и Атлантического совета [Электронный ресурс]: пер. с англ. Под ред. А. Дынкина, М. Барроуза. М.: ИМЭМО РАН, 2016, – 32 с. – Режим доступа: https://www.imemo.ru/publications/info/globalynaya-sistema-na-perelome-puti-k-novoy-normalynosti. – Дата доступа: 10.02.2022.

2. Талеб, Н. Черный лебедь. Под знаком непредсказуемости (2-е изд., доп.) / Талеб Николас Нассим. – М., 2019. – 736 с.

3. Бодрийяр, Ж. Симулякры и симуляции / Ж. Бодрийяр ; [пер. с фр. А.Качалова]. – М.: Издательский дом «ПОСТУМ», 2015. – 240 с.

4. Князев, С. Н. Управление: искусство, наука, практика: Учеб. пособие. – Мн.: Армита-Маркетинг, Менеджмент, 2002. – 512 с.

5. Худяков, А. В. Информационно-аналитическое обеспечение политического управления: политологический анализ : автореф. дис... канд. полит. наук: 23.00.01. – Мн.: Академия управления при Президенте Республики Беларусь, 2020. – 23 с.

6. Евелькин, Г. М. Социальные процессы и национальная безопасность. Монография. – Мн.: ИНБ Респ. Беларусь, 2020. – С. 360.

7. Набибекова, Г. Ч. Разработка информационно-аналитической системы поддержки принятия решений в области внешней политики / Г.Ч. Набибекова // Informasiya cəmiyyəti problemləri. – № 2, – 2010. – С.64-72.

8. Конотопов, П. Ю. Аналитика: методология, технология и организация информационно-аналитической работы / П.Ю. Конотопов, Ю.В. Курносов. – М.: РУСАКИ, 2004. – 512 с.

9. Вахрушев, В. Ю. Развитие научно-методических положений по созданию ситуационного центра ФТС России в интересах совершенствования информационно-аналитического обеспечения управления деятельностью таможенных органов : Дис... канд. эконом. наук : 08.00.05. – Москва, 2012. – 166 с.

10. Демидов, А. А. Информационно-аналитические системы поддержки принятия решений в органах государственной власти и местного самоуправления. Основы проектирования и внедрения: учебное пособие / А.А. Демидов, Ю.Н. Захаров. – СПб.: НИУ ИТМО, 2012. – 100 с.

11. Первухин, А. С. Административно-правовое регулирование информационно-аналитической деятельности в системе МВД России : дис... канд. юрид. наук: 12.00.14. – Москва, 2014. – 150 с.

12. Левкин, И. М. Теория и практика информационно-аналитической работы. Курск: НАУКОМ, 2011. – 389 с.

13. Kent, S. Strategic Intelligence for American World Policy. Princeton, NJ: Princeton University Press, 1949. – 226 p.

14. Хилсмен, Р. Стратегическая разведка и политические решения. Пер. с англ. К. П. Сонина и О. Е. Зильберберг. — М.: Издательство иностранной литературы, 1957. — 192 с.

15. Морган, Дж., Решение проблем по методикам спецслужб. 14 мощных инструментов / Морган Джонс ; пер. с англ. Н. Брагиной. – М. : Манн, Иванов и Фербер, 2017. – 432 с.

16. Иванова, А. Роль научно-аналитической деятельности в системе торгово-промышленных палат германии / А. Иванова // Современная Европа, 2021, № 1. – С. 121–129.

17. Баньковский, А. Л. Основные направления совершенствования информационно-аналитической деятельности в системе обеспечения национальной безопасности // Проблемы обеспечения национальной и региональной безопасности: правовые и организационные аспекты : Международная науч.-практ. конф., Минск, 2 ноября 2017 года : в 2 т. / Ин-т нац. безопасности Респ. Беларусь ; редкол.: А.Л.Лычагин (гл.ред.) [и др.]. – Минск, 2018. – Т.2 – 308 с. – С.144-148.

УДК 342.723

О НЕКОТОРЫХ ВОПРОСАХ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

В.А. Шаршун

Национальный центр правовой информации Республики Беларусь,
ул. Берсона 1а, г. Минск, 220030, Беларусь

В статье исследуются вопросы понятия информационной безопасности личности, а также правовое регулирование и некоторый зарубежный опыт в данной сфере. Автором вносится ряд предложений по совершенствованию законодательства Республики Беларусь как в области обеспечения информационной безопасности в целом, так и информационной безопасности личности в частности.

***Ключевые слова*:** правовое регулирование, информационная безопасность, информационная безопасность личности.

ON SOME ISSUES OF LEGAL REGULATION OF ENSURING PERSONAL INFORMATION SECURITY

V.A. Sharshun

National Center for Legal Information of the Republic of Belarus,
1a Bersona street, Minsk, 220030, Belarus

The article examines the issues of the concept of personal information security, as well as legal regulation and some foreign experience in this area. The author makes a number of proposals for improving the legislation of the Republic of Belarus both in the field of information security in general and information security of the individual in particular.

Keywords: legal regulation, information security, personal information security.

В настоящее время приоритетной тенденцией общественного развития во многих странах является формирование цифровой экономики, характерной особенностью которой является активное использование информационно-коммуникативных технологий и сети Интернет. Одним из важных факторов, влияющих на развитие такой экономики, является информационная безопасность.

Информационная безопасность является составной частью системы национальной безопасности государства, имеет собственное содержание и представляет собой многоаспектное явление. Несмотря на то, что

информационная безопасность призвана обеспечить защиту от угроз именно в информационной сфере, фактически она проникает во все сферы общественных отношений. Являясь сложной категорией, информационная безопасность включает в себя различные элементы, среди которых можно выделить доступность, конфиденциальность и целостность информации. При этом для различных субъектов информационных отношений эти элементы информационной безопасности имеют разное значение. Если для граждан и субъектов хозяйствования на первом месте находится доступность информации, то для государства самым главным элементом является конфиденциальность. При этом целостность информации одинаково важна для всех субъектов.

Развитие цифровых технологий, наиболее динамично происходящее в последнее десятилетие, несет в себе не только массу дополнительных возможностей, но и угроз. Так, в Республике Беларусь за семь месяцев прошлого года число хищений денег с банковских счетов увеличилось более чем на 70% по сравнению с 2020 г. Из 10 тысяч киберпреступлений, совершенных в стране за семь месяцев 2021 г., на их долю приходилось почти 9 тысяч [1]. Также в 2021 г. хакеры выложили в открытый доступ файл с более чем 8 млрд. паролей. Это количество больше всего населения Земли и почти вдвое больше суммарного числа пользователей интернета. По информации профильного портала CyberNews, документ имел объем около 100 ГБ и содержал свыше 8,459 млрд строчек, каждая из которых – это отдельный пароль. Это крупнейшая утечка паролей в истории человечества [2].

Внедрение информационно-коммуникационных технологий (далее – ИКТ) стало основой построения современного информационного общества, что актуализирует проблему обеспечения информационной безопасности личности. При этом обеспечение информационной безопасности личности становится важной проблемой обеспечения суверенитета и национальной безопасности государства.

Актуальность исследования вопросов информационной безопасности, с точки зрения обеспечения конституционных прав личности обусловлена следующим. В соответствии со статьей 2 Конституции Республики Беларусь человек, его права, свободы и гарантии их реализации являются высшей ценностью и целью общества и государства. Этой норме корреспондирует статья 21 Конституции Республики Беларусь, согласно которой государство гарантирует права и свободы граждан Беларуси, закрепленные в Конституции, законах и предусмотренные международными обязательствами государства. Одним из фундаментальных и неотъемлемых прав человека согласно статье 34 Конституции Республики Беларусь является право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, о политической,

экономической, культурной и международной жизни, состоянии окружающей среды. Значительное количество средств массовой информации и бурное развитие Интернета, ставшие основой современного информационного общества, дают широкие возможности для реализации гражданином указанного права.

Вместе с тем, увеличение объема производимой и распространяемой информации таит в себе угрозы безопасности как отдельной личности, так и общества и государства, которые могут выражаться в распространении персональных данных, экстремистских материалов, разглашении коммерческой, служебной и государственной тайны. Поэтому неотъемлемой частью информационного общества является информационная безопасность как один из элементов национальной безопасности.

Следует отметить, что конституционное право гражданина на получение и распространение информации, будучи личным и неотъемлемым правом, не является абсолютным. Для предотвращения угроз национальной безопасности государство вправе вводить ограничения в реализации данного права. Но любые ограничения не могут быть произвольными, они должны быть обоснованы и соразмерны конституционно значимым целям. Поэтому в настоящее время чрезвычайную актуальность приобретает проблема нахождения баланса между правами человека в информационной сфере и необходимостью обеспечения информационной безопасности.

Феномен информационной безопасности личности является сложным и многоаспектным. Его изучают представители технических и гуманитарных наук. Несмотря на разнообразие научных подходов, большинство определений понятия информационной безопасности схожи с определением, содержащимся в Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575. В соответствии с данным определением под информационной безопасностью понимается состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Под угрозой же понимается потенциальная или реально существующая возможность нанесения ущерба национальным интересам Республики Беларусь. Согласно пункту 14 указанной Концепции одним из основных национальных интересов в информационной сфере является реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации. Концепция информационной безопасности Республики Беларусь, утвержденная постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 содержит аналогичное определение информационной безопасности.

В юридической литературе нет единых подходов к определению понятия «информационная безопасность личности». Так, А.С. Жаров предлагает следующее определение: «информационная безопасность личности – это совокупность общественных отношений, складывающихся в процессе защиты ее конституционных прав и свобод от угроз в информационной сфере» [3].

С.В. Нуянзин и О.С. Нуянзин предлагают учитывать сознание личности: «информационная безопасность личности – это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию человека» [4].

С.В. Баринов предлагает обозначить в составе информационной безопасности личности четыре составляющие: информационно-техническую, информационно-идеологическую, информационно-психологическую и информационно-правовую безопасность личности [5].

Ю.И. Богатырева под информационной безопасностью личности понимает состояние и условие жизнедеятельности личности, при которых отсутствует или минимизирована угроза нанесения вреда личному информационному пространству и той информации, которой обладает индивид, [6, с.18].

Согласно И.В. Роберт информационная безопасность личности рассматривается как защита от внешней неэтичной, нелегитимной, противозаконной, агрессивной информации; некачественной педагогической продукции, реализованной на базе ИКТ, не отвечающей педагогико-эргономическим требованиям; заимствования результатов интеллектуальной собственности, представленной в электронном виде, влекущие за собой потерю авторских прав [7, с. 33].

Более подробную характеристику информационной безопасности личности представил в своей диссертации А.А. Тамодлин. По его мнению, информационная безопасность в широком смысле определяется как состояние, при котором отсутствует возможность причинения пользователю ущерба информацией из внешнего мира. Что касается информационной безопасности в узком значении, то это прежде всего состояние защищенности конституционных прав человека и гражданина на поиск, получение, передачу информации, а также защиту персональной информации и психики от негативных воздействий. Данный автор представил собственную классификацию, в соответствии с которой информационная безопасность выражена совокупностью таких элементов, как информационно-психологическая и информационно-правовая безопасности. Информационно-правовая безопасность личности охватывает право человека на различные операции с информацией без учета ее содержания и назначения, а также право на неприкосновенность персональных данных. Она связана с правом на защиту от общественно опасной информации, содержащей экстремистские лозунги,

пропаганду ненависти, войны, недостоверные, неэтичные сведения, которые оказывают деструктивное воздействие на пользователя. [8, с. 3-5].

Определение понятия «информационная безопасность личности» обязательно должно учитывать гуманитарный аспект. По нашему мнению, под информационной безопасностью личности следует понимать состояние защищенности, обеспечивающее реализацию конституционного права гражданина на информацию и исключающее причинение вреда с помощью информации и информационных технологий здоровью и имуществу человека, его физическому, психическому и нравственному развитию.

Следует отметить, что в настоящее время ни в Концепции национальной безопасности Республики Беларусь, ни в Концепции информационной безопасности Республики Беларусь не содержится четких научно обоснованных механизмов решения проблем информационной безопасности личности. По нашему мнению, необходимо нормативное определение основ государственной политики в области информационной безопасности личности. При этом нормативное закрепление определения информационной безопасности личности может стать той отправной точкой, от которой будет в дальнейшем происходить формирование соответствующей государственной политики. В дальнейшем это может повлечь за собой корректировку ряда задач государственных органов Республики Беларусь, являющихся регуляторами в сфере информационной безопасности.

В настоящее время четко не определено, какой государственный орган и каким образом реализует функции государственного регулирования в области обеспечения информационной безопасности личности. При этом в Беларуси существуют несколько основных регуляторов в сфере информационной безопасности: Оперативно-аналитический центр при Президенте Республики Беларусь, Национальный центр персональных данных Республики Беларусь, Национальный банк Республики Беларусь, Министерство связи и информатизации; Министерство внутренних дел и другие.

Опыт развитых в вопросах обеспечения информационной безопасности стран показывает целесообразность создания и функционирования единого государственного органа в указанной сфере. Так в Сингапуре с 2015 года функционирует Национальное Агентство Кибербезопасности (Cyber Security Agency of Singapore – CSA), координирующее усилия государства в области информационной безопасности. Отношение официальных властей Сингапура к обеспечению информационной безопасности граждан показывает сравнение помощником начальника CSA Гаурава Киртхи информационной безопасности с общественным благом. По его словам, «правительство Сингапура будет намерено обеспечить гражданам и компаниям безопасную информационную среду точно так же, как обеспечивает их другими общественными благами, такими как водопровод и канализация» [9].

Представляется целесообразным определить единый государственный орган в Республике Беларусь, координирующий деятельность остальных государственных органов в вопросах обеспечения информационной безопасности личности. Одним из направлений деятельности такого государственного органа должно стать формирование и реализация государственной политики в области обеспечения информационной безопасности граждан. Соответствующие полномочия могут быть возложены на Оперативно-аналитический центр при Президенте Республики Беларусь или Национальный центр персональных данных Республики Беларусь.

В настоящее время в законодательстве Республики Беларусь нет единой целостности в правовом регулировании информационной безопасности, эти вопросы во многом урегулированы фрагментарно. Методологические основы информационной безопасности заложены в Концепции информационной безопасности Республики Беларусь, которая определяет систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности. Базовые нормы относительно защиты информации как составной части информационной безопасности содержатся в главе 7 Закона Республики Беларусь «Об информации, информатизации и защите информации». Ряд вопросов, касающихся информационной безопасности, содержится в законах, правовых актах Главы государства, постановлениях Правительства Республики Беларусь. Единый правовой классификатор Республики Беларусь, утвержденный Указом Президента Республики Беларусь от 4 января 1999 г. № 1 (далее – ЕПК), в настоящее время не содержит рубрики по вопросам информационной безопасности. По нашему мнению, есть необходимость ее введения, в том числе включения в ее состав вопросов информационной безопасности личности. Например, в рубрике 12 ЕПК «Законодательство в области обороны, национальной безопасности, правоохранительной деятельности, борьбы с преступностью и судебно-экспертной деятельности» целесообразно ввести подрубрику 12.04 «Законодательство в области информационной безопасности». С помощью классификатора можно будет структурно выделить массив законодательства в такой важнейшей в настоящее время сфере, как информационная безопасность, и систематизировать его. В перспективе на этой основе возможна подготовка консолидированного нормативного правового акта по вопросам информационной безопасности. Как вариант, это может быть раздел или глава в Информационном кодексе Республики Беларусь, о необходимости подготовки которого высказывались такие известные белорусские ученые, как Г.А. Василевич и М.С. Абломейко [10, с. 100].

Также следует отметить недостаток специальных правовых актов, связанных с противодействием информационно-психологическим атакам в Интернет-пространстве. В действующей нормативной базе отсутствуют четкие определения таких распространенных явлений, как троллинг, кибербуллинг, хэппислепинг, кибersталкинг, преследование в виртуальном пространстве и другие, а также не указаны правовые способы защиты от них. В связи с этим жертвы киберпреступников вынуждены обороняться доступными методами и надеяться на собственные силы.

Поэтому полагаем целесообразным корректировку действующих нормативных правовых актов в части формирования нормативной правовой базы государственной политики в сфере информационной безопасности личности. По нашему мнению, в Концепции информационной безопасности Республики Беларусь целесообразно закрепить определение термина «информационная безопасность личности», а также определить правовые основы ее обеспечения, который в последующем должны быть детализированы в иных нормативных правовых актах.

Следует также рассмотреть вопрос о разработке нормативных правовых актов в сфере информационно-психологической безопасности личности с уточнением базовых терминов и понятий, определением способов защиты от негативных воздействий в информационном пространстве.

Это будет способствовать более полной реализации конституционных информационных права граждан, успешному и безопасному взаимодействию пользователей в киберпространстве и в целом обеспечению информационной безопасности и суверенитета государства.

Библиографический список

1. Число хищений денег с банковских счетов в 2021 году увеличилось более чем на 70% // Сайт БЕЛТА. – Режим доступа: https://www.belta.by/incident/view/chislo-hischenij-deneg-s-bankovskih-schetov-v-2021-godu-uvelichilos-bolee-chem-na-70-457235-2021/. – Дата доступа: 07.04.2022.

2. Произошла крупнейшая в истории утечка паролей. Под ударом все пользователи интернета // CNews. – Режим доступа: https://www.cnews.ru/news/top/2021-06-08_proizoshla_krupnejshaya_v_istorii. – Дата доступа: 07.04.2022.

3. Жаров, А.С. Конституционно-правовое регулирование информационной безопасности личности в Российской Федерации // disserCat – электронная библиотека диссертаций. – Режим доступа: https://www.dissercat.com/content/konstitutsionno-pravovoe-regulirovanie-informatsionnoi-bezopasnosti-lichnosti-v-rossiiskoi-f. – Дата доступа: 07.04.2022.

4. Нуянзин, С.В., Нуянзин, О.С. Информационная безопасность личности и некоторые организационно-правовые меры по ее обеспечению // CYBERLENINKA. – Режим доступа: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-lichnosti-i-nekotorye-organizatsionno-pravovye-mery-po-ee-obespecheniyu. – Дата доступа: 07.04.2022.

5. Баринов С.В. О правовом определении понятия «Информационная безопасность личности» // CYBERLENINKA. – Режим доступа: https://cyberleninka.ru/article/n/o-pravovom-opredelenii-ponyatiya-informatsionnaya-bezopasnost-lichnosti. – Дата доступа: 07.04.2022.

6. Богатырева Ю.И. Подготовка будущих педагогов к обеспечению информационной безопасности школьников: автореферат дис. ... доктора педагогических наук: 13.00.08 / Богатырева Ю. И.; [Место защиты: Тул. гос. ун-т]. – Тула, 2014. – 47 с.

7. Роберт И.В. Современное состояние информатизации отечественного образования: фундаментальные и прикладные исследования // Сборник материалов международной научно-практической конференции «Информатизация образования – 2017». Издательство: Чувашский государственный педагогический университет им. И.Я. Яковлева. Чебоксары, 2017. – С. 23- 49.

8. Тамодлин, А.А. Государственно-правовой механизм обеспечения информационной безопасности личности : автореф. дис. ... канд. юрид. наук : 12.00.01 / А.А. Тамодлин ; Сарат. юрид. ин-т МВД РФ. – Саратов., 2006. – 23 с.

9. Власти Сингапура предложили относиться к ИБ как общественному благу // SecurityLab.ru. – Режим доступа: https://www.securitylab.ru/news/512644.php. – Дата доступа: 07.04.2022.

10. Абламейко, М.С., Василевич, Г.А. Подготовка и принятие Информационного кодекса Республики Беларусь – настоятельная потребность времени // Веснік БДУ. Сер. 3. – 2012. – № 2. – С. 98-102.

УДК 347.9 (476)

О НЕКОТОРЫХ АСПЕКТАХ ЗАЩИТЫ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ В ПРОЕКТЕ КОДЕКСА ГРАЖДАНСКОГО СУДОПРОИЗВОДСТВА

В.П. Скобелев

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье рассматриваются некоторые аспекты защиты государственных секретов в проекте Кодекса гражданского судопроизводства. По итогам проведенного исследования автором предложено, что порядок допуска участников судопроизводства к информации госсекретах, содержащейся в материалах гражданского дела, должен регулироваться не общими нормами законодательства о госсекретах, а специальными предписаниями процессуального законодательства, то есть Кодексом гражданского судопроизводства.

Ключевые слова: государственные секреты, защита государственных секретов, гражданское судопроизводство, ознакомление с материалами дела.

ON SOME ASPECTS OF THE PROTECTION OF STATE SECRETS IN THE DRAFT CODE OF CIVIL JUDICIAL PROCEEDINGS

V.P. Skobelev

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article discusses some aspects of the protection of state secrets in the draft Code of Civil Procedure. Based on the results of the study, the author proposed that the procedure for admitting participants in legal proceedings to information in state secrets contained in the materials of civil case should be regulated not by the general norms of the legislation on state secrets, but by special provisions of procedural legislation, that is, the Code of Civil Procedure.

Keywords: state secrets, protection of state secrets, civil proceedings, familiarization with the case materials.

В Республике Беларусь одним из векторов развития процессуального законодательства был избран путь унификации ГПК и ХПК посредством их замены единым Кодексом гражданского судопроизводства (далее – КГС). К настоящему времени проект КГС уже подготовлен [1] и прошел процедуру общественного обсуждения [2]. Вместе с тем анализ норм КГС показывает, что в части регулирования вопросов защиты госсекретов в КГС допущены

те же самые ошибки (за счет некритического заимствования соответствующих норм), которые сейчас имеются в ГПК, ХПК и на которые мы уже обращали внимание [3; 4, с. 53-58]. Очевидно, что до того, как проект КГС будет принят в качестве нормативного правового акта, указанные ошибки из него должны быть устранены.

В статье 58 КГС «Особенности осуществления участниками гражданского судопроизводства отдельных прав по гражданским делам, в материалах которых содержатся сведения, составляющие государственные секреты» (она соответствует ст. 57-1 ГПК, ст. 56-1 ХПК) закреплены следующие положения:

«1. Ознакомление с материалами гражданских дел, содержащими сведения, составляющие государственные секреты, выписки из них, снятие копий с документов, не содержащих сведений, составляющих государственные секреты, осуществляются участниками гражданского судопроизводства с соблюдением требований законодательства о государственных секретах.

2. Суд обязан определить место и срок ознакомления участников гражданского судопроизводства с процессуальными документами или их копиями, содержащими сведения, составляющие государственные секреты, и обеспечить такое ознакомление с соблюдением требований законодательства о государственных секретах».

Но наряду с этим в ч.2 ст. 85 КГС присутствует норма о том, что «эксперт, являющийся иностранным гражданином, лицом без гражданства или гражданином Республики Беларусь, постоянно проживающим за пределами Республики Беларусь, вправе знакомиться с материалами дела, содержащими сведения, составляющие государственные секреты, после получения допуска в порядке, установленном законодательными актами» (в настоящее время такое же правило содержится в ч.2 ст. 97 ГПК, ч.6 ст. 70 ХПК). Аналогичные нормы предусмотрены также в отношении специалиста (ч.6 ст. 88 КГС, ей соответствует ч.2 ст. 100 ГПК, ч.6 ст. 71 ХПК), переводчика (ч.2 ст. 90 КГС, ей соответствует ч.4 ст. 102 ГПК, ч.6 ст. 74 ХПК), представителя (ч.3 ст. 97 КГС, ей соответствует ч.3 ст. 79 ГПК, ч.3 ст. 79 ХПК).

На наш взгляд, наличие в КГС ст. 58, имеющей общей характер, говорит о том, что норм ч.2 ст. 85, ч.6 ст. 88, ч.2 ст. 90, ч.3 ст. 97, регулирующих частные случаи, в нем быть не должно. Данный вывод подтверждают и коллизии в регламентации идентичных вопросов, присутствующие между ст. 58 КГС, с одной стороны, и ч.2 ст. 85, ч.6 ст. 88, ч.2 ст. 90, ч.3 ст. 97 КГС, с другой стороны:

- ч.2 ст. 85, ч.6 ст. 88, ч.2 ст. 90, ч.3 ст. 97 КГС предусматривают ограничения процессуальных прав только для экспертов, специалистов, переводчиков, представителей, в то время как ст. 58 КГС – для абсолютно любых участников гражданского судопроизводства, в том числе для участвующих

в деле лиц, которые имеют непосредственную заинтересованность в исходе дела (в исковом производстве таковыми являются стороны и третьи лица);

- согласно ч.2 ст. 85, ч.6 ст. 88, ч.2 ст. 90, ч.3 ст. 97 КГС ограничения действуют только для тех экспертов, специалистов, переводчиков, представителей,, которые являются иностранными гражданами, лицами без гражданства или гражданами Республики Беларусь, постоянно проживающим за пределами Республики Беларусь; между тем ст. 58 КГС никаких оговорок относительно гражданства участников судопроизводства не содержит;
- в соответствии с ч.2 ст. 85, ч.6 ст. 88, ч.2 ст. 90, ч.3 ст. 97 КГС условием ознакомления с материалами дела, содержащими госсекреты, является «получение допуска в порядке, установленном законодательными актами», а по ст. 58 КГС – «соблюдение требований законодательства о государственных секретах».

В пользу изъятия указанных норм из КГС говорят и другие обстоятельства. Так, положения ст. 58 КГС в большей мере соответствуют Закону Республики Беларусь от 19 июля 2010 г. №170-З «О государственных секретах» (далее – Закон №170-З), который условием осуществления деятельности с использованием госсекретов определяет наличие допуска к госсекретам у любых физических лиц – как граждан Республики Беларусь, так и иностранных граждан и лиц без гражданства (см. абз.4 ст. 1, ст. 10), а также не дифференцирует участников судопроизводства в зависимости от наличия (отсутствия) потребности получения ими указанного доступа – такой доступ необходим для всех из них (см. абз.2 ч.7 ст. 33, абз.5 ч.1 ст. 34, абз.4 ч.6 ст. 39).

Кроме того, нормы ч.2 ст. 85, ч.6 ст. 88, ч.2 ст. 90 КГС изложены таким образом, будто у экспертов, специалистов и переводчиков, имеется право на ознакомление с материалами любого гражданского дела и в любом объеме, данное право является их обычным (традиционным, ординарным) правомочием и ограничивается лишь присутствием в материалах дела сведений, составляющих госсекреты. В действительности, однако, это не так.

Например, эксперт вправе знакомиться с материалами гражданского дела лишь «в части, относящейся к предмету экспертизы» (п.1 ч.1 ст. 85 КГС). Специалист может лишь «с разрешения суда знакомиться с материалами дела» (ч.4 ст. 88 КГС), причем, мы бы добавили (и этот момент стоило бы отразить в КГС), знакомиться только в части, относящейся к поставленному перед специалистом вопросу. Что касается переводчика, то по смыслу ч.1 ст. 89 КГС не исключается осуществление им перевода для лица, не владеющего языком судопроизводства, и письменных материалов дела, однако подобную деятельность переводчика нельзя трактовать как реализацию им права на ознакомление с материалами дела, такое право здесь реализует только лицо, для которого осуществляется перевод, а переводчик выполняет

лежащую на нем обязанность по осуществлению точного и полного перевода. Вместе с тем свои изъяны имеет и ст. 58 КГС:

- создается впечатлением, что теми правами, о которых говорит статья, обладает любой участник гражданского судопроизводства, в частности, знакомиться с материалами гражданского дела, делать выписки из них, снимать копии с документов могут в том числе свидетели, эксперты, специалисты, переводчики, хотя, как видно из п.2 ч.2 ст. 57 КГС, это прерогатива только участвующих в деле лиц (т.е. лиц, обладающих заинтересованностью в исходе дела);
- поскольку КГС не относит представителей к лицам, участвующим в деле, то получается, что представители выпали из сферы регулирования ст. 58 КГС и (если ч.3 ст. 97 КГС к тому же будет исключена) ни при каких обстоятельствах не смогут реализовать предусмотренные ею полномочия;
- непонятно, почему снятие участниками гражданского судопроизводства копий с документов, не содержащих сведений, составляющих госсекреты, ч.1 ст. 58 КГС обязывает делать с соблюдением требований законодательства о госсекретах;
- из ч.1 ст. 58 КГС следует, что участники гражданского судопроизводства вправе знакомиться с любыми материалами дел, содержащими госсекреты, между тем ч.2 ст. 58 КГС упоминает об ознакомлении лишь с «процессуальными документами или их копиями», тем самым упуская из виду судебные документы (т.е. судебные постановления и протоколы – см. ч.5 ст. 99 КГС), а также те материалы дела, которые по смыслу ст. 99 КГС не относятся ни к процессуальным, ни к судебным документам, – судебные извещения, доверенности представителей, доказательства и пр.;
- совершенно неясно, что в ч.2 ст. 58 КГС понимается под местом (это какой-то кабинет в здании суда, зал судебного заседания, помещение другого государственного органа или нечто иное) и сроком (это конкретные дата и время, когда участники судопроизводства должны явиться в определенное место, или максимальный промежуток времени, в течение которого им будет разрешено работать с материалами дела), которые суд должен определить для целей ознакомления участников судопроизводства с соответствующими документами;
- нет никакой определенности относительного того, что значит «обеспечить такое ознакомление с соблюдением требований законодательства о государственных секретах», поскольку Закон №170-З не регулирует вопрос, каким именно образом (способом) участников судопроизводства нужно знакомить с материалами гражданского дела;
- наконец, самый главный недостаток ст. 58 КГС в том, что она пытается регулировать особенности реализации отдельных прав участниками гражданского судопроизводства по поводу госсекретов, что вряд возможно

успешно осуществить – ведь эти особенности, как и сами права, весьма и весьма разнообразны; в действительности данная статья должна определять только общие условия допуска участников процесса к информации о госсекретах; конкретные же способы, формы и объемы получения подобной информации всегда будут находиться в зависимости от процессуального положения, занимаемого в деле тем или иным лицом (например, сторона процесса сможет получить секретную информацию в результате реализации своего права на ознакомление с материалами гражданского дела, эксперт – посредством получения от суда для проведения экспертизы материалов, содержащих госсекреты, свидетель – через восприятие в судебном заседании информации, относящейся к госсекретам и озвучиваемой судом или участниками судопроизводства, и т.д.).

КГС (см. ст. 58, ч.5 ст. 111, п.18 ч.2 ст. 251, ч.3 ст. 300) возможность ознакомления участников гражданского судопроизводства с госсекретами обусловливает «соблюдением требований законодательства о государственных секретах» (нормы ч.2 ст. 85, ч.6 ст. 88, ч.2 ст. 90, ч.3 ст. 97 КГС, которые требуют от экспертов, специалистов, переводчиков, представителей «получения допуска в порядке, установленном законодательными актами», мы в расчет не берем, поскольку, как уже отмечалось выше, они из проекта КГС должны быть однозначно исключены). Очевидно, под законодательством о госсекретах в приведенных нормах подразумевается прежде всего Закон №170-З. Однако соблюдение его требований для указанных целей весьма проблематично, потому что, во-первых, Закон №170-З содержит большое количество самых разнообразных требований (вследствие чего сложно сказать, какие именно из них упомянутые нормы КГС имеют в виду); во-вторых, требования носят достаточно общий характер и почти не учитывают особенностей такой сферы, как гражданское судопроизводство; в-третьих, на что мы уже обращали внимание [3, с. 68-71], многие из требований Закона №170-З о порядке получения участниками гражданского судопроизводства допуска к госсекретам весьма несовершенны, что порождает немалое число сложностей и проблемных вопросов.

С учетом изложенного полагаем, что порядок допуска участников судопроизводства к информации госсекретах, содержащейся в материалах гражданского дела, должен регулироваться не общими нормами законодательства о госсекретах (т.е. Законом №170-З), а специальными предписаниями процессуального законодательства – КГС. Предписания КГС должны иметь примерно следующее содержание: допуск участников судопроизводства к госсекретам осуществляет состав суда первой инстанции, рассматривающий дело, путем отобрания подписки о том, что они предупреждены об ответственности за разглашение сведений, составляющих госсекреты. Такой допуск являлся бы основанием для доступа участников

судопроизводства к госсекретам на всех последующих стадиях процесса (в апелляционном производстве и т.д.).

Заметим, что подобная норма уже присутствует в ч.6 ст. 256 КГС: «В целях защиты сведений, составляющих государственные секреты или содержащих охраняемую законом тайну в материалах дела, суд предупреждает лиц, участвующих в закрытом судебном заседании, об ответственности за разглашение таких сведений, о чем у них берется подписка» (данному правилу соответствует ч.5 ст. 267 ГПК, абз.10 ч.2 ст. 176 ХПК). Недостаток данной нормы только в том, что она находится в особенной части КГС и касается защиты госсекретов лишь в судебном заседании. Но если перенести эту норму в общую часть КГС и сформулировать как регулирующую в целом порядок допуска участников судопроизводства к госсекретам, содержащимся в материалах гражданского дела, то потребность в регламентации на уровне Закона №170-З процедуры допуска участников судопроизводства к госсекретам полностью отпадет, равно как и потребность в упомянутых выше нормах ч.5 ст. 111, п.18 ч.2 ст. 251, ч.3 ст. 300 КГС.

Библиографический список

1. Проект Кодекса гражданского судопроизводства Республики Беларусь [Электронный ресурс] // Правовой форум Беларуси. – Режим доступа: https://forumpravo.by/publichnoe-obsuzhdenie-proektov-npa/forum15/16857-proekt-kodeksa-grazhdanskogo-sudoproizvodstva-respubliki-belarus. – Дата доступа: 10.08.2022.
2. Проект Кодекса гражданского судопроизводства Верховным Судом вынесен на общественное обсуждение [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/novosti/novosti-pravo-by/2022/mart/69019/?fbclid=IwAR12pX4i85 UY6Mqj3pGODp5hYEXj96mtQSFDMm77_ATuwMTOFd82nuMJHWw. – Дата доступа: 10.08.2022.
3. Скобелев, В. Нововведения в правилах рассмотрения судами гражданских дел: еще раз о качестве нормотворчества (начало) / В. Скобелев // Юридический мир. – 2020. – №7. – С. 61-71.
4. Скобелев, В. Нововведения в правилах рассмотрения судами гражданских дел: еще раз о качестве нормотворчества (окончание) / В. Скобелев // Юридический мир. – 2020. – №8. – С. 53-63.

УДК 342.951+351.81

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА СОВРЕМЕННОМ ЭТАПЕ

Д.В. Перевалов

Государственное учреждение образования
«Институт пограничной службы Республики Беларусь»,
ул. Славинского 4, г. Минск, 220103, Беларусь

В статье рассматриваются отдельные проблемные вопросы правового регулирования обеспечения безопасности критически важных объектов информатизации Республики Беларусь в современных условиях. В качестве решение имеющихся проблем предлагается на основе подходов, сложившихся в юридической науке, осуществить восполнение пробелов в законодательстве, регулирующим отношения в области обеспечения безопасности критически важных объектов информатизации, административную и уголовную ответственность за правонарушения в данной области. В первую очередь это относится к регулированию импортозамещения оборудования и программного обеспечения для соответствующих категорий объектов.

***Ключевые слова*:** критически важные объекты информатизации, обеспечение безопасности, правовое регулирование, кибербезопасность, хакерские атаки, административные правонарушения в области информации, преступления против компьютерной безопасности.

SEPARATE PROBLEMS OF LEGAL REGULATION SAFETY CRITICAL OBJECTS OF INFORMATIZATION AT THE PRESENT STAGE

D.V. Perevalov

State Educational Institution
«Institute of the Border Service of the Republic of Belarus»,
4 Slavinsky street, Minsk, 220103, Belarus

The article deals with certain problematic issues of legal regulation of ensuring the security of critically important objects of informatization of the Republic of Belarus in modern conditions. As a solution to the existing problems, it is proposed, on the basis of approaches that have developed in legal science, to fill in the gaps in the legislation governing relations in the field of ensuring the security of critical informatization objects, administrative and criminal liability for offenses in this area. First of all, this applies to the regulation of import substitution of equipment and software for the relevant categories of objects.

Keywords: critical objects of informatization, security, legal regulation, cybersecurity,

hacker attacks, administrative offenses in the field of information, crimes against computer security.

Введение

Современное общество характеризуется переходом к качественно новому состоянию – информационному обществу, в котором отмечается подавляющее влияние новых информационных технологий на все сферы общественной жизни, обусловленное лавинообразным развитием систем передачи данных. Разработка новейших технологий, которые призваны обеспечить потребности личности и общества в информации, влечет за собой поступательное развитие новых средств коммуникации, рост их производства и модификации. Вместе с тем, трансформация общества в условиях информационной революции формирует новые угрозы информационной безопасности как отдельных государств, так и конкретных регионов. Актуальной данная проблема является и для государств – членов Организации Договора о коллективной безопасности, в том числе и Республики Беларусь.

Так, число кибератак в мире в 2021 г. выросло на *50 %* по сравнению с 2020 г. В России количество атак увеличилось на *54 %*. Экспертами отмечается, что большая часть кибератак в 2021 г. пришлась на государственные учреждения – почти *20 %* преступлений. В *10 %* случаев жертвами кибермошенников становятся промышленные предприятия, по *8 %* атак направлены на медицинские и образовательные учреждения, а также финансовые организации [1], [2].

При этом хакерским атакам во многих случаях подвергаются объекты, которые в Беларуси отнесены к критически важным объектам (далее – КВОИ) – IT-инфраструктуры топливно-энергетических, производственных, транспортных, информационно-коммуникационных, коммунальных, финансовых и других систем жизнеобеспечения государства и населения. В частности, 7 мая 2021 г. один из крупнейших трубопроводных операторов в США – Colonial Pipeline Company – подвергся хакерской атаке и был вынужден приостановить работу трубопровода. В 19 штатах был объявлен режим чрезвычайной ситуации. Стоимость нефти отреагировала коротким взлетом, вернувшись вечером 10 мая 2021 г. к уровню до остановки. Эксперты называют происходящее крупнейшей в истории кибератакой на энергетическую инфраструктуру, которая может повлиять и на мировой рынок нефти, и на политику всей отрасли в области безопасности [3]. В начале июня 2021 г. была произведена кибератака на крупнейшего в мире производителя мяса JBS SA, которая вызвала остановку всех заводов по производству говядины в США, обеспечивающих почти четверть американских поставок. Все мясокомбинаты компании и региональные предприятия по производству говядины были вынуждены закрыться, а работа остальных мясоперерабатывающих предприятий JBS проходила со сбоями [1].

В России в 2021 г. было зафиксировано свыше *300 кибератак*, совершенных профессионалами, что на треть превышает показатели 2020 г. При этом абсолютное большинство (*92 %*) проведенных попыток профессиональных кибератак было направлено на объекты критической информационной инфраструктуры (далее – КИИ) – государственные организации, предприятия энергетики, промышленности и военно-промышленного комплекса [4], [5]. В результате киберпреступлений российские компании понесли колоссальные убытки, по некоторым оценкам они достигают *6 трлн рублей*. Основной ущерб связан с последствиями инцидентов – хищением денежных средств со счетов, выходом из строя оборудования, а также с перерывами в хозяйственной деятельности организации [1], [6]. Так, в августе и сентябре 2021 г. Альфа-банк, ВТБ, Сбербанк подверглись мощным DDoS-атакам, которые в ряде случаев повлияли на проведение платежей клиентов в удаленных каналах обслуживания и привели к сбоям на стороне внешнего поставщика услуг, что могло повлечь непродолжительные задержки в работе отдельных сервисов [7].

В Беларуси в 2021 г. установлено около *1 100* кибератак, которые были осуществлены в том числе и на КВОИ [8]. В частности, 25 апреля 2021 г. Министерство энергетики Республики Беларусь сообщило о взломе сайта Белорусской атомной электростанции. В результате кибератаки хакеры разместили на интернет-ресурсе предприятия фейковую информацию. В конце июля 2021 г. стало известно о взломе в Беларуси автоматизированной информационной системы «Паспорт», которая является инструментом автоматизации служебной деятельности подразделений паспортно-визовой службы уровня ГУВД Мингорисполкома, УВД облисполкомов, а также подчиненных им подразделений паспортно-визовой службы территориальных органов внутренних дел [1]. 24 января 2022 г. возникли проблемы с доступом к справочным web-ресурсам Белорусской железной дороги и сервисам оформления электронных проездных документов. На предприятии это связали с техническими причинами и заявили, что занимаются восстановлением работоспособности системы. На этом фоне одна из группировок, признанная в Беларуси террористической, заявила о проведении атаки на предприятие, целью которой было «замедлить и нарушить работу дороги», утверждалось, что для этого ее представители зашифровали основную часть серверов, баз данных и рабочих станций [9].

Несмотря на актуальность проблемы обеспечения безопасности КВОИ в специальной литературе ей уделяется недостаточно внимания. Рассматриваются лишь отдельные вопросы применительно к техническим мерам обеспечения безопасности таких объектов [10, с. 2-18], [11, с. 666–677], [12, с. 39-40]. Правовые аспекты исследуются фрагментарно [13, с. 57–61]. В связи с этим представляется обоснованным рассмотреть актуальные

современные проблемы правового регулирования обеспечения безопасности КВОИ и определить пути их преодоления.

Основная часть

В настоящее время актами национального законодательства ***КВОИ*** - определяется как объект информатизации, который на основании критериев отнесения объектов информатизации к КВОИ и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах включен в Государственный реестр КВОИ (*абз. 7 п. 33 Положения о технической и криптографической защите информации», утв. Указом Президента Республики Беларусь от 16.04.2013 № 196 (в ред. Указа Президента Республики Беларусь от 09.12.2019 № 449) [14]*). При этом ***объект информатизации*** рассматривается как средства электронной вычислительной техники вместе с программным обеспечением, в том числе системы управления различного уровня и назначения, информационные системы и сети, автономные стационарные и персональные электронные вычислительные машины, используемые в соответствии с заданной информационной технологией, системы управления информационными, производственными и (или) технологическими процессами (*абз. 10 п. 33 указанного Положения*).

Специалисты отмечают, что объектам критической инфраструктуры и органам власти важно в принципе не допустить реализации кибератак. Это требует принципиально нового подхода к выстраиванию информационной безопасности. В ее рамках нужно сформировать единую дорожную карту по цифровой трансформации и проектам информационной безопасности. Они должны включать повышение порога входа в базовую инфраструктуру, процессы обеспечения безопасности, особенно в уязвимых точках (удаленный доступ, управление доступом и двухфакторная аутентификация, контроль ИТ-подрядчиков). Затем требуется сформировать план экстренного восстановления систем при сбое или атаке и отработать все взаимодействия внутри этого плана, чтобы они были слаженными. Работу должна контролировать независимая группа профессионалов, которые организуют киберучения. Отдельного внимания требует повышение киберграмотности сотрудников – это позволит вовремя распознать методы социальной инженерии, используемой хакерами. Наконец, необходимо создать центр управления безопасностью, который будет не только выявлять и реагировать на возникающие инциденты, но и оценивать защищенность болевых точек компании, новых систем защиты, контролировать цифровизацию [15].

Однако это, в первую очередь, – меры технического, аппаратно-программного характера. Вместе с тем требует совершенствования и правовое регулирование обеспечения безопасности КВОИ.

Учитывая это, в современный период в Беларуси можно выделить ряд проблем в рассматриваемой сфере правового регулирования.

1. Пробелы в формировании системы правовых норм, регулирующих обеспечение безопасности КВОИ.

В настоящее время рассматриваемая сфера правового регулирования распространяется на:

деятельность владельцев КВОИ по обеспечению информационной безопасности соответствующих объектов;

деятельность уполномоченных государственных органов, осуществляющих контроль в этой сфере;

противоправную деятельность лиц, создающих угрозы информационной безопасности КВОИ.

Деятельность первых двух групп в современный период регламентируется следующими актами законодательства:

Положение о технической и криптографической защите информации», утв. Указом Президента Республики Беларусь от 16.04.2013 № 196 (в ред. Указа Президента Республики Беларусь от 09.12.2019 № 449);

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 65 «О показателях уровня вероятного ущерба национальным интересам Республики Беларусь» [16];

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 44» [17], которым, в частности, утверждаются: Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено; Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено; Положение о порядке технической и криптографической защиты информации, обрабатываемой на КВОИ, и ряд других комплексов нормативных требований в области информационной безопасности КВОИ.

Вместе с тем видится, что объем регулирования деятельности владельцев КВОИ является недостаточным.

Так, например, руководство профильного управления Федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК) считает, что одним из главных условий сложившейся ситуации в сфере обеспечения безопасности объектов КИИ является невыполнение владельцами таких объектов требований законодательства о безопасности КИИ (в первую очередь – требований Федерального закона «О безопасности критической информационной инфраструктуры Российской

Федерации» [18]). В качестве характерных неправомерных действий таких субъектов выделяются [19]:

многие пытаются уклониться от реализации федерального закона: с одной стороны – не относят себя к субъектам КИИ, несмотря на то, что все прямые и косвенные признаки на это указывают; с другой – отрицают, что у них есть объекты КИИ, которые необходимо категорировать;

ряд владельцев объектов КИИ нарушают сроки предоставления перечней объектов КИИ;

отдельные организации уведомляют регулятора не обо всех имеющихся у них объектах КИИ;

нарушаются сроки категорирования объектов КИИ;

искусственно занижаются категории значимости имеющихся объектов КИИ;

предоставляются недостоверные сведения об объектах КИИ и учитывают не все показатели;

субъекты КИИ недооценивают потенциал нарушителя и имеют проблемы с силами безопасности – у отдельных организаций безопасность значимых объектов обеспечивают подразделения по экономической безопасности, у некоторых – вообще юридические службы;

на многих объектах, особенно это касается автоматизированных систем управления технологическими процессами, применяются только средства антивирусной защиты и штатные средства операционных систем, что недостаточно для противостояния серьезным угрозам.

Для решения указанных проблем ФСТЭК во взаимодействии с заинтересованными государственными органами в начале 2021 г. был разработан и внесен в Государственную Думу РФ проект закона, предусматривающий изменения и дополнения в Кодекс Российской Федерации об административных правонарушениях в части введения административной ответственности за нарушение норм законодательства о безопасности КИИ, который был принят 26 мая 2021 г. [20]. В указанный Кодекс введены:

ст. 13.12.1, устанавливающая ответственность за Нарушение требований в области обеспечения безопасности КИИ Российской Федерации;

ст. 19.7.15, закрепляющая ответственность за непредставление сведений, предусмотренных законодательством в области обеспечения безопасности КИИ Российской Федерации.

При этом ст. 13.12.1 предусматривает ответственность за следующие нарушения:

часть 1 – нарушение требований к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов КИИ Российской Федерации, установленных федеральными законами и

принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие действия (бездействие) не содержат признаков уголовно наказуемого деяния, – влечет наложение административного штрафа на должностных лиц в размере от 10 000 до 50 000 рублей (примерно от 400 до 2 000 белорусских рублей); на юридических лиц – от 50 000 до 100 000 рублей (примерно от 2 000 до 4 000 белорусских рублей);

часть 2 – нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ Российской Федерации, установленного федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, – влечет наложение административного штрафа на должностных лиц в размере от 10 000 до 50 000 рублей (примерно от 400 до 2 000 белорусских рублей); на юридических лиц – от 100 000 до 500 000 рублей (примерно от 4 000 до 20 000 белорусских рублей);

часть 3 – нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ Российской Федерации, между субъектами КИИ Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, – влечет наложение административного штрафа на должностных лиц в размере от 20 000 до 50 000 рублей (примерно от 800 до 2 000 белорусских рублей); на юридических лиц – от 100 000 до 500 000 рублей (примерно от 4 000 до 20 000 белорусских рублей).

Положения ст. 19.7.15 предусматривает ответственность за следующие нарушения:

часть 1 – непредставление или нарушение сроков представления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ Российской Федерации, сведений о результатах присвоения объекту КИИ Российской Федерации одной из категорий значимости, предусмотренных законодательством в области обеспечения безопасности КИИ Российской Федерации, либо об отсутствии необходимости присвоения ему одной из таких категорий – влечет наложение административного штрафа на должностных лиц в размере от 10 000 до 50 000 рублей (примерно от 400 до 2 000 белорусских рублей); на юридических лиц – от 50 000 до 100 000 рублей (примерно от 2 000 до 4 000 белорусских рублей);

часть 2 – непредставление или нарушение порядка либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации информации, предусмотренной законодательством в

области обеспечения безопасности КИИ Российской Федерации, за исключением случаев, предусмотренных ч. 2 ст. 13.12.1 рассматриваемого Кодекса, – влечет наложение административного штрафа на должностных лиц в размере от 10 000 до 50 000 рублей (примерно от 400 до 2 000 белорусских рублей); на юридических лиц – от 100 000 до 500 000 рублей (примерно от 4 000 до 20 000 белорусских рублей).

Представляется, что рассмотренная ситуация является характерной и для Республики Беларусь. В связи с этим видится целесообразным внести соответствующие изменения и в Кодекс Республики Беларусь об административных правонарушениях.

Основным способом борьбы с противоправной деятельностью лиц, создающих угрозы информационной безопасности КВОИ, можно обоснованно рассматривать использование норм административного и уголовного права. Так, незаконные действия указанных лиц образуют следующие административные правонарушения и преступления:

несанкционированный доступ к компьютерной информации (*ст. 23.4 Кодекса Республики Беларусь об административных правонарушениях [21], ст. 349 Уголовного кодекса Республики Беларусь [22] (далее – УК)*);

уничтожение, блокирование или модификация компьютерной информации (*ст. 350 УК*);

разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (*ст. 354 УК*).

При этом в Беларуси в 2021 г. из всего числа совершенных киберпреступлений (*16 446*) по фактам совершения преступлений, предусмотренных ст. 349 УК, было возбуждено *6,7 %* (*1 104*) уголовных дел. По остальным статьям, предусматривающим ответственность за данные преступные деяния уголовные дела не возбуждались [8].

В Российской Федерации в 2021 г. было возбуждено *70 уголовных дел* из-за кибератак и другого неправомерного воздействия на КИИ [23]. Это составило *0,013 %* от всего числа возбужденных уголовных дел, связанных с киберпреступлениями (*518 000*) [24]. При этом отмечается, что половина уголовных дел, о которых идет речь, касается использования программ, заведомо предназначенных для неправомерного использования на КИИ. Например, по одному из дел работники локомотивных бригад Российской железной дороги воспользовались нештатным программным обеспечением, чтобы пройти тест на знание технически-распорядительных актов железнодорожных станций. По другому делу сотрудник Пермского порохового завода скачал нелицензионную версию Microsoft Word, генератор ключа для которой, по версии обвинения, установил канал обмена информацией с «принадлежащим США» IP-адресом [23].

Необходимо отметить, что в июне 2017 г. в Уголовный кодекс Российской Федерации была введена ст. 274.1, которая устанавливает повышенную уголовную ответственность за неправомерное воздействие на КИИ Российской Федерации [25]. В частности, ответственность предусмотрена за следующие противоправные действия:

часть 1 – создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, – наказываются принудительными работами на срок до 5 лет с ограничением свободы на срок до 2 лет или без такового либо лишением свободы на срок от 2 до 5 лет со штрафом в размере от 500 000 до 1 млн рублей (примерно от 20 000 до 40 000 белорусских рублей) или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет;

часть 2 – неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на КИИ Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда КИИ Российской Федерации, – наказывается принудительными работами на срок до 5 лет со штрафом в размере от 500 000 до 1 млн рублей (примерно от 20 000 до 40 000 белорусских рублей) или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет и с ограничением свободы на срок до 2 лет или без такового либо лишением свободы на срок от 2 до 6 лет со штрафом в размере от 500 000 до 1 млн рублей (примерно от 20 000 до 40 000 белорусских рублей) или в размере заработной платы или иного дохода осужденного за период от одного 1 до 3 лет;

часть 3 – нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда КИИ Российской Федерации, – наказывается принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового

либо лишением свободы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового;

часть 4 – деяния, предусмотренные ч.ч. 1, 2 или 3 данной статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения, – наказываются лишением свободы на срок от 3 до 8 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового;

часть 5 – деяния, предусмотренные частью 1, 2, 3 или 4 настоящей статьи, если они повлекли тяжкие последствия, – наказываются лишением свободы на срок от 5 до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового.

Представляется, что в настоящее время подобные преступные деяния характерны и для Республики Беларусь. В связи с этим видится обоснованным внести соответствующие изменения и в УК.

2. Пробелы в правовом регулировании использования оборудования и программного обеспечения на КВОИ.

Во многих случаях для обеспечения деятельности КВОИ используется иностранное оборудование и программное обеспечение.

В Российской Федерации отмечают, что есть порядка 10-15 импортных программных продуктов, которые широко используют ведущие российские промышленные предприятия, и ограничение или прекращение доступа к которым несет в себе критические риски. Один из популярных продуктов – платформа передачи данных PI System от Aveva (изначально разрабатывалась OSI Soft). Если вендор решит отозвать лицензии, то крупнейшие нефтеперерабатывающие предприятия России останутся без системы диспетчеризации. Более того, 90 % непрерывных производств в России используют PI System в качестве базы данных реального времени, которая собирает промышленную информацию, на основе которой осуществляется оперативное управление производством. Еще один пример – продукты для сбора данных и диспетчерского контроля уровня SCADA. Так, «Транснефть» и Мосводоканал применяют HMI/SCADA iFIX компании GE. В первом случае – для управления заглушками, насосами нефти, во втором случае – воды. Эти системы являются критически важными. Их отключение в «Транснефти» может привести к полной остановке транспортировки нефти и нефтепродуктов по трубопроводам компании и к необходимости перейти на ручное локальное управление. А если аналогичное произойдёт в Мосводоканале, то риск связан с перебоями водоснабжения многих районов мегаполиса. При этом можно перейти на полуавтоматическое локальное управление процессами,

насосами и задвижками и восстановить водоснабжение, но для этого потребовалось бы удвоить штат операторов. На большинстве российских нефтеперерабатывающих заводов для установок первичной и глубокой переработки нефти используется программное обеспечение класса DCS (распределенных систем управления (РСУ)) компаний Honeywell, Emerson, ABB, Yokogawa. Отключение РСУ приведет к остановке заводов [26].

В целях обеспечения технологической независимости и безопасности КИИ Президент России В. В. Путин 30 марта 2022 г. подписал Указ № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [27]. Данный документ предусматривает с 31.03.2022 запрет на закупку иностранного программного обеспечения для обеспечения деятельности значимых объектов КИИ и услуг, необходимых для использования этого программного обеспечения, а с 01.01.2025 – запрет на использование иностранного программного обеспечения на таких объектах. При этом Правительству РФ предписано в 6-месячный срок реализовать комплекс мероприятий, направленных на обеспечение преимущественного применения субъектами КИИ российских радиоэлектронной продукции и телекоммуникационного оборудования на принадлежащих им значимых объектах КИИ.

Актуальность данного шага подтверждена последующими событиями – в начале июня 2022 г. Китайская Республика (Тайвань) в связи с военными действиями на территории Украины ограничила поставки в Россию любых чипов с тактовой частотой свыше 25 МГц, а также микросхем с количеством контактов до 144 единиц, а также литографического оборудования, которое может быть использовано для изготовления подобных микросхем (на долю Тайваня приходится более 90 % такой продукции). Как отмечается, указанные микросхемы используются повсеместно: от компьютеров до автомобилей. Поэтому найти равноценную замену чипам и микросхемам будет крайне сложно. Кроме того, процессоры российского происхождения Baikal и «Эльбрус» также до недавнего времени собирались на Тайване. Беларусь при этом указана как страна, которая способна помочь РФ действовать в обход санкций [28].

Представляется, что данные проблемы характерны и для Республики Беларусь. В связи с этим представляется необходимым уже сейчас начать разрабатывать комплекс организационно-правовых мер, в первую очередь в области правового регулирования разработки и использования оборудования и программного обеспечения для КВОИ. Такие меры могут включать как разработку и совершенствование национальных актов законодательства, регламентирующих отношения в данной области, (например, по импортозамещению) так и заключение международных договоров с

дружественными странами о кооперации в сфере разработки и использования соответствующих технических и программных продуктов для КВОИ.

Заключение

Изложенное позволяет сделать следующие выводы.

1. В современный период обеспечение безопасности КВОИ является одним из важнейших направлений обеспечения национальной безопасности каждого государства, в том числе и Республики Беларусь. Актуальными угрозами безопасности КВОИ являются недостаточность мер, принимаемых собственниками (владельцами) данных объектов по созданию необходимых условий для их нормальной деятельности, а также совершение различного характера преступлений в отношении таких объектов (кибератак). Одним из ключевых факторов, способствующими реализации таких угроз, является использование на КВОИ иностранного оборудования и программного обеспечения.

2. Характер имеющих место угроз безопасности КВОИ обуславливает необходимость адекватного реагирования на них уполномоченных субъектов. Для достижения стабильного и бесперебойного функционирования КВОИ уполномоченными государственными органами и собственниками (владельцами) данных объектов предпринимаются различные меры, в том числе правового характера. В настоящее время первоочередными из них являются меры, направленные на устранение пробелов в правовом регулировании деятельности собственников (владельцев) КВОИ и противодействие угрозам таким объектам.

3. Совершенствование правового регулирования обеспечения безопасности КВОИ в современных условиях целесообразно осуществлять по следующим направлениям:

принятие национальных актов законодательства, устанавливающих требования в области разработки и использования оборудования и программного обеспечения для КВОИ, а также заключение международных договоров с дружественными странами о кооперации в данной сфере;

установление мер административной ответственности для владельцев (собственников) КВОИ за невыполнение владельцами таких объектов требований законодательства об их безопасности;

установление уголовной ответственности за деяния, направленные на неправомерное воздействие на КВОИ.

Библиографический список

1. Кибератаки [Электронный ресурс] / Tadviser: Государство.Бизнес.Технологии: 2022/02/04. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D

0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8. – Дата доступа: 07.04.2022.

2. Check Point Research : Cyber Attacks Increased 50 % Year over Year [Electronic resource] // Check Point. – Режим доступа: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/. – Access date: 07.04.2022.

3. Бесполезные ископаемые [Электронный ресурс] / А. Наумов, Е. Черненко, О. Мордюшенко // Комменрсантъ: 10.05.021. – Режим доступа: https://www.kommersant.ru/doc/4802807. – Дата доступа: 07.04.2022.

4. Более 90% кибератак в 2021 г. пришлось на объекты критической инфраструктуры РФ [Электронный ресурс] // INTERFAX.RU: 7 декабря 2021. – Режим доступа: https://www.interfax.ru/russia/806997. – Дата доступа: 07.04.2022.

5. Хакеры с квалификацией выбирают КИИ / К. Скурат // ComNews: 08.12.2021. – Режим доступа: https://www.comnews.ru/content/217824/2021-12-08/2021-w49/khakery-kvalifikaciey-vybirayut-kii. – Дата доступа: 07.04.2022.

6. Почему киберпреступления – угроза национальной безопасности Электронный ресурс] // ВЕДОМОСТИ: 7 декабря 2021. – Режим доступа: https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti. – Дата доступа: 07.04.2022.

7. Замедление взлому подобно [Электронный ресурс] / М. Буйлов, Ю. Степанова, А. Гаврилюк // Коммерсантъ: 04.09.2021. – Режим доступа: https://www.kommersant.ru/doc/4974831. – Дата доступа: 07.04.2022.

8. Начальник ГУПК МВД Андрей Ковалев: «В текущем году прогнозируется рост интернет-мошенничеств, в том числе связанных с криптовалютой» [Электронный ресурс] // Официальный сайт МВД Республики Беларусь: 23.02.2022. – Режим доступа: https://www.mvd.gov.by/ru/news/9084. – Дата доступа: 07.04.2022.

9. БЖД восстановила онлайн-продажу билетов на электрички и дизель-поезда [Электронный ресурс] // Sputnik Беларусь: 03.02.2022. – Режим доступа: https://sputnik.by/20220203/bzhd-vosstanovila-onlayn-prodazhu-biletov-na-elektrichki-i-dizel-poezda-1060029514.html#pv=g%3D1060029514%2Fp%3D1043362160. – Дата доступа: 07.04.2022.

10. Маликов, В. В. Повышение эффективности информационных и инженерно-технических систем защиты критически важных объектов : автореф. дис. ... канд. техн. наук : 05.13.19 / В. В. Маликов ; Бел. гос. ун-т информатики и радиоэлектроники. – Минск, 2010. – 23 с.

11. Мелех, О. В. Классификация критически важных объектов информатизации по требованиям физической защиты с использованием методов кластерного анализа / О. В. Мелех, Е. П. Максимович, В. К. Фисенко // Искусственный интеллект. – 2010. – № 4. – С. 666–677.

12. Барановский, О. К. Актуальные вопросы технической защиты информации в системах физической защиты объектов критической инфраструктуры / О. К. Барановский // Технологии безопасности. – 2012. – № 3. – С. 39–40.

13. Рябоволов, В. Правовые аспекты государственного регулирования системы обеспечения безопасности критически важных объектов информатизации / В. Рябоволов, А. Чернолевский // Юстиция Беларуси. – 2016. – № 7. – С. 57–61.

14. Положение о порядке отнесения объектов информатизации к критически важным объектам информатизации [Электронный ресурс] : Указ Президента Республики Беларусь, 16 апр. 2013 г. № 196 : в ред. Указа Президента Респ. Беларусь от 09.12.2019 //

ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

15. Киберхулиганы и кибернаемники: как бороться с новыми угрозами инфобеза [Электронный ресурс] / Мария Решетникова // РБК: 21.12.2021. – Режим доступа: https://trends.rbc.ru/trends/industry/61c1951e9a79475fdac24d4c. – Дата доступа: 07.04.2022.

16. О показателях уровня вероятного ущерба национальным интересам Республики Беларусь [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 20 фев. 2020 г., № 65 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

17. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 44 [Электронный ресурс]: приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 20 фев. 2020 г., № 66 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

18. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: Федер. закон, 26 июля 2017 г., № 187-ФЗ // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2022.

19. Безопасность критической информационной инфраструктуры РФ [Электронный ресурс] / Tadviser: Государство.Бизнес.Технологии: 2021/12/08. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D1%8B_%D0%A0%D0%A4. – Дата доступа: 07.04.2022.

20. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс] : Федер. закон, 26 мая 2021 г., № 141-ФЗ // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2022.

21. Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс]: 6 янв. 2021 г., № 92-З: принят Палатой представителей 18 дек. 2020 г.: одобр. Советом Респ. 18 дек. 2020 г.: в ред. Закона Респ. Беларусь от 04.01.2022 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2022.

22. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г.: в ред. Закона Респ. Беларусь от 05.01.2022 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

23. Уголовные дела на рынке информационных технологий России [Электронный ресурс] / Tadviser: Государство.Бизнес.Технологии: 2022/02/04. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D1%8B%D0%B5_%D0%B4%D0%B5%D0%BB%D0%B0_%D0%BD%D0%B0_%D1%80%D1%8B%D0%BD%D0%BA%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D1%85_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B9_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8. – Дата доступа: 07.04.2022.

24. Число киберпреступлений в России [Электронный ресурс] / Tadviser: Государство.Бизнес.Технологии: 2022/02/18. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D0%B9_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8#:~:text=%D0%9F%D0%BE%20%D1%81%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B5%20%D0%9C%D0%92%D0%94%2C%20%D0%B7%D0%B0%20%D1%81%D0%B5%D0%BC%D1%8C,104%20%D1%82%D1%8B%D1%81%D1%8F%D1%87%D0%B8%20%E2%80%94%20%D1%81%20%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5%D0%BC%20%D0%BA%D0%B0%D1%80%D1%82. – Дата доступа: 07.04.2022.

25. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] : Федер. закон, 26 июля 2017 г., № 194-ФЗ // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2022.

26. Критическая инфраструктура России [Электронный ресурс] // Tadviser: Государство.Бизнес.Технологии: 2022/03/30. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8. – Дата доступа: 07.04.2022.

27. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс] : Указ Президента Рос. Федерации, 30 марта 2022 г., № 166 // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2022.

28. Тайвань ввел запрет на поставку электронных чипов в Россию / А. Абрамов // SPBITRU: 03.06.2022. – Режим доступа: https://spbit.ru/news/n211027/. – Дата доступа: 05.06.2022.

УДК 342.4

ТРАНСФОРМАЦИЯ ПОНИМАНИЯ КОНСТИТУЦИОННЫХ ЦЕННОСТЕЙ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ[1]

А.С. Бакун

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

Статья посвящена вопросам изменения понимания конституционных ценностей в контексте обеспечения информационной безопасности Республики Беларусь. Особое внимание автор статьи уделяет таким конституционным ценностям как права человека. На основе обобщения делается вывод о том, что новое понимание прав человека в информационном пространстве предусматривает как дополнительные возможности по их обеспечению и реализации, так указывает на дополнительные риски и угрозы их нарушения в информационной среде. Предложены рекомендации по дальнейшему совершенствованию отечественного законодательства в сфере реализации конституционных ценностей при обеспечении информационной безопасности.

Ключевые слова: конституционные ценности, информационная безопасность, права человека, личные права человека, политические права человека, социально-экономические и культурные права человека.

TRANSFORMATION OF THE UNDERSTANDING OF CONSTITUTIONAL VALUES WHILE ENSURING INFORMATION SECURITY OF THE REPUBLIC OF BELARUS

A.S. Bakun

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article is devoted to the changes in the understanding of constitutional values in the context of ensuring information security of the Republic of Belarus. The author of the article pays special attention to such constitutional values as human rights. Based on the generalization, it is concluded that a new understanding of human rights in the information space provides both additional opportunities for their provision and implementation, and indicates additional risks and threats of their violation in the information environment. Recommendations are proposed for further improvement of domestic legislation in the field of implementation of constitutional values while ensuring information security.

[1] Статья подготовлена в рамках участия в НИР ГПНИ «Информационная безопасность личности и государства в современном международном праве» ГПНИ № ГР 20212197.

Keywords: constitutional values, information security, human rights, personal human rights, political human rights, socio-economic and cultural human rights.

Введение

Всеобщность информационного пространства предполагает обеспечение его защиты. Это обусловлено, в первую очередь, увеличением количества пользователей интернетом в мире и ростом показателей глобального проникновения интернета [1], а, во вторую, – интенсификацией неправомерных действий со стороны других государств или других пользователей.

С развитием информационного общества совершенствуются и способы нарушения информационной безопасности, следовательно, безопасность в информационной сфере приобретает особое значение. Каждое государство в отдельности, а также мировое сообщество в целом не только принимают, но и постоянно модернизируют различные меры защиты информации. Такие понятия как, например, цифровая гигиена [2], персональные данные в информационных технологиях [3], кибервойска [4], киберпреступность [5], информационный суверенитет [6] с определенного времени стали объектом научных исследований, в том числе, правовых.

Безусловно, в период активного развития цифровизации и информатизации трансформации подвергается и традиционное восприятие основополагающих конституционных ценностей государства, таких как, например, права человека, правовая государственность, социальная государственность, государственный суверенитет, гражданство, демократия, разделение властей, республиканская форма правления. Однако основными конституционными ценностями, понимание которых в контексте информационной безопасности государства подвергается трансформации и отличается от традиционного, являются права человека. Новое понимание каталога прав человека в информационном пространстве предусматривает, с одной стороны, дополнительные возможности по их реализации, а, с другой стороны, указывает на дополнительные угрозы их нарушения в информационной среде.

Основная часть

Обеспечение государством информационной безопасности в последнее время приобретает основополагающее значение как в международно-правовой сфере, так и в национальном сегменте сети Интернет. Информационная сфера представляет собой самостоятельную сферу национальной безопасности, в которой необходимо обеспечить защиту информационных ресурсов, систем их формирования, распространения и использования, информационной инфраструктуры, реализацию прав на информацию государства, юридических лиц, граждан [7, с. 56].

Проблеме безопасности в информационной сфере в настоящее время уделяется много внимания, в том числе государственном уровне. На современном этапе развития человечества информация затрагивает все сферы

жизнедеятельности человека, например, политику, экономику, образование, культуру, здравоохранение, безопасность, досуг, развлечение и т.д. Особую актуальность информационная безопасность приобретает в связи с проникновением технических средств обработки и передачи данных практически во все сферы человеческой деятельности. В научной юридической литературе исследуются различные аспекты информационной безопасности [2; 3; 4; 5; 6; 8].

Универсального понимания информационной безопасности в научной литературе не существует. Имеющие место в научной и учебной литературе определения можно свести к пониманию информационной безопасности как защищенности информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации [9, с. 18]. Следовательно, информационная безопасность государства предполагает такое состояние, при котором обеспечивается сохранность информационных ресурсов государства и защищенность законных прав личности и общества в информационной сфере [10, с. 121]. Полагаем, что в основу данного определения взято техническое определение информационной безопасности, однако постепенно его стали понимать таким образом не только в технической, но и в иных сферах.

На законодательном уровне определения и вопросы обеспечения информационной безопасности в Республике Беларусь урегулированы. Отечественный законодатель закрепил определение информационной безопасности в двух основополагающих нормативных документах государства. Так, в соответствии с п. 4 Концепции национальной безопасности Республики Беларусь «информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере» [11]. Данное определение продублировано в п. 8 Концепции информационной безопасности Республики Беларусь [12]. В п. 5 Концепции информационной безопасности Республики Беларусь белорусский законодатель также обосновал необходимость принятия данной концепции, которая «определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности», а также «обеспечивает комплексный подход к проблеме информационной безопасности, создает методологическую основу для совершенствования деятельности по ее укреплению, служит основанием для формирования государственной политики, выработки мер по совершенствованию системы обеспечения информационной безопасности, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере» [12]. Полагаем, что принятие такого рода концептуальных нормативных документов является важным этапом для государства в обеспечении собственной национальной

безопасности в информационной сфере, легализирующем проводимую информационную внешнюю и внутреннюю политику. Такие нормативные документы, как Концепция информационной безопасности Республики Беларусь, принимаются для защиты в информационной сфере конституционного строя государства, закрепленных в Основном законе ценностей. Обеспечение национальной безопасности в информационной сфере представляется важнейшей функцией государства на современном этапе в связи с увеличением значения данной сферы для личности, общества и самого государства и интенсификации общественных отношений в рассматриваемой области.

В международном праве постоянно идут процессы накопления опыта в сфере обеспечения информационной безопасности в рамках деятельности таких международных организаций, как ООН, Совет Европы, Европейский союз, БРИКС, ШОС, ЕАЭС, СНГ, ОДКБ, а также Союзного государства Республики Беларусь и России и др. Среди международных актов в информационной сфере можно отметить Окинавскую хартию глобального информационного общества [13], итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества (2003 г. в Женеве и 2005 г. в Тунисе) [14], а также Генеральной Ассамблеей ООН [15], ОБСЕ [16] принят ряд резолюций в области обеспечения международной информационной безопасности, которые являются основополагающими политико-правовыми документами, направленными на ускорение формирования постиндустриальных тенденций в экономической, социально-политической и духовной сферах жизни общества. Построение информационного общества в качестве глобальной задачи также закреплено в Декларации принципов, принятой на Всемирной встрече на высшем уровне в Женеве в 2003 г. [14] по вопросам информационного общества. В данной Декларации указано, что при построении информационного общества необходимо обеспечить безопасность при использовании информационных технологий.

Однако все упомянутые международные акты приняты в начале нового тысячелетия и представляют собой декларации действий государств и международного сообщества по формированию информационного общества, и только как следствие, – обеспечения информационной безопасности при его построении и развитии. В доктрине международного права отмечается, что в настоящее время вопросы обеспечения информационной безопасности не получили закрепления в специальном международном договоре, заключенном под эгидой ООН. Указанные аспекты преимущественно урегулированы на региональном и двустороннем уровне [17]. Таким образом, универсализация правовой регламентации и правового регулирования информационной безопасности на международном уровне предположительно станет следующим этапом в построении международно-правовой парадигмы в информационной сфере.

Повсеместное проникновение информатизации формирует иное восприятие общепринятых правовых категорий в контексте необходимости обеспечения информационной безопасности на государственном и международном уровнях. Одними из таких правовых категорий, подвергшиеся наиболее заметному влиянию информатизации, представляются правовые ценности. Анализ научной юридической литературы показал, что существует классификация правовых ценностей. Так, Т. С. Масловская выделяет три уровня ценностей. Первый уровень представляет собой общечеловеческие ценности, «то есть универсальные социальные ценности, признаваемые всеми людьми» [18]. Такие универсальные ценности представляются социальными аксиомами и не зависят от экономического, политического, исторического факторов. Второй уровень составляют региональные ценности [18]. Главным отличием универсальных от региональных ценностей представляется влияние экономических, географических, политических, исторических или иных факторов того или иного региона. На третьем уровне располагаются «национальные конституционные ценности общества и государства, базирующиеся на общечеловеческих ценностях» [18]. В конституционных ценностях сохраняется национальная идентичность, отражающая особенности исторического развития государства. Конституционные ценности индивидуализируются в зависимости от приоритетов государства.

Особую значимость упоминание о ценностях приобретает в тексте конституции, которая сама по себе является общегосударственной ценностью, ведь каждое государство формирует свои базовые ценности [19]. В Республике Беларусь конституционными ценностями являются классические правовые ценности демократического государства. Так, в Разделе I «Основы конституционного строя» Конституции Республики Беларусь [20] закреплены все основополагающие конституционные ценности белорусского государства, такие как права человека (ст. 2), социальная государственность (ст. 1), государственный суверенитет (ст. 3), гражданство (ст. 10), демократия (ст. 4), разделение властей (ст. 6), верховенство права (ст. 7), республиканская форма правления (ст. 1) и др.

Главными правовыми ценностями, закрепленными в Конституции Республики Беларусь, являются права человека (ст. 2) [20]. Изменения в понимании прав человека и способов их реализации в информационной сфере касаются всех их видов: личных (гражданских), политических, социально-экономических и культурных.

Трансформации понимания при обеспечении информационной безопасности произошла в отношении личного права «на защиту от незаконного вмешательства в его частную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство» (ст. 28) [20]. Так, например, статья 28 Конституции

Республики Беларусь по результатам республиканского референдума в 2022 году дополнена частью 2, в которой закреплено, что «государство создает условия для защиты персональных данных и безопасности личности и общества при их использовании» [20]. Следовательно, понимание права на неприкосновенность частной жизни значительно расширилось, в него включены цифровые персональные данные. Исходя из уточненного понимания исследуемого права, расширились и способы реализации права на неприкосновенность частной жизни в контексте обеспечения информационной безопасности. Данное право сейчас предполагает защиту от посягательств на него и в информационной сфере.

В конституции любого государства также закреплены опорные ценности, достоверно представляющие соответствующую национально-культурную традицию. Ядром же всякого традиционализма, в том числе и традиционализма восточнославянской цивилизации [21, с. 54], является определенная религия [22]. В конституциях большинства государств закрепляется свобода вероисповедания как правовая форма закрепления религиозных ценностей, отражение потребностей и приоритетов населения, проживающего на территории данного государства, продолжения цивилизации (например, христианской или исламской).

Так, в соответствии со ст. 31 Конституции Республики Беларусь «каждый имеет право самостоятельно определять свое отношение к религии, единолично или совместно с другими исповедовать любую религию или не исповедовать никакой, выражать и распространять убеждения, связанные с отношением к религии, участвовать в отправлении религиозных культов, ритуалов, обрядов, не запрещенных законом» [20]. Полагаем, что непосредственное закрепление в конституционном законодательстве свободы вероисповедания является значительным достижением современной юриспруденции и итогом эволюции законодательства в области прав человека.

Существуют множество философских и правовых подходов к пониманию свободы вероисповедания, следствием систематизации которых выступает выработка интегративно-правового подхода к пониманию указанной свободы. В соответствии с интегративно-правовым подходом под свободой вероисповедания следует понимать фундаментальную, неотъемлемую свободу, выражающуюся в возможности иметь религиозные убеждения, выбирать религиозные учения и действовать в соответствии с ними, пределы которой устанавливаются законодательством [23, с. 69]. Однако свобода вероисповедания представляет собой не только фундаментальную и неотчуждаемую свободу в системе прав и свобод человека, но и одну из важнейших конституционных ценностей.

В отличие от права на неприкосновенность частной жизни понимание свободы вероисповедания не претерпело трансформации. Изменения затронули непосредственно способы осуществления данной свободы.

Так, например, в настоящее время свободу вероисповедания можно реализовывать в информационной сфере посредством просмотра видеозаписей богослужений, духовных программ в Интернете, духовное общение в интернет-чатах со священнослужителями, а также ряд религиозных организаций в период COVID-19 начал предоставляли возможность осуществления виртуальной исповеди верующих [24]. Безусловно, информатизация предполагает определенные изменения даже в таких консервативных институтах как церковь. Однако, на наш взгляд, именно институту церкви необходимо сохранить классические способы реализации свободы вероисповедания, особенно в части осуществления различных таинств. Это необходимо не только, чтобы избежать различных злоупотреблений при использовании новых способов осуществления различных таинств в информационном пространстве, но и с целью сохранения их сакральности.

Рассматривая осуществление политических прав и свобод в информационной сфере, следует указать на применение электронного голосования на выборах [25] в ряде стран как нового способа реализации избирательных прав.

В Республике Беларусь такой способ реализации избирательных прав до настоящего времени не применялся. В ст. 38 Конституции Республики Беларусь закрепляется классическое понимание избирательных прав граждан республики, которые «имеют право свободно избирать и быть избранными в государственные органы на основе всеобщего, равного, прямого или косвенного избирательного права при тайном голосовании» [20]. Анализ избирательных прав показал, что в данном случае также имеет место трансформация способов их реализации, а не их понимания.

В свою очередь, классическое понимание свободы мнений, убеждений и их свободного выражения, закрепленное в ст. 33 Конституции Республики Беларусь [20], претерпело изменения в контексте обеспечения информационной безопасности. К традиционным формам выражения мнений добавились новые формы в информационном пространстве, что существенно расширило понимание рассматриваемой свободы.

Кроме того, существенными отличиями реализации свободы мнений в информационной сфере являются: во-первых, не имеющий границ всеобъемлющий открытый характер скорости распространения суждений отдельной личности; во-вторых, существует возможность фиксации информации анонимно; в-третьих, существуют особые ограничения и способы защиты; в-четвертых, посредством Интернет быстрее реализуется возможность трансформации суждений отдельной личности в феномен общественного

мнения, влияющего на функционирование общества и его политической системы [26]. Все это свидетельствует о росте рисков злоупотребления данной свободой и угроз ее незаконного нарушения иными пользователями Интернет-ресурсов.

Социально-экономические и культурные права и свободы также подверглись пересмотру в период COVID-19, их осуществление интенсифицировалось в информационной сфере.

Примерами такой интенсификации могут служить посещение виртуальных экскурсий по музейным экспозициям как способ реализации права на участие в культурной жизни (ст. 51 Конституции Республики Беларусь) [20], получение образования с использованием информационно-коммуникационных технологий [27] как способ реализации права на образование (ст. 49 Конституции Республики Беларусь) [20], участие в конференциях посредством видеоконференцсвязи, реализация права на труд (ст. 41 Конституции Республики Беларусь) [20] с применением информационных технологий в связи с переводом работников на дистанционный формат работы. Однако все изменения социально-экономических и культурных прав и свобод касаются исключительно способов реализации данной категории прав, а не их классического понимания.

Заключение

В научной юридической литературе исследуются различные аспекты информационной безопасности, а также анализируются отдельные институты и субъекты правовых отношений, которые складываются в информационной сфере. Однако, несмотря на всеобъемлющий характер научных исследований в сфере информационной безопасности, юридическая наука не выработала универсального подхода к ее пониманию. В основу определения информационной безопасности в юридической науке легла дефиниция, используемая в технических науках. Имеющие место в научной и учебной литературе определения можно свести к пониманию информационной безопасности как защищенности информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации. Следовательно, информационная безопасность государства предполагает такое состояние, при котором обеспечивается сохранность информационных ресурсов государства и защищенность законных прав личности и общества в информационной сфере.

Законодательная регламентация информационной безопасности также отличается неопределенностью и некоторой двойственностью. С одной стороны, на национальном законодательном уровне в Республике Беларусь приняты основополагающие документы, регламентирующие проводимую государством информационную внешнюю и внутреннюю политику, такие

как Концепция национальной безопасности Республики Беларусь и Концепция информационной безопасности Республики Беларусь.

Такие нормативные документы принимаются для защиты конституционного строя государства, а также обеспечения безопасной реализации в информационной сфере закрепленных в Основном законе ценностей. С другой стороны, на международном уровне отсутствует специальная международная конвенция в рамках деятельности ООН по вопросам обеспечения информационной безопасности. Указанные аспекты, как правило, урегулированы на региональном и двустороннем уровне. Таким образом, универсализация правовой регламентации и правового регулирования информационной безопасности на международном уровне предположительно станет следующим этапом в построении международно-правовой парадигмы в информационной сфере.

Активизация развития информационной сферы оказывает безусловное влияние на обеспечение реализации основополагающих конституционных ценностей, закрепленных в Основных законах государств.

В период активного развития информационного общества трансформации подвергается устоявшееся понимание прав человека, верховенства права, социальной государственности, государственного суверенитета, гражданства, демократии, разделения властей, республиканской формы правления.

Все вышеперечисленные категории являются не только фундаментальными институтами конституционного права, но и основополагающими конституционными ценностями любого демократического государства. Однако основными конституционными ценностями, понимание которых в контексте информационной безопасности государства подвергается трансформации и отличается от традиционного, являются права человека.

С одной стороны, инновационный подход к пониманию прав человека в контексте развития информационном общества предусматривает дополнительные возможности по их обеспечению и реализации. С другой стороны, при таком подходе возникают дополнительные риски и угрозы информационной безопасности, увеличивается количество злоупотреблений данными правами, правонарушений и преступлений, осуществляемых с использованием информационно-коммуникационных и IT технологий, в процессе реализации тех или иных прав и свобод человека. Последнее свидетельствует о необходимости дальнейшего совершенствования международного права и национального законодательства в области информационной безопасности с целью обеспечения осуществления таких основополагающих конституционных ценностей как права человека.

Библиографический список

1. Digital 2021 : актуальная статистика и аудитория социальных сетей в мире и Беларуси [Электронный ресурс] // Ретинг Байнета. – 2022. – Режим доступа : https://ratingbynet.by/digital-2021-aktualnaya-statistika-i-auditoriya-sotsialnykh-setey-v-mire-i-belarusi/. – Дата доступа : 01.06.2022.
2. Гусев, В. А. Цифровая гигиена vs. киберпреступность / В.А. Гусев // Психопедагогика в правоохранительных органах. – 2022. – Т. 27. – № 1 (88). – С. 102–108.
3. Солдатова, В. И. Защита персональных данных в условиях применения цифровых технологий / В. И. Солдатова // Lex Russia. – 2020. – Т. 73. – № 2 (159). – С. 33–43.
4. Хлопов, О. А. Перспективы создания единых кибервойск США [Электронный ресурс] / О. А, Хлопов // MILITARY SCIENCE / «Colloquium-journal. – 2019. – № 15 (39). – 2022. – Режим доступа : file:///C:/Users/annas/Downloads/perspektivy-sozdaniya-edinyh-kibervoysk-ssha.pdf. – Дата доступа : 01.06.2022.
5. Номоконов, В. А. Киберпреступность как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина // Криминология : вчера, сегодня, завтра. – № 1 (24). – С. 45–55.
6. Мороз, Н. О. Информационный суверенитет Республики Беларусь в контексте современного международного права / Мороз Н. О. // Право.by. – 2022. – № 2. – С. 111–116.
7. Боричевская, В. В. Уголовно-правовые аспекты обеспечения информационной безопасности в Республике Беларусь / В. В. Боричевская // Гуманітарна-эканамічны веснік. – 2010. – № 2. – С. 56–65.
8. Карцхия, А. А. Информационная безопасность: правовые аспекты / А. А. Карцхия, В. Л. Севостьянов // Правовая информатика. 2018. – № 4. – С. 43–48.
9. Гафнер, В. В. Информационная безопасность : учеб. пособие : в 2 ч. / В. В. Гафнер ; ГОУ ВПО «Урал. гос. пед. ун-т». – Екатеринбург, 2009. – Ч. 1. – 155 с.
10. Веруш, А. И. Национальная безопасность Республики Беларусь : курс лекций / А.И. Веруш. – Минск: Амалфея, 2012. – 204 с.
11. Концепция национальной безопасности Республики Беларусь [Электронный ресурс] : утв. Указом Президента Республики Беларусь, 9 нояб. 2010 г., № 575 : в ред. Указа от 24.01.2014 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
12. Концепции информационной безопасности Республики Беларусь [Электронный ресурс]: Постановление Совета Безопасности Республики Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
13. Окинавская хартия глобального информационного общества [Электронный ресурс] // Официальный сайт Президента России. – 2022. – Режим доступа: http://www.kremlin.ru/supplement/3170. – Дата доступа : 01.06.2022.
14. Резолюции Генеральной Ассамблеи ООН по информационно-коммуникационным технологиям // Официальный сайт Организации Объединенных Наций. – 2022. – Режим доступа : https://www.un.org/ru/development/ict/res.shtml. – Дата доступа : 01.06.2022.
15. Ключевые документы СБСЕ/ОБСЕ [Электронный ресурс] // Официальный сайт Организации по безопасности и сотрудничеству в Европе. – 2022. – Режим доступа : https://www.osce.org/ru/resources/csce-osce-key-documents. – Дата доступа : 01.06.2022.

16. Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии», 12 дек. 2003 г., г. Женева [Электронный ресурс] // Официальный сайт Организации Объединенных Наций. – 2022. – Режим доступа : https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf. – Дата доступа : 01.06.2022.

17. Мороз, Н. О. Международно-правовые основы обеспечения международной информационной безопасности / Н. О. Мороз // Труд. Профсоюзы. Общество. – 2016. – № 1 (51). – С. 77–81.

18. Масловская, Т. С. Конституционные ценности и их отражение в междунарождном и национальном законодательстве [Электронный ресурс] / Т. С. Масловская // Ценностная парадигма Основного закона Республики Беларусь : материалы респ. науч.-практ. конф., 14 марта 2013 г., Минск. – 2022. – Режим доступа : http://elib.bsu.by/bitstream/123456789/41970/1/Maslovskaya_Paradigma.pdf. – Дата доступа : 01.06.2022.

19. Крусс, В. И. Российская конституционная аксиология : актуальность и перспективы / В. И. Крусс // Конституционное и муниципальное право. – 2007. – № 2. – С. 7–14.

20. Конституция Республики Беларусь [Электронный ресурс] : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г. и 27 фев. 2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

21. Крусс, В. И. Теория конституционного правопользования : моногр. / В. И. Крусс. – М. : Норма, 2007. – 752 с. – С. 220–221.

22. Перепелица, Е. В. Права человека и ценности восточнославянской цивилизации : моногр. / Е. В. Перепелица. – Минск : Бел. наука, 2006. – 230 с.

23. Бакун, А. С. Конституционно-правовое регулирование реализации свободы вероисповедания религиозными организациями в Республике Беларусь: моногр. / А. С. Бакун. – Минск : Междунар. ун-т «МИТСО», 2018. – 290 с.

24. Католическая церковь одобрила исповедь посредством iPhone [Электронный ресурс] // RU.NY.web. – 2022. – Режим доступа : http://www.runyweb.com/articles/life/gadgets/holy-app-catholic-church-okays-new-confession-app-for-iphone.html. – Дата доступа : 01.06.2022.

25. Дистанционное электронное голосование [Электронный ресурс] // Официальный сайт Центральной избирательной комиссии Российской Федерации. – 2022. – Режим доступа : http://www.cikrf.ru/analog/ediny-den-golosovaniya-2021/distantsionnoe-elektronnoe-golosovanie/. – Дата доступа : 01.06.2022.

26. Анциферова, Э. Ю. Реализация свободы мнений, убеждений и их свободного выражения в условиях цифровизации / Э. Ю. Анциферова // Международное гуманитарное право глазами белорусской общественности : материалы международного научного форума, Минск, 30 октября 2020 г. / [редкол. : Е. Ф. Довгань (гл. ред.) и др.]. – Минск, 2020. – С. 73–80.

27. Об изменении Кодекса Республики Беларусь об образовании [Электронный ресурс] : Закон Республики Беларусь, 14 янв. 2022 г., № 154-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

УДК 340:004

ПУБЛИЧНЫЕ КОММУНИКАЦИИ В ФОКУСЕ ИНФОРМАЦИОННОГО ПРАВА

Е.В. Перепелица

Национальный центр правовой информации Республики Беларусь,
ул. Берсона 1а, г. Минск, 220030, Беларусь

В статье исследуется генезис и имманентные свойства публичных коммуникаций. Раскрываются информационно-правовые характеристики данного явления, а также возможные точки приложения института «паблик рилейшнз» (PR) к общественно-государственному дискурсу. Содержание данной коммуникативной технологии представлено с точки зрения обеспечения действенного присутствия общественности в публичном пространстве, создания предпосылок согласования коллективных и частных интересов. Анализируются функциональные характеристики публичных коммуникаций, имеющие юридическое значение. Особо подчеркивается, что в попытках нормативной регламентации связей с общественностью следует принимать во внимание семантические пределы права. Также показан коммуникативный ресурс «паблик рилейшнз» (PR), пока еще не вполне задействованный в национальной правовой системе Республики Беларусь.

***Ключевые слова*:** публичные коммуникации, коммуникативные технологии, публичное пространство, правовое регулирование.

PUBLIC COMMUNICATIONS IN THE FOCUS OF INFORMATION LAW

E.V. Perepelitsa

National Center for Legal Information of the Republic of Belarus,
1a Bersona street, Minsk, 220030, Belarus

The article examines the genesis and immanent properties of public communications. The information and legal characteristics of this phenomenon are revealed, as well as possible points of application of the institute "public relations" (PR) to public and state discourse. The content of this communication technology is presented from the point of view of ensuring the effective presence of the public in the public space, creating prerequisites for reconciling collective and private interests. The functional characteristics of public communications that have legal significance are analyzed. It is especially emphasized that in attempts to regulate public relations, the semantic limits of law should be taken into account. The communicative resource "public relations" (PR), which is not yet fully involved in the national legal system of the Republic of Belarus, is also shown.

Keywords: public communications, communication technologies, public space, legal regulation.

Введение

Коммуникативное пространство позволяет индивиду входить в различные сетевые сообщества, выходить из них, с легкостью переключаться между ними. Благодаря Интернету активную позицию в диалоге с государством во многих современных юрисдикциях занимает квалифицированное сообщество граждан, связанных высокотехнологическими средствами. Национальные юрисдикции, занимающие ведущие позиции в международных рейтингах открытого правительства, приобрели опыт использования потенциала массовых коммуникаций в том числе для укрепления взаимного доверия граждан и публичной власти. Юрисдикции, ставшие на путь цифровизации исторически позже, осваивают инновационный инструментарий по преимуществу в плане дигитализации управленческих структур. Однако же это не исключает потребности освоения потенциала различных коммуникативных технологий в контексте общественно-государственного взаимодействия. Соответствующие вопросы в настоящее время не привлекли необходимого внимания той части научной юридической общественности Республики Беларусь, которая представляет информационное право.

Основная часть

Публичные коммуникации являют собой особый способ целенаправленной организации коммуникационного пространства. Соответствующий концепт нередко употребляется как тождественный «паблик рилейшнз» (PR), «массовым коммуникациям», связям с общественностью. Все эти механизмы подразумевают диалогическое взаимодействие между индивидами и группами индивидов, не исключая граждан и органы публичной власти [1, с. 117].

Было бы неверным относить публичные коммуникации к реалиям только цифровой эпохи. Соответствующее явления прошло довольно долгую и сложную эволюцию. Не преследуя цели представить публичные коммуникации в исторической ретроспективе, отметим, что они возникли не на путях дигитализации, а гораздо раньше и сопровождали человеческое сообщество от периода Античности, Средних веков, вплоть до Нового и Новейшего времени. Публичные коммуникации не соотнесены и не привязаны к какому-то конкретному периоду, как и не ограничены рамками определенной правовой общности.

В осмыслении данного феномена участвовали самые проницательные умы человечества. Исходные положения о публичных коммуникациях как инструменте управления обществом были сформулированы Платоном. Вслед за ним Аристотель указывал на близость публичных коммуникаций к технологиям военачалия, хозяйствования и красноречия, которые в свою очередь подчинены науке о государстве [2, с. 10]. Притом Аристотель впервые сформулировал принцип «пропорционального равенства» в общении, согласно которому «понесший большие труды получает много, в понесший малые – мало»

[3, с. 325]. В соответствии с аристотелевским учением коммуникация выполняет важнейшую роль в системе социальных отношений за рамками собственно коммуникационного пространства. Над вопросами публичных коммуникаций размышлял в своих трудах Цицерон. Третий президент США Томас Джефферсон в послании к Конгрессу 1802 года заменил слова «состояние умов» выражением «связи с общественностью» [4, с. 10]. Подчеркнем, что в Новое время феномен публичных коммуникаций стал предпосылкой образования профессии журналиста.

Данный феномен с веками не потерял своей привлекательности, но, напротив, заинтересовывал новые поколения мыслителей. В данной связи стоит назвать такие имена, как Н. Макиавелли, Ф. Бэкон, Дж. Локк, Т. Гоббс. Одним из первых теоретиков публичной коммуникации признается Н. Макиавелли. Его трудами подготовлена почва для расширения предметного, функционального и инструментального поля данного явления. В частности, Н. Макиавелли раскрыл, каким образом эффективная коммуникация способна превращать стойких социальных противников монархии и даже целые народы в ее идейных апологетов и союзников.

Краткий экскурс в историю позволяет утверждать, что со временем публичные коммуникации все больше обособлялись от прочих видов коммуникации, что постепенно привело к образованию вполне самостоятельного вида деятельности. Стоит отдать дань публичным коммуникациям, поскольку именно они предопределили формирование так называемого публичного пространства как, в широком смысле слова, пространства диалога государства и общества.

В прошлом публичным называлось физическое, территориальное пространство (место). Сегодня можно говорить о том, что информационные и цифровые средства сообщения и коммуникаций позволяют по-иному использовать горизонты публичности. Паблик рилейшнз определяются современными исследователями как процесс передачи и двустороннего обмена информации посредством технических средств на численно большие, рассредоточенные аудитории [4, с. 39]. Американский теоретик коммуникации У. Шрам представлял данное явление в смысле «модели двустороннего процесса связи, когда и отправитель, и получатель информации действуют в пределах свойственных им рамок соотнесенности, взаимоотношений, сложившихся между ними, и окружающей их социальной средой» [4, с. 39]. Во многих государствах публичные коммуникации позиционируются как управленческая коммуникативная деятельность, направляемая на учет интересов общественных акторов, катализатор роста доверия граждан к органам публичной власти.

Публичные коммуникации – востребованное направление исследований в разных науках, включая филологию, психологию, социологию, политологию, коммуникативистику. Наиболее существенный шаг в познании

публичных коммуникаций сделала журналистика. Отечественными специалистами в данной области накоплен богатый опыт, который может представлять интерес для отраслевой теории информационного права [5]. Такой опыт важен в части определения стратегии совершенствования профильного отечественного законодательства.

Современные теоретики паблик рилейшнз полагают основной задачей этой коммуникативной технологии действенное присутствие общественности в публичном пространстве, создание условий для согласования коллективных и частных интересов, «достижение гармонии между группами и учреждениями посредством взаимопонимания, основанного на правде и полной информированности» [6, с. 154]. Как правило, связи с общественностью представлены системой процедур и способов налаживания публичного диалога. Конкретные формы данной коммуникации обусловлены национальными традициями. Для связей с общественностью определяющее значение имеет конкурентное положение центральных и локальных СМИ на информационном рынке государства, «технологии (информирования, дезинформирования), методы (рассказ, разъяснение и т.д.), модели (манипулятивная, информационная, двухстороння асимметричная, двухстороння симметричная), способы (фильтрации, фрейминг, создание событий и псевдособытий) и т.д.)» [1, с. 117]. Во многих западных юрисдикциях PR-коммуникации способствуют решению жизненно важных проблем, выявлению общественных настроений для адекватной и своевременной реакции на них со стороны публичной власти. PR-коммуникации употребляются в широко практикуемом опыте правительств многих стран, партий, профессиональных союзов, предстают важным средоточием плюралистичности общественных взглядов. Наряду с нормами права такая деятельность сорегулируется международными и национальными кодексами профессиональной этики. Результатом PR-коммуникации должно становиться получение сведений, полезных для широкой аудитории, конструктивное влияние на положение дел в обществе, побуждение граждан к совместному поиску решений, согласование жизненных интересов с запросами участников публичного дискурса, укрепление демократических принципов общественно-государственных взаимоотношений.

Попадая на юридическую почву, идея публичного дискурса перерастает в концепт массовых коммуникаций. В Учебном словаре терминов рекламы и паблик рилейшнз даются развернутые определения средств массовой коммуникации как совокупности каналов неличной коммуникации, используемых с целью воздействия на массовую потребительскую аудиторию. Средства массовой коммуникации включают в себя: печать (газеты, журналы, прямая почтовая реклама); радио и телевидение; наружные средства рекламы (щиты, вывески, баннеры, плакаты); как систематического распространения информации (через печать, радио, телевидение, кино, звукозапись, видеозапись) с

целью утверждения духовных ценностей данного общества и оказания идеологического, политического, экономического и организационного воздействия на оценки, мнения и поведение людей [7, с. 89]. Перечень средств массовой коммуникации пополняется за счет порталов, блогов, социальных сетей, других медиа- и конвергентных технологий.

Области научно-правового поиска, связанные с уяснением природы публичных коммуникаций, их роли в обществе, выявлением закономерностей правового регулирования соответствующих отношений, не могут похвастаться наличием значительного числа сторонников. Одним из немногих на постсоветском пространстве, кто еще в начале 2010-х годов квалифицировал право массовой коммуникации как самостоятельную подотрасль информационного права, является доктор юридических наук А. В. Минбалеев, которому принадлежит первенство в доктринальной разработке искомого понятия.

По формулировке, предложенной А. В. Минбалеевым, связи с общественностью – это «деятельность коммуникаторов по распространению созданной информации, направленной на привлечение к ним или их деятельности внимания общественности (целевых групп) с целью достижения не противоречащего законодательству определенного результата, в том числе формирования определенного мнения о коммуникаторе, повышения или поддержания интереса к нему, совершения определенных действий и др.» [8, с. 9]. Наибольшее юридическое значение имеют следующие функциональные характеристики связей с общественностью: посредством данной разновидности коммуникаций осуществляется передача информации общественности; это неотъемлемая часть всякой управленческой деятельности, связанная с ранжированием мнений физических и юридических лиц, частных и публичных структур; в силу исследовательского характера связи с общественностью могут генерировать объекты авторского права, нуждающиеся в адекватной правовой защите; информация, создаваемая и распространяемая в рамках связей с общественностью, маркирует интересы целевой аудитории, которую составляют физические и юридические лица, властные и невластные акторы, организации, объединения, институты, аналитические центры и группы.

Для юридического концепта связей с общественностью принципиальны вопросы, касающиеся определения участвующих в них субъектов, их основных прав и обязанностей, перечня задач, которые ставятся и решаются в ходе онлайнового и офлайнового взаимодействия, круга объектов правового воздействия. Рекомендации относительно паблик рилейшнз адресованы главным образом профессиональному сообществу журналистов. Тем не менее, коммуникативный ресурс паблик рилейшнз небезынтересен для юридической догматики.

На наш взгляд, исходным моментом для регламентации отношений в данной области является определение семантических пределов права. Соответствующий подход [9, с. 66] ценен с точки зрения ограниченных возможностей

права в цифровой среде. При всем при этом публичные коммуникации представляют одну из тех областей, где критерии семантических пределов права выработаны мировой практикой относительно давно.

Базовый принцип регламентации паблик рилейшнз – саморегулирование – означает первичность самостоятельного упорядочения корпоративных, межличностных, деловых коммуникаций и вторичность всех остальных коррелятов. Саморегуляция имеет значительное количество точек приложения, выступая как «фундаментальное свойство логически и функционально интегрированной системы, заключающееся в определении степени независимости (автономии) от внешних условий и иммунитета к ней» [10, с. 25]. Способность к саморегуляции раскрывается через такие категории, как индивидуальное регулирование, самоуправление. Наличие в общественной практике норм, объективно складывающихся в результате социальной саморегуляции, стало общепризнанным фактом [11, с. 31]. Соморегулирование хорошо иллюстрирует пример рекомендательных актов, принятых European Digital Rights – объединения, включающего «европейские правозащитные организации из более чем 20 стран, осуществляющие деятельность по продвижению, защите и поддержке фундаментальных прав и свобод человека в цифровой среде» [12, с. 65].

В рамках связей с общественностью интересен подход, базирующийся на так называемом законодательном каркасе, когда в нормативный правовой акт интегрируются принципы саморегулирования «с целью их детализации в практических руководствах, кодексах профессиональной этики и других институтах саморегулирования СМИ» [13, с. 123]. Связи с общественностью – довольно сложная система, которая помимо норм права зиждется на коррелятах иной природы. Она демонстрирует черты автономности в разных юрисдикциях.

Соответствующий институт получил развитие в Республике Беларусь как одна из разновидностей информационно-коммуникационной деятельности [14, с. 95]. Высказываются противоположные мнения относительно исторических предпосылок публичных коммуникаций в белорусском обществе [5]. Как таковая дефиниция «связи с общественностью» не нашла легального закрепления в источниках национального права.

Правовую базу связей с общественностью составляет Закон Республики Беларусь «О средствах массовой информации» от 17 июля 2018 г. [15] Требования постоянной коммуникации с общественностью содержит Указ Президента Республики Беларусь № 60 от 1 февраля 2010 г. «О мерах по совершенствованию использования сегмента сети Интернет» [16]. О необходимости обеспечения своевременного и объективного информирования общественности о событиях социально-экономической и общественно-политической жизни говорится в Указе Президента Республики Беларусь № 65 от 6 февраля

2009 г. «О совершенствовании работы государственных органов, иных государственных организаций со средствами массовой информации» [17]. В то же время названные акты не определили принципиальных характеристик данного института. Необходимо учитывать, что наряду с глобальными информационно-телекоммуникационными сетями связи с общественностью реализуются через традиционные средства массовой информации, рекламу. В Беларуси связи с общественностью представлены соответствующими службами в государственных и коммерческих структурах, отделами, носящими аналогичное название, пресс-службами, пресс-центрами, информационными департаментами в организациях. Важно принимать во внимание отличие электронного PR от традиционного, состоящее в «обратной связи, взаимосвязи всех участников целевой группы в Интернет, доступе к различным источникам информации, возможности прямого общения с аудиторией, постоянной связи, глобальной аудитории, более низких затратах на проведение PR-мероприятий» [18, с. 71]. При отсутствии споров по поводу потребности совершенствования связей государства с общественностью, существует недопонимание реального положения дел в данной сфере. Ныне такая деятельность находится в стадии развития, появляются субъекты соответствующих правоотношений – специалисты по связям с общественностью. Как признают эксперты, публичные коммуникации направлены на анализ важных социальных проблем, делают их заметными, видимыми [5, с. 26]. В настоящий момент роль паблик рилейшнз на уровне «государство – гражданин» ситуативна и фрагментарна, не вполне ясны перспективы правовой институционализации данного вида коммуникации.

Среди факторов, сдерживающих правовую институционализацию паблик рилейшнз в Беларуси, следует указать на инертность прежних традиций, связанных со взаимной закрытостью государства и общества. Получает реализацию по преимуществу патерналистский подход к институту публичных коммуникаций, допускающий однолинейное информирование общественности о событиях социально-экономической и общественно-политической жизни государства, регионов, территорий. В то же время, однонаправленное доведение информации от государства – гражданам вряд ли удовлетворяет потребности информационного общества. Нужен диалоговый режим работы с общественным мнением через посредство сети Интернет, чатов, блогов, социальных сетей. Асимметричные отношения государства и общества не предполагают реальной вовлеченности населения в управленческие, правообразовательные и правотворческие процессы.

Заключение

Как и всякое активно развивающееся явление общественной жизни, публичные коммуникации нуждаются в референтном правовом регулировании. Мировой опыт показывает, что вместе с воздействием со стороны государства данная сфера

допускает значительную степень саморегулирования. Теоретический фундамент связей с общественностью как возможного структурного элемента информационного права, а также правовые начала публичных коммуникаций, думается, могут выстраиваться с учетом исследовательского потенциала и практического опыта, накопленного иными, помимо права, областями знания. Разработка оптимальных форм внешней регламентации публичных коммуникаций со стороны государства, определение перечня задач, которые ставятся и решаются в ходе такого взаимодействия, создаст предпосылки для ускоренной правовой институционализации данного явления. Хотелось бы надеяться, что институт паблик рилейшнз заявит о себе в отечественной правовой системе как эффективный способ преодоления коммуникативных барьеров, существующих между государством и обществом.

Библиографический список

1. Смоликова, Т. М. Личность в пространстве медиа: особенности взаимодействия / Т. М. Смоликова. – Минск : Акад. упр. при Президенте Респ. Беларусь, 2018. – 231 с.
2. Кривоносов, А. Д. История публичных коммуникаций : учеб. пособие / А. Д. Кривоносов, Н. И. Данилова. – СПб. : Изд-во С.-Петерб. гос. экон. ун-та, 2018. – 41 с.
3. Аристотель. Соч. – В 4 т. – Т. 4. – М. : Мысль, 1983.
4. Новиков, Д. В. Теория и практика связей с общественностью : учеб. пособие / Д. В. Новиков. – Комсомольск-на-Амуре : Комсом.-на-Амуре гос. техн. ун-т, 2013. – 91 с.
5. Сидорская, И. В. Институт паблик рилейшнз в модернизации информационного пространства Беларуси. Автореф. дис. …д-ра филолог. наук : 10.01.10 / И. В. Сидорская. Минск : БГУ, 2019. – 53 с.
6. Краснянский, Д. Е. Роль и назначение коммуникативных технологий в сфере связей с общественностью / Д. Е. Краснянский // Науч. вестн. Моск. гос. техн. ун-та гражд. авиации. – 2005. – № 95. – С. 153–157.
7. Солдаткина, О. Л. Средства массовой коммуникации / О. Л. Солдаткина // Информационно-правовая политика в современной России : словарь-справочник / под ред. А. В. Малько, О. Л. Солдаткиной. – М., 2019.
8. Минбалеев, А. В. Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества : автореф. дис. … д-ра юрид. наук : 12.00.14 / А. В. Минбалеев ; Юж.-Урал. гос. ун-т. – Челябинск, 2012. – 44 с.
9. Архипов, В. В. Семантические пределы права в условиях медиального поворота: теоретико-правовая интерпретация : дисс. д-ра юрид. наук : 12.00.01 / В. В. Архипов. – СПб, 2019. – 425 л.
10. Скоробогатов, В. Ю. Саморегулирование как свойство правовой системы : дис. канд. юрид. наук : 12.00.01 / В. Ю. Скоробаготов. – Высшая школа экономики. Нац. исслед. ун-т. – М. – 2013. – 186 с.
11. Трофимов, В. В. Социально-интерактивная концепция права (к проблеме обоснования традиции российской и зарубежной философии и социологии права) / В. В. Трофимов // Правоведение. – 2014. – № 2. – С. 19–37.
12. Грачёва, С. А. Основные права и свободы в цифровом измерении / С. А. Грачёва, М. Е. Черемисинова // Вестн. ЮУрГУ. Сер. «Право». – 2021. – № 1. – С. 64–73.

13. Довнар, Н. Н. Правовое обеспечение информационной безопасности СМИ в условиях трансформации медиасистемы / Н. Н. Довнар. – Минск : Белор ус. гос. ун-т, 2019. – 235 с.

14. Воюш, И. Профессия – PR-специалист: 25 лет институционального развития в Беларуси / И. Воюш, И. Сидорская // Беларус. думка. – 2018. – № 9. – С. 94–100.

15. О средствах массовой информации [Электронный ресурс] : Закон Респ. Беларусь, 17 июля 2008 г., № 427-З : в ред. Закона Респ. Беларусь от 17.07.2018 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

16. О мерах по совершенствованию использования национального сегмента сети Интернет [Электронный ресурс] : Указ Президента Респ. Беларусь, 1 февр. 2010 г., № 60 : в ред. Указа Президента Респ. Беларусь от 18.09.2019 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

17. О совершенствовании работы государственных органов, иных государственных организаций со средствами массовой информации [Электронный ресурс] : Указ Президента Респ. Беларусь, 6 февр. 2009 г., № 65 : в ред. Указа Президента Респ. Беларусь от 19.03.2020 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

18. Кучеренко, В. В. Интернет-маркетинг : пособие / В. В. Кучеренко ; Акад. Упр. При Президенте Респ. Беларусь. – Минск : Академия управления при Президенте Республики Беларусь, 2020. – 95 с.

УДК 349

ПРИМЕНЕНИЕ ПРИНЦИПА ДОЛЖНОЙ ОСМОТРИТЕЛЬНОСТИ В ОТНОШЕНИИ АКТОВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, В ПЕРИОД МЕЖДУНАРОДНОГО ВООРУЖЕННОГО КОНФЛИКТА

Н.О. Мороз

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В ходе современных вооруженных конфликтов активно используются различного рода информационно-коммуникационных технологии. Настоящая статья посвящена выявлению применимости принципа должной осмотрительности к актам, совершаемым с использованием информационно-коммуникационных технологий, в ходе вооруженного конфликта в отношениях между воюющими сторонами, а также в их отношениях с третьими государствами.

***Ключевые слова*:** информационная безопасность, международное гуманитарное право, принцип должной осмотрительности, правила ответственного поведения государств в киберпространстве.

APPLICATION OF THE PRINCIPLE OF DUE DILIGENCE WITH RESPECT TO ACTS PERFORMED WITH THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES DURING INTERNATIONAL ARMED CONFLICT

N.A. Maroz

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

In the course of modern armed conflicts, various kinds of information and communication technologies are actively used. This article is devoted to identifying the applicability of the principle of due diligence to acts committed with the use of information and communication technologies during international armed conflict in relations between belligerents, as well as in their relations with third states.

Keywords: information security, international humanitarian law, due diligence principle, rules for the responsible behavior of states in cyberspace.

Принцип должной осмотрительности широко признан в современном международном праве. При этом возможность применения данного принципа к деятельности, связанной с использованием информационно-

коммуникационных технологий (далее – ИКТ), само по себе не оспаривается ни в доктрине, ни в практике. В то же время степень обязательности, а также содержание принципа должной осмотрительности в таком контексте остается предметом научных дискуссий.

В ходе современных вооруженных конфликтов активно используются различного рода ИКТ: начиная с автономных видов вооружения и заканчивая программными средствами для получения доступа, модификации, перехвата компьютерных данных, саботажа работы компьютерных систем и сетей противника. В такой ситуации закономерно возникает вопрос сохраняет ли свое действие обязательство государства заведомо не позволять использование своей территории для совершения частными лицами и третьими государства актов с использованием ИКТ, противоречащих правам других государств, в ходе вооруженного конфликта в отношениях между воюющими сторонами, а также в их отношениях с третьими государствами.

Несмотря на то, что применение принципа должной осмотрительности к деятельности, связанной с использованием ИКТ, исследовалось в научных публикациях, возможности сохранения его действия в период вооруженного конфликта практически не анализировались. Существующие научные публикации рассматривают содержание такого обязательства узко, исключительно исходя из обязательств должной осмотрительности, вытекающих из Женевских конвенций 1949 г. и Дополнительных протоколов к ним [1]. Указанное обстоятельство обуславливает новизну настоящего исследования.

В настоящей статье предпринята попытка выявить условия применимости должной осмотрительности к деятельности, связанной с использованием ИКТ, в период вооруженного конфликта.

Принцип должной осмотрительности является одним из принципов общего международного права. Международный Суд ООН в деле о проливе Корфу заявил, что «каждое государство обязано заведомо не позволять использовать свою территорию для совершения действий, противоречащих правам других государств» [2]. Формулировка «каждое государство» подчеркивает тот факт, что данное обязательство: во-первых, затрагивает любое государство (например, вне независимости от факта его признания), во-вторых, неотъемлемо ему принадлежит (государство не может от него отказаться или быть лишено его).

Принцип распространяется на действия негосударственных субъектов и поведение третьих государств [3, с. 32].

Принцип должной осмотрительности применительно к правоотношениям, возникающим по поводу использования ИКТ, был сформулирован в отчете ГПЭ за 2015 г. В документе указано, что государства не должны заведомо позволять использовать свою территорию для совершения

международно-противоправных деяний с использованием ИКТ [4]. В то же время в доктрине считается, что этот принцип в его применении к киберпространству не получил статуса lex lata [3, с. 31]. В практике государств также нет единства относительно юридической силы принципа, в формулировке предложенной ГПЭ [5]. В то же время в доктрине и практике признается, что норма 13с) отчета ГПЭ за 2015 г. закрепляет хотя и, как минимум добровольный, но ожидаемый для исполнения стандарт ответственного поведения государств в связи с использованием ИКТ (пп. а п. 30 Доклада).

Комментарий к принципу должной осмотрительности, содержащийся в отчете ГПЭ 2015 г., предложенный ГПЭ в ее новом отчете, представленном в 2021 г., значительно конкретизирует содержание обязательства. Так, во-первых, возникновение обязательства не позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ связывается, прежде всего, с осведомленностью государства или его добросовестным уведомлением об инциденте [6]. Во-вторых, инцидент сам по себе должен представлять международно-противоправное деяние, совершенное с использованием ИКТ на территории уведомляемого государства или проходящим через его территорию. В-третьих, обязательство «не допускать использования своей территории» означает «использовать все соответствующие, доступные и возможные – в разумных пределах – шаги для обнаружения, расследования и урегулирования такой ситуации». В-четвертых, субъектами таких инцидентов могут быть как третьи государства, так и негосударственные субъекты.

Формулировка обязательства, содержащаяся в норме 13с) не вполне удачна, поскольку деяния негосударственных акторов, которые не могут быть атрибуированы государству, не могут квалифицироваться в качестве международно-противоправных деяний. В то же время согласно п. 29 Доклада 2021 г., указывается, что в рассматриваемой норме «заложено понимание того, что государство не должно позволять другому государству или негосударственному субъекту использовать ИКТ на своей территории для совершения международно-противоправных деяний».

Таким образом, норма 13с) нуждается в корректировке. Для устранения данной неточности в доктрине предлагалось использование формулировки, содержащейся в решении Международного Суда ООН по делу о проливе Корфу [6]. Полагаем, что использование фразы «противоречащих правам других государств» для уточнения содержания нормы 13с) поскольку сужает международно-правовое обязательство до: а) только одной формы имплементации международно-правового обязательства («соблюдения»); б) соблюдения исключительно прав, вытекающих из международно-правовых обязательств; в) соблюдения прав только государств. В этой связи

предлагается изложить формулировку обязательства должной осмотрительности, содержащуюся в норме 13c) в следующей редакции:

«Государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ и деяний, которые могли бы рассматриваться в качестве международно-противоправных, если бы были совершены государством».

Таллиннское руководство 2.0 содержит толкование принципа должной осмотрительности, которое отличается о предложенного в отчетах ГПЭ 2015 г., 2021 г., и фактически сужает сферу его действия, охватывая лишь необходимость предупреждения актов, которые затрагивают «права других государств и приводят к серьезным негативным последствиям для них». В Таллинском руководстве 2.0 содержится более подробное толкование территориальной сферы действия принципа. В частности, в нем указывается, что «государство должно проявлять должную осмотрительность, не позволяя использовать свою территорию, территорию или кибернетическую инфраструктуру, находящуюся под его контролем, для кибероперaций <…> [3, с. 30].

Следует отметить, что в доктрине не единства относительно необходимости включения элемента «серьезных негативных последствий» как условия возникновения обязательства проявлять должную осмотрительность в киберконтексте. Так, Ф. Делеруа отмечает, что указанный элемент был выработан применительно к международному экологическому праву, в то же время в киберконтексте он не является обязательным компонентом принципа должной осмотрительности [7, с. 364]. Так, обязательство должной осмотрительности одинаково применимо к любым деяниям, которые могли бы рассматриваться в качестве международно-противоправных. В то же время наличие такого ущерба будет влиять на фактическую заинтересованность государства призвать к ответственности другое государство, которое не пресекает кибероперации, которые порождают такой ущерб [4, с. 365].

В настоящем исследовании будет использована трактовка принципа должной осмотрительности, предложенная ГПЭ, поскольку она в определенном смысле отражает позиции государств.

Принцип должной осмотрительности не влечет за собой каких-либо обязательств территориального государства по уголовному преследованию лиц, совершивших какие-либо кибератаки в нарушение прав других государств [3, с. 32, 48]. Фактически, наличие таких обязательств зависит от наличия применимых международных договоров к конкретной ситуации, криминализация конкретного деяния согласно уголовному законодательству территориального государства, осуществляется ли в отношении данного противоправного деяния уголовное преследование и обвинение в суде в публичном порядке и др.

Как было указано выше, принцип должной осмотрительности применительно к правоотношениям, возникающим по поводу использования ИКТ, не получил закрепления в международном договоре универсального характера. Указанное обстоятельство является одной из важнейших причин наличия доктринальных споров и различий в позициях государств о его юридической обязательности.

В то же время на региональном уровне можно проследить урегулирование его отдельных аспектов. Так, принцип должной осмотрительности отчасти нашел отражение в абз. 6-7 ст. 6 Соглашения о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности 2017 г., где указывается, что государства-участники осуществляют самостоятельно или при соответствующем обращении меры для предотвращения использования третьей стороной территории и (или) информационной инфраструктуры, находящейся под юрисдикцией государства – члена ОДКБ, для оказания деструктивного информационного воздействия, в том числе компьютерных атак, на другое государство – член ОДКБ; взаимодействуют в интересах определения источника компьютерных атак, проведенных с использованием их территории, противодействия этим атакам и ликвидации последствий.

Учитывая тот факт, что само по себе обязательство должной осмотрительности вытекает из суверенитета государства, принципа суверенного равенства государств, а «суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ» [4], полагаем, что на исполнимость данного обязательства сам факт вооруженного конфликта не оказывает влияния. В то же время более широкий контекст ситуации безусловно может оказывать влияние на практическую возможность реализации данного принципа.

Комиссией международного права ООН в Проекте статей о последствиях вооруженных конфликтов для международных договоров, было отмечено, что при определении влияния конфликта на международный договор должны приниматься во внимание: a) характер договора, в частности его предмет, его объект и цель, его содержание и количество участников договора; и (b) характеристики вооруженного конфликта, такие как его территориальная протяженность, его масштабы и интенсивность, его продолжительность и, в случае немеждународных вооруженных конфликта, а также степень участия извне.

Как было указано выше, в доктрине возможность применения принципа должной осмотрительности к деяниям, совершаемых с использованием ИКТ, выводится из обязательства должной осмотрительности в контексте обязательств, напрямую вытекающих из норм международного

гуманитарного права (далее – МГП) (ст. 1, общая для всех Женевских конвенций о защите жертв войны 1949 г., п.1 ст. 1 I Дополнительного протокола к Женевским конвенциям 1949 г.) [1]

Не оспаривая наличие обязательства государств предпринимать позитивные меры для обеспечения соблюдения МГП другими образованиями (в частности, частными лицами), тем самым предотвращая совершение нарушений, а также его применимости к кибероперациям, следует отметить, что сужение сферы действия принципа должной осмотрительности в данном контексте не вполне корректно, что обусловлено следующим.

Во-первых, должная осмотрительность в контексте международного гуманитарного права и принцип должной осмотрительности как общий принцип международного права соотносятся как частное и общее. Так, последнее, как уже отмечалось выше, охватывает общее обязательство не позволять использовать свою территорию для совершения действий, противоречащих *любым* международно-правовым обязательствам, а не только тех, которые вытекают из международного гуманитарного права.

Во-вторых, международно-правовые обязательства государств не прекращают (приостанавливают) своего действия автоматически в связи с вооруженным конфликтом. Как указывал Э. Давид «если развязывание войны влечет за собой применение определенных норм, это не означает приостановления действия любой другой правовой нормы» [7, с. 76]. Комиссией международного права ООН также отмечалось, что вооруженный конфликт не прекращает действия международного договора ipso facto. Полагаем, что данный вывод вполне справедлив и по отношению к обычным нормам международного права. Таким образом, ни действие самого принципа должной осмотрительности, ни права государств, фактически нарушаемые в ходе неправомерной деятельности негосударственных акторов или третьих государств с использованием ИКТ, не прекращаются ipso facto в период вооруженного конфликта.

В то же время в соответствии с Венской конвенций о праве международных договоров 1969 г. предусмотрены ситуации, когда государство может приостановить или прекратить международный договор, многие из которых могут быть связаны или стать следствием вооруженного конфликта. К данным ситуациям относятся: существенное нарушение двустороннего договора одним из его участников (ст. 60); невозможность выполнения договора вследствие безвозвратного исчезновения или уничтожения объекта, необходимого для выполнения договора (ст. 61); коренное изменение обстоятельств (ст. 62).

На все указанные ситуации недопустимо ссылаться государству, которое является нарушителем международного договора, применение которого приостанавливается или прекращается. Так, например, если уничтожение

объекта, необходимого для выполнения договора возникло по причине вооруженного конфликта, развязанного определенным государством, последнее не вправе ссылаться на последующую невозможность выполнения договора (п.2 ст. 61 Венской конвенции о праве международных договоров 1969 г.). В то же время в соответствии с п. 5 ст. 60 существенное нарушение международного договора одной стороной тем не менее не является основанием для приостановления или прекращения положений, касающихся «защиты человеческой личности, которые содержатся в договорах, носящих гуманитарный характер, и особенно к положениям, исключающим любую форму репрессалий по отношению к лицам, пользующимся защитой по таким договорам». Таким образом, пострадавшее государство в любом случае остается связанным международно-правовыми обязательствами, которые носят гуманитарных характер и не вправе апеллировать к приостановлению или прекращению их действия даже по причине вооруженного конфликта.

Комиссией международного права ООН также обращалось внимание: а) на недопустимость извлечения выгоды государством-агрессором, связанной с прекращением или приостановлением международного договора по причине вооруженного конфликта (ст. 15 Проекта статей о последствиях вооруженных конфликтов для международных договоров 2011 г.); б) сохраняющуюся обязанность государства, совершившего международно-противоправное деяние, по исполнению нарушенного обязательства (ст. 29 Статей об ответственности государств за международно-противоправные деяния 2001 г.); в) на обязанность всех государств не признавать правомерным положение, сложившееся в результате серьезного нарушения императивной нормы общего международного права, к которому в частности относится и нарушение запрета применение силы по международному праву (п. 2 ст. 41 Статей об ответственности государств за международно-противоправные деяния 2001 г.).

Таким образом, государство, нарушившее запрет применения силы, не только не может приобретать преимущества в связи с прекращением или приостановлением международно-правовых обязательств по причине этого вооруженного конфликта, а также сохраняет обязанность выполнять свои международно-правовые обязательства первичного характера.

В свою очередь пострадавшее государство обязано соблюдать положения норм международного права, сохраняющих свое действие в ходе вооруженного конфликта.

Так, кроме обязательств, вытекающих из норм международного гуманитарного права, государства – стороны вооруженного конфликта обязаны соблюдать и применять Венскую конвенцию о дипломатических сношениях 1961 г., Венскую конвенцию о консульских сношениях 1963 г. (п. 3 резолюции Совета Безопасности ООН 667 от 16 сентября 1990 г.), основные нормы

права прав человека и права окружающей среды (п. 29-31 Консультативного заключения Международного Суда ООН о законности угрозы ядерным оружием или его применения).

В Проекте статей о последствиях вооруженных конфликтов для международных договоров 2011 г. Комиссия международного права ООН представила примерный перечень международных договоров, которые не прекращают свое действие в период вооруженного конфликта. Соответственно, если частные лица будут нарушать положения таких международных договоров в период вооруженного конфликта, воюющие стороны, тем не менее, должны оставаться связаны обязательством прекратить такую деятельность, даже если она направлена против воюющей стороны.

Так, государства кроме использования своего неотъемлемого права на самооборону также могут принимать контрмеры в ответ на нарушение международно-правовых обязательств. При этом как право на самооборону, так и на принятие контрмер не являются неограниченными. Так, в частности, контрмеры должны соответствовать требованиям, установленным в Статьях об ответственности государств за международно-противоправные деяния.

С учетом положений о принятии контрмер, закрепленных в Статьях об ответственности государств за международно-противоправные деяния, пострадавшее государство может отступить от выполнения некоторых своих обязательств. Принятие контрмер предполагает принятие активных мер, то есть действий, а не бездействия (п. 1 ст. 42 Статей об ответственности государств за международно-противоправные деяния). В настоящее время возможность принятия контрмер путем бездействия не нашла четкой поддержки в доктрине [9], в то же время указанные аспекты были предметом научных дискуссий [10, с. 20].

Таким образом, отсутствие реагирования на деяния частных лиц или третьих государств, осуществляемых с использованием ИКТ, против прав других государств не может выступать в качестве контрмер, поскольку представляет собой бездействие. Деяния частных лиц или третьих государств, совершаемые с использованием ИКТ, против прав государства – нарушителя, могут рассматриваться как деяния самого пострадавшего государства, если оно признает и принимает данное поведение в качестве собственного (ст. 11 Статей об ответственности государств за международно-противоправные деяния).

Кибератаки на гражданские объекты, объекты, содержащие опасные силы, объекты, необходимые для выживания населения; медицинские формирования и санитарно-транспортные средства; культурные ценности и места отправления культа будут охватываться принципом должной осмотрительности. При этом роль государства в вооруженном конфликте не будет иметь значения для целей применимости такого обязательства.

В то же время и ряд других атак, которые могут быть квалифицированы как нарушение международно-правовых обязательств, будут по-прежнему запрещены в период вооруженного конфликта, такие, как например, акты, посягающие на свободу морского судоходства, направленные против безопасности гражданской авиации, нарушающие тайну дипломатической переписки и др.

Как уже было указано выше, более широкий контекст ситуации вооруженного конфликта может оказывать влияние на практическую выполнимость принципа должной осмотрительности. Так, в результате вооруженного конфликта государство может не контролировать часть своей территории. В такой ситуации оккупирующее государство будет нести ответственность за осуществление принципа должной осмотрительности с этой территории (ст. 9 Статей об ответственности государств за международно-противоправные деяния, ст. 42-43 Конвенции о законах и обычаях сухопутной войны 1907 г., ст. 64 Конвенции о защите гражданского населения во время войны 1949 г.).

Таким образом, фактически, обязательство должной осмотрительности будет всегда сохранять свое действие, если совершаемое деяние может рассматриваться как нарушение:

а) международного договора, содержащегося в приложении к Проекту статей о влиянии вооруженных конфликтов на действие международного договора;

б) императивных норм общего международного права.

Содержание обязательства осуществления должной осмотрительности требует от государства принятия всех адекватных и разумно доступных мер, а также осуществимых шагов для обнаружения, расследования и урегулирования ситуации. Стандарт требуемого от государства поведения при этом не установился в практике государств [5]. При этом возможности по принятию мер у развитых и развивающихся государств в части недопущения использования их территории для совершения актов, противоречащих правам других государств, будут различными. Более того, возможности государств в этой сфере могут еще более серьезно ограничены в связи с вооруженным конфликтом (так, может быть повреждена соответствующая техническая инфраструктура, могут отсутствовать специалисты, способные пресечь совершение противоправного деяния, может отсутствовать телефонная связь, электричество и Интернет и др.). В то же время принцип должной осмотрительности порождает обязательство действия, не результата [7, с. 361]. Таким образом, недостижение цели предупреждения кибератаки в таких условиях не может рассматриваться в качестве нарушения обязательства должной осмотрительности.

При этом государства могут, но не обязаны обращаться к помощи третьих государств или частных лиц для оказания технической поддержки с целью выполнения обязательства должной осмотрительности (пп. b п. 30 Доклада ГПЭ по продвижению ответственного поведения государств в киберпространстве в контексте международной безопасности 2021 г.). Полагаем, что указанное правило будет применимо и в контексте вооруженного конфликта. При этом любые принудительные действия в отношении частных лиц, осуществляющих злонамеренную деятельность с использованием ИКТ против прав других государств, будут правомерными только с согласия государства, на территории которого они находятся, или с санкции Совета Безопасности ООН. Так, неспособность Сомали пресекать акты морского пиратства, совершаемые ее гражданами, привело к принятию целого ряда резолюций Советом Безопасности ООН, которые, в частности, предусматривали возможность для государств, которые сотрудничают с переходным федеральным правительством Сомали в борьбе с пиратством и вооруженным разбоем на море у побережья Сомали и в отношении которых переходное федеральное правительство Сомали заблаговременно направило уведомление Генеральному секретарю, входить в территориальные воды Сомали в целях пресечения актов пиратства и вооруженного разбоя на море сообразно тому, как это разрешается делать в открытом море в отношении (п. 7 резолюции Совета Безопасности ООН 1816 от 2 июня 2008 г.).

Как уже было указано выше, государство, нарушившее запрет применения силы, не может ссылаться на целый ряд обстоятельств, ставших результатом применения силы, в качестве оправдания для неисполнения международно-правового обязательства (пп. с п. 2 ст. 60, п. 2 ст. 61, пп. b п. 2 ст. 62 Венской конвенции о праве международных договоров 1969 г.; ст. 15 Проекта статей о последствиях вооруженных конфликтов для международных договоров 2011 г.).

В ходе вооруженного конфликта деятельность, совершаемая частными лицами, в ряде случаев может рассматриваться как деяние государства. Так, если частные лица, осуществляющие кибератаки на военную инфраструктуру государства – противника соответствуют признакам комбатанта, установленным в Женевской конвенции и I Дополнительным протоколом, то их деятельность в ряде случаев может рассматриваться как деяние государства. В то же время, например, население неоккупированной территории, которое при приближении неприятеля стихийно берется за оружие для борьбы со вторгающимися войсками, не успев сформироваться в регулярные войска, если оно носит открыто оружие и соблюдает законы и обычаи войны хотя и охватывается понятием «комбатанты» (п. 6 ст. 13 Конвенции об улучшении участи раненых и больных в действующих армиях от 12 августа 1949 г.), фактически не находится под контролем пострадавшего государства.

Такие лица не действуют по указаниям либо под руководством или контролем этого государства, и потому их поведение не может быть атрибуировано государству (ст. 8 Статей об ответственности государств за международно-противоправные деяния), безусловно, если последнее не признает его в качестве собственного поведения (ст. 11 Статей об ответственности государств за международно-противоправные деяния).

Деятельность третьих государств, которая наносит ущерб правам иностранных государств, также может по-разному квалифицироваться в период вооруженного конфликта. Так, если такое третье государство фактически контролирует территорию иностранного государства, с которой осуществляются кибератаки против критически важных объектов инфраструктуры других государств, именно такое третье государство будет обязано придерживаться принципа должной осмотрительности (ст. 9 Статей об ответственности государств за международно-противоправные деяния). В том случае, если государство запросила соответствующую техническую помощь третьего государства и фактически если предоставленные в его распоряжения хакеры действуют для реализации военных целей первого государства, тогда их кибератаки будут считаться актами первого государства (ст. 6 Статей об ответственности государств за международно-противоправные деяния).

Таким образом, на основе проведенного исследования представляется возможным сформулировать следующие выводы:

1. Принцип должной осмотрительности в контексте использования ИКТ имеет обычно-правовую природу и вытекает из общего обязательства каждого государства заведомо не позволять использовать свою территорию для совершения действий, противоречащих правам других государств. Ни сам принцип, ни его действие в отношении определенных международно-правовых обязательств не прекращается в связи с возникновением вооруженного конфликта между государствами ipso facto.

2. Формулировка обязательства, содержащаяся в норме 13c) не вполне удачна. В этой связи предлагается изложить формулировку обязательства должной осмотрительности, содержащуюся в норме 13c) в следующей редакции: «государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ и деяний, которые могли бы рассматриваться в качестве международно-противоправных, если бы были совершены государством».

3. Обязательство должной осмотрительности будет всегда сохранять свое действие в отношениях между воюющими сторонами, если деяние частных лиц или третьих государств может рассматриваться как нарушение: а) международного договора, содержащегося в приложении к Проекту

статей о влиянии вооруженных конфликтов на действие международного договора; б) императивных норм общего международного права.

Библиографический список

1. Dias, T. Cyber due diligence in international law [Electronic resource] / T. Dias, A. Coco // The Oxford Institute for Ethics Law and Armed Conflict. – Mode of access: https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.pdf. – Date of access: 04.06.2022.
2. Corfu Channel case, Judgment of April 9, 1949 : I.C. J. Reports 1949, P. 4. P. 22
3. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 2nd Edition / ed. by Michael N. Schmitt. – Oxford: Oxford University Press, 2017. – 598 p.
4. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015 [Electronic resource] / United Nations. – Mode of access: https://undocs.org/A/70/174. – Date of access: 12.10.2021.
5. Kastelic, A. Due diligence in cyberspace Normative expectations of reciprocal protection of international legal rights / A. Kastelic [Electronic resource] / UNIDIR. – Mode of access: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjxypSd2Z_7AhULiYsKHSbKBT0QFnoECAoQAQ&url=https%3A%2F%2Fwww.unidir.org%2Fpublication%2Fdue-diligence-cyberspace-normative-expectations-reciprocal-protection-international&usg=AOvVaw0hPN1vWTgMMq46z3wJnyAG. – Date of access: 25.05.2022.
6. Report of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (Advance copy), 2021, May [Electronic resource] / United Nations. – Mode of access: https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf. – Date of access: 12.10.2021.
7. Delerue, F. Cyber Operations and International Law / F. Delerue. – Cambridge: Cambridge University Press, 2020. – 513 p.
8. Давид, Э. Принципы права вооруженных конфликтов / Э. Давид. – Москва: МККК, 2011. – 1141 с.
9. Summary record of the 2590th meeting of the International Law Commission, A/CN.4/SR.2590. Extract from the Yearbook of the International Law Commission, – 1999. – Vol. I, § 42-43 [Electronic resource] / United Nations. – Mode of access: https://legal.un.org/ilc/documentation/english/summary_records/a_cn4_sr2590.pdf. – Date of access: 12.10.2021.
10. Murphy, S.D. International Law. Cases and materials / S.D. Murphy, L.F. Damrosch. – Sixth ed., West Academic Publishing, Saint Paul. – 1532 p.

УДК 351.341

ТРАНСНАЦИОНАЛЬНАЯ ОРГАНИЗОВАННАЯ ПРЕСТУПНОСТЬ В КОНТЕКСТЕ СОВРЕМЕННЫХ РИСКОВ, ВЫЗОВОВ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ

В.В. Меркушин

Белорусский государственный университет,
пр. Независимости 4, Минск, 220030, Беларусь

В статье определяются и анализируются современные риски и иные деструктивные воздействия транснациональной организованной преступности на информационную безопасность государств. Предлагаются актуальные теоретико-прикладные и международно-правовые инициативы по противодействию транснациональной организованной преступности в данной сфере.

***Ключевые слова*:** транснациональная организованная преступность, информационная безопасность, угрозы информационной безопасность, международное право.

TRANSNATIONAL ORGANIZED CRIME IN THE CONTEXT OF MODERN RISKS, CHALLENGES AND THREATS TO INFORMATION SECURITY OF STATES

V.V. Merkushin

Belarusian State University,
4 Nezalezhnosti Avenue, Minsk, 220030, Belarus

The article defines and analyzes modern risks and other destructive effects of transnational organized crime on the information security of states. Topical theoretical, practical and international legal initiatives to counter transnational organized crime in this area are proposed.

Keywords: transnational organized crime, information security, threats to information security, international law.

«Кто владеет информацией, тот владеет миром»
Натан Майер Ротшильд

В современных условиях активной эволюции научно-технического прогресса, информатизации современного общества, широкомасштабного доступа к интернет-ресурсам (легальным и нелегальным) [1, с. 5], подключения пользователей большинства стран к глобальным электронным платежным системам и пр., объективизировалась в качестве самостоятельной

сфера высоких технологий, способствовавшая модернизации использования киберпространства и релевантно связанных с ним общественно-опасных деяний – киберпреступлений [2 (пп. 41-42); 3 (п. 6); 4 (п. 9 (b)); 5, с. 44; 6; 7]. Отсюда, «актуализирующаяся проблема борьбы с ними из внутригосударственной превратилась в международную» (А.Г. Волеводз) [8, с. 16], чему способствует перманентное увеличение числа данного рода преступлений, закономерно приобретающих организованный транснациональный характер [9, с. 5; 10; 11; 12].

Более того, как отмечено в Специальном докладе: кибервойны в C-Suite [13], опубликованном в журнале Cybercrime: «глобальные расходы на киберпреступность будут расти на 15% в год в течение следующих пяти лет, достигнув $10,5 трлн в год к 2025 г., по сравнению с $3 трлн в 2015 г. Это представляет собой крупнейшую передачу экономического богатства в истории, ставит под угрозу стимулы для инноваций и инвестиций, экспоненциально превышает ущерб, причиненный стихийными бедствиями за год, и будет более прибыльным, чем глобальная торговля всеми основными незаконными наркотиками вместе взятыми». При этом, С. Морган (главный редактор Cybercrime) особо подчеркивает, что оценка такого ущерба произведена на основе хронологии развития соответствующих статистических данных, включая недавний рост в годовом исчислении (за последние 10 лет – прим. автора), резкого увеличения хакерской деятельности, спонсируемой враждебными национальными государствами и организованными преступными группировками [13].

На сегодняшний день, одной из важнейших составляющих элементов сферы высоких технологий[2], способной напрямую испытать на себе риски воздействий данных противоправных деяний, является инфраструктура информационной безопасности. Особенно в тех случаях, когда антагонистическими субъектами (источниками) выступают коллективные образования, как собственно преступные, так и легальные, но потенциально способные стать таковыми. В данном случае, с одной стороны, речь идет о своеобразных симбиотических связях традиционных [транснациональных] преступных групп с аналогичными сетевыми группами киберпреступников[3]**.** Они, напрямую или анонимно могут сотрудничать в любой точке мира с целью совершения совместных криминальных операций. Причем, использование информационно-коммуникационных технологий (ИКТ) значительно

[2] От англ. *high technology, high tech, hi-tech.* Сфера высоких технологий включает: собственно электроника, программное обеспечение, IT-технологии, смежные с IT-сферой направления (микро-, опто- и наноэлектроника, мехатроника, передача данных, радиолокация, радионавигация, радиосвязь, информационно-коммуникационные технологии, и др.), а также защита информации и создание центров обработки данных (Источник: Парк высоких технологий сегодня. URL:https://www.park.by/htp/about/. - (accessed: 25.05.2022).

[3] Например, Anonymous, LulzSec, NSO Group Technologies, Chaos Computer Club, РедХак, Киберберкут, OurMine, Lizard Squad, Cult of the Dead Cow, Сирийская электронная армия, Power Racing Series, MilwOrm, Israeli Elite Force, Derp, и др.

упрощает, а в иных случаях, устраняет, правовые и организационные «барьеры» для проникновения, как на легальные, так и нелегальные рынки товаров и услуг. С другой стороны, в определенных случаях, новые [квази]-субъекты транснациональной организованной преступности – транснациональные корпорации, частные военные и охранные компании и неправительственные международные организации [14, с. 3-10], используя свои ресурсы, возможности и опираясь окончательно неурегулированный свой [международно]-правовой статус, находятся в перечне рисков и потенциальных угроз информационной безопасности, устойчиво превалируя в сторону последних. Указанные субъекты могут выступать как автономно, в собственных корпоративных интересах, так и в форме соучастия особого рода (sui generis), формируя «теневые» бизнес-модели с использованием коррупционных связей в международных и национальных структурах.

На этом фоне, данные субъекты в той или иной степени, склонны к совершению таких уже достаточно распространенных противоправных деяний, как - мошенничество с электронной почтой и интернет-мошенничество, мошенничество с использованием личных данных (кража и злонамеренное использование личной информации), кража финансовых данных или данных банковских карт, кража и продажа корпоративных данных, кибершантаж (требование денег для предотвращения кибератаки), атаки программ-вымогателей (тип кибершантажа), криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев), кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций) [15]. При этом, по мнению отдельных ученых-экспертов, современная проблема транснациональной организованной преступности еще усугубляется постоянно растущей глобальной связью, предоставляемой ИКТ, безграничной сферой киберпространства и низкими рисками раскрытия и привлечения к ответственности правоохранительными органами [16].

На сегодняшний день, проблематика противодействия транснациональной организованной киберпреступности, в том числе и в контексте обеспечения информационной безопасности, остается практически неизученной в отечественной и российской доктрине международного права, за исключением отдельных подходов и частно-научных точек зрения, обоснованных и разрабатываемых белорусскими, российскими и иными юристами-международниками Е.Ф. Довгань [17], Н.О. Мороз [18], А.Г. Волеводз [8], Д.М. Валеев [19], Е.Е. Королькова [20], О.В. Мозолина [21], Т.Б. Сеитов [22] и др.

Вместе с тем, вопросы информационной безопасности стала достаточно популярной в науке уголовного права, криминологии, криминалистики, а также оперативно-розыскной деятельности и теории обеспечения

национальной безопасности (например, Ю.Н. Жданов, С.К. Кузнецов, В.С. Овчинский [23], В.Е. Козлов [24], В.И. Третьяков [25], А.В. Варданян [26], Т.Л. Тропина [27], О.А. Степанов [28], А.В. Табаков [29], В.Г. Гавриленко [30] и др.), а также западными учеными-экспертами в рамках международных проектов исследований киберпреступности [31; 32].

Отсюда, заявленная проблематика, отражает цель настоящего исследования – изучение основных рисков транснациональной организованной преступности и иных факторов, воздействующих на информационную безопасность государств и их теоретико-правовое обоснование.

Основная часть

Проблематика угроз транснациональной организованной преступности на безопасность государств стала перманентной темой различных повесток дня, вызывающей наиболее пристальное внимание со стороны стран мирового сообщества, начиная с 90-х гг. XX – начала XXI вв. Этому послужили, во-первых, проведение IX Конгресса ООН по предупреждению преступности и обращению с правонарушителями (Каир, 29 апреля – 5 мая 1995 г.) и предшествовавшей ему Всемирной конференции на уровне министров по организованной транснациональной преступности (Неаполь, 21-23 ноября 2004 г.). Эти события актуализировали угрозы транснациональной организованной преступности, предложив их рассматривать в качестве международной в различных сферах межгосударственных отношений, в том числе и информационной. Во-вторых, принятие и подписание Конвенции ООН против транснациональной организованной преступности от 15 ноября 2000 г. зафиксировала рассматриваемое явление в качестве сформировавшегося международно-правового феномена, создав юридическую основу для его дальнейших комплексных научных исследований с различных сторон. Одна из них сфера информационной безопасности, степень рисков воздействия на которую со стороны транснациональной организованной преступности представляется достаточно высокой, а в некоторых случаях – угрожающей. В последнем случае, при условии взаимодействия организованных преступных групп с террористическими организациями, экстремистскими группами и радикально настроенными антиобщественными движениями и ассоциациями. Однако важно учитывать в качестве приоритетной все же экономическую ориентированность транснациональной организованной преступности и ее устойчивые корыстные интересы, направленные на получение максимальных прибылей в результате своей противоправной, латентной деятельности. Поэтому на данном этапе исследования было бы правильнее говорить о значительных рисках информационной безопасности [государств] от транснациональной организованной преступности, чем о непосредственных (экзистенциональных) угрозах. При этом, необходимо учитывать тот факт, что в международно-правовых документах, как правило, не проводят

принципиальных различий между понятиями «угрозы», «опасности», «риски», «вызовы», используя их в комплексе и руководствуясь их близким смысловым содержанием. А применительно к рассматриваемой теме, например, существует еще термин «факторы уязвимости», способные создавать «новые проблемы в плане безопасности» [32]. А именно - преодоление «цифровой пропасти» для обеспечения универсального доступа к информационно-коммуникационным технологиям и для защиты важнейших информационных инфраструктур путем облегчения передачи информационных технологий развивающимся странам, особенно наименее развитым странам, и наращивания их потенциала в вопросах передовой практики и профессиональной подготовки в области кибербезопасности [32] и др. Учитывая при этом тот факт, что обеспечение защищенности важнейших информационных инфраструктур – это обязанность, которую правительства должны систематически выполнять, выступая с соответствующими инициативами на национальном уровне, в координации с заинтересованными сторонами, которые, в свою очередь, должны знать о соответствующих рисках, превентивных мерах и эффективных мерах реагирования [32] …

Так, например, вполне закономерно, Концепция информационной безопасности Республики Беларусь от 18 марта 2019 г. [33], базируясь на Концепции национальной безопасности Республики Беларусь от 9 ноября 2010 г. (п. 6) [34], рассматривает в качестве преступлений в информационной сфере преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети (п. 8), не обходит стороной и транснациональный сегмент данных противоправных деяний. В том числе, совершаемых в составе преступных групп. В частности, говоря о мерах противодействия киберпреступности (гл. 19 Концепции) в рамках реализации международного и регионального сотрудничества в сфере кибербезопасности, Концепция акцентирует внимание на важности отслеживания деятельности преступных групп и отдельных преступников, действующих в киберпространстве (п. 74).

Это обосновывает определение в перечне основных источников угроз в области обеспечения безопасности информационных ресурсов «деятельность отдельных лиц, преступных групп, недобросовестных отечественных и иностранных организаций, объединений или сообществ, направленную на получение неправомерного доступа к этим ресурсам в политических, военных, коммерческих, личных и иных целях…» (п.79).

Идентичный подход присутствует и в Доктрине информационной безопасности Российской Федерации от 5 октября 2016 г. [35] В разделе III (Основные информационные угрозы и состояние информационной безопасности) данной Доктрины, с точки зрения исследуемой проблематики,

существенное значение имеет указание с одной стороны, на транснациональный характер незаконных деяний против информации, широкий спектр и масштаб их применения; с другой - возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности (ст. 10). В нашем случае, еще немаловажна фокусировка Доктрины на криминальном аспекте такой деятельности, включающий: а) рост компьютерной преступности, прежде всего в кредитно-финансовой сфере, б) увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий (ст. 14).

Причем, в новом правовом документе Российской Федерации в сфере обеспечения национальной безопасности – «Стратегии национальной безопасности Российской Федерации», от 2 июля 2021 г. [36] (раздел IV. «Обеспечение национальной безопасности» (п. 47 раздела: Государственная и общественная безопасность)), вполне оправдано то, что в качестве одной из специальных практических задач предусматриваются на федеральном уровне меры по предупреждению и пресечению правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе легализации преступных доходов, финансированию терроризма, организации незаконного распространения наркотических средств и психотропных веществ, а также использованию в противоправных целях цифровых валют (пп.11).

Приведенные тезисы соответствует положениям Конвенции ООН против транснациональной организованной преступности 2000 г. В ней, частности, закреплены два важнейших системообразующих элемента в обозначении контура феномена транснациональной организованной преступности:

Квалификация преступления в качестве транснационального. Согласно п. 2 ст. 3 Конвенции, «преступление носит транснациональный характер, если: а) оно совершено в более чем одном государстве; б) оно совершено в одном государстве, но существенная часть его подготовки, планирования, руководства или контроля имеет место в другом государстве; в) оно совершено в одном государстве, но при участии организованной преступной группы, которая осуществляет свою преступную деятельность в более чем одном государстве; г) оно совершено в одном государстве, но его существенные последствия имеют место в другом государстве» [37].

Определение цели участия в организованной преступной группе. В соответствии с Конвенцией – это получение прямо или косвенно, в результате совершения какого-либо преступления, финансовой или иной материальной выгоды ((п.а) ст. 2).

Представляется очевидной возможность применения положений Конвенции и к киберпреступлениям, что в ряде случаев позволяет относить их к одним из [современных] форм собственно транснациональной [организованной] преступности. Последняя, как отмечалось, a priori представляя угрозу экономическому сектору безопасности государств [38], между тем интегрируется по обоснованному мнению профессора Е.Ф. Довгань еще и в систему современных вызовов и угроз в сфере военно-политической безопасности [17, с. 11], что с точки зрения другого белорусского ученого Н.О. Мороз свидетельствует уже о ее комплексном виде угроз [18, с. 7].

В подтверждение сказанному, приведем мнение одного из ведущих мировых специалистов в сфере информационной безопасности, являющегося также одним из учредителей, основным владельцем и действующим главой АО «Лаборатория Касперского», Е.В. Касперского. Он полагает: «Наиболее важным критерием любого бизнеса является прибыльность. И киберпреступление не является исключением» [39]. Е.В. Касперский также обосновано поддерживает опасения по поводу угрозы киберпреступности (ее кибератак) на критически важные объекты инфраструктуры, которая может привести к катастрофическим последствиям [40] и поддерживает идею (на наш взгляд несколько идеалистическую) о выработки и заключения межгосударственного соглашения о нераспространении кибероружия, считая, что мировое сообщество должно положить конец гонке кибервооружений и противодействовать эскалации киберугроз на глобальном уровне [41].

В целом соглашаясь с мнением Е.В. Касперского, отметим тот факт, что на сегодняшний день в международном праве по вопросам противодействия киберпреступности, особенно ее транснациональным, организованным структурам, отмечается адресно-целевая неурегулированность. В первую очередь, об этом свидетельствует отсутствие единого специализированного международно-правового документа с одной стороны, региональным характером и ограниченным кругом участников существующих конвенций, соглашений – с другой (например, Конвенция Совета Европы о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.) и Дополнительный протокол к ней «О введении уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных сетей» от 21 января 2003 г., Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г., Конвенция Африканского союза о

кибербезопасности и защиты персональных данных от 27 июня 2014 г. (вступила в силу 3 июня 2019 г.) и др.).

Приведем некоторые обоснованные точки зрения. Так, на сегодняшний день, в международном праве выделяют 21 состав преступлений в сфере высоких технологий, содержащихся в различных международных соглашениях, 20 относятся к преступлениям международного характера и одно к международным преступлениям [42, с. 7]. В частности, по мнению отдельных экспертов, совершение акта международного терроризма при помощи информационно-коммуникационных технологий («кибертерроризма» или «информационно-электронного терроризма» [43, с. 3]) является международным преступлением, поскольку объектом такого преступления является международный мир и безопасность [42, с. 15]. Вместе с тем, преступления международного характера (в иной трактовке – транснациональные преступления [44, p. 56]) не что иное, как основные формы деятельности (проявления) самой транснациональной организованной преступности (например, торговля людьми, незаконная торговля оружием, наркотиками, «отмывание» денег, коррупция, преступления против правосудия и т.д.).

Руководствуясь вышеприведенными данными и наращиванием международно-правового потенциала по противодействию [транснациональной организованной] киберпреступности в целом, а в нашем случае - в сфере информационной безопасности, отметим еще некоторые, имеющие достаточно важное значение, положения международно-правовых документов. В первую очередь, стоит отметить Глобальную Программу ООН по киберпреступности 2017 г. [45]. Ее принятие было обусловлено, во-первых, сложным характером киберпреступности, действующей в неограниченном киберпространстве и усугубляемом ростом организованных преступных групп. Во-вторых, необходимостью гибкого реагирования на выявленные потребности в развивающихся странах (в первую очередь, Центральной Америки, Восточной Африки, БВСА, Юго-Восточной Азии и Тихого океана). В-третьих, достижением ее основных целей: 1) повышение эффективности и действенности расследования, судебного преследования и судебного разбирательства по делам о киберпреступлениях, особенно о сексуальной эксплуатации детей в Интернете и надругательствах над ними, в рамках надежной системы прав человека; 2) эффективное и действенное общегосударственное реагирование на киберпреступность в долгосрочной перспективе, включая национальную координацию, сбор данных и эффективную правовую базу, что ведет к устойчивому реагированию и усилению сдерживания; 3) укрепление национальных и международных связей между правительством, правоохранительными органами и частным сектором с повышением осведомленности общественности о рисках киберпреступности.

Кроме того, в соответствии с резолюцией 65/230 Генеральной Ассамблеи [46] и резолюциями 22/7 и 22/8 Комиссии по предупреждению преступности и уголовному правосудию соответственно [47; 48], Глобальная программа по киберпреступности уполномочена оказывать помощь государствам-членам в их борьбе с преступлениями, связанными с киберпреступностью, посредством наращивания потенциала и оказания технической помощи [45].

В этой связи, фокусируясь на исследуемой проблематике, отметим, что в резолюции, принятой Генеральной Ассамблеей ООН 74/173 от 19 декабря 2019 г. с удовлетворением отмечались «усилия Управления Организации Объединенных Наций по наркотикам и преступности, направленные на реализацию Глобальной программы борьбы с киберпреступностью в целях выполнения его мандата по оказанию технической помощи и наращиванию потенциала в области борьбы с киберпреступностью», и что Конвенция ООН против транснациональной организованной преступности 2000 г. «представляет собой инструмент, который могут использовать государства-участники для налаживания международного сотрудничества в деле предупреждения транснациональной организованной преступности и борьбы с ней и который для ряда государств-участников может быть использован в рамках некоторых дел о киберпреступности» [49].

В этой связи нам видится оптимальным и практически целесообразным, исходя из анализированной выше специфики исследуемой проблемы, разработать и принять на обсуждение проект Протокола против использования информационно-коммуникационных технологий в преступных целях, особенно киберпреступлений, дополняющий Конвенцию Организации Объединенных Наций против транснациональной организованной преступности 2000 г.

Однако, учитывая тот факт, что в настоящий момент в рамках Специального комитета [50] по разработке Всеобъемлющей Международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях идет плановая работа (1 сессия, Нью-Йорк, 28 февраля-11 марта 2022 г., 2 сессия, Вена, 30 мая-10 июня 2022 г., 3 сессия, Нью-Йорк, 29 августа-9 сентября 2022 г.) строить иллюзии относительно ее окончательной разработки и своевременного принятия заинтересованными государствами представляется, на наш взгляд, преждевременным. Не смотря на то, что, например, Российская Федерация разработала и внесла в Специальный комитет ООН свой проект конвенции о борьбе с киберпреступностью [51]. Предложение озаглавлено «Конвенция ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях». Это предложение, как сообщается, призывает государства-члены сконструировать внутреннее законодательство для

наказания за ряд конкретных преступлений, связанных с киберпреступностью. Причем, их перечень намного шире, чем те, которые признаны международным правом на данный момент времени. Российский проект представляет собой 55-страничный документ, который охватывает целый ряд вопросов, включая определение 23 видов киберпреступлений, описание процедур между различными странами по выдаче преступников (хакеров), а также оказание правовой помощи по уголовным делам, таким как выявление преступлений, арест и возвращение активов.

Высказанное сомнение обусловлено, с одной стороны, происходящими в настоящее время глобальными общественными трансформациями в странах мирового сообщества, вызванные возрастающим противостоянием стран НАТО под лидерством США против Российской Федерации и ее союзников. С другой стороны, используемые США и их союзниками информационно-коммуникационные технологии умышленно ставятся вне правового поля, подменяя их приоритетностью собственных интересов в сфере квази-национальной безопасности, а латентно – в интересах бенефициаров различного рода корпоративных структур и их аффилированных негосударственных субъектов. Это однозначно нивелирует значимость концепции примата международного права в разрешении любых межгосударственных споров и конфликтов.

Вместе с тем, наше предложение о внесении соответствующего проекта Протокола, дополняющего Конвенцию против транснациональной организованной преступности 2000 г., не противоречит цели самой Конвенции (ст.1), соответствует сферам ее применения (ст. 3), а по состоянию на 19 сентября 2017 года она насчитывает 190 участников, что свидетельствует о ее юридической состоятельности. Разумеется, предлагаемый проект Протокола будет направлен на решение только на определенную часть проблем в рассматриваемой области, однако проблем весьма значимых, актуальных и уже имеющих устойчивую юридическую основу.

Заключение

Предпринятая попытка исследования проблем транснациональной организованной преступности в контексте рисков информационной безопасности безусловно является актуальной, малоизученной и требующей дальнейших предметных исследований с точки зрения международного права, в первую очередь, основываясь на его таких отраслях как право международной безопасности, международное уголовное право и международное гуманитарное право.

В целях придания системности и наполнения определенным смысловым содержанием понятий: «вызовы», «угрозы», «опасности», «риски», «факторы уязвимости», представляется целесообразным их закрепление в разрабатываемом в настоящее время проекте Всеобъемлющей

международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях в силу ее в большей степени ожидаемого декларативного характера.

В качестве практических шагов по противодействию транснациональной организованной преступности в данной сфере, устойчивости и обоснованности международно-правовой позиции Республики Беларусь, предлагается разработка проекта Протокола против использования информационно-коммуникационных технологий в преступных целях, особенно киберпреступлений, дополняющий Конвенцию Организации Объединенных Наций против транснациональной организованной преступности 2000 г.

Библиографический список

1. Арчаков, В.Ю. Даркнет в контексте рисков национальной безопасности / В.Ю. Арчаков, А.Л. Баньковский, Е.В. Зенченко // Право.by. – 2021. – №6(74). – С. 5-10.

2. Сальвадорская декларация ООН о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире [Электронный ресурс]: принята резолюцией Генер. Ассамблеи ООН, 21 дек., 2010 г. №65/230 // Организация Объединенных Наций. – Режим доступа: https://www.un.org/ru/documents/decl_conv/declarations/salvador_declaration.shtml. - Дата доступа: 08.11.2022.

3. Предварительная повестка дня двадцатой сессии Комиссии ООН по предупреждению преступности и уголовному правосудию: «Мировые тенденции в области преступности и новые проблемы в области предупреждения преступности и уголовного правосудия и способы их решения» [Электронный ресурс]: 11-15 апреля 2011 г., E/CN.15/2022/1 // Организация Объединенных Наций. – Режим доступа: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_24/resolutions/L11_Rev1/ECN152015_L11_r_V1503512.pdf. - Дата доступа: 08.11.2022.

4. Дохинская декларация ООН о включении вопросов предупреждения преступности и уголовного правосудия в более широкую повестку дня Организации Объединенных Наций в целях решения социальных и экономических проблем и содействия обеспечению верховенства права на национальном и международном уровнях, а также участию общественности [Электронный ресурс]: 12-19 апреля 2015 г., A/CONF.222/L.6 // Организация Объединенных Наций. – Режим доступа: https://www.unodc.org/documents/congress/Declaration/V1504153_Russian.pdf. - Дата доступа: 08.11.2022.

5. Руководство для дискуссий: док. ООН A/CONF.234/PM.1 // Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, Киото, Япония, 20-27 апреля 2020 г. [Электронный ресурс] // Организация Объединенных Наций. –Режим доступа: https://undocs.org/pdf?symbol=ru/A/CONF.234/PM.1. – Дата доступа: 07.11.2022.

6. Конвенция Совета Европы о киберпреступности (в отдельных источниках трактуется как Конвенция о преступности в сфере компьютерной информации) [Электронный ресурс]: 23 ноября 2001 г., ETS № 185. – Режим доступа: http://base.garant.ru/4089723/. - Дата доступа: 08.11.2022.

7. Доклад межправительственной группы экспертов открытого состава о всестороннем исследовании проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора. Двадцатая сессия

Комиссии Организации Объединенных Наций по предупреждению преступности и уголовному правосудию [Электронный ресурс]: 11-15 апреля 2011 г., E/CN.15/2011/19 // Организация Объединенных Наций. – Режим доступа: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf. – Дата доступа: 07.11.2022.

8. Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М.: ООО «Юрлитинформ», 2001. – 496 с.

9. Глобальная программа кибербезопасности [ГПК] МСЭ: Основа для международного сотрудничества в области кибербезопасности. Международный союз электросвязи. Отдел корпоративной стратегии. Place des Nations. CH-1211 Geneva 20 [Электронный ресурс]. – Режим доступа: https://ifap.ru/pr/2008/080908aa.pdf. – Дата доступа: 07.11.2022.

10. Межгосударственная программа совместных мер по борьбе с преступностью на 2019-2023 [Электронный ресурс]. - Режим доступа: https://e-cis.info/cooperation/3192/83381/. - Дата доступа: 08.11.2022.

11. Kramer, A.E. Cyberweapon Warning From Kaspersky, a Computer Security Expert /A.E. Kramer. The New York Times (3 June 2012).

12. The Globalization of Crime: A Transnational Organized Crime Threat Assessment (United Nations Office on Drugs and Crime) [Electronic resource]. – Mode of access: https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf. - Date of access: 08.11.2022.

13. Cybercrime to cost the world $10.5 trillion annually by 2025: special report: cyberwarfare in the c-suite. Sausalito, Calif. – Nov. 13, 2020 [Electronic resource]. – Mode of access: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025// - Date of access: 08.11.2022.

14. Меркушин, В.В. О некоторых проблемах международно-правового регулирования противодействия транснациональной организованной преступности в контексте обеспечения безопасности государств / В.В. Меркушин // Журнал международного права и международных отношений. 2021. 3(98). С. 3–10.

15. Советы по защите от киберпреступников [Электронный ресурс]. - Режим доступа: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime. - Дата доступа: 08.11.2022.

16. Овчинский, В. Организованная киберпреступность / В. Овчинский, Ю. Жданов [Электронный ресурс]. - Режим доступа: https://zavtra.ru/blogs/organizovannaya_kiber-prestupnost_ - Дата доступа: 08.11.2022.

17. Довгань, Е.Ф. Международные организации и поддержание международного мира и безопасности: моногр. / Е.Ф. Довгань. – Минск: Междунар. ун-т «МИТСО», 2016. – 262 с.

18. Мороз, Н.О. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий: моногр. / Н.О. Мороз. – Минск: Междунар. ун-т «МИТСО», 2017. – 266 с.

19. Валеев, Д.М. Международно-правовые основы сотрудничества по борьбе с транснациональной организованной преступностью: дис. канд. юрид. наук: 12.00.10 / Д.М. Валеев. – Казань, 2016. – 227 с.

20. Королькова, Е.Е. Международно-правовое регулирование деятельности частных военных и охранных компаний: дис. … канд.юрид. наук: 12.00.10 / Е.Е. Королькова. – М., 2019. – 212 с.

21. Мозолина, О.В. Публично-правовые аспекты международного регулирования отношений в Интернете: автореф. дисс. … канд. .юрид. наук: 12.00.10 / О.В. Мозолина. – М., 2008. – 26 с.

22. Сеитов, Т.Б. Международно-правовое сотрудничество государств в борьбе с компьютерной преступностью: автореф. дисс. … канд. юрид. наук: 12.00.10 / Т.Б. Сеитов. – Алматы, 2002. – 23 с.

23. Жданов, Ю.Н. COVID-19: преступность, кибербезопасность, общество, полиция / Ю.Н. Жданов, [и др.]. – М.: Междунар. отношения, 2020. – 448 с.

24. Козлов, В.Е. Противодействие компьютерной преступности: проблемы и пути их разрешения: монография / В.Е. Козлов. – Минск: Акад. МВД Респ. Беларусь, 2006. – 256 с.

25. Третьяков, В.И. Организованная преступность и легализация криминальных доходов: автореф. дис. ... доктора юрид. наук: 12.00.08 / В.И. Третьяков. – Ростов-на-Дону, 2009. – 56 с.

26. Варданян, А.В. Расследование преступлений в сфере высоких технологий и компьютерной информации / А.В. Варданян, Е.В. Никитина. – М.: Юрлитинформ, 2007. – 307 с.

27. Тропина, Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы / Т.Л. Тропина. – Владивосток: Изд-во Дальневосточного ун-та, 2009. – 237 с.

28. Степанов, О.А. Теоретико-правовые аспекты безопасного функционирования и развития информационно-электронных систем: автореф. дис. ... доктора юрид. наук: 12.00.01 / О.А. Степанов. – М., 2005. - 53 с.

29. Табаков, А.В. Современное состояние и основные тенденции развития транснациональной организованной наркопреступности: моногр. / А.В. Табаков; СПбГАСУ. – СПб., 2018. – 259 с.

30. Гавриленко, В.Г. Правовые основы и механизмы обеспечения национальной безопасности и суверенитета Республики Беларусь / В.Г. Гавриленко. – Минск: Право и экономика, 2019. – 1104 с.

31. Всестороннее исследование проблемы киберпреступности: проект, февраль [Электронный ресурс]: Вена, 2013 г. // Управление ООН по наркотикам и преступности. - Режим доступа: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf. – Дата доступа: 08.11.2022.

32. Создание глобальной культуры кибербезопасности и защита важнейших информационных структур [Электронный ресурс]: резолюция Генер. Ассамблеи ООН, 23 дек. 2003 г., №58/199 // Организация Объединенных Наций. – Режим доступа: https://undocs.org/ru/A/RES/58/199. - Дата доступа: 08.11.2022.

33. О Концепции информационной безопасности Республики Беларусь от 18 марта 2019 г. [Электронный ресурс]: Постановление Совета Безопасности Республики Беларусь № 1/ - Режим доступа: https://www.sb.by/articles/kontseptsiya-informatsionnoy-bezopasnosti-respubliki-belarus.html. - Дата доступа: 08.11.2022.

34. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс]: Указ Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. - Минск, 2020.

35. Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента РФ от 5 декабря 2016 г. № 646 [Электронный ресурс]: - Режим доступа: http://kremlin.ru/acts/bank/41460/page/1. - Дата доступа: 08.11.2022.

36. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 г. №400 [Электронный ресурс]: - Режим доступа: https://www.garant.ru/products/ipo/prime/doc/401325792/. - Дата доступа: 08.11.2022.

37. Конвенция Организации Объединенных Наций против транснациональной организованной преступности: принята резолюцией Генеральной Ассамблеи 15 ноября 2000 г. [Электронный ресурс] // Организация Объединенных Наций. – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml. – Дата доступа: 08.11.2022.

38. Edie, E. Economics of crime / E. Edie [et oth.] // Foundations and Trends in Microeconomics. – 2006. – №3, Vol. 2. Emory Law and Economics Research Paper №11-114, Available at SSRN [Electronic resource]. – Mode of access: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1912073. – Date of access: 08.11.2022.

39. Официальный сайт Евгения Касперского [Электронный ресурс]. – Режим доступа: https://e-kaspersky.livejournal.com/. – Дата доступа: 07.11.2022.

40. Новый, В. Если будут "валить" регион, город или страну целиком – до свиданья / В. Новый [Электронный ресурс]. – Режим доступа: kommersant.ru (28 марта 2013). - Дата доступа: 08.11.2022.

41. Kramer, Andrew E. Cyberweapon Warning From Kaspersky, a Computer Security Expert (англ.), The New York Times (3 June 2012).

42. Мороз, Н.О. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий: автореф. дис. ... канд. юрид. наук: 12.00.10 / Н.О. Мороз. – Минск, 2014. – 23 с.

43. Степанов, О.А. Теоретико-правовые аспекты безопасного функционирования и развития информационно-электронных систем: автореф. дис. ... доктора юрид. наук: 12.00.01 / О.А. Степанов. – М., 2005. – 53 с.

44. Bassiouni, M.Ch. A draft international criminal code and draft statute for an international criminal tribunal / By M. Cherif Bassiouni. - Dordrecht et al.: Nijhoff, 1987. P. 56-57.

45. Global Programme on Cybercrime [Electronic resource] // United Nations Organization. – Mode of access: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html. – Date of access: 08.11.2022.

46. Twelfth United Nations Congress on Crime Prevention and Criminal Justice: General Assembly resolution 65/230 [21 December 2010] [Electronic resource] // United Nations Organization. – Mode of access: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2010/General_Assembly/A-RES-65-230.pdf. – Date of access: 08.11.2022.

47. The Commission on Crime Prevention and Criminal Justice [Electronic resource]: Res. 22/7 “Strengthening international cooperation to combat cybercrime”. – Mode of access: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-7.pdf. – Date of access: 08.11.2022.

48. The Commission on Crime Prevention and Criminal Justice [Electronic resource]: Res. 22/8 “Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime” [Electronic resource]. – Mode of access: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-8.pdf. – Date of access: 08.11.2022.

49. Резолюция Генеральной Ассамблеей от 18 декабря 2019 г. [по докладу Третьего комитета (A/74/400)]: содействие оказанию технической помощи и наращиванию

потенциала для усиления национальных мер и укрепления международного сотрудничества в целях борьбы с киберпреступностью, включая обмен информацией [A/RES/74/173] [Электронный ресурс] // Организация Объединенных Наций. – Режим доступа: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/429/95/PDF/N1942995.pdf?OpenElement. – Дата доступа: 07.11.2022.

50. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Organizational session. New York, 10–12 May 2021. Agenda item 6. [A/AC.291/L.1] [Electronic resource] // United Nations Organization. – Mode of access: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Organizational_session/V2200692.pdf. – Date of access: 08.11.2022.

51. Russia gives the UN draft convention to fight cybercrime [Electronic resource]. – Mode of access: https/previewtech.net/russia-gives-the-un-draft-convention-to-fight-cybercrime/. – Date of access: 08.11.2022.

УДК 336.027

НАЛОГОВОЕ КОНСУЛЬТИРОВАНИЕ В СИСТЕМЕ МЕР ПОЗИТИВНОГО ИНФОРМИРОВАНИЯ НАЛОГОПЛАТЕЛЬЩИКОВ

А.А. Пилипенко

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье анализируются научные подходы по вопросу определения налогового консультирования и предлагается авторская дефиниция данного феномена. Делается вывод о необходимости налогоплательщиками с помощью налоговых консультантов выбора рациональной стратегии поведения. Обосновываются предложения, направленные на совершенствование налогового консультирования в Республике Беларусь.

***Ключевые слова*:** налоговое консультирование, налогообложение, налоговое право.

TAX CONSULTING IN THE SYSTEM OF POSITIVE INFORMING OF TAXPAYERS

A.A. Pilipenko

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article analyzes scientific approaches to the definition of tax consulting and proposes the author's definition of this phenomenon. It is concluded that taxpayers, with the help of tax consultants, need to choose a rational strategy of behavior. Proposals aimed at improving tax consulting in the Republic of Belarus are substantiated.

Keywords: tax consulting, taxation, tax law.

С учетом мировых тенденций в сфере налогообложения Республика Беларусь постоянно находится в поиске оптимальных механизмов взаимодействия различных субъектов налоговых отношений, одним из которых является налоговое консультирование. Объективная необходимость данного института обусловлена переоценкой качественных ориентиров налоговых отношений и необходимостью достижения, в первую очередь, баланса интересов государства и налогоплательщиков.

Нормативное признание рассматриваемого института в Республике Беларусь связано с Указом Президента Республики Беларусь от 19 сентября

2017 г. № 338 «О налоговом консультировании» (далее – Указ № 338), который, в том числе, закрепил понятие налогового консультирования. В соответствии с п. 41 Положения о налоговом консультировании, утв. Указом № 338 (далее – Положение) налоговое консультирование представляет собой предпринимательскую деятельность по оказанию консультационных и иных сопутствующих услуг в сфере отношений, регулируемых налоговым законодательством.

Следует обратить внимание, что, как и в приведенном легальном определении, терминологической особенностью налогового консультирования является детерминирование в научных изысканиях предпринимательской деятельности как его атрибутивного признака. Например, с точки зрения Л.С. Кириной и Н.А. Назаровой, «как предпринимательская деятельность консультирование по налогам и сборам (налоговое консультирование) – это вид профессиональной вневедомственной деятельности по оказанию заказчику (консультируемому лицу) на платной основе услуг, содействующих оптимальному и должному исполнению налогоплательщиками обязанностей, предусмотренных законодательством о налогах и сборах, по исчислению и уплате налогов и сборов» [1, с. 18].

В то же время, доминирующим взглядом на налоговое консультирование следует признать постулирование оптимизационной содержательной компоненты, направленной на оказание помощи налогоплательщикам при принятии решений в сфере налогообложения. По мнению А.К. Кобылинского, «институт налогового консультирования можно представить как систему поддержки решений налогообязанными лицами (налогоплательщиками, плательщиками сборов, налоговыми агентами, банками), основанную на использовании профессиональных суждений и тенденциях правоприменительной практики относительно применения нормативно закрепленных правил исполнения налоговой обязанности и принуждения к ее исполнению» [2, с. 8]. Суждение Т.А. Ефимовой и Е.Б. Шуваловой состоит в том, что «предоставление услуг по разъяснению налогового законодательства и предоставлению рекомендаций по наиболее оптимальному его применению в конкретной ситуации» [3, с. 25]. Белорусские исследователи Д.А. Панков и Л.В. Пашковский рассматривают налоговое консультирование как «оказание квалифицированных услуг независимыми аттестованными консультантами гражданам и юридическим лицам при планировании, оптимизации, начислении и уплате ими всех видов налоговых обязательств, предусмотренных действующим законодательством страны» [4, с. 36].

Существует точка зрения, которая достойна отдельного внимания в контексте системного межотраслевого и междисциплинарного подхода к пониманию налогового консультирования. Н.Н. Баширов и Е.Б. Сугробова полагают, что налоговое консультирование – это «предоставление

комплекса услуг, оказываемых на основе взаимосвязи норм налогового и отраслевого законодательства, методов финансово-экономического анализа в области управления налогообложением для целей финансового менеджмента и заключающихся в выработке квалифицированного мнения по налоговым вопросам; подготовке рекомендаций по формированию налоговой базы по видам налогов и сборов, использованию налоговых льгот; помощи при составлении налоговой отчетности налогоплательщика» [5, с. 9].

Конфликтность государства и налогоплательщиков зачастую связана с тем, что для последних, с общественной точки зрения, фискально-экономические обязательства носят, как правило, абстрактный и сопутствующий (вторичный, производный) характер. В силу этого, неся предметно-непосредственное налоговое бремя, они оптимизируют вышеуказанные обязательства. По нашему мнению, налоговые консультанты призваны придать процессу налоговой оптимизации (налогового планирования) не только легитимный характер, что является атрибутивным признаком оптимизационных процессов в налоговой сфере, но и обеспечить рациональный выбор стратегии поведения налогоплательщика. Данная стратегия позволит не только снизить налоговые риски (в первую очередь, на микроуровне – для налогоплательщиков), но и создаст обширный регулятивный потенциал снижения градуса конфликтности налоговых отношений. Также государством рациональная стратегия налогоплательщика, которая всегда будет ему имманентна в силу желания оптимизировать налоговые платежи, должна рассматриваться как направленность на снятие существующей налоговой неопределенности посредством последующей модификации законодателем нормативных конструкций. В данном контексте, хотелось бы высказать некоторые соображения об участии консультантов в налоговых отношениях на высоком профессиональном уровне.

Одним из дискуссионных вопросов в правоприменительной деятельности оказания бухгалтерских услуг, который экстраполируется на возможность быть налоговым консультантом, является вопрос наличия соответствующего образования. В настоящее время, в соответствии с п. 6 Положения о налоговом консультировании к квалификационному экзамену допускаются физические лица, имеющие: высшее экономическое и (или) юридическое образование и стаж работы по специальности после получения высшего образования не менее трех лет; иное высшее образование при условии прохождения переподготовки на уровне высшего образования по специальности экономического и (или) юридического профиля и наличия стажа работы по этим специальностям не менее трех лет.

Учитывая, что оказание услуг по ведению бухгалтерского и (или) налогового учета, довольно часто оказывают лица, не имеющие вышеуказанные образования, но имеющие среднее специальное образование и обладающие

достаточно большим опытом и профессиональными знаниями в экономической и правовой сферах, возникает критическая неустойчивость (с точки зрения проявления элементов запрета на профессию) их жизненно предпринимательского статуса. Так как большинство таких лиц, как правило, работают в регионах, то может сложиться ситуация, когда субъекты предпринимательской деятельности не смогут воспользоваться соответствующими услугами.

Однако мы хотели бы дистанцироваться от критических суждений практикующей аудитории по изложенным выше мотивам в контексте необходимости придания налогово-законодательным конструкциям упрощенного характера без необходимости привлечения для их бухгалтерского и налогового «обрамления» соответствующих специалистов. Т.е. законодатель не должен без должной необходимости вводить налогово-правовые нормы, исполнение которых невозможно без участия соответствующих специалистов. Например, в рамках применения единого налога с индивидуальных предпринимателей и иных физических лиц, п. 14 ст. 342 НК предусматривает, что при превышении валовой выручки над сорокакратной суммой единого налога за соответствующий отчетный период индивидуальными предпринимателями исчисляется доплата единого налога в размере 5 процентов с суммы такого превышения. Наличие данной нормы не только нивелирует правоприменительное значение особого режима налогообложения, суть которого состоит, в том числе, и в упрощении (отсутствии) бухгалтерского и налогового учета, но и требует от индивидуальных предпринимателей привлечения специалистов в указанных сферах. Таким образом, упрощение налогового законодательства в русле создания все больших условий для самостоятельного исчисления фискальных платежей (или снижения необходимости обращения к налоговым консультантам), естественным образом приведет к повышению конкуренции на рынке налогового консультирования. В данном случае одним из конкурентных преимуществ будет наличие одного или нескольких высших образований.

Постулируемый нами тезис о сохранении повышенных требований к налоговым консультантам побуждает к критической переоценке положений подп. 1.5 п. 1 Указа № 338, который определяя сферы, на которые не распространяются положения Указа № 338, указывает оказание услуг по ведению бухгалтерского учета и составлению отчетности, осуществляемых организациями и (или) индивидуальными предпринимателями на основании договора. При этом, п. 2 Положения о налоговом консультировании, раскрывая содержание налогового консультирования, включает в него отношения по оказанию услуг по ведению бухгалтерского и (или) налогового учета, составлению отчетности, налоговых деклараций (расчетов) и иных документов, в том числе жалоб. Полагаем, что одним из приоритетных

направлений правового регулирования областей, связанных с исчислением фискальных платежей, является высокий профессиональный уровень субъектов, их исчисляющих. Статус налоговых консультантов для таких субъектов создает дополнительные гарантии для всех участников налоговых отношений, в том числе и государства, в полноте и своевременности выполнения налоговых обязанностей. В этой связи полагаем целесообразным исключить из подп. 1.5 п. 1 Указа № 338 слова «а также на оказание услуг по ведению бухгалтерского и (или) налогового учета, составлению отчетности, налоговых деклараций (расчетов) и иных документов, представлению интересов в налоговых правоотношениях в налоговых и иных государственных органах, организациях, осуществляемых организациями и (или) индивидуальными предпринимателями на основании договора». Предлагаемая новация должна корреспондироваться с повышенным переходным (адаптационным) периодом, в течение которого можно осуществлять соответствующие услуги без статуса налогового консультанта.

Делая акцент на необходимости сохранения повышенных требований к налоговым консультантам, хотелось бы отметить, что в силу сложности и перманентной изменчивости налогового законодательства, для его четкого и правильного понимания и применения необходимы высоко профессиональные и подготовленные физические лица и организации, которые не только владеют всеми тонкостями и нюансами налогообложения, но и способны дать объективную экономико-правовую оценку как отельным хозяйственным операциям, так и бизнес-стратегии, в целом.

Подпункт 1.2 п. 1 Указа № 338 предусматривает обязанность налоговых консультантов возмещать убытки, причиненные, в том числе, вследствие неисполнения или ненадлежащего исполнения своих обязанностей по договору возмездного оказания услуг по налоговому консультированию. При этом диспозитивные элементы правового регулирования налогового консультирования (определение в договоре на оказание возмездного оказания услуг по налоговому консультированию ответственности сторон за невыполнение или ненадлежащее выполнение обязательств) (ч. 2 п. 3 Положения о налоговом консультировании) сочетаются с императивными, которые предусматривают обязанность страхования убытков (попд. 1.2 п. 1 Указа № 338). Законодатель прямо определяет, что под убытками понимаются пени, начисленные в соответствии со ст. 55 Налогового кодекса Республики Беларусь от 19 декабря 2002 г. юридическому, физическому лицу, в том числе индивидуальному предпринимателю, заключившим договор возмездного оказания услуг по налоговому консультированию, и (или) сумма примененных к этим лицам административных взысканий. Обратим внимание, что из отрицательных претерпеваний для субъектов предпринимательской деятельности, которые могут иметь место по результатам проведения

контрольных мероприятий, не указана недоимка, являющаяся, с количественной точки зрения, наиболее обременительной. Последние тенденции в нормативном регулировании контрольной деятельности направлены на проведение в отношении субъектов предпринимательской деятельности не проверок, а профилактических мероприятий, о чем, в частности, свидетельствует резкое сокращение количества выборочных проверок по областям и г. Минску, включенных в соответствующие планы. Это, в свою очередь, должно привести к сокращению недоимок, пеней и административных взысканий. Соответственно, видится целесообразным уменьшение обязательной страховой суммы на покрытие убытков, причиненных налоговыми консультантами при неисполнении или ненадлежащем исполнении ими обязательств по договору возмездного оказания услуг по налоговому консультированию. В свете вышесказанного возможные перспективы законодательного регулирования видятся в изложении первого предложения ч. 2 подп. 1.2 п. 1 Указа № 338 в следующей редакции: «Страховая сумма по договору страхования ответственности коммерческих организаций, индивидуальных предпринимателей, осуществляющих деятельность по налоговому консультированию, за причинение убытков в связи с ее осуществлением не может быть менее пятисот базовых величин».

Библиографический список

1. Налоговое консультирование: теория и практика : учебник / Н.И. Малис [и др.] ; под ред. Н.И. Малиса. – М. : Магистр : ИНФРА-М, 2018. – 416 с.

2. Кобылинский, А.К. Совершенствование налогового консультирования корпоративных налогоплательщиков : дис. … канд. экон. наук : 08.00.10 / А.К. Кобылинский. – Ростов н/Д, 2015. – 163 л.

3. Шувалова, Е.Б. Налоговое консультирование (правовой аспект) : учеб. пособие / Е.Б. Шувалова, Т.А. Ефимова. – М. : Изд. центр ЕАОИ, 2011. – 136 с.

4. Панков, Д.А. Институциональные основы налогового консультирования как нового вида предпринимательской деятельности в Республике Беларусь / Д.А. Панков, Л.В. Пашковский // Бухгалтерский учет и анализ. – 2014. – № 11. – С. 19–38.

5. Баширова, Н.Н. Основы налогового консультирования: учеб. пособие / Н.Н. Баширова, Е.Б. Сугубова ; под ред. Л.И. Гончаренко. – М. : Магистр, 2010. – 175 с.

УДК 355.1

О НЕКОТОРЫХ ПРОБЛЕМАХ ОБЕСПЕЧЕНИЯ ПОГРАНИЧНОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ

В.Н. Будько[1)],
В.В. Меркушин [2)]

[1)]Государственное учреждение образования
«Институт пограничной службы Республики Беларусь»,
ул. Славинского 4, г. Минск, 220103, Беларусь
[2)]Белорусский государственный университет,
пр. Независимости 4, Минск, 220030, Беларусь

В статье раскрываются правовые и теоретико-прикладные вопросы обеспечения пограничной безопасности в информационном сегменте национальной безопасности Республики Беларусь. Предлагаются адресно-целевые инициативы правового и институционального характера по урегулированию наиболее существенных аспектов пограничной безопасности в информационной сфере.

***Ключевые слова*:** пограничная безопасность, национальная безопасность, информационная безопасность, информационная сфера.

ON SOME PROBLEMS OF ENSURING BORDER SECURITY IN THE INFORMATION SPHERE

V.N. Budko[a],
V.V. Merkushin[b]

[a]State Educational Institution
«Institute of the Border Service of the Republic of Belarus»,
4 Slavinsky street, Minsk, 220103, Belarus
[b]Belarusian State University,
4 Nezalezhnosti Avenue, Minsk, 220030, Belarus

The article reveals the legal, theoretical and practical issues of ensuring border security in the information segment of the national security of the Republic of Belarus. Targeted initiatives of a legal and institutional nature are proposed to regulate the most significant aspects of border security in the information sphere.

Keywords: border security, national security, information security, information sphere.

В современных условиях обеспечение пограничной безопасности Республики Беларусь в информационной сфере является одним из важнейших функциональных элементов национальной безопасности государства,

качественным показателем состояния информирования общественности о ситуациях (текущих событиях) на Государственной границе Республики Беларусь, оперативной оценки и адекватного принятия мер уполномоченными субъектами по противодействию вновь возникающим рискам, вызовам и угрозам в пограничном пространстве Республики Беларусь. Особенно этому способствует резкое обострение противостояния России и Беларуси со странами НАТО с момента начала проведения специальной военной операции на территории Украины.

Важность информационного сегмента в обеспечении пограничной безопасности, основывается на двух основных нормативно-правовых документах: Концепции национальной безопасности Республики Беларусь 2010 г. и Концепции информационной безопасности Республики Беларусь 2019 г., и зафиксирована в: Концепции обеспечения пограничной безопасности Республики Беларусь на 2018–2022 годы (утверждена Указом Президента Республики Беларусь №410 от 16 октября 2018 г.).

Прочие вопросы, в основном административно-правового и организационного характера, установлены в Законе об органах пограничной службы Республики Беларусь от 11 ноября 2008 г.; Военной доктрине Республики Беларусь от 20 июля 2016 г., а также в ряде ведомственных и межведомственных специальных актах и распоряжениях.

Общими и объективно значимыми угрозами для основ безопасности государств (в т.ч. пограничной безопасности) являются способность применения некоторыми враждебными субъектами новых способов и методов развязывания войны (особенно, информационно-пропагандистской) и иных агрессивных воздействий на государственный суверенитет, тем самым транслируя собственные национальные интересы в ущерб иным суверенным правам, в том числе всеобъемлющей сфере международной безопасности и сложившейся системе мирового правопорядка [1, с. 9-12; 2, с. 5-9].

Не остаются в стороне от этих процессов и общеизвестные виды угроз и воздействий на безопасность государств – международный терроризм и вооруженный экстремизм, трансграничная организованная преступность и коррупция, противоправная деятельность международных транснациональных корпораций и сетевых объединений киберпреступников, а также некоторых частных военных и охранных компаний и неправительственных международных организаций [3, с. 4-6].

Следует отметить, что в юридической науке общие и специальные вопросы пограничной безопасности государства, в т.ч. и применительно к информационной сфере, рассматривались также в работах таких ученых, как: В.Ю. Арчаков, А.Л. Баньковский, А.Л. Зенченко [4], А.И. Бородич [5], С.В. Верлуп [6], В.Ф. Ермолович, С.Н. Князев [7], А.А. Павловский [8], С.А. Трахименок [9], В.Г. Гавриленко [10], и др. Вместе с тем, проблематика

обеспечения пограничной безопасности в информационной сфере остается практически неисследованной. Отсюда, основной целью данной работы является исследование наиболее важных вопросов, касающихся современных информационных аспектов пограничной безопасности Республики Беларусь и выработка адресно-целевых мер по их фиксации в общей системе национальной безопасности Республики Беларусь.

Доказательством важности затрагиваемой проблематики является то, что в настоящее время вопросы противодействия современным вызовам и угрозам пограничной безопасности в информационной сфере затрагиваются (хотя и опосредовано) в международных соглашениях и иных обязательствах Республики Беларусь. В первую очередь, это в Уставе Содружества Независимых Государств от 22 января 1993 г., Соглашении об обмене информацией по вопросам охраны внешних границ государств - участников Содружества Независимых Государств от 12 апреля 1996 г., Конвенции о приграничном сотрудничестве государств-участников Содружества Независимых Государств от 10 октября 2008 г., Договоре о сотрудничестве в охране границ государств–участников Содружества Независимых Государств с государствами, не входящими в Содружество от 26 мая 1995 г., а также Договоре о создании Союзного государства России и Беларуси от 8 декабря 1999 г. и Организации Договора о коллективной безопасности (ОДКБ) от 7 октября 2002 г., и др.

Особого внимания заслуживает прошедшее 4 ноября 2021 г. заседание *Высшего Государственного Совета Союзного государства России и Беларуси*. В принятом по итогам заседании комплексном масштабном документе «Об основных направлениях реализации положений Договора о создании Союзного государства России и Беларуси на 2021-2023 гг.», одними из важнейших 28 утвержденных документов стали *Концепция миграционной политики Союзного государства и Военная доктрина Союзного государства*.

Концепция миграционной политики Союзного государства определила создание единого миграционного и визового пространства России и Беларуси, а также совместное противодействие угрозам безопасности Союзного государства, связанных с незаконной миграцией, обеспечение партнерства в интересах граждан в сфере труда и занятости.

Принятие Военной доктрины Союзного государства было обусловлено изменениями военно-политической обстановки в регионе, возникновением новых вызовов и угроз для России и Беларуси, беспрецедентным внешним давлением. Был отмечен также высокий уровень взаимодействия в сфере обороны, свидетельствующий о том, что границы Союзного государства надежно защищены. В этой связи Президент Российской Федерации В.В. Путин по представлению Президента Республики Беларусь А.Г. Лукашенко подчеркнул, что «… особое значение приобретает задача формирования на

наших внешних границах атмосферы стабильности и безопасности. Мы намерены сообща противостоять любым попыткам вмешательства во внутренние дела наших суверенных государств…» [11].

Приведенные примеры, подчеркивают значимость информационной сферы пограничной безопасности *как одного из важнейших элементов «первого рубежа обороны»,* превентивно направленного на противодействие вновь возникающим векторам вызовов и угроз, а также их негативным последствиям на «красных линиях» соприкосновения с национальными интересами государства. Но, самое главное, как отмечают ученые-эксперты С.В. Верлуп и В.П. Шкред, в первую очередь векторы угроз (особенно внешнего происхождения) направлены на территориальную целостность, суверенитет (особенно информационный), независимость и конституционный строй, а также действия по их реализации проявляются на Государственной границе Республики Беларусь [12, с. 83]. А с точки зрения отдельных военных экспертов (В.А. Ксенофонтов) уровень развития современных информационно-коммуникационных технологий и получения информации являются критически важными и для сферы военной безопасности [13, с. 163].

Более того, по мнению других экспертов в области национальной безопасности (В.Ю. Арчакова, А.Л. Баньковского, Е.В. Зенченко), противоправные возможности трансграничной передачи информации обуславливают необходимость их учета при совершенствовании действующей Концепции национальной безопасности Республики Беларусь [4, с. 5]. И эти замечания не случайны. Поскольку, с методолого-правовой позиции профессора С.А. Трахименка на фундаментальные аспекты безопасности государства, основной причиной значимости информационной безопасности является прогрессирующая информатизация общества и рост социальной роли информатики [9, с. 37].

Таким образом, в целях обеспечения национальных интересов Республики Беларусь в информационном пространстве, в том числе и в рамках конструирования пограничной безопасности, представляется необходимым:

Рассмотреть и обосновать вопрос о формировании Центрального оперативного руководства киберпространством и создать «Антикибертеррористический Комитет» (в рамках ОДКБ-СНГ) и их аналоги (структурные подразделения) на национальном уровне.

В проекте новой Концепции Пограничной безопасности Республики Беларусь в соответствии с положениям Концепции национальной безопасности Республики Беларусь, определить в качестве одного из приоритетных направления деятельности органов пограничной службы Республики Беларусь:

«в информационной сфере –

противодействие пропаганде войны, национальному, расовому и религиозному экстремизму и ксенофобии;

пресечение нарушений территориальной целостности, неприкосновенности государственной границы Республики Беларусь и вмешательства в ее внутренние дела,

активная разработка и внедрение современных методов и средств защиты информационных технологий и персональных данных, непосредственно используемых в автоматизированных системах управления органами пограничной службы».

В системе органов пограничной службы продолжить разработку практически применимых методик противодействия современным вызовам и угрозам пограничной безопасности Республики Беларусь, особенно посредством создания многовариантных программных продуктов, формируемых в виде целевого операционно-информационного модуля, который может постоянно совершенствоваться разработчиками, а также динамично развиваться непосредственно специалистами-пользователями взаимодействующих субъектов.

Библиографический список

1. Выступление Президента Республики Беларусь А.Г. Лукашенко 9 мая 2022 г. – Режим доступа: https://www.youtube.com/watch?v=XByEOlkdNP0. – Дата доступа: 10.05.2022.

2. Довгань, Е.Ф. Международные организации и поддержание международного мира и безопасности: моногр. / Е.Ф. Довгань. – Минск: Междунар. ун-т «МИТСО», 2016. – 262 с.

3. Мороз, Н.О. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий: моногр. / Н.О. Мороз. – Минск: Междунар. ун-т «МИТСО», 2017. – 266 с.

4. Меркушин, В.В. О некоторых проблемах международно-правового регулирования противодействия транснациональной организованной преступности в контексте обеспечения безопасности государств / В.В. Меркушин // Журнал международного права и международных отношений. 2021. – 3(98). – С. 3-10.

5. Арчаков, В.Ю. Даркнет в контексте рисков национальной безопасности / В.Ю. Арчаков, А.Л. Баньковский, Е.В. Зенченко // Право.by. – 2021. – №6(74). – С. 5-10.

6. Бородич, А.И. Пограничная безопасность Республики Беларусь: монография / А.И. Бородич. – Минск: Издательские решения, 2019. – 340 с. – ил.

7. Верлуп, С.В. Национальная безопасность на государственной границе: идеи, мнения, предложения: моногр. / С.В. Верлуп. – Минск: ВА РБ, 2017. – 156 с.

8. Ермолович, В.Ф. Теоретические и международно-правовые проблемы противодействия транснациональной организованной преступности: моногр. / В.В. Меркушин, В.Ф. Ермолович, С.Н. Князев. – Минск: Междунар. ун-т «МИТСО», 2016. – 318 с.

9. Павловский, А.А. Обоснование перспективных направлений развития и применения пограничных войск Республики Беларусь в интересах пограничной безопасности

Союзного государства: дис… канд. воен. наук : 20.03.09 / А.А. Павловский. – М., 2000. – 236 с.

10. Трахименок, С.А. Безопасность государства. Методолого-правовые аспекты: моногр. / С.А. Трахименок. – Минск: Бел. изд. тов-о «Хата», 1997. – 192 с.

11. Гавриленко, В.Г. Правовые основы и механизмы обеспечения национальной безопасности и суверенитета Республики Беларусь / В.Г. Гавриленко; под науч. ред. П.Г. Никитенко. – Минск: Право и экономика, 2019. – 1104 с.

12. Информационно-аналитический портал Союзного государства [Электронный ресурс]. – Режим доступа: https://soyuz.by/multimedi/zasedanie-vysshego-gossoveta-soyuznogo-gosudarstva-translyaciya. - Дата доступа: 07.11.2021.

13. Верлуп, С.В. Перспективы научного обеспечения пограничной безопасности Республики Беларусь / С.В. Верлуп, В.П. Шкред // Вестник Военной академии Республики Беларусь. – 1’21. – С. 83-91.

14. Ксенофонтов, В.А. Военная сфера национальной безопасности: приоритеты развития / В.А. Ксенофонтов/ Современный мир и национальные интересы Республики Беларусь: Белорус. гос. ун-т; Е.А. Достанко (гл.ред.) [и др.]. – Минск: БГУ, 2021. – С. 160-164.

УДК 004.056:341(4)(075.8)

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЕВРОПЕЙСКОМ СОЮЗЕ: СУЩНОСТНО-СОДЕРЖАТЕЛЬНЫЕ АСПЕКТЫ

Н.В. Валюшко-Орса

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье рассмотрены сущностно-содержательные аспекты правового регулирования защиты персональных данных в Европейском союзе. Отмечается, что положительный опыт Европейского союза по правовому регулированию защиты персональных данных оказал определенное влияние на развитие законодательства в этой сфере в Республике Беларусь.

***Ключевые слова*:** персональные данные, защита персональных данных, согласие субъекта данных, Европейский союз.

LEGAL REGULATION OF PERSONAL DATA PROTECTION IN THE EUROPEAN UNION: ESSENTIAL AND CONTENT ASPECTS

N.V. Valyushko-Orsa

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article considers the essential and substantive aspects of the legal regulation of the protection of personal data in the European Union. It is noted that the positive experience of the European Union on the legal regulation of the protection of personal data had a certain impact on the development of legislation in this area in the Republic of Belarus.

Keywords: personal data, protection of personal data, consent of the data subject, European Union.

На современном этапе, ввиду активного развития информационно-коммуникационных технологий, весьма актуальным является вопрос, касающийся защиты персональных данных индивидуума. В частности, в связи наличием глобальной компьютерной сети Интернет, имеется возможность свободного доступа практически к любой информации. Кроме того, существование различных автоматизированных баз данных помогает более оперативно разрабатывать и принимать решения на разных уровнях, в том числе, в процессе осуществления государственного управления. Однако,

при даче лицом согласия на обработку своих персональных данных в глобальной компьютерной сети Интернет различными субъектами (например, органами государственной власти, предприятиями, учреждениями и иными организациями), возникает риск завладения названными данными сторонними лицами, что, в свою очередь, может повлечь за собой нарушение конституционного права на неприкосновенность частной жизни.

Следует отметить, что право на неприкосновенность частной жизни, в том числе, включает в себя право на защиту персональных данных.

В частности, согласно ст. 12 Всеобщей декларации прав человека от 10 декабря 1948 года «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств» [1, с. 2]. Подобного рода норма закреплена в ст. 8 Конвенции о защите прав человека и основных свобод от 4 ноября 1950 г., согласно которой «каждый человек имеет право на уважение его личной и семейной жизни, неприкосновенности его жилища и тайны корреспонденции» [2, с. 763].

Обратим внимание на то, что основным законодательством Европейского союза в сфере защиты персональных данных являются:

- Регламент Европейского парламента и Совета Европейского союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных (GDPR)) (далее – Общий регламент) [3];

- Регламент 2018/1725 Европейского парламента и Совета Европейского союза от 23 октября 2018 г. о защите физических лиц при обработке персональных данных институтами, органами, учреждениями и агентствами Союза и о свободном перемещении таких данных и отмене Регламента (ЕС) № 45/2001 и Решения № 1247/2002/ЕС (далее – Регламент 2018/1725) [4];

- Директива 2002/58/ЕС Европейского парламента и Совета Европейского союза от 12 июля 2002 г. об обработке персональных данных и защите конфиденциальности в секторе электронных коммуникаций (Директива о конфиденциальности и электронных коммуникациях) (далее – Директива 2002/58) [5];

- Директива 2016/680 Европейского парламента и Совета Европейского союза от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных компетентными органами в целях предотвращения, расследования, выявления или уголовного преследования или исполнения

уголовных наказаний, а также о свободном перемещении таких данных и отмене Рамочного решения Совета 2008/977/JHA (далее – Директива 2016/680) [6];

Одним из важных вопросов является понимание того, как трактуется дефиниция «персональные данные» в соответствии с законодательством Европейского союза, поскольку от того, насколько точно будет дано определение персональным данным, зависит и то, на что будет направлена защита по отношению к субъекту персональных данных.

Принципы и правила защиты физических лиц в отношении обработки их персональных данных должны, независимо от их гражданства или места жительства, уважать их основные права и свободы, в частности их право на защиту персональных данных. Общий регламент призван способствовать формированию пространства свободы, безопасности и правосудия и экономического союза, экономическому и социальному прогрессу, укреплению и сближению экономик в рамках внутреннего рынка, а также содействовать благосостоянию физических лиц [3, п. 2].

Согласно ст. 4 Общего регламента под персональными данными понимается любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъект данных») [3]. Такой подход к трактовке понятия «персональные данные» является оправданным, поскольку определение названной дефиниции, например, через установление закрытого перечня персональных данных, приведет к возникновению правовой неопределенности в связи с постоянным развитием информационных технологий и появлением новых способов идентификации лиц [7].

Положительный опыт Европейского союза, касающийся правового регулирования защиты персональных данных, оказал определенное влияние на развитие законодательства в этой сфере в Республике Беларусь. В частности, 7 мая 2021 г. был принят Закон Республики Беларусь «О защите персональных данных» [8] в соответствии с которым дано новое определение понятию «персональные данные». Так, согласно ст. 1 Закона Республики Беларусь от 7 мая 2021 г. «О защите персональных данных» под персональными данными понимается любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано [8]. Данное определение по сути является идентичным определению, которое дано в ст. 4 Общего регламента. Таким образом, понятие «персональные данные», согласно Закону Республики Беларусь от 7 мая 2021 г. «О защите персональных данных», стало толковаться шире, что, в свою очередь, свидетельствует о том, что объем информации, который можно отнести к персональным данным также стал значительно шире, по сравнению с предыдущим определением персональных данных.

Следует отметить, что Общий регламент вводит различного рода понятия, например, такие ка «контролер данных», «обработчик», «получатель», «третье лицо».

Кроме того, следует сделать акцент на такое понятие как «согласие» субъекта данных. Согласно ст. 4 Общего регламента под согласием субъекта данных понимается добровольное, конкретное, информированное и однозначное волеизъявление, в котором субъект данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих персональных данных [3].

Далее, обратим внимание на то, что Общий регламент имеет прямое действие по отношению к государствам-членам Европейского союза. Однако, согласно, п. 1 ст. 8 Общего регламента государства-члены Европейского союза могут установить более низкий возраст на дачу согласия по обработке персональных данных, но не ниже 13 лет, по сравнению с тем возрастом, который установлен в п. 1 ст. 8 Общего регламента (ребенок может дать согласие на обработку своих персональных данных с 16 лет, но если ребенок еще не достиг 16-го возраста, то такая обработка будет являться законной только когда согласие было дано лицом, обладающим родительскими правами в отношении ребенка, или было дано с его одобрения) [3].

Нижний возрастной порог (до 13 лет) на дачу согласия по обработке персональных данных несовершеннолетнего установлен и в п. 1 ст. 8 Регламента 2018/1725 [4].

На практике, предоставленная Общим регламентом возможность государствам-членам Европейского союза самостоятельно определять возраст ребенка при даче согласия им на обработку своих персональных данных, вызвала определенные проблемы [9].

По данным Европейской комиссии, только в девяти государствах Европейского союза (Венгрии, Германии, Ирландии, Люксембурге, Нидерландах, Польше, Румынии, Словакии и Хорватии) власти решили придерживаться установленного Общим регламентом возрастного порога: до достижения лицом 16 лет создание аккаунта и последующая обработка персональных данных ребенка допускается лишь с согласия родителей [9].

В других странах Европейского союза возраст на дачу согласия ребенком на обработку своих персональных данных, понижен до 13 лет, например, в Бельгии, Дании, Латвии, на Мальте, в Швеции, Финляндии, Эстонии; до 14 лет – в Австрии, Болгарии, Испании, Италии, на Кипре и в Литве и до 15 лет – в Чехии, Франции [9].

Существующая разница в возрасте согласия влечет неопределенность относительно прав детей на защиту персональных данных. «Это также создает проблемы для компаний с трансграничным бизнесом и тех, что разрабатывают технологические решения в сфере кибербезопасности» [9].

Следует отметить, что дети нуждаются в особой защите своих персональных данных, так как они в меньшей степени осознают риски, последствия, гарантии и права при обработке своих персональных данных. Такого рода особая защита должна применяться при использовании персональных данных детей в целях маркетинга, при создании личного профиля или профиля пользователя, а также при реализации услуг, предлагаемых непосредственно ребенку. Согласие лиц, которые несут родительскую ответственность, не требуется при профилактических и консультационных услугах, которые предлагаются непосредственно ребенку [3, п. 38].

В отчете Европейской комиссии было обращено внимание на то, что «для эффективного функционирования внутреннего рынка и чтобы избежать ненужной нагрузки на компании, важно, чтобы национальное законодательство не выходило за рамки, установленные GDPR, и не вводило дополнительных требований» [9]. По нашему мнению, такой подход является оправданным, ввиду стремления Европейского союза к гармонизации законодательства с его государствами-членами.

Кроме того, в п. 8 Директивы 2002/58 определено, что правовые, нормативные и технические положения, принятые государствами-членами в отношении защиты персональных данных, конфиденциальности и законных интересов юридических лиц в секторе электронных коммуникаций, должны быть гармонизированы, чтобы избежать препятствий для внутреннего рынка электронных коммуникаций. Гармонизация должна быть ограничена требованиями, необходимыми для гарантии того, что продвижение и развитие новых услуг и сетей электронных коммуникаций между государствами-членами не будет затруднено [5].

Далее, следует обратить внимание на Директиву 2016/680. Согласно п. 1 ст. 1 данная Директива устанавливает правила, касающиеся защиты физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, выявления или уголовного преследования или исполнения уголовных наказаний, включая защиту и от предотвращения угроз общественной безопасности [6].

В соответствии с Директивой 2016/680 государства-члены должны:

- защищать основные права и свободы физических лиц и, в частности, их право на защиту персональных данных;

- обеспечить, чтобы обмен персональными данными компетентными органами в рамках Европейского союза, если такой обмен требуется законодательством Европейского союза или государства-члена, не ограничивался и не запрещался по причинам, связанным с защитой физических лиц в отношении обработки персональных данных (п. 2 ст. 1) [6].

В целях обеспечения безопасности и предотвращения обработки, нарушающей Директиву 2016/680, контролер или обработчик должны оценить

риски, связанные с обработкой персональных данных, и должны принять меры для снижения этих рисков, такие как шифрование. Данные меры должны обеспечивать надлежащий уровень безопасности, включая конфиденциальность, и учитывать уровень техники, затраты на внедрение в зависимости от риска и характера защищаемых персональных данных. При оценке рисков безопасности данных следует учитывать риски, связанные с обработкой данных, такие как случайное или незаконное уничтожение, потеря, изменение или несанкционированное раскрытие или доступ к передаваемым, хранящимся или иным образом обрабатываемым персональным данным, которые могут, в частности, привести к физическому, материальному или нематериальному ущербу. Контролер и обработчик должны обеспечить, чтобы обработка персональных данных не осуществлялась неуполномоченными лицами [6, п. 60].

В общей сложности в процессе становления и развития законодательства о защите персональных данных в Европейском союзе «стало очевидным, что потребуется внедрение новых способов защиты данных таких, как профилирование и псевдонимизация, так как современная глобализация обусловливает активное развитие и совершенствование информационных технологий, стирание границ передачи данных, использование новых типов персональных данных (например, биометрических, генетических) и автоматизированных систем обработки» [10].

Таким образом, правовое регулирование защиты персональных данных в Европейском союзе достаточно развито, а Общий регламент является основополагающим законодательным актом, который, в свою очередь, направлен на унификацию защиты персональных данных в государствах-членах Европейского союза.

Библиографический список

1. Всеобщая декларация прав человека: принята резолюцией 217 А (III) Генер. Ассамблеи ООН, 10 дек. 1948 г. // Права человека: сб. междунар.-правовых док. / сост. В.В. Щербов. – Минск: Белфранс, 1999. – С. 1–5.

2. Конвенция о защите прав человека и основных свобод: совершено г. Рим, 4 нояб. 1950 г. // Права человека: сб. междунар.-правовых док. / сост. В.В. Щербов. – Минск: Белфранс, 1999. – С. 761–772.

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Electronic resource] // EUR-Lex. – Mode of access: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679. – Date of access: 31.05.2022.

4. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such

data, and repealing Regulation (EC) № 45/2001 and Decision № 1247/2002/EC [Electronic resource] // EUR-Lex. – Mode of access: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725. – Date of access: 31.05.2022.

5. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [Electronic resource] // EUR-Lex. – Mode of access: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058. Date of access: 31.05.2022.

6. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision [Electronic resource] // EUR-Lex. – Mode of access: 2008/977/JHA https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680. – Date of access: 31.05.2022.

7. Gabel, D., Hickman, T. The International Comparative Legal Guide to: Data Protection [Electronic resource] / D. Gabel, T. Hickman. – 6th Edition. – 2019. – Mode of access: https://by1lib.org/book/5631910/353f79?id=5631910&secret=353f79. – Date of access: 11.04.2022.

8. О защите персональных данных : Закон Респ. Беларусь, 7 мая 2021 г., № 99-З // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

9. Как ЕС реализует обязательства по внедрению GDPR [Электронный ресурс] // RSpectr.com. – Режим доступа: https://rspectr.com/articles/kak-es-realizuet-obyazatelstva-po-vnedreniyu-gdpr. – Дата доступа: 31.05.2022.

10. Шадрин, С.А. Правовое регулирование защиты персональных данных в Европейском Союзе: генезис и перспективы развития: дис. … канд. юрид. наук: 12.00.10 [Электронный ресурс] / С.А. Шадрин; ФГАОУ ВО «Казанский (Приволжский) федеральный университет» // disserCat – электронная библиотека диссертаций. – 2019. – Режим доступа: https://www.dissercat.com/content/pravovoe-regulirovanie-zashchity-personalnykh-dannykh-v-evropeiskom-soyuze-genezis-i-perspek**.** – Дата доступа: 01.06.2022.

УДК 342.57

ПРОБЛЕМАТИКА ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ ОТКРЫТОСТИ В ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВЕННЫХ ОРГАНОВ

А.В. Карамышев

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье рассматриваются некоторые существенные аспекты системного правового обеспечения общественного доступа к информации о деятельности государственных органов в Республике Беларусь. Анализируются концептуальные подходы, реализованные в законодательстве, рассматриваются вопросы их модернизации в свете международных стандартов.

***Ключевые слова*:** транспарентность, коммуникативная открытость, общедоступная информация, базовый закон, запрос, процедура.

THE PROBLEM OF LEGAL SUPPORT OF INFORMATION OPENNESS IN THE ACTIVITIES OF STATE BODIES

A.V. Karamyshev

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article discusses some significant aspects of the systemic legal support of public access to information about the activities of state bodies in the Republic of Belarus. The conceptual approaches implemented in the legislation are analyzed, the issues of their modernization in the light of international standards are considered.

Keywords: transparency, communicative openness, public information, basic law, request, procedure.

Проблематика информационной безопасности при всей своей значимости не может рассматриваться в качестве самодостаточной и должна решаться в контексте базовой парадигмы информационной прозрачности, открытости как определяющего фактора открытости публичной деятельности в правовом демократическом государстве. Тем более, что данная парадигма имеет фундаментальное конституционное обоснование (статьи 34 и 37 Конституции Республики Беларусь). Ее программное содержание нашло отражение и в Концепции информационной безопасности Республики Беларусь (далее - Концепция), утвержденной Постановлением Совета Безопасности

Республики Беларусь от 18.03.2019 N 1. Концепция в числе ключевых задач государственных органов формулирует защиту общедоступной информации от блокирования правомерного доступа, необоснованного засекречивания, сокрытия, несвоевременного распространения или предоставления. Важными являются государственные гарантии, обеспечивающие оперативность общедоступной информации, расширение сервисных возможностей, наконец, реализацию концепции «открытых данных».

Согласно Международной хартии открытых данных, принятой в 2015 г. на Глобальном саммите «Партнерство открытого правительства», открытые данные – цифровые данные, доступные с техническими и юридическими характеристиками, необходимыми для их свободного использования, повторного использования и распространения кем угодно, в любое время и в любом месте. Открытые данные имеют особую ценность для создания более прозрачных, подотчетных, эффективных, быстро реагирующих и действенных правительств.

Без преувеличения, информационная транспарентность и открытость публичных институтов сегодня имеют глобальную, наднациональную значимость. Это отражено в содержании целого ряда международных актов. Так, Конвенция Совета Европы о доступе к официальным документам (далее - Конвенция CETS № 205) в своей преамбуле содержит следующее базовое положение: *прозрачность государственных органов является одним из важнейших компонентов эффективного управления и показателем того, является ли общество подлинно демократическим и плюралистическим (в противовес всем формам коррупции), способным критиковать лиц, отвечающих за государственное управление, и открытым для осознанного участия граждан в решении вопросов, представляющих общественный интерес.*

В научных публикациях приводятся методологически важные дефиниции информационной открытости органов государственной власти. Например, данная модель в системно деятельностном ее наполнении определяется как организационно-правовой режим предоставления достаточного и необходимого объема общественно значимых сведений о деятельности органов власти, базирующийся на конституционном праве граждан свободного доступа к информации, где прослеживается координационное взаимодействие общества со структурами власти [1, с.21].

В приближении к практическому форматированию этого важного координационного механизма информационная открытость государственных органов артикулируется как целостный комплекс совместных мер системы государственного управления и общественного контроля, направленных на предоставление сведений о деятельности государственных органов, предусмотренных законодательством, обществу в целом или конкретным лицам

в целях обеспечения прозрачности и подотчетности государственных органов в рамках установленного порядка на началах равенства доступа к информации[2, с. 84].

Как концептуальную, так и организационно-практическую значимость имеют и такого рода формулы – открытость подразумевает наличие в системе правовых отношений широких каналов взаимопроникновения для всего спектра социальных, экономических и политических сил; прозрачность (транспарентность) характеризуется максимально возможной доступностью информации о деятельности управленческого аппарата и формированием жесткого механизма общественного воздействия на сферу государственного администрирования. Прозрачность носит функциональный характер, который ведет к регулированию общественных процессов, а открытость – социально-коммуникативный [3, с. 44–45].

Понятно, что в таком динамичном (коррелятивном) понимании информационная открытость деятельности публичных властей предполагает формирование и развитие структурированной правовой основы. В этом ключе актуальным является «спектральный анализ» белорусского законодательства. Декларируемые информационные модели требуют пристрастного внимания, прежде всего, с конституционных позиций (статьи 34 и 23 Основного Закона).

Следует отметить, что отечественное законодательство содержит целый набор «разноформатных», иногда амплитудных регуляторов, использующих категории «гласность», «открытость», «транспарентность». Например, Закон Республики Беларусь от 12.12.2013 N 94-З «О противодействии монополистической деятельности и развитии конкуренции» закрепляет в числе основных принципов обеспечение информационной открытости проводимой антимонопольным органом государственной политики в сфере противодействия монополистической деятельности и развития конкуренции, в том числе посредством размещения информации о своей деятельности в средствах массовой информации, на своем официальном сайте в глобальной компьютерной сети Интернет (принцип информационной открытости). Как представляется, данная позиция в большей степени формулируется и приобретает значение полномерной доступности (транспарентности) сведений в данной специфической сфере публичной деятельности.

Что касается критерия организационно-коммуникативной открытости, то здесь целеполагания в большей степени достигаются иными регуляциями. В сфере антимонопольного и конкурентного регулирования, как и в других сферах публичного администрирования важно использовать возможности, которые дает механизм общественных (публичных) обсуждений на базе Закона Республики Беларусь от 17.07.2018 N 130-З «О нормативных

правовых актах». В ряде сфер (экология, градостроительство) действуют и иные (специальные) механизмы общественного контроля и участия.

Концентрированное выражение открытость публичной деятельности отчетливо проявляется в плоскости законодательства процедурно-процессуального характера – как важная гарантия для участников. Так, согласно Закону Республики Беларусь от 28.10.2008 N 433-З «Об основах административных процедур» открытость административной процедуры - предоставление возможности заинтересованному лицу знакомиться с материалами, связанными с рассмотрением своего заявления, и принимать участие в рассмотрении такого заявления лично и (или) через своих представителей.

Насыщенная коммуникативная динамика прозрачности и открытости, как показывает мировая практика, характеризует широко демократическую систему общего управления административными территориями (местного самоуправления). В принципе, на это сориентирована содержащаяся в Законе Республики Беларусь от 04.01.2010 N 108-З «О местном управлении и самоуправлении в Республике Беларусь» формула: «гласность и учет общественного мнения, постоянное информирование граждан о принимаемых решениях по важнейшим вопросам местного значения». Однако важно, чтобы она не была декларативной, усеченной и обеспечивалась комплексом организационно-правовых конструкций и процедур. Такой вектор развития был заложен еще Законом Республики Беларусь от 02.02.1988 N 2010-XI «О народном обсуждении важных вопросов государственной жизни Республики Беларусь».

В этом плане заслуживает критической оценки следующее. Так, определенная постановлением Совета Министров Республики Беларусь от 23.12.2015 N 1080 Стратегия реформирования системы управления государственными финансами Республики Беларусь (далее – Стратегия финансов) в разделе «Формирование и ведение общедоступных информационных ресурсов» категорично ставит эффективность налоговой и бюджетной политики в зависимость от доверия населения страны, открытости, прозрачности деятельности государственных органов и организаций, объяснения обществу причин принятия тех или иных решений, задач и перспектив деятельности государственных органов. В Стратегии финансов сформулирован комплекс норм надлежащей практики в области обеспечения прозрачности бюджетного процесса. Все это призвано реально обеспечить транспарентность государственного управления на основе положений статьи 34 Конституции Республики Беларусь.

Однако, если критерии прозрачности бюджетной сферы и средства ее обеспечения в Стратегии финансов определены достаточно емко и системно, то вопросы коммуникационной открытости определены невнятно – только обозначен ориентир на участие граждан в «формировании» местных

бюджетов. Можно только предполагать, что такое участие не связывается с закрепленным в законодательстве в качестве некоего довеска к бюджету «добровольным самообложением» жителей сельских населенных пунктов. Этим характерен и Бюджетный кодекс Республики Беларусь от 16.07.2008 N 412-З, декларирующий принцип прозрачности и открытости бюджетной системы и очерчивающий его реализацию рамками информационной доступности. О каком-либо общественном участии в бюджетном процессе кодекс не говорит.

Данная проблема видится отчетливее, если обратиться к положениям Закона Республики Беларусь от 17.07.2018 N 130-З «О нормативных правовых актах», согласно которым проекты актов бюджетного законодательства не могут быть предметом общественного (публичного) обсуждения по установленной правовой процедуре. С одной стороны, проекты республиканского и местных бюджетов (проекты закона и решений Советов депутатов) обнародуются, в том числе размещаются на официальных сайтах государственных органов в виде «гражданского бюджета» (адаптированной версии для граждан), с другой – закон прямо исключает их общественное обсуждение.

Характерно, что Закон Республики Беларусь от 02.02.1988 N 2010-XI «О народном обсуждении важных вопросов государственной жизни Республики Беларусь» предусматривал обязательное вынесение на обсуждение с населением проектов местных бюджетов. Современная открытая бюджетная практика также использует этот демократический инструмент, реализуя институт обязательных публичных слушаний по проектам местных бюджетов и отчетам об их исполнении. Он предусмотрен в модельном законе «Об общих принципах организации местного самоуправления», принятом Постановлением Межпарламентской Ассамблеи государств - участников Содружества Независимых Государств N 43-11 от 27.11.2015. Более того, во многих странах достаточно эффективно применяется партиципаторное (инициативное) бюджетирование, предполагающее прямое участие местного населения в принятии и реализации в том или ином объеме бюджетных решений.

Рассматривая примеры ограничительных практик информационной транспарентности государственной (публичной) деятельности, нельзя не обратить внимание на служебное право Беларуси. В Законе Республики Беларусь от 14.06.2003 N 204-З «О государственной службе в Республике Беларусь» закреплен принцип гласности. Парадоксально, но данный принцип существенно ограничен нормой Закон Республики Беларусь от 15.07.2015 N 305-З «О борьбе с коррупцией», установившей общий запрет на распространение сведений, содержащихся в декларациях о доходах и имуществе государственных служащих. Положение о порядке проверки и хранения

деклараций о доходах и имуществе (постановление Совета Министров Республики Беларусь от 16.01.2016 N 19 «О некоторых вопросах декларирования доходов и имущества государственными служащими и иными категориями лиц» эти сведения отнесены к служебной тайне, то есть к государственным секретам. Согласно Закону Республики Беларусь от 19.07.2010 N 170-З «О государственных секретах» служебная тайну составляют сведения, в результате разглашения или утраты которых может быть причинен существенный вред национальной безопасности Республики Беларусь. В то же время, мировая практика свидетельствует, что именно в антикоррупционном или ином законе предусматривается обнародование таких сведений. Как указано в Конвенции CETS № 205, понятие «безопасность государства» не должно применяться ненадлежащим образом, в том числе для защиты информации, которая попросту является щекотливой для государственных должностных лиц или государственных органов.

Для эффективного, системного решения вопросов информационно-коммуникационной открытости публичных институтов важное значение имеет наличие базового закона. Зарубежные примеры показывают, насколько акцентированы уже сами наименования такого закона - Закон об открытости публичных документов (Финляндия), Закон о свободе информации (США), Закон о доступе к административным документам (Дания, Франция), Закон об установлении правил открытости административного управления (Нидерланды), Закон о раскрытии административного управления (Бельгия), Закон о гарантиях и свободе доступа к информации (Кыргызстан); Закон о свободе информации (Грузия); Закон о доступе к информации (Молдова).

В Республике Беларусь, видимо, из соображений «экономии правового регулирования», был выбран иной подход. Данный блок вопросов встроен в канву Закона от 10.11.2008 N 455-З «Об информации, информатизации и защите информации» (далее - Закон об информации). Закон об информации, непосредственно регулируя достаточно широкий спектр информационных отношений, включил и вопросы, касающиеся распространения и предоставления информации о деятельности государственных органов, придав ей статус общедоступной. Специфику ситуации характеризовало то, что только через пять лет своего действия (в 2014 г.) закон дополнился, с одной стороны, видами общедоступной информации (в рассматриваемом случае – применительно к деятельности государственных органов) и способами распространения (предоставления) и, с другой - перечнем изъятий из общедоступной информации.

Также значительное время потребовалось, например, для выработки структурного механизма информационной открытости в экологической сфере. Инициативу проявил Конституционный Суд Республики Беларусь

(далее - Конституционный суд). В своем решении от 26.08.2005 N П-141/2005 «О мерах по защите конституционных прав и законных интересов граждан в области охраны окружающей среды» Конституционный суд сослался на Конвенцию о доступе к информации, участии общественности в процессе принятия решений и доступе к правосудию по вопросам, касающимся охраны окружающей среды, принятой на Четвертой конференции министров «Окружающая среда для Европы» в г.Орхусе (Дания) 25 июня 1998 г. (далее – Орхусская конвенция). Она утверждена Указом Президента Республики Беларусь от 14 декабря 1999 г. N 726 и вступила в силу для Республики Беларусь 30 октября 2001 г.

Конституционный суд обратил внимание на необходимость имплементации положений Орхусской конвенции, определяющих порядок участия общественности в решении вопросов, касающихся планов, программ и политики, связанных с охраной окружающей среды, участия общественности в подготовке государственными органами нормативных положений, имеющих непосредственную исполнительную силу, и других общеприменимых юридически обязательных правил, которые могут оказать существенное воздействие на окружающую среду. Законом Республики Беларусь от 21.12.2007 N 298-З были внесены существенные дополнения и изменения в Закон Республики Беларусь от 26.11.1992 N 1982-XII «Об охране окружающей среды» по вопросам экологической информации и общественного участия. Анализ этих положений показывает достаточно высокий уровень проработки, детализации информационного взаимодействия, сориентированный на положения Орхусской конвенции.

Такой подход нельзя связывать исключительно со спецификой природоохранной сферы. Общий закон о свободе информации также должен быть в необходимой степени детализирован в материальном и процедурном аспектах как полновесный нормативный документ прямого действия. Что же касается Закона об информации, характерным для данного («комбинаторного») регулятора является наличие в нем большого числа (вариаций) отсылок к иным нормативным правовым актам, имея в виду и действующие, и вновь принимаемые. Этому субсидиарному сегменту нормотворчества придано важное, фактически системоформирующее значение. На уровне принципа это сформулировано следующим образом: установление ограничений распространения и (или) предоставления информации только законодательными актами. Здесь заложена модель, сочетающая «расширение» (набор ограничительных нормативных правовых актов) и «сжатие» (исключительно законодательные акты).

В этом плане Закон об информации содержит изрядное, пожалуй, преобладающее количество отсылок именно к ограничительным нормам. Так, установлено, что порядок распространения и (или) предоставления

информации определяется соглашением субъектов соответствующих информационных отношений, если иное не установлено законодательными актами; общедоступная информация может не предоставляться … в иных случаях, установленных законодательными актами; государственные органы, указанные в Законе, самостоятельно определяют порядок подготовки и проведения ими открытых заседаний, если иное не предусмотрено актами законодательства; открытые заседания государственных органов, не указанных в Законе, проводятся по решению их руководителей и в установленном ими порядке, если иное не предусмотрено законодательными актами.

Давая общую оценку этой модели, необходимо опираться на норму статьи 23 Конституции, согласно которой ограничение прав и свобод личности допускается только в случаях, предусмотренных законом. С позиции Конституции - в прежней редакции, применительно к норме статьи 101 о запретительных пределах делегирования Президенту Республики Беларусь прерогатив закона в вопросах ограничения прав и свобод, и, тем более, в действующей редакции, в принципе «снявшей» эту проблему корректировкой статьи 85 в части декретов Президента Республики Беларусь, исключением статьи 101 о делегировании Президенту прерогатив закона и статьи 137 о конкуренции законов и актов Главы государства, - отсылка к ограничивающим свободу информации законодательным актам (указам), не говоря уже об иных нормативных правовых актах, явно проблематична.

Критически можно оценить и отсылочную норму закона, согласно которой порядок подачи обращений за получением общедоступной информации, а также порядок их рассмотрения определяются законодательными актами. Что здесь требует внимания. В первоначальной редакции закона для терминологического обозначения такого обращения использовалось понятие «запрос». Оно используется в Конвенции CETS 205, Орхусской конвенции, зарубежных информационных законах. При этом весь комплекс вопросов, касающихся этой формы предоставления информации, сведен в один блок (крупный) и детально регулируется. Действительно, современная информационная парадигма, правовая логика и техника предполагают именно такой подход. Белорусский же акт смоделирован на «разрыв цепи»: закон только определил формы запроса – устную и письменную, а также обозначил формы предоставления информации по запросу, во всем остальном закон апеллировал к иным нормативным правовым актам. На несбалансированность, разноречивость такой модели (при сопоставлении норм законодательства об обращениях граждан и юридических лиц, об административных процедурах, трудового и др.) указывалось в комментариях исследователей информационной проблематики и обосновывалась необходимость принятия специального закона, который бы комплексно регулировал вопросы доступа

к информации о деятельности государственных органов [4]. На это указывалось и в Стратегии финансов.

В последующем, при корректировке закона термин «запрос» заменен на используемый в юридическом обороте растяжимый термин «обращение», что внешне сгладило проблему системной регламентации процедуры запроса в информационном законе. Составлен также перечень базовых оснований для отказа в предоставлении информации. Процедурно-отсылочная норма, с заменой термина, сохранилась. В принципе, отсылка к процедурам допустима. Но это может касаться только специфических детализированных процедур рассмотрения обращений (по сути - запросов), к примеру, той процедуры, что закреплена в Законе Республики Беларусь от 26.11.1992 N 1982-XII «Об охране окружающей среды» на конвенциональной Орхусской платформе.

В этом плане в законодательстве можно найти и иные (единичные) примеры специального регулирования порядка рассмотрения информационных обращений о предоставлении информации: из Единого государственного регистра юридических лиц и индивидуальных предпринимателей; из Государственного регистра лиц, подвергшихся воздействию радиации вследствие катастрофы на Чернобыльской АЭС, других радиационных аварий; из Государственного судового реестра Республики Беларусь и др. Они содержатся в перечнях административных процедур, сформированных во исполнение Закона Республики Беларусь от 28.10.2008 N 433-З «Об основах административных процедур».

В связи с этим возникает вопрос, могут ли нормы данного закона служить непосредственным процедурным алгоритмом и для других информационных обращений (запросов)? Исходя из концепции закона, обозначенной уже в его названии и реализуемой в нормах (сама концепция нуждается в отдельном критическом анализе с позиций общепризнанной административной процедуры), рассчитывать на этот закон нет оснований. В подтверждение можно сослаться на его нормы, определяющие сами критерии законодательства об административных процедурах: оно должно содержать наименования процедур, сведения об уполномоченных органах и др. То есть, все административные процедуры должны быть определены перечневым методом, систематизированы и структурированы, что как раз и характерно для приведенных примеров информационных административных процедур.

С другой стороны, также будет явно некорректным, ссылаясь на наименование закона и какие-то общие его позиции, наделять закон свойствами регулятивной универсальности. Здесь условно можно допустить лишь субсидиарное применение закона к какой-либо процедуре администрирования,

которая имеет регламент, но в какой-то части не урегулирована соответствующим специальным законодательством.

Использование термина «обращение» никоим образом не подводит к тому, чтобы задействовать регулятивный инструментарий Закона Республики Беларусь от 18.07.2011 N 300-З «Об обращениях граждан и юридических лиц» в качестве общей процедурной платформы рассмотрения запросов о предоставлении информации, которые не включены в перечни административных процедур. Это принципиально нарушило бы обозначенные для них сферы регулирования, создав тем самым существенную коллизию.

Представляется, что рассмотренные в статье проблемные вопросы еще раз подтверждают необходимость критической переоценки существующего правового обеспечения информационных отношений и, в конечном счете, возвращают к вопросу о разработке системного закона об информационно-коммуникативной открытости государственной (публичной) деятельности.

Библиографический список

1. Резер, Т.М. Информационная открытость органов государственного и муниципального управления// Т.М.Резер. – Екатеринбург: Изд-во Урал.ун-та, 2018. – 160 с.
2. Малахова, О.В. Информационная открытость деятельности органов государственной власти: региональные практики / О.В. Малахова, В.А. Суханова // Среднерусский вестник общественных наук. – 2015. – № 2 (38). – С. 83–91.
3. Чуклинов, А. Е. «Прозрачная» государственная политика: некоторые проблемы теории и практики / А.Е. Чуклинов // Вестн. РУДН. – Сер. : Политология. – 2006. – № 8. – С. 44–50.
4. Саванович, Н.А. Право на информацию о деятельности государственных органов (по состоянию на 13.08.2013) [Электронный ресурс] / Н.А. Саванович // СПС Консультант Плюс. – Дата доступа: 29.05.2022.

УДК 349

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОСРЕДСТВОМ ОХРАНИТЕЛЬНЫХ НОРМ

Д. Г. Полещук

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

Становление информационного общества неразрывно связано с рисками совершения противоправной деятельности в цифровой среде, для предупреждения которой задействованы нормы административно-деликтного и уголовного права. В публикации раскрывается содержание актуальных направлений правового обеспечения информационной безопасности с использованием охранительных норм, рассматриваются текущее состояние, проблемы и перспективы совершенствования законодательства с учетом последних его изменений.

Ключевые слова: информационная безопасность; кибербезопасность; охранительные нормы; искусственный интеллект, персональные данные, фейки.

TOPICAL DIRECTIONS OF LEGAL SUPPORT OF INFORMATION SECURITY THROUGH PROTECTIVE NORMS

D.G. Poleshchuk

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The formation of the information society is inextricably linked with the risks of illegal activities in the digital environment, for the prevention of which the norms of administrative-tort and criminal law are involved. The publication reveals the content of current trends in the legal support of information security through protective norms, discusses the current state, problems, and prospects for improving legislation, taking into account its latest developments.

Keywords: information security; cybersecurity; protective norms; artificial intelligence, personal data, fakes.

В современном обществе, характеризующемся масштабным процессом цифровизации, об информационной безопасности говорится немало. Новые цифровые технологии наряду с формированием условий для экономического роста и упрощением коммуникации создают значительные риски совершения противоправных действий в отношении личности, организаций и даже целых государств. Это отражается и в национальной Концепции

информационной безопасности Республики Беларусь, определяющей *информационную безопасность* как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1].

В то же время информационная сфера достаточно широка, что позволяет говорить о различных общественных отношениях, подлежащих охране нормами Кодекса Республики Беларусь об административных правонарушениях (далее – КоАП) и Уголовного кодекса Республики Беларусь (далее – УК), не ограничиваясь лишь защитой цифровой информации и поддерживающей ее инфраструктуры. Как отмечает О.С. Макаров, проблема нормативного обеспечения информационной безопасности во многих государствах – участниках СНГ, включая и Беларусь, заключается в том, что в этой сфере не проводилась систематизация законодательства и нормы хаотично «размазаны» по разным сферам и отдельным нормативным правовым актам [2, с. 124].

В этой связи полагаем возможным выделить следующие аспекты правового обеспечения информационной безопасности с использованием охранительных норм:

кибербезопасность или компьютерная безопасность (ст. 23.4 КоАП, гл. 31 УК) и противодействие связанным с ними административным правонарушениям и преступлениям (ст. 11.1-11.2 КоАП, ст. 208, 209, 212, 216 УК);

защита информации, распространение и (или) предоставление которой ограничено законодательными актами (ст. 23.5-23.8 КоАП, ст. 177, 178, 203, 203^1, 203^2, 226^1, 254-255, 373-375, 375^1, 407-408 УК);

защита от информации негативного характера, в том числе от «фейков», деструктивного информационного воздействия (ст. 19.6-19.8, 19.10-19.12, ч. 4 и 5 ст. 23.5, ч. 1 ст. 24.26, КоАП, ст. 130, 130^1, 130^2, 198^1, 340, 341^1, 342^1, 343, 343^1, 361, 369^1 УК).

Как видим, «локомотивом» в формировании публичной ответственности за посягательства против информационной безопасности выступают уголовно-правовые нормы. До принятия в 2021 г. соответствующих изменений в раздел XII и гл. 31 УК [3], которые действовали еще с момента его принятия и ранее именовались «Преступления против информационной безопасности», для целей уголовного закона информационная безопасность фактически сужалась исключительно до компьютерной безопасности. Это стало предпосылкой изменения наименований данных структурных элементов УК («Преступления против компьютерной безопасности»).

Наряду с уточнением объекта данной группы преступлений под влиянием требований времени и на основе наработанной правоприменительной практики впервые произошел комплексный их пересмотр, включающий изменение порядка уголовного преследования (введено частное обвинение в

отношении близких лица), используемой терминологии, конструкций и признаков составов преступлений, а также их санкций. Так, введены специальные положения об уголовной ответственности за распространение вредоносных компьютерных программ (а не только носителей с ними) и их сбыт, имеющие место в сети Интернет.

Следует отметить, что компьютерная преступность в настоящее время все больше носит ярко выраженный транснациональный и сетевой характер, по сути вызывая объективную необходимость построения эффективной системы обеспечения международной кибербезопасности. Как минимум, на уровне охранительных норм для этого требуется взаимное согласование и совершенствование положений материального права государств, устанавливающего преступность и наказуемость деяний, посягающих на цифровую информацию, информационные (компьютерные) системы, сети и машинные носители.

Тем не менее, по результатам проведенных за последнее время корректировок отечественного охранительного законодательства, направленного в том числе на усиление кибербезопасности (компьютерной безопасности), в масштабах белорусской юрисдикции в определенной степени сохраняется и даже возник ряд проблемных вопросов, требующих своего осмысления на перспективу.

В частности, в числе таковых можно назвать:

гармонизацию норм охранительного законодательства Республики Беларусь и других государств в сфере кибербезопасности, особенно в рамках Евразийского экономического союза, СНГ и с учетом прошедших апробацию подходов Европейской конвенции о киберпреступности [4], соответствующих национальным интересам в информационной сфере (например, в Беларуси однозначно не решен вопрос об ответственности за незаконный оборот паролей, кодов доступа и иных аналогичных данных, существуют различия в признаках несанкционированного доступа к компьютерной информации);

определение оптимальной конструкции уголовного наказуемого *несанкционированного доступа к компьютерной информации* (принимая во внимание признаки иных составов преступлений гл. 31 УК и правонарушения в ст. 23.4 КоАП, на практике могут быть затруднения в оценке того, как последствия в виде существенного вреда могут находиться в причинно-следственной связи с фактом несанкционированного доступа к компьютерной информации (деяние фактически окончено при ознакомлении с информацией);

оценку необходимости применения мер ответственности за уничтожение, блокирование или модификацию компьютерной информации при отсутствии существенного вреда или наличии реальной угрозы его

наступления (это связано с трансформацией ранее действующей ст. 351 УК в материальный состав преступления (теперь ст. 350 УК), а также установлением в КоАП административной ответственности только за несанкционированный доступ к компьютерной информации);

единообразное использование квалифицирующих признаков в конструкциях всех составов преступлений против компьютерной безопасности (например, признак повторности не включен в ст. 354 УК);

определение эффективной санкции за совершение компьютерных правонарушений и преступлений (используемая санкция должна иметь реальный предупредительный эффект, поскольку во многих случаях виновные лица сознательно готовы претерпеть наказание в обмен на достижение цели противоправной деятельности);

предупреждение и профилактику мошенничества, совершаемого с использованием мобильных телефонов и мессенджеров («вишинга»), формирование цифровой грамотности всех слоев населения (учитывая совершение многих преступлений с использованием информационных технологий на территории различных государств, значительно проще и экономически выгоднее выработать комплекс мер по их профилактике (возможно и на межгосударственном уровне), чем затем их расследовать).

Обособленное место в контексте обеспечения кибербезопасности и информационной безопасности в целом занимает *проблема появления искусственного интеллекта и роботов в охранительных правоотношениях*.

Вероятно, иные аспекты информационной безопасности уже находятся под их воздействием (например, распространение фейковых новостей, анализ поведения человека посредством его личной информации, «больших данных» и др.). Значительное число правонарушений и преступлений фактически может быть совершено с использованием новых технологий, однако возникает вопрос о субъекте ответственности в таких случаях. В данном аспекте позволим себе согласиться с А.Л. Савенком, что пока не будут разработаны соответствующие правовые нормы, человек не может возлагать на технику (робота) ответственность за вред, причиненный в процессе ее функционирования, при этом вряд ли допустимо передавать искусственному интеллекту право на создание другого искусственного интеллекта [5 с. 9–10]. В силу непредсказуемости последствий, в том числе связанных с совершением незаконных действий с вредоносными компьютерными программами, персональными данными, различных компьютерных атак на критически важные объекты информатизации, автономия искусственного интеллекта может быть чрезвычайна опасна. Это обусловливает характер и степень публичной ответственности человека (пользователя, разработчика) за противоправную деятельность, вызванную использованием искусственного интеллекта или робота.

Информация подлежит защите не только в зависимости от ее формы, но и от содержания, в связи с чем КоАП и УК обеспечивают соблюдение правового режима информации, распространение и (или) предоставление которой ограничено законодательными актами (информация о частной жизни и персональные данные, охраняемые законом тайны, государственные секреты и др.). Актуальным направлением правового обеспечения информационной безопасности личности является формирование охранительных норм о защите персональных данных, без оборота которых уже невозможно представить отношения в цифровой среде. Данное направление получило широкую огласку в 2021 г. в результате принятия первого в республике Закона от 7 мая 2021 г. № 99-З «О защите персональных данных» (вступил в силу с 15 ноября 2021 г.), введения специальных статей об ответственности за незаконные действия с персональными данными – ст. 23.7 КоАП (с 1 марта 2021 г.), а при наличии существенного вреда правам, свободам и законным интересам гражданина или тяжких последствий – ст. 203^1 и 203^2 УК (с 19 июня 2021 г.). Правильное применение указанных охранительных норм требует знания особенностей нового законодательства (например, оно распространяет свое действие в основном на автоматизированную обработку персональных данных), а также разграничения с другими категориями информации ограниченного распространения, которые могут включать в себя персональные данные. Кроме того, по мере становления правоприменительной практики в рамках указанного аспекта обеспечения информационной безопасности усматриваются предпосылки для разрешения следующих вопросов:

разграничение ответственности за посягательства в отношении специальных персональных данных и персональных данных, которые к ним не относятся, что косвенно находит отражение в Классификации информационных ресурсов (систем), содержащих персональные данные, в целях определения предъявляемых к ним требований технической и криптографической защиты персональных данных, утвержденной приказом Национального центра защиты персональных данных от 15 ноября 2021 № 12 [6] (видится, что посягательства в отношении персональных данных, касающихся религиозных убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности являются более общественно опасными, чем деяния в отношении фамилии, имени, отчества и даты рождения гражданина);

установление справедливой сопоставимой санкции за посягательства в отношении персональных данных и иных категорий информации ограниченного распространения (например, разглашение врачебной тайны, повлекшее тяжкие последствия, по своему характеру, видимо, должно

наказываться строже, чем распространение персональных данных любым лицом, повлекшее существенный вред).

Защита информационного пространства от информации негативного характера также является одним из стратегических направлений обеспечения информационной безопасности и сохранения информационного суверенитета. В условиях глобального использования сети Интернет особую актуальность на государственном уровне приобретает противодействие различного рода заведомо ложной информации или «фейкам» (от англ. fake – подделка, фальшивка) – не соответствующей действительности, вводящей в заблуждение информации, которая может причинить вред государственным или общественным интересам. Фактически, с учетом положений ст. 38 Закона от 17 июля 2008 г. № 427-З «О средствах массовой информации» такая информация, равно как и гиперссылки на нее, относятся к категории запрещенной.

В силу меняющейся геополитической обстановки защита от фейков как элемент информационной безопасности, в отличие от противодействия преступлениям против кибербезопасности, слабо поддается регулированию на межгосударственном уровне и даже наоборот становится ключевым средством ведения информационной войны.

Зачастую в обществе можно услышать тезис о том, что распространение фейков оправдывается конституционным правом на свободу выражения мнения (слова). Однако это не абсолютное право, поскольку законом допускается его ограничение в целях защиты государственных и общественных интересов, прав и свобод других лиц, что влечет уголовно-правовые и иные санкции и основано как на международных стандартах (п. 3 ст. 19 Международного пакта о гражданских и политических правах), так и на положениях Конституции Республики Беларусь (ст. 23).

Помимо возможности применения мер административного воздействия, предусмотренных законодательством о средствах массовой информации (например, ограничение доступа к интернет-ресурсам), национальное административно-деликтное и уголовное законодательство устанавливает определенный пласт норм, направленных на защиту от наиболее общественно опасных (вредных) фейков (ст. 19.6, ч. 4 и 5 ст. 23.5 КоАП, ст. 130^1, 130^2, 340, 369^1 УК и др.). Тем не менее, учитывая скорость распространения информации в цифровой среде, уже сейчас существуют предпосылки для оценки достаточности имеющихся на национальном уровне мер уголовной ответственности за распространение фейков, влекущих общественно опасные последствия, или создающих реальную угрозу их наступления (например, за доведение до неопределенного круга лица заведомо ложной информации, способствующей установлению социальной напряженности, информации, влекущей причинение вреда здоровью, крупного ущерба гражданам

и организациям, а также иной фейковой информации, фактически побуждающей к причинению лицом самому себе телесных повреждений).

На основании изложенного следует резюмировать, что правовое обеспечение информационной безопасности посредством охранительных норм за последнее время претерпело значительные изменения, отражает процессы всеобщей цифровизации, имеет предпосылки для совершенствования по направлениям усиления кибербезопасности и безопасности использования искусственного интеллекта, защиты информации ограниченного распространения, защиты от «фейков» и в перспективе призвано учитывать актуальные угрозы причинения вреда интересам личности, общества и государства в информационной сфере на национальном и международном уровнях.

Библиографический список

1. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Макаров, О. С. Системный взгляд на нормативное обеспечение информационной безопасности в Республике Беларусь / О. С. Макаров // Право и государство. – 2020. – № 8. – С. 124–129.

3. Об изменении кодексов по вопросам уголовной ответственности [Электронный ресурс] : Закон Респ. Беларусь, 26 мая 2021 г., № 112-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

4. Конвенция о преступности в сфере компьютерной информации [Электронный ресурс] : [заключена в г. Будапеште 23.11.2001 г.] // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2022.

5. Савенок, А. Л. Правовое регулирование применения технологий искусственного интеллекта / А. Л. Савенок // Право в современном белорусском обществе : сб. науч. тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь, редкол.: Н. А. Карпович (гл. ред.) [и др.]. – Минск : Колорград, 2021. – Вып. 16. – С. 4–10.

6. О классификации информационных ресурсов (систем) [Электронный ресурс] : приказ Нац. центра защиты перс. данных Респ. Беларусь, 15 нояб. 2021 г., № 12 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

УДК 342.9

ОСНОВНЫЕ НАПРАВЛЕНИЯ ЦИФРОВИЗАЦИИ АДМИНИСТРАТИВНОГО ПРОЦЕССА

В.Ю. Чешко

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье анализируется уровень цифровизации порядка привлечения к административной ответственности. Рассматриваются особенности использования электронных средств в административном процессе. Обосновываются основные направления развития цифровизации в данной сфере.

***Ключевые слова*:** цифровизация, административный процесс, электронное дело.

MAIN DIRECTIONS FOR THE DIGITALIZATION OF THE ADMINISTRATIVE PROCESS

V.Yu. Cheshko

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article analyzes the level of digitalization of the procedure for bringing to administrative responsibility. The features of the use of electronic means in the administrative process are considered. The main directions for the development of digitalization in this area are substantiated.

Keywords: digitalization, administrative process, electronic business.

Актуальность цифровизации порядка привлечения к ответственности не вызывает сомнения. Учеными в области уголовного процесса в настоящее время уже выработаны определённые рекомендации по цифровизации данного процесса. Исследования в сфере административного процесса присутствуют в несколько усеченном спектре, в связи с чем нами будут использоваться мнения и наработки специалистов по цифровизации уголовного процесса.

По мнению П. П. Ищенко цифровизация уголовного процесса позволит:

произвести экономию ресурсов, как материально-технических, так и трудовых, за счет облегчения труда субъектов и участников судопроизводства;

ускорить и повысить прозрачность досудебного производства;

упростить и удешевить процесс хранения архивных уголовных дел, а также восстановление утраченных уголовных дел;

обучить следователей приемам расследования и составления процессуальных документов на примерах архивных уголовных дел и др. [1, с. 68]

Об актуальности цифровых технологий неоднократно заявляли представители Верховного Суда Республики Беларусь, Следственного комитета Республики Беларусь и других государственных органов.

Первый заместитель председателя Верховного Суда Республики Беларусь В. Л. Калинкович в своем интервью заявил, что «так складывается, что современные информационные технологии проникли во все сферы нашей жизни, и мы последовательно развиваем возможности электронного судопроизводства. В текущем году мы запустили в промышленную эксплуатацию самый большой и серьезный модуль единой компьютерной системы, который непосредственно связан с судопроизводством. Это позволило оптимизировать учетную политику с точки зрения судебного администрирования, прозрачно получать информацию о движении практически всех конкретных судебных дел. Для наших граждан это возможность удаленного доступа к информации о движении собственного дела» [2].

Также им отмечены направления интеграции цифровых технологий в судебную систему. По его словам, в экономическом судопроизводстве совершенствуется удаленное обращение, появилась возможность при производстве по конкретному делу получать необходимые сведения от информационных ресурсов других государственных органов, что существенно упрощает и удешевляет судопроизводство. Дополнительно были внедрены современные средства извещения о времени и месте судебного разбирательства для сторон и других участников процесса, которые позволяют многократно ускорять коммуникацию, получать нужную гражданам информацию о движении собственных дел и в целом повышать уровень открытости и доступности белорусского правосудия, осуществлен переход на аудио- и видеофиксацию судебных процессов и бумажный протокол судебного заседания заменяется на электронные версии, что также упрощает жизнь участникам процесса, а также работу суда по исследованию, анализу и оценке собираемых по каждому делу доказательств.

Представители Следственного комитета Республики Беларусь отмечают, что «В направлении информатизации уголовного процесса СК движется несколько лет. Оптимизировать и упростить работу здесь пытаются именно за счет внедрения различного рода информационных технологий. Конечной целью должно стать создание электронного уголовного дела. При этом белорусские следователи учитывают наработки и ошибки зарубежных

партнеров. В частности, элементы электронного уголовного дела уже внедрены в уголовном процессе Грузии, Казахстана, Армении» [3].

Анализ возможностей цифровизации административного процесса проведен по трем направлениям:

использование электронных доказательств;

цифровизация порядка ведения процесса;

электронное дело об административном правонарушении.

Использование электронных доказательств. Данное направление является одним из основных по цифровизации административного процесса, поскольку, прежде всего, правовая наука сталкивается с новым явлением и необходимостью его оценки для обеспечения справедливости при осуществлении правосудия и привлечении виновных лиц к ответственности. А. И. Зазулин отмечает, что «внедрение цифровых технологий – не просто способ модернизации уголовного судопроизводства, а жизненно важное условие его дальнейшего существования в мире бесконечных массивов данных и информационных потоков» [4, с. 81].

Дискуссия в сфере применения цифровых доказательств в отечественном процессе уже приобрела определенные очертания, в связи с чем можем привести основные проблемные вопросы, на которые обращают внимание эксперты:

отсутствие понятия электронного доказательства в процессуальных кодексах, несмотря на его использование на практике и в научной литературе. Данный пробел вызывает отождествление электронных доказательств с письменными доказательствами (общедоступная информация, размещенная в сети Интернет, переписка по электронной почте и в мессенджерах, выписки с расчетных счетов, информация из баз данных) или к звуко- и видеозаписями;

отсутствие единого подхода оценки доказательств. Исходя из общего подхода к оценке доказательств, судам и правоохранительным органам доказательства следует оценивать с точки зрения относимости, допустимости и достоверности через взаимную связь со всеми представленными доказательствами по соответствующему делу в их совокупности. В отношении цивилистического процесса справедливо отмечено, что «Исходя из диспозитивных и состязательных начал цивилистического процесса стороны сами в каждом конкретном случае принимают решение, в каком виде они будут представлять электронные доказательства в подтверждение своих требований или возражений, а также несут риск того, что на момент рассмотрения дела в суде информация будет изменена и суд не признает установленными те факты, на которые они ссылаются». При оценке доказательств, полученных уполномоченными должностными лицами, следует обращать внимание на наделение соответствующим полномочием этого должностного лица на

осуществление процессуальных действий. Хорошей основой для развития данного направления является электронная цифровая подпись (далее – ЭЦП);

отсутствие подходов по сбору и фиксации электронных доказательств. Справедливо по этому поводу замечают С. В. Зуев и А. С. Титова «оперирование электронной (цифровой) информацией не вписывается в традиционную систему следственных действий» [5, с, 52]. Безусловно, что проблем в данной сфере не избежать, но сам технологический прогресс позволит обеспечить надлежащими средствами по сбору и фиксации доказательства, а также облегчит проведение процессуальных действий;

идентификация лица, которое направило или получило электронное доказательство. При возникновении спора о принадлежности доказательства, суды исходят из того, что сохраненное в памяти мобильного телефона СМС-сообщение, полученное от конкретного адресата, может быть идентифицировано через номер телефона отправителя, который автоматически определяется мобильным телефоном и сохраняется в памяти устройства вместе с текстом СМС-сообщения. Аналогичным образом в случае, если электронная переписка проводилась с использованием мессенджеров (Viber, WhatsApp и т.п.), и аккаунт адресата привязан к определенному номеру телефона, его можно связать с лицом, на чье имя зарегистрирована сим-карта на основании данных оператора мобильной связи, если по делу отсутствуют основания полагать, что соответствующей сим-картой воспользовалось иное лицо. Например, в случаях с перепиской по электронной почте, идентификация отправителя или получателя сообщения может быть осуществлена если адрес электронной почты систематически используется отправителем или в деле имеются сообщения, авторство которых не оспаривается, а также с использованием содержания самого сообщения. Однако не во всех случаях идентификация отправителя или получателя сообщения может быть осуществлена даже в случаях неоднократного использования электронного ящика во взаимоотношениях сторон, поскольку необходимо учитывать наличие полномочий у лица на совершение определенных действий;

обеспечение баланса соблюдения права субъекта на пользование личными данными и методов получения доказательств. Данная проблема не может быть разрешима без надлежащей системы надзора за соблюдением законности при осуществлении деятельности правоохранительных органов, а также необходимо обеспечить прозрачность системы привлечения к ответственности [6].

Указанные проблемы имеют очерченные границы своего разрешения, о чем также упоминают представители Верховного Суда Республики Беларусь [6]. В частности, имеется подход к определению электронных доказательств в уголовном процессе, под которыми понимаются все средства, при

помощи которых в ходе судебного разбирательства устанавливаются факты, касающиеся виновности или невиновности лица, существующие в электронной или цифровой форме. К ним следует отнести электронные записи, электронную почту, файлы обработки информации, файлы с изображениями, записи, хранящиеся сетевыми или интернет-провайдерами. Отмечается, что в современном мире практически вся деятельность в цифровой среде оставляет следы, что с одной стороны упрощает порядок доказывания, но с другой вызывает необходимость подтверждения происхождения такого доказательства и верификации его изменений.

В целом, можно утверждать, что судами и правоохранительными органами выработан целостный подход к электронным доказательствам. Основные проблемы в данной сфере находятся в плоскости сбора, фиксации, формы обращения и оценки доказательств. При построении системы оценки доказательств следует исходить из того, каким субъектом было получено данное доказательство, способ получения должен быть надлежащим, а также источник получения доказательства должен соответствовать нормативным процессуальным критериям.

В настоящее время в Процессуально-исполнительном кодексе Республики Беларусь об административных правонарушениях (далее – ПИКоАП) подход к определению доказательств позволяют применять их в электронной (цифровой форме). Так, в соответствии со ст. 6.3 ПИКоАП доказательствами являются любые фактические данные, полученные в порядке, определенном ПИКоАП и иными законодательными актами, на основе которых суд, орган, ведущий административный процесс, устанавливают наличие или отсутствие административного правонарушения, предусмотренного КоАП, оснований и условий административной ответственности юридического лица, виновность или невиновность физического лица, привлекаемых к административной ответственности, и иные обстоятельства, имеющие значение для принятия решения по делу об административном правонарушении [7].

К источникам доказательств ПИКоАП относит объяснения лица, в отношении которого ведется административный процесс, потерпевшего, свидетеля, в том числе полученные путем использования систем видеоконференцсвязи, заключение эксперта, вещественное доказательство, протокол об административном правонарушении, протокол процессуального действия, иной документ и другой носитель информации, полученные в порядке, определенном ПИКоАП и иными законодательными актами.

Подход, закрепленный в ПИКоАП, позволяет даже использовать электронные (цифровые) доказательства, полученные по порядке, определенном не только ПИКоАП, но и иными законодательными актами. Основными

требованиями к электронным (цифровым) являются соответствие критериям относимости, допустимости и достоверности.

Цифровизация административного процесса. Переходя к исследованию цифровизации административного процесса следует отметить, что определенная работа в данной сфере уже проведена. Ряд норм уголовно-процессуального и процессуально-исполнительного законодательства уже был модернизирован. В связи с этим нами будут проанализированы мнения ученых о направлениях цифровизации данных процессов, внесенные изменения, регулирующие применение цифровых технологий, и на основе данного анализа будут выработаны предложения по совершенствованию цифровизации административного процесса.

С. В. Зуев отмечает, что наиболее перспективными направлениями по развитию информационных технологий в уголовном процессе в Российской Федерации являются следующие

1) переход на фиксацию хода процессуальных, в том числе следственных, действий с помощью технических средств и сохранение результатов в электронном виде;

2) внедрение в уголовно-процессуальную материю удобной и надежной технологии удостоверения процессуального документа любым участником уголовного процесса вместо его обычной подписи;

3) разработка пилотного проекта «Электронное уголовное дело» и апробация его в отдельных субъектах Российской Федерации;

4) широкое применение дистанционных форм проведения процессуальных действий на любой стадии уголовного судопроизводства, включая участие в судебных заседаниях всех заинтересованных лиц;

5) предоставление потерпевшему в режиме онлайн через Интернет возможности отслеживать движение уголовного дела от подачи заявления в электронной форме до вынесения приговора;

6) использование электронного помощника судьи для оценки фактических данных, имеющихся в уголовном деле, а также при назначении научно обоснованного и соразмерного совершенному противоправному деянию наказания [8, с. 120].

Таким образом, можно определить следующие направления цифрового развития административного процесса:

цифровизация процессуальных действий. В данном направлении следует выделить два элемента: фиксация в электронном виде процессуальных действий (например, осмотр места происшествия с использование технических средств фиксации следов правонарушения), в том числе судебного заседания; дистанционная форма проведения судебных заседаний, процессуальных действий, а также подачи заявлений и ходатайств (опрос, подача заявления);

использование электронной цифровой подписи. Данное нововведение позволит ввести систему контроля за изменениями различных процессуальных документов, сроком их реализации, что особенно важно при надзоре за законностью применения мер обеспечения административного процесса;

внедрение электронного помощника судьи (должностного лица органа, ведущего административный процесс). Реализация этого направления может существенно снизить время на составление процессуальных документов (использование автоматического заполнения формы процессуального документа), перевода слов должностного лица или судьи в текстовую информацию. Также в данном аспекте может быть реализован искусственный интеллект, который может самостоятельно обучиться и проводить первоначальный анализ материалов дела;

электронное дело об административном правонарушении. Данное направление будет рассмотрено ниже.

Анализ норм ПИКоАП показывает, что по сравнению с УПК использование цифровых технологий не получило такого же развития в данном кодексе.

Так, при ускоренном порядке ведения административного процесса копия постановления может быть отправлена лицу, в отношении которого оно вынесено, по его ходатайству посредством электронной или другой связи, в том числе с использованием глобальной компьютерной сети Интернет [7, ст. 10.3, 10.5].

Использование электронной или другой связи, в том числе с использованием глобальной компьютерной сети Интернет предусмотрено также как один из возможных способов вызова лиц, участвующих в административном процессе [7, ст. 11.6].

По аналогии с уголовным процессом использование цифровых технологий возможно при фиксировании хода судебного заседания. На основании ст. 12.9 ПИКоАП ход судебного заседания фиксируется с использованием средств звуко- или видеозаписи и составлением краткого протокола судебного заседания с соблюдением требований ПИКоАП. При отсутствии технической возможности вести звуко- или видеозапись ход судебного заседания фиксируется составлением протокола судебного заседания. Фиксирование хода судебного заседания необязательно в случае неявки в судебное заседание всех лиц, участвующих в рассмотрении дела об административном правонарушении. Лицо, в отношении которого ведется административный процесс, другие участники административного процесса вправе в течение десяти суток со дня вынесения постановления по делу об административном правонарушении ходатайствовать об ознакомлении с кратким протоколом, протоколом судебного заседания, со звуко- или видеозаписью хода закрытого судебного заседания, о получении копии звуко- или видеозаписи хода

открытого судебного заседания на предоставленном ими электронном носителе информации [7].

Кроме того, после объявление постановления копия по делу об административном правонарушении в случае отсутствия лица, в отношении которого вынесено постановление, при рассмотрении дела об административном правонарушении либо по его ходатайству направлена посредством электронной или другой связи, в том числе с использованием глобальной компьютерной сети Интернет, а также органу, направившему дело об административном правонарушении на рассмотрение.

На основании изложенного можно сделать вывод о том, что в административном процессе использование цифровых не получило необходимого закрепления. Особенно это видно при анализе норм, закрепляющих порядок проведения процессуальных действий. Использование звуко- и видеозаписи предусмотрено только при проведении осмотра транспортного средства [7, ч. 6 ст. 11.10]. Стоит отметить, что в целом применение цифровых технологий в административном процессе возможно с учетом положений, ст. 6.3 ПИКоАП (Доказательства), однако закрепление порядка использования цифровых технологий в иных нормах ПИКоАП будет способствовать более широкому их использованию и повышению эффективности.

Дополнительно отметим, что подача заявлений и ходатайств схожа с УПК. В соответствии со 9.2 ПИКоАП Заявление физического лица об административном правонарушении может быть устным или письменным. Устное заявление заносится в протокол, который подписывается заявителем и лицом, принявшим заявление. Протокол устного заявления должен содержать сведения о заявителе. Если заявитель не может представить документ, удостоверяющий его личность, должны быть приняты меры для проверки сведений о его личности. Заявитель предупреждается об ответственности, установленной КоАП, за заведомо ложное заявление, о чем расписывается в протоколе. Письменное заявление должно быть подписано заявителем.

В связи с этим остается не ясным каким образом относится к электронному документу, подписанному ЭЦП. Представляется, что это может ограничить в некоторых случаях права заявителей. Кроме того, также, как и в УПК, вопрос использования электронного помощника судьи (должностного лица) остался не раскрытым.

Отдельно остановимся на том, что ПИКоАП предусматривает возможность фиксации хода судебного заседания с использованием технических средств. При этом такая возможность отсутствует в отношении иных должностных лиц государственных органов или коллегиальных органов (например, комиссия по делам несовершеннолетних). Представляется, что данный подход является существенным и внедрение цифровых технологий в порядок фиксации рассмотрения дела об административном правонарушении

данными субъектами будет способствовать повышению защиты участников административного процесса, в том числе лиц, в отношении которых ведется административный процесс, а также позволит обеспечить прозрачность принятия решений должностными лицами при принятии решений по делам об административных правонарушениях.

Электронное дело об административном правонарушении.

Начиная рассматривать концепцию электронного дела об административном правонарушении (далее – электронное дело), стоит определить, что является делом об административном правонарушении.

В соответствии со ст. 1.4 ПИКоАП делом об административном правонарушении является обособленное производство, которое включает в себя заявление, сообщение об административном правонарушении, протокол об административном правонарушении, постановление по делу об административном правонарушении и иные материалы, относящиеся к административному правонарушению.

Исходя из приведенных процессуальных норм можно сделать вывод что данное дело представляет собой обособленное производство, которое ведется уполномоченным органом в соответствии нормами процессуального права (ПИКоАП) за совершение субъектом деяния, предусмотренного нормой материального права (КоАП), которое включает определенные процессуальные документы. Переходя к рассмотрению возможности цифровизации данного производства следует отметить, что для признания их электронными они должны существовать в цифровой среде.

А. Ф. Абдулвалиев при рассмотрении цифровизации уголовного процесса полагает, что электронное уголовное дело представляет собой «электронный носитель, предназначенный для хранения цифровой информации – материалов уголовного дела, полностью заменяющий собой бумажный вариант уголовного дела, позволяющий использовать его вместе с портативным компьютером для собирания доказательств в рамках расследования и рассмотрения уголовного дела» [9, с. 59].

По мнению О. А. Адамовича возможными положительными сторонами электронного уголовного дела являются следующие аспекты:

существенное сокращение времени, затраченного следователем на оформление документов;

сведение к минимуму организационных причин, увеличивающих срок расследования (например, нахождение длительное время уголовного дела у прокурора в рамках прокурорского надзора либо у начальника следственного подразделения при проверке уголовных дел);

упрощение процедуры собирания доказательств и составления процессуальных документов;

повышение качества расследования, так как в большей мере произойдет исключение возможности фальсификаций и исправлений в материалах уголовных дел [10, с. 8-9].

Ю. А. Мартынов при рассмотрении перспектив электронного уголовного дела пишет, что «внедрение электронного делопроизводства в уголовный процесс решает проблему расследования и окончания производства по сложным (многотомным) уголовным делам путем замены бумажных носителей на электронные и возможностью знакомить с электронной копией уголовного дела неограниченный круг лиц (пострадавших и иных участников уголовного процесса)» [11].

Рассматривая положительные стороны внедрения электронного дела отечественные авторы, как правило, не раскрывают весь спектр проблем, с которыми придется столкнуться при внедрении данной технологии в белорусский уголовный или административный процесс.

Так, С. В. Зуев в своей работе рассматривает основные проблемы и риски, с которыми уже сталкиваются правоприменители в других странах, а также оцениваются возможные проблемы электронного дела [15]. К этим проблемам он относит следующие:

сложность в обеспечении информационной безопасности. Проблемы использования современных технологий связаны с идентификацией личности, возможностью внесения извне изменений в сохраненные электронные документы, используемые в уголовном деле. Для решения этого вопроса потребуется качественное техническое решение. При этом технологии, поддерживающие, к примеру, биткойн, вряд ли могут удовлетворить национальные потребности в этом вопросе. Подобные программы не в полной мере отвечают интересам государства, его безопасности. Прогнозируется, что отечественные аналоги могут быть получены спустя некоторое время при значительных материальных затратах;

возможность фальсификации следователем информации. Возможность будет вызывать сомнения в достоверности, и быть лишним поводом к ее дополнительной проверке. Несмотря на существующие различные методы защиты целостности цифровых данных, проблема связана с возможностью раскрытия персональных данных, кражи коммерческой, профессиональной, служебной и государственной тайны. Возникают вопросы, требующие дополнительной защищенности. Это относится к носителям электронной информации, а также к сведениям, содержащих секретную информацию (например, данные о лице, участвующим в уголовном деле в рамках государственной защиты);

сложность в предоставлении участникам процесса для ознакомления в силу легкости внесения изменений и дополнений в цифровую информацию. На практике уже имеют место случаи отказа обвиняемому осмотреть,

находящуюся на электронном носителе, информацию на этапе ознакомления с материалами дела по окончанию расследования;

необоснованный отказ в приобщении к материалам дела электронных носителей информации, что в дальнейшем приводит к направлению официальных запросов этой информации из учреждений, организаций и предприятий. Это в определенной степени может усложнить процедуру получения нужной информации по делу.

Обратим внимание, что, говоря об электронном деле, авторы в основном рассматривают только электронное уголовное дело, административный процесс и электронное дело об административном правонарушении является мало разработанной темой. На наш взгляд, схожие проблемы возможны и при внедрении концепции электронного дела об административном правонарушении.

Выводы:

1. При рассмотрении анализа возможностей развития цифровизации административного процесса следует отметить, что законодателем уже проведена определенная работа в данной сфере и возможности для использования цифровых (электронных) средств в административном процессе имеются. Данное направление безусловно является актуальным и может поспособствовать следующим положительным аспектам:

уменьшение стоимости проведения административного процесса, поскольку некоторые процессуальные действия возможно производить с помощью электронных средств (видеосвязь, технические средства фиксации следов правонарушения), что также позволит уменьшить сроки расследования дел;

повышение эффективности надзорной деятельности за ведением административного процесса, поскольку должностным лицам органов прокуратуры не потребуется истребовать материалы дела, а только получить доступ к данному делу;

обеспечение прозрачности проведения процессуальных действий (действий должностных лиц), порядка приобщения и исследования доказательств, законности и обоснованности вынесенных решений по существу рассмотрения материалов дела. Кроме того, это позволит обеспечить четкий контроль за соблюдением процессуальных сроков и прохождения материалов дела об административном правонарушении, что несомненно повысит правовую защиту субъектов, в отношении которых ведется процесс;

повышение правовой защиты участников процесса, обеспечение их правом подачи электронных документов, подписанных ЭЦП, контролем за их соблюдением. Создание возможности дистанционного обращения в правоохранительные органы при отсутствии возможности личного обращения;

консолидирование в одном месте всех материалов дела об административном правонарушении и возможности контролируемого доступа к нему.

2. Основными проблемами, которые в настоящее время требуют разрешения и от которых зависит дальнейшее развитие направления цифровизации административного процесса:

отсутствие разработанных определений понятий «электронное доказательство», «электронное дело об административном правонарушении». Это не позволяет сформировать целостное представление о данных явлениях и выработать системный подход к их интеграции в административном процессе;

обеспечение защиты информации и организации защищенного доступа к нему. Данная проблема может быть решена путем создания системы защищенных серверов хранения такой информации и механизма строгого контролируемого доступа к данным материалам, а также создание системы контроля изменений и отслеживания субъектов, уполномоченных на внесение таких изменений, и их полномочий;

отсутствие единой системы подготовки кадров правоохранительных органов по использованию современных технических средств сбора, фиксации, оценки доказательств, а также проведения процессуальных действий с помощью цифровых технологий;

невозможность одномоментной интеграции цифровых технологий в административный процесс. Это возможно только поэтапно, поскольку развитие технологий и необученность (не желание или отсутствие возможности к обучению) всех категорий субъектов. Разрешение данной проблемы может быть осуществлено только путем создания системной модели такой интеграции и обучения, а также обеспечения ЭЦП.

3. Практическими рекомендациями по дальнейшей цифровизации административного процесса, по нашему мнению, являются следующие предложения:

внесение изменений в ст. 9.2 ПИКоАП (Заявление физического лица) нормы, по которой поводом для начала процесса может являться электронное заявление, удостоверенное ЭЦП;

дополнение ПИКоАП нормой о возможности проводить рассмотрение дела об административном правонарушении должностным лицом органа, ведущего административный процесс (коллегиальным органом), с использованием технических средств фиксации хода рассмотрения дела, порядком внесения в него изменений, рассмотрения заявлений и ходатайств и возможности ознакомления.

закрепление в ПИКоАП понятий «электронное доказательство», «электронное дело об административном правонарушении».

Библиографический список

1. Ищенко, П. П. Современные подходы к цифровизации досудебного производства по уголовным делам / П. П. Ищенко // Lex Russica. – 2019. – № 12 (157). – С. 68-79.

2. Калинкович: в Беларуси развивается электронное судопроизводство [Электронный ресурс] // Белта. – Режим доступа: https://www.belta.by/society/view/kalinkovich-v-belarusi-razvivaetsja-elektronnoe-sudoproizvodstvo-466802-2021/?fbclid=IwAR1Qic6srowy2r1scYathGEkeOS8mzBA86w-awncTTqJvU4dLj35pw-bpFw/. – Дата доступа: 20.02.2022.

3. При внедрении элементов электронного уголовного дела учитывается зарубежный опыт [Электронный ресурс] // Белта. – Режим доступа: https://www.belta.by/society/view/pri-vnedrenii-elementov-elektronnogo-ugolovnogo-dela-uchityvaetsja-zarubezhnyj-opyt-noskevich-298383-2018/. – Дата доступа: 20.02.2022.

4. Зазулин, А. И. Функции цифровой информации и технологий в уголовном процессе / А. И. Зазулин // Сибирское юридическое обозрение. – 2020. – Т. 17. – № 1. – С. 75-82.

5. Зуев, С. В. Слабые стороны информационного подхода в свете цифровизации уголовного судопроизводства / С. В. Зуев, А. С. Титова // Правопорядок: история, теория, практика. – 2019. – № 1 (20). – С. 49-54.

6. Вопросы использования электронных доказательств обсудили в Верховном Суде [Электронный ресурс] // Официальный сайт Верховного Суда Республики Беларусь. – Режим доступа: https://court.gov.by/ru/justice/press_office/874b1f48adc54a25.html/. – Дата доступа: 20.03.2022.

7. Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс] : 6 янв. 2021 г., N 91-З : принят Палатой представителей 18 дек. 2020 г. : одобр. Советом Респ. 18 дек. 2020 г. // КонсультантПлюс. Беларусь / ООО “ЮрСпектр”, Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

8. Зуев, С. В. Цифровая среда уголовного судопроизводства: проблемы и перспективы / С. В. Зуев // Сибирский юридический вестник. – 2018. – № 4 (83). – С. 118-123.

9. Абдулвалиев, А. Ф. Предпосылки и перспективы внедрения электронной формы уголовного дела в деятельность судебных органов / А. Ф. Абдулвалиев // Право и политика. – 2013. – № 1. – С. 58-65.

10. Адамович, О. А. Электронное уголовное дело: перспективы и проблемы внедрения / О. А. Адамович // Теоретико-прикладные вопросы развития досудебного производства по уголовным делам на современном этапе : сб. ст. междунар. науч.-практ. конф., Новополоцк, 26–27 сент. 2019 г. : в 2 т. / Полоц. гос. ун-т ; редкол.: И. В. Вегера (отв. ред) [и др.]. – Новополоцк : Полоц. гос. ун-т, 2019. – Т. 2.С. 5-17.

11. Мартынов, Ю. А. Электронное уголовное дело: возможности и перспективы [Электронный ресурс] / Ю. А. Мартынов // institutemvd.by – Режим доступа: https://elib.institutemvd.by/bitstream/MVD_NAM/4399/1/martynov.pdf. – Дата доступа: 20.04.2022.

15. Зуев, С. В. Электронное уголовное дело: за и против / С. В. Зуев // Правопорядок: история, теория, практика. – 2018. – № 4 (19). – С. 6-12.

УДК 336

ФОРМИРОВАНИЕ ПОДХОДОВ К ПРАВОВОМУ ОБЕСПЕЧЕНИЮ КРАУД-ФИНАНСИРОВАНИЯ: ОПЫТ КИТАЯ

О.Р. Кочерга

Белорусский государственный университет
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье анализируется опыт развития рынков крауд-финансов и их правового регулирования в Китае на примере долгового крауд-финансирования. Отмечено, что китайский опыт функционирования рынка краудлендинга наглядно демонстрирует актуальность обеспечения своевременности государственного вмешательства в экономику и учета сущностных особенностей регулируемых отношений во избежание регуляторного арбитража и формирования теневого банкинга. Сделан вывод о том, что отрицательная динамика объемов китайского рынка крауд-финансов отражает в большей степени не падение рынка вследствие ужесточения регуляторного воздействия, а результат борьбы с теневым банкингом.

Ключевые слова: крауд-финансы; краудфандинг; краудлендинг; правовое регулирование; теневой банкинг; Китай.

FORMING APPROACHES TO THE LEGAL SUPPORT OF CROWD FINANCING: THE EXPERIENCE OF CHINA

O.R. Kocherga

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article analyzes the experience of the development of crowd finance markets and their legal regulation in China on the example of debt crowd financing. It is noted that the Chinese experience of the functioning of the crowdlending market clearly demonstrates the relevance of timeliness state intervention in the economy as well as taking into account the essential features of regulated relations in order to avoid regulatory arbitrage and the formation of shadow banking. It is concluded that the negative dynamics of the Chinese crowd finance market reflects, to a greater extent, not the market decline due to the tightening of regulatory impact, but the result of the fight against shadow banking.

Keywords: crowd finance; crowdfunding; crowdlending; legal regulation; shadow banking; China.

Экономические и технологические факторы, возникшие после финансового кризиса 2008 г., способствовали развитию децентрализации и дезинтермедиации на финансовых рынках, в результате чего возникло новое

направление – крауд-финансы. Базовой категорией крауд-финансов выступает краудсорсинг – процесс мобилизации различных ресурсов неопределенного круга лиц посредством использования информационных технологий. В свою очередь, процесс аккумулирования финансовых ресурсов большого количества физических и юридических лиц посредством глобальной сети Интернет в целях реализации различных некоммерческих или коммерческих проектов, именуется краудфандингом. Помимо специфики, присущей краудфандингу как разновидности краудсорсинга, рассматриваемый феномен также обладает признаками пиринговых (P2P, от англ. «peer-to-peer» – одноранговый) отношений, а также венчурных инвестиций.

Особое место в отношениях крауд-финансирования занимает оператор специализированного интернет-ресурса – крауд-платформы, благодаря которой спонсор узнает о потребности реципиента в финансировании его проекта. Ключевой особенностью краудфандинга, обусловленной его одноранговым характером, выступает непосредственное финансовое взаимодействие между реципиентом и спонсором при отсутствии прямого посредничества финансовых учреждений. Например, в отличие от банковского посредничества при кредитовании, кредитор в краудфандинге самостоятельно принимает решения об объекте инвестирования и формирует свой инвестиционный портфель.

Популярность краудфандинга как формы альтернативного финансирования наглядно демонстрирует положительная динамика объемов мирового рынка крауд-финансов. При этом лидером (71% мирового объема привлеченных средств) во всех трех сегментах крауд-финансов – краудлендинге, краудинвестинге и краудфандинге – до 2019 года был Китай, в связи с чем китайский опыт функционирования и правового регулирования рынков крауд-финансов представляет особый исследовательский интерес.

Необходимо отметить, что предпосылки развития крауд-финансов в Китае имеют свою специфику: если в США и Европе в результате кризисных событий 2008 г. на финансовых рынках возникли свободные ниши, которые удалось занять краудфандинговым платформам, то в Китае финансовый рынок изначально функционировал иначе. Так, в финансовой системе Китая доминирует государственный банковский сектор, созданный для поддержки крупных государственных предприятий, являющихся основой реальной экономики Китая. Одновременно с сильной ориентацией банковского сектора на корпоративное обслуживание китайская финансовая система характеризуется низкой доступностью финансовых услуг в секторе потребительского кредитования, а также в секторе малого и среднего бизнеса, вследствие чего значительная часть населения и предпринимателей практически не имеет доступа к финансовым услугам [1].

Подавляющий объем рынка крауд-финансов в Китае принадлежал краудлендингу – пиринговому кредитованию. Активное восприятие

китайским рынком долговых моделей крауд-финансирования обусловлено как общей популярностью рассматриваемого вида крауд-финансов в силу относительной простоты оформления договорных отношений, так и широкой распространенностью в Китае схожих форм самоорганизации участников финансовых отношений – сберегательно-кредитных ассоциаций, взаимного кредитования, ростовщичества и др.

Эмпирические исследования позволили установить, что с 2011 г. по 2018 г. 84% краудлендинговых платформ перестали функционировать в силу банкротства или мошеннических действий [2]. Зачастую исследователи в качестве основной причины сложившейся ситуации называют отсутствие надлежащего правового регулирования рассматриваемой сферы.

Так, операторы пиринговых платформ проходили регистрацию в органах местного управления в сфере промышленности и торговли в качестве предприятий по оказанию «информационных услуг», а сделки оформляли в соответствии с нормами договорного права Китая [3]. По мере увеличения числа действующих платформ и усиления конкуренции у указанных субъектов возникла мотивация привлекать клиентов посредством предоставления различного рода гарантий как в форме фиксированного дохода, так и в форме условия о возврате суммы кредита в случае неплатежеспособности заемщика. Таким образом, пиринговые платформы приняли на себя кредитные риски и ответственность за дефолт заемщиков и стали формировать резервные фонды для выплат кредиторам, аналогичные по функциям страхованию вкладов в традиционном банковском секторе. В результате возникла ситуация, при которой риск неплатежеспособности каждого конкретного заемщика, который распространялся на соответствующих кредиторов и мог быть уменьшен посредством диверсификации, трансформировался в риск банкротства платформы, который распространялся на всех ее кредиторов. Ситуация осложнялась отсутствием у операторов соответствующих платформ опыта профессионального управления рисками и объемов резервных фондов, вследствие чего в отсутствие стабильного притока новых инвесторов или ухудшения макроэкономических условий даже незначительное количество невыплаченных кредитов было способно в короткие сроки истощить резервные фонды и вызвать своего рода «банковскую панику».

Иными словами, краудлендинговые платформы, зарегистрированные в качестве информационных посредников, стали выполнять функции и осуществлять деятельность финансовых посредников, возложив на себя кредитные риски, в результате чего практически все платформы пирингового кредитования к 2016 году осуществляли незаконную финансовую деятельность и сформировали сектор теневого банкинга. Кроме того, аккумулирование средств зачастую проходило вне банковской системы, а для привлечения кредиторов использовались схемы Понци и поддельные данные

заемщиков, в результате чего около 25% платформ прекратили работу из-за мошенничества со стороны их управляющих [4].

Своевременное государственное реагирование на кризис рынка пирингового кредитования затруднялось в силу несовершенства китайской модели распределения полномочий в сфере финансового регулирования и надзора. Так, в отсутствие реакции центральных правительственных органов Китая на рост рынка пирингового кредитования, органы местного управления не имели возможности эффективно контролировать операции краудлендинговых платформ, которые распространяли свое действие по всему Китаю, а также не имели полномочий на вмешательство в деятельность крауд-платформ до тех пор, пока выплаты не прекратятся, а сами платформы – не обанкротятся. Кроме того, муниципальные органы власти были заинтересованы в дальнейшем функционировании краудлендинговых платформ, несмотря на возникший кризис, в связи с тем, что зачастую займы, полученные на платформах, по соглашению с государственными органами, направлялись на реализацию проектов муниципального значения, не финансируемых банками [3]. Указанное не позволило органам местного управления обеспечить баланс между поощрением инновационного развития и принятием мер по защите прав кредиторов.

Тем не менее, с 2015 г. в Китае принят ряд НПА, направленных на регламентацию деятельности краудлендинговых платформ, в соответствии с которыми крауд-платформам дозволялось выполнять исключительно посредническую функцию и оказывать услуги по информационному обмену между кредиторами и заемщиками; предусматривался прямой запрет на незаконное привлечение средств, предоставление гарантий кредиторам, секьюритизацию, осуществление деятельности по модели акционерного краудфандинга; устанавливалось обязательство платформ осуществлять комплексную оценку рисков в отношении каждого кредитора, обеспечивать идентификацию клиентов, хранение средств клиентов в банковских учреждениях, раскрывать информацию о заемщиках, о возможных рисках и др.

Важно отметить, что параллельно с формированием правовой базы пирингового кредитования в Китае осуществлялась политика по минимизации рисков онлайн-финансов в отношении действующих платформ, основными целями которой являлись: 1) выявление, «исправление» и/или запрет деятельности платформ, которая нарушает законодательство, выходит за рамки информационного посредничества и т.д.; 2) поддержка и поощрение платформ, соблюдающих законодательство в сфере пирингового кредитования, содействие их развитию; 3) формирование долгосрочного механизма регулирования отрасли, устранение пробелов, обеспечение баланса между регулированием и инновациями.

Реализация указанных целей обеспечивалась посредством аккумулирования и анализа органами местного управления информации от участников рынка, в ходе которого выявлялись субъекты, допускающие нарушение финансового законодательства. В отношении ряда из них выносились требования о приведении своей деятельности в соответствие с положениями законодательства, а другие подлежали ликвидации и привлечению к административной или уголовной ответственности. При этом распространенным основанием для привлечения к ответственности был незаконный фандрайзинг (сбор денежных средств), который представляет собой аккумулирование средств неопределенного круга лиц, сопровождаемое обещанием выплаты основной суммы инвестиций с процентами или предоставления иных инвестиционных доходов, в отсутствие разрешения органов финансового регулирования и надзора или осуществляемое с нарушением финансового законодательства [5].

Кампания по устранению рисков в секторе интернет-финансов должна была завершиться в 2017 году. Однако рекордное количество «проблемных» платформ было зафиксировано в 2018 году, уже после формирования правовой базы пирингового кредитования и осуществления надзорных мероприятий. Указанное обусловлено двумя основными факторами: во-первых, увеличением затрат на соблюдение нормативных требований и операционных расходов действующих крауд-платформ. [6]. Во-вторых, контролирующие государственные органы в Китае продлевали сроки льготного периода, предусмотренного для приведения своей деятельности в соответствие с законодательством и осуществляемыми надзорными мероприятиями, что мотивировало операторов платформ продолжать осуществлять свою деятельность в нарушение законодательства с целью получения прибыли вплоть до ликвидации, поскольку ориентироваться на соответствующие сроки было затруднительно [7].

В дальнейшем при проведении межведомственных совещаний по вопросу управления рисками в сфере пирингового кредитования был принят ряд дополнительных мер, среди которых запрет на регистрацию новых платформ пирингового онлайн-кредитования, а в ноябре 2020 г. Комиссия по регулированию банковской и страховой деятельности Китая (CBIRC) объявила, что количество P2P-платформ сократилось до нуля.

Таким образом, китайский опыт функционирования рынка долгового крауд-финансирования наглядно демонстрирует актуальность обеспечения своевременности государственного вмешательства в экономику и учета сущностных особенностей регулируемых отношений во избежание регуляторного арбитража и формирования теневого банкинга. В данном контексте представляется необходимым правильно расставлять акценты и определять проблему: так, например, некоторые исследователи, анализируя опыт Китая

в регулировании крауд-финансов, приходят к выводу, что «отсутствие законодательного регулирования приводит к резкому росту инвестиций», а «введение жестких законодательных ограничений и запретов в дальнейшем отрицательно влияет на объемы инвестирования» [8]. В то же время, не оспаривая значимость влияния нормативного правового регулирования на развитие экономических отношений, отметим ряд существенных аспектов, не позволяющих в полной мере согласиться с данными выводами:

- во-первых, специфика финансовой системы Китая с ее ориентацией на корпоративное обслуживание содействовала формированию спроса и предложения финансовых ресурсов среди субъектов, не имеющих доступа к финансовым услугам, что в совокупности с низкими процентными ставками по депозитам, стремительным развитием и распространением в Китае интернет-коммуникаций, отсутствием конкуренции с банками стимулировало появление и распространение финансовых услуг, предлагаемых крауд-платформами. В отсутствие указанных экономических условий использование регуляторного арбитража не позволило бы достичь таких объемов рынка;

-во-вторых, как показали результаты проведенного исследования, государственно-правовое вмешательство в экономические отношения на рынке крауд-финансов в Китае было направлено в первую очередь не на упорядочение деятельности крауд-платформ посредством формирования специального законодательства, а на выявление и недопущение случаев нарушения действующего законодательства в сфере финансов, включая законодательство о противодействии незаконному сбору средств и лицензирования финансовой деятельности;

-в-третьих, основой мер, направленных на минимизацию последствий кризиса и дальнейшего регулирования крауд-финансов выступил подход, в соответствии с которым трансформация формы финансовых отношений не влияет на их содержание, иными словами, интернет-финансы – это те же финансовые отношения, с присущими им рисками, подлежащими соответствующему контролю. В свою очередь, деятельность подавляющего большинства крауд-платформ на китайском рынке заключалась в осуществлении финансового посредничества в обход предусмотренной законодательством разрешительной системы и системы финансового контроля и надзора.

Исходя из изложенного, можно сделать вывод о том, что, во-первых, рост рынка краудлендинга в Китае был обусловлен не столько отсутствием специального законодательства, сколько несовершенством системы финансового контроля и надзора, информационного обмена и моделей распределения полномочий между государственными органами. Во-вторых, объемы китайского рынка крауд-финансов не соответствуют действительности,

поскольку включают в себя не только собственно пиринговые транзакции между реципиентами и спонсорами, которые представляют собой истинную сущность рассматриваемых отношений, в которых крауд-платформа играет роль инфраструктурного (информационного) посредника, но и транзакции, в которых крауд-платформы выступали финансовыми посредниками в нарушение законодательства. В результате отрицательная динамика объемов китайского рынка крауд-финансов отражает в большей степени не падение рынка вследствие ужесточения регуляторного воздействия, а результат борьбы с теневым банкингом.

В этой связи следует положительно оценить принятие Указа Президента Республики Беларусь от 25 мая 2021 г. № 196 «О сервисах онлайн-заимствования и лизинговой деятельности», который учитывает характер посреднической деятельности краудлендинговых платформ, а также позволит обеспечить финансовую поддержку МСП в кризисных условиях, когда существенно возрастает спрос на финансовые ресурсы для поддержания операционной деятельности. В то же время при стабилизации макроэкономических условий восстанавливается спрос на инвестиционные ресурсы, вследствие чего представляется целесообразным обеспечить своевременную разработку НПА, направленных на формирование регуляторной базы и стимулирование развития инвестиционных форм крауд-финансов, а также иных моделей краудфандинга, например, основанных на торговле счетами-фактурами, коммерческой недвижимости и др.

Библиографический список

1. Renjie, T. Real Estate Crowdfunding in China [Electronic resource] / T. Renjie // Massachusetts Institute of Technology, 2022. – Mode of access: https://dspace.mit.edu/bitstream/handle/1721.1/123597/1135864260-MIT.pdf?sequence=3. – Date of access: 10.06.2022.

2. He, Q. The failure of Chinese peer-to-peer lending platforms: Finance and politics [Electronic resource] / Q. He, X. Li // ScienceDirect, 2022. – Mode of access: https://www.sciencedirect.com/science/article/abs/pii/S0929119920302960. – Date of access: 10.06.2022.

3. Chorzempa, M. P2P Series Part 1: Peering Into China's Growing Peer-to-Peer Lending Market [Electronic resource] / M. Chorzempa // Peterson Institute for International Economics, 2022. – Mode of access: https://www.piie.com/blogs/china-economic-watch/p2p-series-part-1-peering-chinas-growing-peer-peer-lending-market. – Date of access: 10.06.2022.

4. Huang, Y. Why did the Peer-to-peer Lending Market Fail in China? [Electronic resource] / Y. Huang // IDEAS, 2022. – Mode of access: https://iems.ust.hk/assets/presentation-slides/2021/huang-p2p_fail_slides_hkustiems_nov2021.pdf. – Date of access: 10.06.2022.

5. Приказ Государственного совета Китайской Народной Республики № 737 «Об утверждении Положения о предупреждении и пресечении незаконного сбора средств» от 26 января 2021 г. [Электронный ресурс]. – Режим доступа:

http://www.gov.cn/zhengce/content/2021-02/10/content_5586632.htm. – Дата доступа: 10.06.2022.

6. Tao, Y., Wei Sh. Funds sharing regulation in the context of the sharing economy: Understanding the logic of China's P2P lending regulation [Electronic resource] / Y. Tao, Sh. Wei // ScienceDirect, 2022. – Mode of access: https://www.sciencedirect.com/science/article/pii/S0267364918303686#tb2fn4. – Date of access: 10.06.2022.

7. Chorzempa, M. P2P Series Part 3: China's Online Lending Consolidates As Market Grows [Electronic resource] / M. Chorzempa // Peterson Institute for International Economics, 2022. – Mode of access: https://www.piie.com/blogs/china-economic-watch/p2p-series-part-3-chinas-online-lending-consolidates-market-grows. – Date of access: 10.06.2022.

8. Чудиновских, М.В. Регулирование модельных типов краудфандинга: опыт Китая и возможности его применения в России [Электронный ресурс] / М.В. Чудиновских, Ю.В. Куваева // Nota Bene, 2022. – Режим доступа: https://nbpublish.com/library_read_article.php?id=34030#13. – Дата доступа: 10.06.2022.

УДК 340

ПРАВОВЫЕ АСПЕКТЫ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ НАЛОГОВУЮ ТАЙНУ

Ар.А. Пилипенко

Белорусский государственный университет
ул. Ленинградская 8, Минск, 220030, Беларусь

Статья посвящена отдельным вопросам правовой характеристики сведений, составляющих налоговую тайну. Делается вывод о том, что опубликование большого объема данных о налогоплательщике и его деятельности – это повышение гарантий соблюдения налогового законодательства плательщиками, повышение эффективности налогового администрирования, снижение рисков применения плательщиками различных схем уклонения от уплаты налогов и, в конечном итоге, роста налоговых отчислений. Правомерное разглашение сведений, составляющих налоговую тайну, возможно только в процессе реализации налоговыми и иными государственными органами предоставленных им дискреционных полномочий.

***Ключевые слова*:** налоговая тайна, правовое регулирование, информация ограниченного доступа, налоговое законодательство.

LEGAL ASPECTS OF INFORMATION CONSTITUTING A TAX SECRET

Ar.A. Pilipenko

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article is devoted to certain issues of the legal characteristics of information constituting a tax secret. It is concluded that the publication of a large amount of data about a taxpayer and his activities is an increase in guarantees of compliance with tax legislation by taxpayers, an increase in the efficiency of tax administration, a reduction in the risks of taxpayers using various tax evasion schemes and, ultimately, an increase in tax deductions. Lawful disclosure of information constituting a tax secret is possible only in the process of exercising the discretionary powers granted to them by tax and other state bodies.

Keywords: tax secrecy, legal regulation, restricted information, tax legislation.

Несмотря на то, что вопрос правовой характеристики сведений, составляющих налоговую тайну, носит ярко выраженный нормативный характер, отметим, что точки зрения С.И. Токарева «сведения, составляющие налоговую тайну», под которыми предлагается понимать налоговую информацию

о налогоплательщике и об иных участниках налоговых правоотношений, полученную налоговыми и иными уполномоченными органами в связи с исполнением своих полномочий» [1, с. 45].

Согласно п. 1 ст. 29 Налогового кодекса Республики Беларусь от 19 декабря 2002 г. № 168-З (далее – НК) налоговую тайну составляют любые сведения, которые могут получить органы, поименованные данной норме. Понятие «любые сведения» отражает закрепленное ст. 1 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», под которой понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. В связи с указанным представляется более обоснованным определять налоговую тайну через получение соответствующими субъектами информации, а не любых сведений.

Законодатель при введении дефиниции налоговой тайны предпринял попытку закрепления в п. 1 ст. 29 НК перечня сведений, которые могут быть разглашены. По своей юридической природе и назначению институт налоговой тайны имеет публично-правовой характер и означает защиту сведений, разглашение которых может нарушить права граждан и организаций.

Как справедливо отмечает А.К. Саркисов, «вопросы сохранности сведений, составляющих налоговую тайну, должны постоянно находиться в центре внимания не только налоговых или таможенных органов, органов внутренних дел, органов государственных внебюджетных фондов, но и общества в целом, в том числе каждого налогоплательщика. Причем любой запрос о предоставлении таких сведений необходимо подвергать тщательному анализу, чтобы исключить неправомерность их предоставления» [2, с. 255]. Солидарное мнение высказывает и Ю.А. Крохина, которая отмечает, что «основная проблема в российской правоприменительной практике заключается в том, что объем сведений, относимых к налоговой тайне, изначально не является точно определенным. Это порождает множественность подходов к толкованию его содержания, обжалованию действий (бездействия) налоговых органов, связанных с вопросами предоставления информации о налогоплательщике» [3, с. 27].

Поскольку в национальном законодательстве отсутствует единый критерий, позволяющий разграничить сведения, которые составляют или не составляют налоговую тайну, заслуживает внимание позиция М.Ю. Костенко. Она заключается в том, что «случаи правомерного разглашения налоговой тайны необходимо рассматривать как исключение из налоговой тайны, а не конкретный перечень сведений, как это имеет место в ст. 102 Налогового кодекса Российской Федерации» [4, с. 76].

Развивая данную мысль, отметим, что правомерное разглашение сведений, составляющих налоговую тайну, по нашему мнению, возможно только

в процессе реализации налоговыми и иными государственными органами предоставленных им дискреционных полномочий.

Режим налоговой тайны стал предметом рассмотрения Конституционного Суда Российской Федерации, который отметил, что специальный правовой статус сведений, составляющих налоговую тайну, закреплен ст. 102 Налогового кодекса Российской Федерации от 31 июля 1998 г. № 146-ФЗ. При этом законодатель исходил из интересов налогоплательщиков и необходимости соблюдения принципа баланса публичных и частных интересов в указанной сфере.

Налоговые органы в процессе осуществления своих функций получают доступ к значительному объему информации об имущественном состоянии каждого налогоплательщика. Распространение данной информации может причинить ущерб не только интересам отдельных граждан, частная жизнь которых является неприкосновенной и охраняется законом. Ущерб возможен и для юридических лиц, чьи коммерческие и иные интересы могут быть нарушены в случае произвольного распространения в конкурентной или криминальной среде значимой для бизнеса конфиденциальной информации.

Потому федеральное законодательство и предусматривает ограниченный режим доступа к такой информации. Именно для этого устанавливается исчерпывающий перечень субъектов, обладающих в силу закона правом обращаться к налоговым органам за предоставлением сведений, содержащих налоговую тайну [5].

Перечень сведений, составляющих налоговую тайну, по своей правовой конструкции является открытым, так как в него включаются все сведения, кроме тех, которые перечислены в исчерпывающем перечне сведений, не являющихся тайной.

В этой связи их предполагаемый состав является крайне многообразным. Поэтому в целях упрощения их научного осмысления и изучения С.И. Токарев полагает необходимым сгруппировать сведения, получаемые налоговым органом при осуществлении своих полномочий и подлежащие охране, т. е. являющиеся объектом налоговой тайны, следующим образом:

«– сведения о финансово-хозяйственной деятельности: о содержании договоров, расчете себестоимости продукции, о доходах и объемах продаж, об имуществе, в том числе о денежных средствах, запасах сырья и материалов, о товарно-денежном балансе, о дебиторской и кредиторской задолженности, о банковских операциях, о содержании бухгалтерского и налогового регистров и т. п.);

– сведения, непосредственно связанные с уплатой налогов: об объектах налогообложения, в том числе об имуществе налогоплательщика, о размере

налоговой базы, составе применяемых налоговых льгот, размерах уплачиваемых налогов и суммах возмещения из бюджета;

– сведения о структуре организации: о персонале (возраст, стаж, образование, доход), об организационной структуре, о составе топ-менеджмента, функциях подразделений;

– сведения об отношениях с клиентами, конкурентами и партнерами: о составе поставщиков и покупателей, о подготовке и ведении переговоров и др.» [6, с. 93–94].

Закрепленное в действующем налоговом законодательстве определение налоговой тайны исходит не из перечня сведений о налогоплательщике, не подлежащих разглашению, а из перечня субъектов, имеющих доступ к налоговой тайне. Перечень сведений, составляющих налоговую тайну, законодательно не закреплен, он формируется в процессе практической деятельности органов налогового контроля.

В этой связи основная проблема в правоприменительной практике состоит в том, что объем сведений, относимых к налоговой тайне, изначально не является точно определенным, что порождает множественность подходов к толкованию его содержания, обжалование действий (бездействия) налоговых органов по вопросам предоставления информации о налогоплательщиках. Например, постановлением Министерства по налогам и сборам Республики Беларусь и Национального банка Республики Беларусь от 29 апреля 2015 г. № 10/258 «О сведениях, составляющих банковскую тайну физических лиц, представляемых налоговым органам» определено, что перечень сведений, составляющих банковскую тайну физических лиц, представляемых Национальным банком Республики Беларусь, банками, небанковскими кредитно-финансовыми организациями налоговым органам на основании соглашения, заключенного с Министерством по налогам и сборам Республики Беларусь, включает в себя сведения, входящие в состав кредитной истории. Соответственно, сведения, составляющие банковскую тайну физических лиц (входящие в состав кредитной истории), после того, как они стали известны налоговым органам, переходят в режим налоговой тайны.

Вместе с тем Указом Президента Республики Беларусь от 31 декабря 2019 г. № 503 «О налогообложении» (далее – Указ № 503) установлен режим свободного доступа к ряду сведений, которые были исключены из состава налоговой тайны (п. 14 Указа № 503).

Так, из состава налоговой тайны исключены сведения (ч. 1 подп. 14.3 Указа № 503):

– об уплачиваемых видах налогов, сборов (пошлин) и применяемых особых режимах налогообложения;

– о среднесписочной численности работников;

– содержащиеся в годовой бухгалтерской и (или) финансовой отчетности.

Информация, указанная в ч. 1 подп. 14.3 Указа № 503, предоставляется посредством единого портала электронных услуг общегосударственной автоматизированной системы в отношении организаций и физических лиц, зарегистрированных в качестве индивидуальных предпринимателей (http://portal.gov.by, раздел «Сведения о плательщиках (иных обязанных лицах), не составляющие налоговую тайну»).

В настоящее время перечень сведений, не относящихся к налоговой тайне определен в попд. 1.1–1.13 ст. 29 НК.

Отдельные сведения, не относящиеся к налоговой тайне, указанные в подп. 1.1–1.13 ст. 29 НК, могут быть получены, например, на сайте МНС (http://nalog.gov.by, разделы «Сведения о бизнес-партнере», «Сведения о задолженности по платежам»; портал http://www.portal.nalog.gov.by, сервис «Поиск сведений из Государственного реестра плательщиков (иных обязанных лиц)»; сайт http://egr.gov.by/, раздел «Информация о ЮЛ (ИП), разместивших сведения об их ликвидации (прекращении деятельности) на официальном сайте журнала «Юстиция Беларуси»).

Положением о порядке хранения сведений, составляющих налоговую тайну, доступа к ним и их разглашения, утв. постановлением Совета Министров Республики Беларусь от 16 сентября 2004 г. № 1149 определен перечень плательщиков (категорий плательщиков), в отношении которых сведения, предоставляемые посредством единого портала электронных услуг общегосударственной автоматизированной информационной системы, составляют налоговую тайну согласно приложению. Приложение имеет ограничительный гриф «Для служебного пользования».

Следует отметить наблюдающуюся тенденцию сокращения перечня информации, подлежащей установленной ст. 29 НК охране в качестве налоговой тайны. Представляется, что опубликование большого объема данных о плательщике и его деятельности – это повышение гарантий соблюдения налогового законодательства плательщиками, повышение эффективности налогового администрирования, снижение рисков применения плательщиками различных схем уклонения от уплаты налогов и в конечном итоге – рост налоговых отчислений.

Библиографический список

1. Токарев, С.И. Налоговая тайна в современных условиях налогового администрирования / Т.С. Токарев. – СПб. : Центр научно-производственных технологий «Астерион», 2019. – 280 с.

2. Саркисов, А.К. Правовое регулирование охраны информации, составляющей налоговую тайну / А.К. Саркисов // Вопр. экономики и права. – 2012. – № 3. – С. 251–256.

3. Крохина, Ю.А. Принципы определения налоговой тайны в законодательстве России и зарубежных странах / Ю.А. Крохина // Финансовое право. – 2015. – № 8. – С. 26–30.

4. Костенко, М.Ю. Правовые проблемы налоговой тайны : дис. ... канд. юрид. наук : 12.00.14 / М.Ю. Костенко. – М., 2002. – 146 л.

5. Об отказе в принятии к рассмотрению жалобы гражданина Ламбина Александра Ивановича на нарушение его конституционных прав статьей 102 Налогового кодекса Российской Федерации [Электронный ресурс] : определение Конституц. Суда Рос. Федерации, 30 сент. 2004 г., № 317-О // Консультант Плюс : Версия Проф. Технология 3000 / ЗАО «Консультант Плюс». – М., 2022.

6. Токарев, С.И. Правовой режим тайны в налоговых правоотношениях : дис. … канд. юрид. наук : 12.00.04 / С.И. Токарев. – М., 2018. – 217 л.

УДК 341

СОВРЕМЕННЫЕ ПРОБЛЕМЫ МЕЖДУНАРОДНО-ПРАВОВОГО СОТРУДНИЧЕСТВА ГОСУДАРСТВ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ

А.А. Рипинская

Национальный центр законодательства и правовых исследований Республики Беларусь,
ул. Берсона 1а, г. Минск, 220030, Беларусь

Развитие высоких технологий создает угрозу совершения кибертерроризма, который по своему характеру и способу совершения может нанести вред масштабнее, чем терроризм с использованием оружия либо взрывных устройств. Настоящая статья направлена на выявление проблемных аспектов противодействия использованию информационных технологий для совершения террористических актов. В статье разработаны рекомендации по осуществлению эффективного противодействия кибертерроризму.

Ключевые слова: терроризм, кибертерроризм, международное право, права человека.

CONTEMPORARY PROBLEMS OF INTERNATIONAL LEGAL COOPERATION OF STATES IN THE FIELD OF COUNTERING CYBERTERRORISM

A.A. Ripinskaya

National Center for Legislation and Legal Research of the Republic of Belarus,
1a Bersona street, Minsk, 220030, Belarus

The development of high technologies creates a threat of cyberterrorism, which, by its nature and method of commission, can cause harm on a larger scale than terrorism using weapons or explosive devices. This article is aimed at identifying the problematic aspects of countering the use of information technology to commit terrorist acts. The article developed recommendations for the implementation of effective counteraction to cyberterrorism.

Keywords: terrorism, cyberterrorism, international law, human rights.

Терроризм и его последствия являются одним из наиболее опасных вызовов современности. Сегодня ни одно государство полностью не ограждено и не защищено от угрозы совершения на его территории актов терроризма, поэтому одной из основных задач, стоящих перед каждым

государством и международным сообществом, является противодействие терроризму.

Генеральный секретарь ООН Антониу Гутерриш справедливо указал, что борьба с терроризмом перешла в виртуальное пространство и социальные сети, зашифрованные сообщения и черный интернет активно используются для распространения пропаганды, вербовки «новобранцев» и координации преступлений [1]. На современном этапе с помощью информационных технологий осуществляется, в том числе, финансирование террористической деятельности (S/RES/2462 (2019) [2], подстрекательство к совершению террористических актов (S/RES/1624 (2005) [3]), распространение террористической идеологии (S/RES/2354 (2017) [4]) и вербовка в террористические организации (S/RES/2462 (2019) [2], [5]). Вместе с тем кибертерроризм, безусловно, носящий трансграничный характер, приводит к ухудшению и нарушению дипломатических и экономических отношений между государствами. Кибертерроризм является серьезной угрозой для банковской, транспортной и энергетической систем государств и особенно для государств, в которых правительство, государственный и частный сектора экономики функционируют с помощью информационных сетей и доступа к высоким технологиям [6, с. 42].

Международно-правовое регулирование противодействия терроризму в науке международного права становилось предметом многочисленных исследований. Непосредственно вопросы кибертерроризма и связанных с ним аспектов ранее находили свое отражение в трудах Е. А. Антонян [7], В. А. Голубева [8], Е. Ф. Довгань [9; 10; 11], Н. О. Мороз [12], У. Тафойи [13]. Одновременно с этим большинство исследований направлены на изучение вопроса статуса кибератак, криминализации актов кибертерроризма, при этом не фокусируясь на проблемах, осложняющих противодействие кибертерроризму. Настоящее исследование представляет собой комплексный анализ, направленный на выявление факторов, затрудняющих эффективную деятельность по борьбе с кибертерроризмом.

Международно-правовое сотрудничество государств в области борьбы с терроризмом развивается во многих направлениях. Основной упор делается на предупреждение возникновения и распространения терроризма, пресечение терроризма, ликвидацию последствий террористических актов, привлечение виновных в совершении терроризма лиц к ответственности. При этом, несмотря на обширную сферу взаимодействия, противодействие кибертерроризму осложняется многочисленными факторами и вопросы международного правового сотрудничества государств в борьбе с кибертерроризмом в настоящее время на универсальном уровне не урегулированы [12, с. 80].

Отсутствие определения термина «кибертерроризм». Как и в случае с термином «терроризм» «кибертерроризм» также не нашел своего единого отражения в универсальных соглашениях. Вместе с тем существующие доктринальные взгляды позволяют очертить исследуемое понятие. Так, например, В. А. Голубев и Т. А. Сайтарлы под «кибертерроризмом» понимают «преднамеренную, мотивированную атаку на информацию, обрабатываемую компьютером, компьютерную систему и сети, которая создает опасность для жизни или здоровья людей или наступление других тяжких последствий, если такие действия были содеянные с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта» [14]. Дж. Льюис определяет понятие «кибертерроризм» как «использование компьютерных сетевых инструментов для прекращения функционирования критических объектов национальной инфраструктуры (в частности, энергетических, транспортных, правительственных), либо для принуждения или устрашения правительства или гражданского населения» [15, с. 1]. У. Тафойа указывает, что «кибертерроризм – это запугивание населения посредством использования высоких технологий для достижения политических, религиозных или идеологических целей, а также действия, приводящие к отключению или удалению данных или информации о критической инфраструктуре» [13]. Д. Дэннинг определяет исследуемое понятие как «политически мотивированные хакерские операции, направленные на причинение серьезного вреда, такого как гибель людей или серьезный экономический ущерб» [16]. Вышерассмотренные определения позволяют выделить характерные для кибертерроризма признаки, в частности, использование для атак компьютерных систем и сетей с целью нарушения общественной опасности, запугивания гражданского населения, причинения ущерба и вреда критическим объектам инфраструктуры государства.

Управление ООН по наркотикам и преступности (далее – УНП ООН) отмечает, что сегодня кибертерроризм рассматривается как «киберзависимое» преступление, совершаемое в политических целях для причинения вреда критической инфраструктуре, однако такое толкование кибертерроризма, ограничивающееся только киберпреступлениями, совершаемыми в отношении критически важной инфраструктуры, не получило широкого распространения при обсуждении. УНП ООН также справедливо указывает, что неоправданное отнесение каких-либо действий к кибертерроризму может иметь пагубные последствия и привести к вынесению несоразмерных мер наказания в отношении лиц, преследуемых за совершение таких преступлений [17]. Одновременно представляется необходимым рассмотреть современные формы совершения преступлений в информационном пространстве, такие, например, как массовые рассылки о минировании объектов. Отмечается, что в последнее время получил распространение такой

способ совершения преступлений как «сваттинг», под которым рассматривают тактику, направленную на введение спецслужб в заблуждение [18]. В Российской Федерации в феврале 2022 г. были задержаны члены «сваттинговых» интернет-групп, которые оставляли ложные сообщения о минировании зданий в РФ, Беларуси, Азербайджане, Армении, Казахстане, Молдавии. Федеральная служба безопасности РФ отметила, что авторы ложных сообщений о минировании занимались этим «в целях дестабилизации обстановки в Российской Федерации и сопредельных государствах, вымогательства денежных средств из хулиганских побуждений» [19].

Сегодня все чаще можно встретить информацию об использовании беспилотных летательных аппаратов в целях нанесения ущерба и вреда. Например, в 2019 г. на крупных месторождениях компании Saudi Aramco в Абкайке и Хурайсе (Саудовская Аравия) произошли пожары, причиной которых стала атака беспилотных летательных аппаратов [20]. В марте 2022 г. нефтеперерабатывающий завод в Эр-Рияде (Саудовская Аравия) был также атакован беспилотниками [21]. Еще одним примером является удар беспилотника в Кабуле (Афганистан), в котором погибли 10 человек, за несколько дней до вывода из Афганистана войск США. Генерал Центрального командования США при этом отметил, что американская разведка следила за машиной сотрудника гуманитарной организации, подозревая, что он был связан с организацией «Исламское государство» (организация признана террористической в соответствии с резолюцией 1267 (1999) Совета Безопасности ООН), однако подтверждения в дальнейшем найдено не было [22].

Террористические организации используют информационное пространство в преступных целях для совершения террористических преступлений, в частности, для пропагандистской деятельности, осуществления вербовки в террористические ряды, подстрекательства к совершению террористических преступлений. В общем и целом, представляется очевидным, что информационное пространство является наиболее «удобной» территорией для преступной, в частности, террористической деятельности, поскольку отличается оперативностью, экономичностью и доступностью; слабой цензурой или полным отсутствием цензуры; наличием большой аудитории пользователей; быстрым и относительно дешевым распространением специально подобранной информации, комплексностью ее подачи и восприятия; анонимностью связи и скрытностью источника воздействия; возможностью несанкционированного подключения к компьютерным сетям управления стратегическим объектами, в том числе военными; дистанционным характером воздействия на компьютерные системы в различных регионах мира и др. [23].

Интересным примером использования информационного пространства в террористических целях является, журнал «Inspire», интернет-издание,

выпускаемое «Аль-Каидой» (организация признана террористической в соответствии с резолюцией 1267 (1999) Совета Безопасности ООН) с целью дать мусульманам возможность готовиться к участию в джихаде. В журнале содержатся идеологические материалы, направленные, как отмечается, на поощрение терроризма [24, с. 8]. На наш взгляд, понятие «кибертерроризм» довольно многогранное и может объединять в себе различные проявления терроризма в информационном пространстве. Представляется справедливым мнение УНП ООН о том, что не только конкретные акты с целью повреждения критически важное инфраструктуры являются кибертерроризмом. Использование, например, беспилотных летательных аппаратов, работающих с помощью различных программных обеспечений или создание атмосферы страха и угрозы жизни, осуществляющиеся с помощью массовых рассылок в интернете, также могут рассматриваться как подпадающие под понятие «кибертерроризм».

Нарушение прав человека. Меры, принимаемые государствами в контексте борьбы с терроризмом (кибертерроризмом), могут ставить под угрозу реализацию прав человека. Совет Безопасности ООН в своих резолюциях (1456 от 20 января 2003 г., 2178 от 18 сентября 2014 г., 2395 от 21 декабря 2017 г.) отмечает, что государства должны соблюдать права человека в рамках проведения контртеррористических операций. Специальный докладчик по вопросам поощрения и защиты прав человека и основных свобод в условиях борьбы с терроризмом указывает, в частности, на необходимость защиты права на жизнь, осуществления справедливого и беспристрастного расследования в ходе борьбы с терроризмом, защиты жертв терроризма (доклад 34/61 (2017)), соблюдение прав человека при объявлении чрезвычайной ситуации в государстве из-за террористических угроз (доклад 37/52 (2018)). Отдельным аспектом, вызывающим беспокойство, является введение без каких-либо расследований и судебных разбирательств санкций против лиц, которые, по мнению того или иного государства, причастны к преступной деятельности.

В науке международного права обсуждается аспект правомерности/неправомерности осуществления целенаправленного убийства лиц, подозреваемых в терроризме (*Targeted Killing of Suspected Terrorists*), в частности, вопрос о том, можно ли рассматривать подозреваемых в терроризме в качестве «законной военной цели» во время вооруженных конфликтов, вне зависимости от того, носит конфликт международный или немеждународный характер. Прежде всего, ст. 6 Международного пакта о гражданских и политических правах 1966 г. определяет, что «право на жизнь есть неотъемлемое право каждого человека. Это право охраняется законом. Никто не может быть произвольно лишен жизни». Одновременно с этим международное гуманитарное право (далее – МГП) защищает лиц, более не принимающих

участие в военных действиях и гражданское население, в частности, МГП защищает всех лиц от произвольного и незаконного лишения жизни, а также указывает на необходимость проведения надлежащих судебных процедур в рамках привлечения к ответственности за участие в военных действиях без права на это, за военные преступления и иные преступления [25, с. 45]. Более того, такого рода действие, как лишение жизни подозреваемых в терроризме лиц, может быть квалифицировано как применение смертной казни без соблюдения каких-либо норм, что противоречит международным стандартам осуществления правосудия за международные преступления, в том числе военные [11, с. 262].

Нехватка квалифицированных специалистов в области противодействия кибертерроризму. Обучение, проведение учений и наличие квалифицированного персонала являются важнейшими областями, определяющими успех в деятельности по борьбе с преступлениями в информационном пространстве [26, с. 60]. Вместе с тем одной из проблем в области противодействия кибертерроризму сегодня является нехватка квалифицированных специалистов в сфере кибербезопасности. Сотрудникам правоохранительных органов может не хватать навыков и опыта проводить работу по выявлению преступлений и виновных в преступлениях в сфере информационной безопасности. Безусловно, для такой работы необходимо освоение специальных программ, а также постоянное повышение квалификации, что обусловлено быстроразвивающейся сферой информационных технологий и растущей угрозой совершения новых преступлений в информационном пространстве.

Подводя итог можно отметить, что вышерассмотренные факторы оказывают негативный эффект на действенное противодействие кибертерроризму, в связи с чем представляется необходимым.

1. Разработать и закрепить понятие «кибертерроризм» в соответствующих законодательных актах.

2. Правоохранительным органам и иным специализированным учреждениям государств эффективно взаимодействовать между собой, а также с международными организациями с целью обмена опытом в деле борьбы с кибертерроризмом.

3. Пресекать акты кибертерроризма на стадии их подготовки, проводить мониторинг состояния информационно-коммуникационного пространства [27, с. 16].

4. Обеспечивать соответствие принимаемых мер по борьбе с терроризмом международному праву прав человека, международному гуманитарному праву.

5. При отсутствии вносить соответствующие изменения и дополнения, предусматривающие ответственность за совершение кибертерроризма, в национальное уголовное законодательство.

6. Создать аппарат, специализирующийся на выявлении и раскрытии преступлений в киберпространстве.

7. Осуществлять специальную подготовку кадров для работы с раскрытием преступлением в информационном пространстве.

Библиографический список

1. «Объединиться для противодействия терроризму» – комментарий Генерального секретаря о конференции Организации Объединенных Наций высокого уровня по борьбе с терроризмом 26 июня 2018 г. // Организация Объединенных Наций [Электронный ресурс]. – Режим доступа: https://www.un.org/sg/ru/content/sg/articles/2018-06-26/uniting-world-against-terrorism. – Дата доступа: 25.03.2022.

2. Резолюция Совета Безопасности Организации Объединенных Наций 2462 (2019) // Организация Объединенных Наций [Электронный ресурс]. – Режим доступа: https://undocs.org/S/RES/2462(2019). – Дата доступа: 25.03.2022.

3. Резолюция Совета Безопасности Организации Объединенных Наций 1624 (2005) // Организация Объединенных Наций [Электронный ресурс]. – Режим доступа: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/510/54/PDF/N0551054.pdf?OpenElement. – Дата доступа: 25.03.2022.

4. Резолюция Совета Безопасности Организации Объединенных Наций 2354 (2017) // Организация Объединенных Наций [Электронный ресурс]. – Режим доступа: https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=S/RES/2354(2017)&Lang=R. – Дата доступа: 25.03.2022.

5. Террористы осваивают киберпространство и вербуют «одиночек» // Организация Объединенных Наций [Электронный ресурс]. – Режим доступа: https://news.un.org/ru/story/2021/01/1394092. – Дата доступа: 25.03.2022.

6. Мазуров, В. А. Кибертерроризм: понятие, проблемы противодействия / В. А. Мазуров / Доклады ТУСУР. – 2010. – № 1(21). – Ч. 1. – С. 41–45.

7. Антонян, Е. А. Блокчейн технологии в противодействии рискам кибертерроризма / Е. А. Антонян. – Москва : Научный консультант, 2019. – 60 с.

8. Голубев, В. А. Кибертерроризм как новая форма терроризма [Электронный ресурс]. – Режим доступа: https://www.crime-research.ru/library/Gol_tem3.htm. – Дата доступа: 25.03.2022.

9. Довгань, Е. Ф. Права человека в контексте борьбы с международным терроризмом /Е. Ф. Довгань // Труд. Профсоюзы. Общество. – 2019. – №2. – С. 54–60

10. Довгань, Е. Ф. Правомерность целевых санкций Совета Безопасности ООН в рамках борьбы с терроризмом / Е. Ф. Довгань // Право.by. – 2011. – № 3. – С.11–21.

11. Douhan, A. F. Adapting the Human Rights System to the Cyber Age /A. F. Douhan // Max Planck Yearbook of United Nations Law Online. – 2020. – № 23 (1). – P. 249–289.

12. Мороз, Н. О. Международно-правовая квалификация кибертерроризма / Н.О. Мороз / Вестник Марийского государственного университета. Серия «Исторические науки», «Юридические науки». – 2016. – № 2 (6). – С. 79–82.

13. Tafoya, W. L. Cyber Terror [Electronic resource]. – Mode of access: https://leb.fbi.gov/articles/featured-articles/cyber-terror. – Date of access: 25.03.2022.

14. Голубев, В. А., Сайтарлы, Т. А. Проблемы борьбы с кибертерроризмом в современных условиях [Электронный ресурс]. – Режим доступа: https://www.crime-research.org/library/e-terrorism.htm. – Дата доступа: 25.03.2022.

15. Lewis, J. A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats [Electronic resource]. – Mode of access: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf. – Date of access: 28.03.2022.

16. Denning, D. E. Is Cyber Terror Next? [Electronic resource]. – Mode of access: http://essays.ssrc.org/sept11/essays/denning.htm. – Date of access: 28.03.2022.

17. Кибертерроризм [Электронный ресурс]. – Режим доступа: https://www.unodc.org/e4j/ru/cybercrime/module-14/key-issues/cyberterrorism.html. – Дата доступа: 25.03.2022.

18. Что такое сваттинг и какая ответственность за него предусмотрена? [Электронный ресурс]. – Режим доступа: https://centr.minsk.gov.by/be/sfery-deyatelnosti/zakonnost-i-pravoporyadok/pravookhranitelnye-organy/ruvd-tsentralnogo-rajona-g-minska/novosti-ruvd-tsentralnogo-rajona-g-minska/10672-chto-takoe-svatting-i-kakaya-otvetstvennost-za-nego-predusmotrena. – Дата доступа: 25.03.2022.

19. ФСБ раскрыла, кто стоит за ложными минированиями в России [Электронный ресурс]. – Режим доступа: https://www.gazeta.ru/social/2022/02/10/14519713.shtml. – Дата доступа: 25.03.2022.

20. Атака дронов на нефтяные объекты Саудовской Аравии. Главное [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/politics/14/09/2019/5d7d05639a79479b16755e08. – Дата доступа: 25.03.2022.

21. В Саудовской Аравии беспилотники атаковали нефтеперерабатывающий завод [Электронный ресурс]. – Режим доступа: https://eadaily.com/ru/news/2022/03/11/v-saudovskoy-aravii-bespilotniki-atakovali-neftepererabatyvayushchiy-zavod. – Дата доступа: 25.03.2022.

22. США признали, что их беспилотник по ошибке убил в Кабуле мирных афганцев [Электронный ресурс]. – Режим доступа: https://www.bbc.com/russian/news-58604726. – Дата доступа: 28.03.2022.

23. Киберпространство и информационный терроризм [Электронный ресурс]. – Режим доступа: http://scienceport.ru/news/kiberprostranstvo-i-informatsionnyy-terrorizm/. – Дата доступа: 28.03.2022.

24. Использование Интернета в террористических целях [Электронный ресурс]. – Режим доступа: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf. – Дата доступа: 28.03.2022.

25. Targeted Killing of Suspected Terrorists During Armed Conflicts: Compatibility with the Rights to Life and to a Due Process [Electronic resource]. – Mode of access: https://www.corteidh.or.cr/tablas/r27148.pdf. – Date of access: 28.03.2022.

26. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства // Организация по безопасности и сотрудничеству в Европе [Электронный ресурс]. – Режим доступа: https://www.osce.org/files/f/documents/5/2/110472.pdf. – Дата доступа: 25.03.2022.

27. Молодчая, Е. Н. Политика противодействия кибертерроризму в современной России: политологический аспект: автореф. дис. ... канд. полит. наук : 23.00.02 / Е. Н. Молодчая ; ФГБОУ ВПО «Российский государственный социальный университет». – Москва, 2011. – 30 с.

УДК 339.5

МЕСТО И РОЛЬ ТАМОЖЕННОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Т.П. Яцко

Национальный центр законодательства и правовых исследований Республики Беларусь, ул. Берсона 1а, г. Минск, 220030, Беларусь

Экономическая безопасность, как часть национальной безопасности обеспечивается рядом государственных органов в пределах их компетенции. Процессы глобализации, рост применяемых санкционных мер предопределяют особое внимание к вопросам экономической безопасности. В статье анализируется деятельность таможенных органов в разрезе вопросов экономической безопасности.

Ключевые слова: таможенные органы, экономическая безопасность.

PLACE AND ROLE OF CUSTOMS REGULATION IN THE SPHERE OF ECONOMIC SECURITY

T.P. Yatsko

National Center for Legislation and legal research of the Republic of Belarus, 1a Bersona street, Minsk, 220030, Belarus

Economic security, as part of national security, is ensured by a number of state bodies within their competence. The processes of globalization and the increase in adopted sanctions measures predetermine special attention to issues of economic security. The article analyzes the activities of customs authorities in the context of economic security.

Keywords: customs authorities, economic security.

Введение

Развитие глобализации, введение санкций являются теми процессами, которые существенно влияют на экономику практически каждого государства. Если процессы глобализации приводит к возникновению новых взаимосвязей национальных экономик, то есть активному взаимодействию субъектов внешнеэкономической деятельности, то санкционные меры приводят к диаметральным последствиям – это и разрыв существовавших ранее экономических связей, потеря традиционных рынков сбыта и логистических схем, маршрутов, поиск новых экономических партнеров. Такая

реальность обуславливает необходимость защиты экономических интересов и обеспечения экономической безопасности государства.

Вопросам экономической безопасности уделяется внимание многими представителями наука. В частности представитель российской науки Л.П. Васильева, рассматривает экономическую безопасность как сферу научного знания [1], в контексте которой изучают, в том числе защиту интересов государства на национальном и международном уровне вторами национальной и российской научной среды; В.И.Лукашин приходит к выводу о том, что экономическая безопасность тесно связана с понятием экономической независимости и зависимости, стабильности и уязвимости экономического давления, шантажа, принуждения и агрессии… [2]; Г.С. Вечканов рассматривает как влияют внешнеэкономические аспекты на экономическую безопасность [Величканов]. Белорусские представители науки В.Г Булавко, П.Г Никитенко, С.Ю. Солодовников; Л.П. Шахотько; В.Г Гусаков, З.М Ильина, Н.Н.Батова, Л.Т Енчик С. А. Кондратенко; Г.Т Кулаков, В.М Цилибина, Левкевич В.Е., Пилецкий К.В., Иванов Ф.Ф. рассматривают проблемы, связанные с формированием организационно-экономического механизма обеспечения экономической безопасности [3]. Актуальность исследования обусловлена необходимостью установления в деятельности таможенных органов Республики Беларусь механизмов по защиты экономической безопасности страны.

Основная часть

Экономическая безопасность является одним из основных приоритетов любого государства. Значение и роль экономической безопасности состоят в том, чтобы формировать и укреплять позиции государства в глобальной мировой системе интересы государства соблюдаются и принимаются эффективные экономические решения, если достигнута экономическая безопасность страны [1; с.7]. Осуществляемые преобразования в таможенной сфере диктуются усложнением структуры международных отношений, перераспределением мировых экономических ресурсов, смещением вектора развития мировой экономики, что актуализирует проблемы экономической безопасности страны [3; с.49].

Санкционные меры, отсутствие таможенного контроля в рамках таможенного союза ЕАЭС, применением современных информационных технологий, проблемы экономического и политического характера на международном уровне вызывают необходимость более пристального внимания к вопросу экономической безопасности страны. В связи, с чем вопросы, связанные с ролью и значение таможенных органов в обеспечении экономической безопасности, преобразованием в таможенной сфере являются наиболее актуальными и практикоориентированными.

Экономическая безопасность Республики Беларусь является неотъемлемой частью национальной безопасности Республики Беларусь и представляет собой состояние экономики, при котором гарантировано, обеспечивается защищенность национальных интересов Республики Беларусь от внешних и внутренних угроз. В рамках поддержания экономической безопасности также реализуются потребности государства по защите сбалансированных интересов личности, общества и государства в целях обеспечения конституционных прав, свобод, высокого качества жизни граждан, а также независимости, территориальной целостности, суверенитета и устойчивого развития Республики Беларусь [5].

Функцию по обеспечению в пределах своей компетенции экономической безопасности Республики Беларусь, защиту ее экономических интересов выполняют таможенные органы Республики Беларусь [6, ст.12].

Главной стратегической целью развития таможенной службы Республики Беларусь определено обеспечение безопасности в сфере внешнеэкономической деятельности и содействие внешней торговле. Таким образом, можно выделить следующие приоритетные задачи в деятельности таможенных органов: повышение уровня экономической безопасности страны, обеспечение полноты поступлений в республиканский бюджет доходов от деятельности таможенных органов, создание благоприятных условий для ведения бизнеса и привлечения инвестиций в национальную экономику, защита интересов отечественных производителей и максимальное содействие их внешнеторговой деятельности за счет повышения качества таможенного администрирования [7].

Таможенные органы Республики Беларусь в своей деятельности руководствуются не только законодательством Республики Беларусь в сфере таможенного регулирования. Поскольку Республика Беларусь является государством-участником Евразийского экономического союза, основным правовым актом в сфере таможенного регулирования выступает Таможенный кодекс Евразийского экономического союза (далее – ТК ЕАЭС). В ТК ЕАЭС закреплено, что таможенные органы в пределах своей компетенции на территории Евразийского экономического союза обеспечивают выполнение задачи по защите национальной безопасности государств-членов [5, ст.351]. Таким образом, создание единого экономического пространства в рамках Евразийского экономического союза не снимает с таможенных органов Республики Беларусь функции по обеспечению в пределах своей компетенции экономической безопасности Республики Беларусь и защиты ее экономических интересов. Такая реалия требует от таможенных органов системного подхода, к выполнению возложенных на них функций и задач.

В целях обеспечения выполнения данных задач одной из функций таможенных органов является совершение таможенных операций и

проведение таможенного контроля, в том числе в рамках оказания взаимной административной помощи. Совокупность совершаемых таможенными органами действий, направленных на проверку и (или) обеспечение соблюдения международных договоров и актов в сфере таможенного регулирования и законодательства государств-членов о таможенном регулировании является таможенным контролем. [8, ст.2]

На состояние экономической безопасности и таможенного дела существенное влияние оказывают внешние факторы. В связи с этим необходима системная работа по недопущению перемещения товаров и транспортных средств с нарушением законодательства в сфере таможенного регулирования. Это в свою очередь, позволяет определить, таможенный контроль как один из основных инструментов, направленных на обеспечение экономическую безопасность. Необходимость проведения эффективного таможенного контроля не должна негативно сказываться на развитии внешнеэкономической деятельности, но должна обеспечивать экономическую безопасность. Основным элементом, направленным на обеспечение баланса эффективности таможенного контроля и интересов участников внешнеэкономической деятельности является система анализа и управления рисками (далее – СУР), позволяющая проводить таможенный контроль исходя из принципа выборочности и ограниченности только теми формами таможенного контроля, которые достаточны для обеспечения соблюдения законодательства. [7] СУР позволяет эффективно использовать ресурсы таможенных органов, повышая качество и эффективность таможенного контроля, поскольку направлена на проведение таможенного контроля в минимальном объеме, обеспечивающем соблюдение законодательства. Таможенный контроль после выпуска товаров позволяет выработать механизм обеспечивающий экономические интересы государства и интересы добросовестных участников внешнеэкономической деятельности, в части временных и материальных затрат, связанных с выпуском товаров. Реалиям времени будет отвечать проведение таможенного контроля с использованием информационных технологий на всех его этапах, что будет способствовать развитию механизма прослеживаемости товаров, таможенного аудита. Прослеживаемость товаров позволит обеспечить легальный оборот товаров, что положительно скажется на полноте и своевременности уплаты таможенных платежей. Развитие межведомственного информационного взаимодействия между всеми органами, осуществляющими контрольно-надзорную деятельность на границе, позволит сделать механизм таможенного контроля эффективным и оперативным, что минимизирует издержки внешнеэкономической деятельности. На решение это задачи направлено электронное предварительное информирование. Электронный документооборот таможенных органов с

субъектами внешнеэкономической деятельности также сокращает их материальные издержки.

На эффективность, проводимого таможенного контроля, полноту и своевременность уплаты таможенных платежей влияет и взаимодействие с таможенными органами государств-членов ЕАЭС. Поскольку необходимая информация для принятия решения таможенным органов Республики Беларусь в ряде случаев может быть предоставлена только таможенными органами государств-членов ЕАЭС. Такое сотрудничество осуществляется в рамках информационного взаимодействия, а также в рамках заключенных международных соглашений и ТК ЕАЭС. Взаимодействие таможенных органов с таможенными органами государств-членов ЕАЭС призвано не только разрешать, стоящие перед таможенными органами Республики Беларусь задачи, но обеспечивает защиту экономических интересов Республики Беларусь в рамках ЕАЭС.

В настоящее время наиболее актуальными являются вопросы, противодействия санкционным мерам, принимаемым в отношении страны. Установленный запрет на перемещение по территории Республики Беларусь грузовых автомобилей и тягачей, зарегистрированных в государствах – членах Европейского союза постановлением Совета Министров Республики Беларусь от 22 апреля 2022 г. № 247 «О перемещении транспортных средств», потребовал от таможенных органов принятия организационно-информационных мер по его безусловному выполнению.

Выполнение возложенных на таможенные органы задач и функции, обеспечивает экономическую безопасность Республики Беларусь, защиту ее экономических интересов. Следовательно, эффективность функционирования таможенных органов предопределяет уровень экономической безопасности.

Заключение

Таможенные органы, осуществляя таможенный контроль, вносят свой вклад в экономическую безопасность. Выполняя фискальную функцию по контролю за своевременностью и полнотой уплаты таможенных платежей таможенные органы обеспечивают формирование доходной части бюджета. Применение нетарифных мер таможенного регулирования обеспечивает защиту национальных товаропроизводителей, наличие на рынке товаров соответствующего качества. Внедрение цифровых технологий и электронного взаимодействия с представителями бизнеса и государственными органами ведет к сокращению издержек при совершении внешнеэкономических операций. Прозрачность и надежность транзитных перевозок позволяет обеспечить наличие на товарном рынке легально ввезенной продукции. Развитие предварительного информирования минимизируют временные и материальные затраты при проведении таможенного контроля, путем выбора его

оптимальных форм до прибытия товара. Повышение эффективности таможенного контроля предопределяет необходимость совершенствования деятельности таможенных органов в части расширения сферы использования информационных технологий в таможенной деятельности, повышения эффективности таможенного администрирования, совершенствования системы управления рисками, дальнейшей реализации механизма прослеживаемости товаров, развития таможенного аудита, технических средств таможенного контроля. Построение цифрового общества диктует необходимость использование информационных технологий на этапе предварительного информирования, при проведении таможенного контроля до выпуска товаров и таможенного контроля после выпуска товаров. Информационно-технологическое совершенствование работы таможенных органов должно включать в себя информационное взаимодействие с иными государственными органами, таможенными органами ЕАЭС и субъектами таможенных отношений.

Библиографический список

1. Васильева Л. П. Экономическая безопасность: определения и сущность // Журнал прикладных исследований. – 2020. – № 3. – с.6-14 – [Электронный ресурс] – Режим доступа: https://pegaspress.ru – Дата доступа: 25.05.2022.
2. Лукашин В.И. Экономическая безопасность : учебно-практическое пособие / В.И. Лукашин. – М.Моск.гос.ун-т экономики, статистики и информатики, 1999. – 134с.
3. Экономическая безопасность : теория, методология, практика / под науч. Ред. Никитенко П.Г., Булавко В.Г.; Институт экономики НАН Беларуси. – Минск : Право и экономика, 2009. – 394с.
4. Пилипчук В.В., Плоткина Н.П. Роль таможенных органов в обеспечении экономической безопасности страны. – 2020. – № 2. – с.48-59 – [Электронный ресурс] – Режим доступа: https://vfrta.customs.gov.ru – Дата доступа: 25.05.2022
5. Указ Президента Республики Беларусь от 09 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» СПС «КонсультантПлюс: Беларусь» : [Электронный ресурс]. – 2022.
6. Закон Республики Беларусь от 10 января 2014 г. № 129-з «О таможенном регулировании в Республике Беларусь» СПС «КонсультантПлюс: Беларусь» : [Электронный ресурс]. – 2022.
7. Информация о деятельности Евразийской экономической комиссии // Официальный сайт Евразийской экономической комиссии [Электронный ресурс]. – 2021. – Режим доступа: http://www.eurasiancommission.org. – Дата доступа: 25.05.2022.
8. Таможенный кодекс Евразийского экономического союза СПС «КонсультантПлюс: Беларусь» : [Электронный ресурс]. – 2022.
9. Постановление Совета Министров Республики Беларусь от 22 апреля 2022 № 247 «О перемещении транспортных средств» СПС «КонсультантПлюс: Беларусь» : [Электронный ресурс]. – 2022.

УДК 349:681

РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В СЕТИ ИНТЕРНЕТ КАК ФАКТОР ПОДДЕРЖАНИЯ КИБЕРБЕЗОПАСНОСТИ: ТЕОРЕТИКО- И СРАВНИТЕЛЬНО-ПРАВОВОЕ ОСМЫСЛЕНИЕ

В.П. Сухопаров

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье комплексно исследуется проблематика регулирования информационных отношений в сети Интернет, включая теоретические, международно-правовые, зарубежные и национальные аспекты данного регулирования, а также дефинитивный анализ кибербезопасности как одного из регулируемых информационным правом направлений. Автор выявляет проблемы терминологии по теме интернет-регулирования и обосновывает необходимость в формировании единого категориального аппарата в указанной области. В результате выявляются подходы и раскрывается содержание модели системного правового регулирования интернет-отношений в современных странах.

***Ключевые слова*:** информационные правоотношения; интернет-отношения; Интернет; регулирование Интернета; модели правового регулирования; управление в киберпространстве; юрисдикция в сети Интернет; кибербезопасность.

REGULATION OF INFORMATION RELATIONS ON THE INTERNET AS A FACTOR OF MAINTAINING CYBER SECURITY: THEORETICAL AND COMPARATIVE LEGAL REFLECTION

V.P. Sukhoparov

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article comprehensively explores the problems of regulating information relations on the Internet, including theoretical, international legal, foreign and national aspects of this regulation, as well as a definitive analysis of cybersecurity as one of the areas regulated by information law. The author reveals the problems of terminology on the topic of the Internet regulation and substantiates the need for the formation of a single categorical apparatus in this area. As a result, approaches are identified and the content of the model of systemic legal regulation of Internet relations in modern countries is revealed.

Keywords: information legal relations; Internet relations; Internet; regulation of the Internet; models of legal regulation; management in cyberspace; jurisdiction on the Internet; cybersecurity.

Проблематика регулирования информационных отношений в сети Интернет в контексте поддержания кибербезопасности является в достаточной степени широкой и комплексной, т. к. напрямую касается таких межотраслевых юридических аспектов, как:

– источники международного права, регулирующие информационную сферу глобальной компьютерной сети;

– зарубежный и национальный опыт регулирования интернет-отношений;

– нормативно-правовое обеспечение кибербезопасности в системе источников правового регулирования информационных отношений в сети Интернет;

– правотворческие направления по регулированию информационных отношений в сети Интернет, включая кибербезопасность; а также ряд других.

Сложность и комплексность выбранной темы обусловлена также системой научных терминов, используемых в данной области, а также некоторым «сужением» объекта настоящего исследования информационно-правовой характеристикой. Система научных терминов в отношении регулирования информационных отношений в сети Интернет обусловлена, во-первых, тем, что первоначально глобальная компьютерная сеть как система объединенных компьютерных сетей, обеспечивающая доступ к информации, ее хранению и обмену по всему миру, формировалась как *саморегулируемая* (курсив здесь и далее – авт. В.С.) информационно-технологическая и социальная среда. J. P. Barlow, соучредитель Фонда электронных границ, известный своим эссе «Декларация независимости киберпространства», написанным в ранние годы функционирования сети Интернет [1], отмечал, что юридические категории собственности, свободы выражения, личности, «передвижения» не применимы в глобальной компьютерной сети, ведь они основываются на материи, которой нет в Интернете. При этом, по «декларативному» мнению J. P. Barlow, киберпространство состоит из транзакций и отношений и облекается в «стойкую волну» виртуальных коммуникаций, выражающихся «везде и нигде», вне границ, установленных государствами, которые «не имеют морального права» управлять киберпространством [2].

Феномен саморегулирования интернет-отношений, т. е. регулирование фактически без вмешательства права и государства в интернет-пространство, обусловил рассмотрение данного вопроса в правовых исследованиях функционирования глобальной компьютерной сети и формирующихся в ней общественных отношений в историческом контексте, а также в обоснование свободы развития интернет-отношений без излишней правовой регламентации.

По мере развития интернет-отношений в русле саморегулирования и предпринимаемых государствами мер по управлению в киберпространстве на практике начала реализовываться идея *сорегулирования* (совместного регулирования), суть которого заключается в сочетании законодательного регулирования с саморегулированием интернет-отношений [3, с. 39; 4, с. 38]. Соответственно, стали применяться и исследоваться правотворческие подходы и модели правового регулирования общественных отношений, в том числе информационных, в сети Интернет. *Саморегулирование, сорегулирование и правовое регулирование интернет-отношений формируют таким образом систему научных терминов, относящихся к регулированию интернет-пространства*. Причем эта система не ограничивается указанными феноменами, а включает в себя и другие социальные и технические регуляторы.

Еще русский дореволюционный профессор Н. М. Коркунов подразделял все «человеческие» нормы на две главные группы: нормы этические и нормы технические, относя к последним нормы о том, как «построить здание» и другие правила технологического, естественно-научного и ремесленного содержания, направленные на достижение конкретных целей [5, с. 30–31]. Совершенно естественно, что глобальная компьютерная сеть Интернет (являясь информационно-технологическим достижением, включающим технические составляющие) поддерживается, ограничивается, а, значит, и регулируется технологическими и техническими возможностями и границами. Как отмечается в науке, активность пользователей в Интернете регулируется, в частности, правилами цифровых платформ «при помощи кода, составляющего архитектуру всей Сети и отдельных ее компонентов»; код, в свою очередь, выполняется программным обеспечением и аппаратными средствами [6, с. 17; 7, с. 121].

В зависимости от общественной среды, в которой используется Интернет, различается и степень влияния различных социальных регуляторов интернет-отношений. К примеру, в Израиле существует особое отношение к Интернету: «старейшины ультраортодоксальных общин Израиля полагают, что Интернет – это один из самых серьезных врагов традиций и религии государства», «в еврейских религиозных домах даже существует запрет на использование Интернета». В то же время израильские традиции и религия оказывают влияние на формирование в Израиле саморегулирования и самоцензуры в рамках информационных отношений в сети Интернет [8, с. 81].

Таким образом, говоря о саморегулировании, сорегулировании, правовом, техническом, ином социальном регулировании Интернета и формирующихся в нем общественных отношений, на наш взгляд, подразумеваются *виды регулирования* глобальной компьютерной сети и формируемого ей информационного пространства. Хотя в юридической литературе встречаются

различные формулировки относительно регулирования интернет-отношений, в том числе информационных. Поэтому одной из целей настоящей статьи является систематизация, обособление и разграничение категорий в области регулирования информационных отношений в сети Интернет.

С. В. Чубейко и Ю. А. Тимакина выделяют *«подходы»* (курсив – авт. В.С.) к регулированию правоотношений в сфере ИТ: европейский, строящийся на демократичных принципах и свободе пользования сетью, и азиатский подход с характерным контролем информационных потоков в национальных сегментах Интернета [9, с. 120]. К. В. Синкевич, рассматривая содержание отдельных норм в области регулирования интернет-сетей в общем массиве международного, зарубежного и национального нормативно-правового обеспечения интернет-отношений, также оперирует категорией «*подходов к правовому регулированию*» социальных сетей [10, с. 58–62]. А. А. Дрога и М. А. Дрога, определяя эффективные «*направления развития*» правового регулирования Интернета, по сути, говорят об информационно- и международно-правовом регулировании, а также о сорегулировании интернет-пространства [11, с. 155]. К. А. Гаджиева, анализируя международно-правовые основы регулирования онлайн-платформ в Европейском союзе, оперирует категориями основных *подходов* в отношении онлайн-платформ и приоритетных *моделей регулирования* отношений в онлайн-пространстве ЕС, определяя в качестве последних совместное регулирование и саморегулирование (исходя из позиции Европейской Комиссии) [4, с. 38].

Е. В. Михайленко пишет о трехстороннем рассмотрении в юридической литературе *возможности регулирования* интернет-отношений: «отказ от любого “внешнего” вмешательства в Интернет; создание самими участниками Интернет-отношений определенных норм с последующей придачей им юридической силы; “регулирование на общих основаниях”», т. е. регулирование правом «в обычном порядке» [12, с. 17]. Как видим, под выделенными *возможностями регулирования* интернет-отношений «скрываются», по мнению автора настоящей статьи, такие *виды их регулирования*, как саморегулирование, сорегулирование и правовое регулирование общественных отношений в сети Интернет.

В качестве *предпосылок* к установлению эффективного правового регулирования в сети Интернет Е. В. Михайленко указывает: необходимость жесткого регулирования экономических и административных отношений в сети Интернет; применение либерального *подхода* к регулированию иных интернет-отношений; и др. [12, с. 17–18]. К. П. Курылев, Н. П. Пархитько, Н. Г. Смолик в отношении регулирования общественных отношений в сети Интернет применяют категорию «национального *режима регулирования*». При этом речь ведется о направлениях информационного и административного законодательства в области регулирования интернет-отношений, а

также о государственном управлении информационным пространством сети Интернет [13, с. 709–715].

Таким образом, в правовых исследованиях имеет место многообразная терминология в отношении регулирования интернет-пространства. С учетом вышеизложенного нами насчитывается более 5 формулировок, касающихся регулирования отношений в сети Интернет. Среди них:

1) подходы к правовому регулированию;

2) модели регулирования;

3) направления правового регулирования;

4) возможности регулирования;

5) режим регулирования;

6) предпосылки к правовому регулированию;

7) а также выдвинутый нами термин «виды регулирования» интернет-отношений.

При этом подчеркнем, что выявленные вариации терминов не обозначают различные правовые аспекты регулирования интернет-пространства, а, напротив, указывают на достаточно близкие по значению элементы и проявления регулятивного воздействия в сети Интернет. Это обусловливает необходимость приведения в единообразие категориального аппарата по теме регулирования интернет-отношений, что позволит более точно и упорядоченно раскрыть ее и выявить перспективы развития в этой области. Принципиальным в формировании единообразного категориального аппарата, характеризующего регулирование общественных отношений, в том числе информационных, в сети Интернет, является не только «предметная» часть категории (например, «подход», «направление» или «модель» регулирования), но и наделение ее «правовым» признаком. Ведь в регулирование интернет-пространства включается саморегулирование, сорегулирование, техническое и иные виды регулирования (как было отмечено нами выше).

Наиболее точными по значению терминами представляются нам *«виды регулирования»* глобальной компьютерной сети Интернет и формирующихся в ней отношений; *«подходы к правовому регулированию»; «модели правового регулирования»* информационных отношений в сети Интернет; *«направления правового регулирования»* интернет-отношений. Последняя категория в зависимости от признания за интернет-правом самостоятельного характера может быть также сформулирована как *«сферы» или «институты правового регулирования»* интернет-отношений. Соответственно, в зависимости от рассмотрения интернет-права в качестве комплексной подотрасли информационного права к первой категории (*«виды регулирования» сети Интернет и интернет-отношений*) можно также добавить термин *«виды правового регулирования»* общественных отношений в сети Интернет, который будет указывать на отраслевую принадлежность правового

регулирования отдельных групп интернет-отношений (международно-, гражданско-, хозяйственно-, административно-правовое регулирование и др.).

Раскроем суть выдвинутых нами понятий категориального аппарата в области регулирования информационных отношений в сети Интернет. Однако здесь следует обратить внимание на обозначенное нами в начале статьи «сужение» объекта настоящего исследования информационно-правовой характеристикой интернет-отношений. Дело в том, что в сети Интернет находят свое выражение не только информационные правоотношения, но и правоотношения других отраслей (конституционное, административное, гражданское, банковское и др.) и даже правовых систем (международное, европейское право). Однако в рамках настоящей статьи нами была поставлена цель раскрыть регулирование именно информационных отношений в сети Интернет (в контексте поддержания кибербезопасности). Следовательно, при анализе категорий в отношении регулирования интернет-отношений внимание будет обращаться на их информационно-правовой аспект.

Важно также оговорить, что, с одной стороны, информационные правоотношения в сети Интернет – это более узкая правовая категория (в сравнении с правоотношениями в сети Интернет в целом), но с другой – включает в себя правоотношения, непосредственно связанные с сетью Интернет, элементами, уровнями его архитектуры, а также особенностями его функционирования, помимо иных информационных правоотношений в сети Интернет (оборот информации в сети Интернет, функционирование электронных библиотек, блогосфера и др.). Это связано с тем, что глобальная компьютерная сеть Интернет рассматривается в качестве объектов информационного права и должна им быть, как минимум, по причине того, что сеть Интернет является примером информационной сети (глобальной). По причине включения правоотношений, непосредственно возникающих по поводу сети Интернет, элементов ее архитектуры и иных особенностей, информационные правоотношения в некотором смысле могут охватывать правоотношения иных отраслей права. К примеру, блокировка Правительством Китайской Народной Республики иностранных веб-сайтов (CNN, BBC, Washington Post, Yahoo! и др.) на территории Китая [14, с. 112–113] является, с одной стороны, государственно-управленческим актом и находится в сфере административного права, а с другой – может рассматриваться как публичное информационно-правовое действие в сети Интернет. В силу вышеизложенного границы между информационными правоотношениями в сети Интернет и правоотношениями иных отраслей права в сети Интернет имеются, но, с нашей точки зрения, не являются жесткими, носят условный характер и во многом обусловлены комплексностью информационного права.

В качестве одного из подходов к правовому регулированию информационных отношений в сети Интернет может быть рассмотрен международно-правовой, значение которого заключается в определении того, каким образом должна быть разделена юрисдикция государств в киберпространстве. Отнесение данного вопроса к подходу, а не к модели правового регулирования интернет-отношений связано с тем, что подход является «способом рассмотрения какой-либо проблемы» [15] в то время, как модель представляет собой конструкцию, форму, в которой выражается правовое регулирование интернет-отношений. Модель правового регулирования отражает связь с видами и предметами источников права в сфере интернет-отношений, а также с их количеством и степенью их системности, разрозненности и (или) обособленности. Таким образом, подход к правовому регулированию интернет-отношений – это «концептуальная» установка, способ, публично-правовое решение, предопределяющее содержание правового регулирования интернет-отношений, облекаемое в определенную модель (форму).

На уровне Европейского союза концепция суверенитета в киберпространстве основывается, в частности, на финальном докладе открытой рабочей группы по развитию в области информации и телекоммуникаций в контексте международной безопасности, рассмотренном 10 марта 2021 г. Генеральной Ассамблеей ООН (доклад также известен как UN OEWG-report) [16, с. 114; 17]. Согласно рекомендациям данного документа государства не должны сознательно поддерживать ИКТ-деятельность вразрез с их обязательствами по международному праву, т. е. запрещается намеренное разрушение критической инфраструктуры или ее использования и функционирования. Государства должны продолжать усиливать меры по защите всей критической инфраструктуры от ИКТ-угроз, повышать обмен опытом в части защиты критической инфраструктуры [17].

Согласно другим международно-правовым положениям, также используемым на уровне Европейского союза, международное право применяется в сфере использования ИКТ государствами на основе следующих принципов:

– государства обладают юрисдикцией над ИКТ-инфраструктурой, размещенной в пределах своих территорий;

– в рамках использования ИКТ государства должны соблюдать принципы международного права, включая принцип суверенитета государств и их суверенного равенства, принцип разрешения споров мирными средствами, а также принцип невмешательства государства во внутренние дела другого;

– государства не могут использовать полномочия для совершения международных неправомерных действий с использованием ИКТ и должны

стремиться к обеспечению того, чтобы их территории не использовались негосударственными субъектами для совершения таких действий [16, с. 114–116].

Территория государства как указатель его юрисдикции в отношении информационных правоотношений в сети Интернет принимается во внимание Европейским Судом по правам человека. Так, ЕСПЧ в 2005 г. постановил, что пребывание лица в одном государстве и его деятельность в сети Интернет на территории этого же государства влечет за собой однозначную необходимость соблюдения правил государства пребывания [18, с. 7]. Однако данная позиция не до конца объясняет, как определяется юрисдикция государства в случаях, когда распространение информации в сети Интернет рассчитано на зарубежную аудиторию пользователей.

К обозначенной проблеме был разработан, в частности, американский подход, суть которого заключается в следующем: юрисдикция государства, прежде всего, «фокусируется» вокруг информации. «Ориентирование» интернет-ресурса служит главным в понимании применимости права определенного государства. Несмотря на глобальность доступа к интернет-ресурсам, большинство из них ориентировано на конкретный регион. Также во внимание могут приниматься закрытые группы интернет-пользователей в рамках регионов. Весьма важным аспектом международно-правового подхода к регулированию информационных отношений в Интернете является язык веб-страницы. Если же содержание информационных материалов в сети Интернет рассчитано на «глобальное восприятие», то важное значение для юрисдикции будет иметь влияние на субъекта правоотношения [18, с. 8].

Резюмируя вышеизложенное, отметим, что американский концептуальный подход к международно-правовому регулированию информационных отношений в сети Интернет основывается на таких юридических свойствах информации, как территориальный фактор ее влияния на аудиторию, непосредственно субъектный состав, для которого информация распространяется в Интернете, а также учет негативных последствий для потерпевшей стороны от распространенной информации. Учет данных свойств информации, распространяемой в сети Интернет и носящей трансграничный характер, представляется обоснованным в формировании международно-правового подхода к регулированию интернет-отношений. Однако, на наш взгляд, требуется его конкретное закрепление и механизм реализации на международно-правовом уровне. На сегодняшний день эффективным в правоприменительном плане видится применимость норм международного публичного и частного права к интернет-отношениям, включая принцип распространения суверенитета государства на соответствующую территорию, а, значит, и ИКТ-инфраструктуру, размещенную в пределах данной

территории, а также положение о том, что права и обязанности по обязательствам, возникающим вследствие причинения вреда, определяются по праву страны, где имело место действие или иное обстоятельство, послужившее основанием для требования о возмещении вреда (п. 1 ст. 1129 ГК Республики Беларусь) [19; 20].

Помимо международно-правового подхода к регулированию интернет-отношений, можно выделить также национальные правовые подходы, которых, как уже было отмечено, имеется несколько: 1 – характеризующийся либеральными методами регулирования интернет-отношений; 2 – азиатский с характерным контролем над информационными потоками в национальном сегменте Интернета [9, с. 120]. С нашей точки зрения, данные подходы не влияют на модели правового регулирования информационных отношений в сети Интернет, поскольку заключаются не в специфике формально-юридического закрепления интернет-регулирования, а в методах управления национальным интернет-пространством и сущностно определяют содержание законодательства в сфере регулирования интернет-отношений.

Говоря о моделях правового регулирования информационных отношений в сети Интернет, следует учитывать факт, констатируемый в научной литературе по интернет-праву в абсолютном большинстве источников: «ни в одной стране мира нет кодифицированного законодательства по Интернету» [11, с. 154]. Как отмечают А. А. Дрога и М. А. Дрога, действующие нормативные акты регулируют частные аспекты функционирования сети, в числе которых вопросы подключения к ней через поставщиков интернет-услуг, предоставления соответствующих линий связи и т.д. Нормы, применяемые в отношении интернет-пространства, содержатся в законодательных актах различных отраслей права [11, с. 154].

Изложенные теоретические положения указывают на распространенную в современных странах модель правового регулирования отношений, в том числе информационных, в сети Интернет, представляющую собой не единый кодифицированный нормативный правовой акт по интернет-праву, а систему нормативных правовых актов, регулирующих отдельные аспекты или группы общественных отношений в сети Интернет. Данная система, на наш взгляд, обусловлена комплексностью информационных и интернет-правоотношений и действует в противовес идее кодификации и (или) консолидации законодательства в сфере регулирования общественных отношений в сети Интернет. Рассматриваемая тенденция является обоснованной, поскольку виртуальное пространство восприняло многие сферы фактических общественных отношений и существует «параллельно» (наряду) с ними, а потому не может ни заменить законодательство, ни продублировать его. Иными словами, имеется потребность:

1) в специальном правовом регулировании отдельных аспектов информационных отношений в сети Интернет;

2) в уточняющем правовом регулировании данных отношений, т. е. дополняющем условно «общее» правовое регулирование общественных отношений конкретной сферы (как, например, нормы законодательства о защите интеллектуальной собственности в информационной сфере сети Интернет);

3) а также в правовом регулировании интернет-отношений «общими» нормами права, которые прямо не уточняют их применение в интернет-пространстве, но и не исключают его.

Указанные способы правового регулирования информационных отношений в сети Интернет отражают устоявшуюся модель их правового регулирования, заключающуюся в системе нормативных правовых актов, которые по причине их некодифицированности регулируют интернет-отношения именно такими способами. Ведь в случаях разнородности и обширности групп регулируемых общественных отношений в законодательстве формируется соответствующая система нормативных правовых актов, среди которых имеются:

1) специальные;

2) содержащие отдельные нормы права, применяемые в определенных сферах (т. е. в норме права имеется прямое указание на сферу применения);

3) а также содержащие нормы права, которые могут быть применены в определенных сферах, поскольку из содержания норм не следует обратного.

Для стран СНГ характерна модель системного правового регулирования информационных отношений в сети Интернет.

Так, в Азербайджанской Республике отдельные аспекты интернет-отношений регулируются законодательством в области телекоммуникаций, СМИ, чрезвычайных ситуаций (к примеру, Министерству транспорта, связи и высоких технологий разрешено приостанавливать оказание интернет-услуг в случаях нарушения абонентами законодательства в области телекоммуникаций). В Республике Армения законодательство в сфере регулирования сети Интернет и телекоммуникаций не слишком обширно и включает в себя, в частности, Закон Республики Армения от 8 июля 2005 г. «Об электронной коммуникации» и Закон Республики Армения от 25 декабря 2003 г. «О комиссии по регулированию общественных услуг». В Республике Казахстан законодательным актом, регулирующим правоотношения в интернет-пространстве, является Закон Республики Казахстан от 10 июля 2009 г. № 178-IV «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационно-коммуникационных сетей». Помимо этого, интернет-отношения в Казахстане регулируются законодательством о связи. В Киргизской Республике отдельные аспекты распространения информации в сети Интернет регулируются

Законом 2005 г. «О противодействии экстремистской деятельности», Законом 2021 г. «О защите от недостоверной (ложной) информации». В Республике Молдова основным нормативным правовым актом, регулирующим интернет-отношения и телекоммуникации, является Закон 2008 г. «Об электронной связи». При этом законодательство Молдовы о прессе не регулирует деятельность сетевых изданий, блогосферу и не распространяется на интернет-ресурсы СМИ. Также в Республике Молдова отсутствует специальный закон об информации. В Туркменистане действуют законы о правовом регулировании развития сети Интернет и оказания интернет-услуг, о связи, об информации и ее защите. С января 2007 г. законодательство Республики Узбекистан о СМИ приравнивает интернет-ресурсы к СМИ. Отдельные аспекты интернет-отношений в Узбекистане регулируются и другими законами, в частности Законом Республики Узбекистан от 2 июля 2019 г. № ЗРУ-547 «О персональных данных». Во многом регулирование и управление национальным сегментом Интернета в Узбекистане осуществляется через исполнительную ветвь власти [13, с. 709–715].

В Российской Федерации к системе законодательства в области регулирования информационных правоотношений в сети Интернет относятся следующие нормативные правовые акты:

1) Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»;

2) законы, вносящие изменения в указанный Закон об информации, в частности вносящие изменения в части необходимости удаления ссылок на информацию (недостоверную, неактуальную, распространенную с нарушением законодательства) о гражданах из поисковой выдачи по их требованию. Также это «Закон о блогерах», на основании которого к владельцам страниц в сети Интернет стали применяться ограничения, установленные в России для СМИ;

3) Федеральный закон № 139-ФЗ от 28 июля 2012 г., на основании которого был создан «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов»;

4) Федеральный закон № 114-ФЗ от 25 июля 2002 г. «О противодействии экстремистской деятельности»;

5) Федеральный закон № 3-ФЗ от 8 января 1998 г. «О наркотических средствах и психотропных веществах», запрещающий распространение сведений о наркотических средствах, психотропных веществах и их прекурсорах, способах их разработки и использования посредством информационно-телекоммуникационных сетей;

6) Гражданский кодекс Российской Федерации (в части регулирования вопросов авторского права, запрета клеветы в сети Интернет);

7) Уголовный кодекс Российской Федерации и др. [8, с. 75–77; 21, с. 68–72; 22, с. 94].

В ряде других зарубежных стран также реализуется модель системного правового регулирования информационных отношений в сети Интернет.

В Соединенном Королевстве законодательство в области интернет-пространства составляют: Закон 2010 г. «О цифровой экономике», касающийся защиты авторских прав в сети Интернет, правового статуса и ответственности провайдеров, владельцев сайтов и интернет-пользователей; Закон 2003 г. «Об электронных коммуникациях»; Закон «О непристойных выражениях» [8, с. 79].

В США к нормативным правовым актам, регулирующим интернет-отношения, относятся: Закон 1998 г. «Об авторском праве цифрового тысячелетия»; Закон 1999 г. «Об информационно-технологической поддержке правоохранительных органов»; Закон 2000 г. «О защите прав детей в Интернете»; Закон «О противодействии насилию женщин и о полномочиях Департамента юстиции» (в соответствии с которым запрещается анонимная рассылка «раздражающих» сообщений и публикация комментариев «оскорбительно-раздражающего» характера в сети Интернет); Закон «О мошенничестве и злоупотреблении с использованием компьютеров»; Национальная кибер-стратегия США [8, с. 79–80; 9, с. 119; 23, с. 39].

Частный аспект регулирования кибербуллинга в Австралии также указывает на системную модель правового регулирования информационных отношений в сети Интернет. A. Srivastava и J. Boey пишут, что в условиях отсутствия в Австралии специального законодательства в области кибербуллинга составляющие его общественные отношения регулируются в контексте уголовной или гражданско-правовой ответственности [24, с. 309]. Следовательно, к отношениям в области кибербуллинга в Австралии применяется система правовых норм, защищающих честь и достоинство личности, в том числе в сети Интернет.

В Германии, в частности, действует Закон от 30 июня 2017 г. «Об улучшении правоприменения в социальных сетях», согласно которому провайдеры крупных социальных сетей (Facebook, Instagram, Twitter и др.) обязаны удалять противозаконный контент, а также предоставлять полугодовые отчеты об обработке жалоб на него и опубликовывать данные отчеты в Федеральном вестнике, а также на соответствующем сайте не позднее 1-го месяца после отчетного полугодия [9, с. 120; 10, с. 60].

В Новой Зеландии действует Закон 2015 г. № 63 «О негативном воздействии цифровых коммуникаций», который устанавливает ответственность за оскорбления в сети Интернет, которую несут как владельцы интернет-ресурсов, содержащих оскорбительные комментарии, так и лица, непосредственно причинившие вред посредством цифрового общения [8, с. 81–82].

В Республике Беларусь также реализуется системная модель правового регулирования информационных правоотношений в сети Интернет, которую составляют следующие нормативные правовые акты: Конституция Республики Беларусь; Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»; Указ Президента Республики Беларусь от 18 сентября 2019 г. № 350 «Об особенностях использования национального сегмента сети Интернет»; Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь»; Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»; Закон Республики Беларусь от 17 июля 2008 г. № 427-З «О средствах массовой информации»; Закон Республики Беларусь от 17 мая 2011 г. № 262-З «Об авторском праве и смежных правах»; Кодекс Республики Беларусь об административных правонарушениях; Уголовный кодекс Республики Беларусь; постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» и др.

Таким образом, распространенная современная модель системного правового регулирования информационных отношений в сети Интернет является показательной с точки зрения практичности и эффективности правового регулирования указанных отношений, поскольку информационное пространство сети Интернет является достаточно обширным и касается широкого круга аспектов и групп общественных отношений. Тесная связь последних с информацией и сетью Интернет не дает им «обойти» систему правового регулирования информационных отношений в сети Интернет, которые носят комплексный характер.

Как отмечает А. С. Агейчев, помимо правоохранительных норм, применяемых в рамках интернет-отношений, «регулирование в сфере онлайн-коммуникаций в большинстве стран происходит за счет других смежных законов» [8, с. 82].

Из предметного анализа рассмотренной модели системного правового регулирования интернет-отношений в современных странах следует выделение существующих *направлений правового регулирования* в рамках данной модели, которые в контексте развития интернет-пространства важно так же развивать. При этом *направления* правового регулирования информационных правоотношений в сети Интернет в современных странах примерно одинаковые, что подтверждает правильность и результативность правового регулирования интернет-пространства, столь сложного и комплексного информационно-технологического, технического и общественного явления, находящегося «на стыке» различных видов регулирования человеческой

деятельности и ее результатов. Среди направлений правового регулирования информационных отношений в сети Интернет с учетом рассмотренного международно-правового, зарубежного и национального опыта можно выделить:

1) регулирование оборота информации в глобальной компьютерной сети Интернет (включая деятельность СМИ, блогеров в сети Интернет; противодействие распространению экстремистских материалов в сети Интернет; регулирование вопросов, связанных с недопущением распространения клеветнеческих, диффамационных сообщений в интернет-пространстве; регулирование вопросов, связанных с недопущением распространения спама; запрет распространения отдельных видов информации и др.);

2) защита персональных данных в Интернете;

3) правовая защита объектов интеллектуальной собственности в информационной сфере сети Интернет;

4) правовое регулирование использования доменных имен;

5) оказание интернет-услуг (деятельность поставщиков интернет-услуг и иных интернет-провайдеров);

6) ответственность информационных посредников и пользователей в сети Интернет;

7) деятельность государственных органов и должностных лиц в информационной сфере сети Интернет;

8) юрисдикция государств в интернет-пространстве;

9) вопросы киберпреступности и кибербезопасности;

10) и др.

Как видим, кибербезопасность представляет собой одно из направлений правового регулирования информационных отношений в сети Интернет как на международном, так и на национальных уровнях. При этом рассматриваемый социально-технологический феномен тесно связан с таким понятием, как информационная безопасность.

И. Л. Бачило, М. А. Вус, О. С. Макаров, Р. М. Юсупов в контексте рассмотрения ряда вопросов в сфере информационной безопасности обращают отдельное внимание на информационную безопасность глобальных компьютерных информационных и телекоммуникационных сетей [25, с. 6–7].

Т. А. Полякова определяет информационную безопасность как состояние защищенности национальных интересов государства в информационной сфере, состоящих из совокупности сбалансированных интересов личности, общества и государства, от внутренних и внешних угроз, что соответствует принципу обеспечения национальной безопасности в информационной сфере [26, с. 19]. Следовательно, понимание информационной безопасности достаточно широкое и включает в себя кибербезопасность (в силу глобальной компьютерной сети как части информационного пространства),

а также в целом обеспечивается соблюдением международного права и законодательства в информационной сфере, поскольку в состоянии правомерных форм информационной деятельности достигается практически полная минимизация рисков наступления ИТ-угроз.

Н. О. Мороз выявляет следующую закономерность в использовании терминов «информационная безопасность» и «кибербезопасность»: в силу отсутствия универсального международно-правового регулирования сотрудничества государств в сфере информационной безопасности специального характера «сложилось два региональных подхода к определению наиболее значимых терминов в рассматриваемой сфере»: «западный», в котором преобладает использование термина «кибербезопасность» (НАТО, ОБСЕ, ЕС, ОАГ), и «восточный», в котором используется термин «информационная безопасность» (СНГ, ОДКБ, ШОС) [27, с. 124].

Использование термина «информационная безопасность» в международно-правовых актах СНГ подтверждается также тем, что среди комплекса отношений, подлежащих правовому обеспечению на уровне СНГ, кибербезопасность не выделяется.

В то же время правовое обеспечение СНГ в комплексе регулируемых информационных отношений предусматривает, в частности, «противодействие деструктивному информационному воздействию», «противодействие преступлениям в информационной сфере» и «обеспечение безопасности информации государственного значения (в том числе защита государственных секретов)» [28, с. 62].

Как подчеркивает О. С. Макаров, оценка состояния нормативного обеспечения информационных отношений государств-участников СНГ «должна учитывать ряд параметров», среди которых выделяется «регламентация системы субъектов обеспечения информационной безопасности и нормативное закрепление их функций и полномочий» [28, с. 60–61].

С нашей точки зрения, оба термина («кибербезопасность» и «информационная безопасность») применимы к состоянию защищенности использования глобальной компьютерной сети, ее национальных сегментов, интересов субъектов информационных правоотношений в сети Интернет.

Применение термина «кибербезопасность» в отношении глобальной компьютерной сети Интернет обусловлено ее информационно-технологической и технической природой. Применение термина «информационная безопасность» к сети Интернет обусловлено информационным пространством Интернета, которое составляет значительную часть информационной сферы, охраняемой информационным правом.

Подытожим:

1. К *видам* регулирования информационных отношений в сети Интернет относятся: саморегулирование, сорегулирование, правовое

регулирование, техническое и иные виды социального регулирования указанных отношений.

Среди *подходов* к правовому регулированию информационных отношений в сети Интернет можно выделить: международно-правовой и национальные. *Международно-правовой подход* к регулированию информационных отношений в сети Интернет заключается в решении вопроса юрисдикции государств в киберпространстве. Исходя из международных документов концептуального значения (UN OEWG-report и некоторые другие) за государствами признается суверенитет над ИКТ-инфраструктурой, размещенной на их территориях, что базируется на общепризнанных принципах международного права. Встречаются также научные концепции применения норм права определенного государства к интернет-отношениям в связи природой, ориентированностью информации, размещенной в Интернете, на конкретную территорию и (или) аудиторию, языком распространяемой информации, причиненным вредом гражданину. Однако конкретного международно-правового закрепления данные идеи пока еще не нашли, хотя этот факт не умаляет их обоснованности.

На наш взгляд, данные концепции так или иначе основываются на общепризнанных принципах международного права, а также действующих нормах международного частного права и коллизионных привязках (в первую очередь, касающихся обязательств из причинения вреда). Среди *национальных подходов* к правовому регулированию интернет-отношений существует два основных: либеральный; и характеризующийся контролем информационных потоков в национальных сегментах Интернета со стороны государства.

2. На сегодняшний день в современных странах находит свое выражение и реализацию *модель системного правового регулирования* информационных отношений в сети Интернет, заключающаяся в системе нормативных правовых актов по вопросам регулирования интернет-отношений. Данный факт обусловлен комплексностью информационного и интернет-права и представляется перспективным для развития, поскольку интернет-отношения существуют параллельно с фактическими отношениями материального мира, которые формируют обширный круг социальных взаимодействий различной природы и характера.

Среди *направлений* правового регулирования информационных отношений в сети Интернет можно выделить: регулирование оборота информации в глобальной компьютерной сети Интернет; защита персональных данных в Интернете; правовая защита объектов интеллектуальной собственности в информационной сфере сети Интернет; правовое регулирование использования доменных имен; оказание интернет-услуг (деятельность поставщиков интернет-услуг и иных интернет-провайдеров); ответственность

информационных посредников и пользователей в сети Интернет; деятельность государственных органов и должностных лиц в информационной сфере сети Интернет; юрисдикция государств в интернет-пространстве; вопросы киберпреступности и кибербезопасности; и др.

3. Феномен кибербезопасности имеет несколько значений: направление правового регулирования интернет-отношений; состояние защищенности глобальной компьютерной сети и формирующихся в ней отношений от ИКТ-угроз (как вид информационной безопасности); и в широком смысле – как «цель» правового регулирования интернет-отношений, достигаемая полным соблюдением норм международного права и национальных законодательств в сфере киберпространства.

Библиографический список

1. Boyle, J. The Past and Future of the Internet: A Symposium For John Perry Barlow [Electronic resource] / J. Boyle // Duke Law and Technology Review. – 2019. – Vol. 18. – Mode of access : https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1336&context=dltr. – Date of access : 15.08.2022.

2. Barlow, J.P. A Declaration of the Independence of Cyberspace / J.P. Barlow // Duke Law & Technology Review. – 2019. – Vol. 18. – Mode of access :

https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1337&context=dltr. – Date of access : 17.08.2022.

3. Леанович, Е.Б. Проблемы правового регулирования интернет-отношений с иностранным элементом / Е.Б. Леанович // Белорус. журн. междунар. права и междунар. отношений. – 2000. – № 4. – С. 39–44.

4. Гаджиева, К.А. Правовое регулирование онлайн-платформ в Европейском союзе / К.А. Гаджиева // Информац. право. – 2021. – № 1 (67). – С. 36–38.

5. Коркунов, Н.М. Лекции по общей теории права / Н.М. Коркунов. – 9-е изд. (без изм.). – С-Пб. : Юрид. книж. магазин Н. К. Мартынова, 1909. – 354 с.

6. Маркевич, Д.С. Некоторые аспекты государственного регулирования деятельности цифровых платформ / Д.С. Маркевич // Право.by. – 2019. – № 5 (61). – С. 16–20.

7. Lessig, L. Code Version 2.0 / L. Lessig. – New York : Basic Book. – 2006. – 410 p.

8. Агейчев, А.С. Законодательство в сфере интернет-коммуникаций: российский и международный опыт / А.С. Агейчев // Сравнительная политика. – 2016. – № 2 (23). – С. 73–84.

9. Чубейко, С.В. Особенности правового регулирования информационной сферы иностранных государств и Российской Федерации / С.В. Чубейко, Ю.А. Тимакина // Философия права. – 2019. – № 4 (91). – С. 116–121.

10. Синкевич, К.В. Современные подходы к правовому регулированию социальных сетей в цифровую эпоху / К.В. Синкевич // Юстиция Беларуси. – 2021. – № 7. – С. 58–63.

11. Дрога, А.А. Актуальные проблемы правового регулирования Интернет-пространства / А.А. Дрога, М.А. Дрога // Вестн. Омского ун-та. Сер. Право. – 2015. – № 3 (44). – С. 153–156.

12. Михайленко, Е.В. Проблемы информационно-правового регулирования отношений в глобальной компьютерной сети Интернет : автореф. дис. … канд. юрид. наук : 12.00.14 / Е.В. Михайленко ; Москов. гуманит. ун-т. – М., 2004. – 25 с.

13. Курылев, К.П. Национальные режимы регулирования сети интернет в странах СНГ / К.П. Курылев, Н.П. Пархитько, Н.Г. Смолик // Постсовет. исследования. – 2021. – Т. 4, № 8. – С. 705–718.

14. Svantesson, D.J.B. Internet Law and Policy in the People's Republic of China / D.J.B. Svantesson // Masaryk University J. of Law and Technology. – 2007. – Vol. 1, № 1. – P. 109–120.

15. Дмитриев, Д.В. Подход [Электронный ресурс] / Д.В. Дмитриев // Толковый словарь русского языка Дмитриева. 2003 г. (Словари и энциклопедии на Академике). – Режим доступа : https://dic.academic.ru/dic.nsf/dmitriev/3767/%D0%BF%D0%BE%D0%B4%D1%85%D0%BE%D0%B4. – Дата доступа : 20.08.2022.

16. Osula, A.-M. EU Common Position on International Law and Cyberspace / A.-M. Osula, A. Kasper, A. Kajander // Masaryk University J. of Law and Technology. – 2022. – Vol. 16, № 1. – P. 89–123.

17. Open-ended working group on developments in the field of information and telecommunications in the context of international security [Electronic resource] // United Nations. General Assembly. A/AC.290/2021/CRP.2. Conference room paper 10 March 2021. – Mode of access : https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf. – Date of access : 25.08.2022.

18. Heissl, G. Jurisdiction for Human Rights Violations on the Internet / G. Heissl // Europ. J. of Law and Technology. – 2011. – Vol. 2, № 1. – P. 1–15.

19. Устав Организации Объединенных Наций [Электронный ресурс] // Организация Объединенных Наций. – Режим доступа : https://www.un.org/ru/about-us/uncharter/full-text. – Дата доступа : 25.08.2022.

20. Гражданский кодекс Республики Беларусь [Электронный ресурс] : 7 дек. 1998 г., № 218-З : принят Палатой представителей 28 октября 1998 г. : одобр. Советом Респ. 19 ноября 1998 г. : в ред. Закона Респ. Беларусь от 31.12.2021 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

21. Микаева, А.С. Проблемы правового регулирования в сети Интернет и их причины / А.С. Микаева // Актуальные проблемы рос. права. – 2016. – № 9 (70). – С. 67–75.

22. Рассолов, И.М. Информационное право и информационное законодательство в условиях инновационного развития / И.М. Рассолов // Актуальные проблемы рос. права. – 2016. – № 4 (65). – С. 92–96.

23. Анисимова, А.С. Анализ правотворческой политики зарубежных стран в сфере регулирования интернет-отношений / А.С. Анисимова // Вестн. Саратов. гос. юрид. акад. – 2014. – № 5 (100). – С. 38–44.

24. Srivastava, A. Online Bullying and Harassment: An Australian Perspective / A. Srivastava, J. Boey // Masaryk University J. of Law and Technology. – 2012. – Vol. 6, № 2. – P. 299–320.

25. Макаров, О.С. Разработки модельного законодательства для сферы информационной безопасности / О.С. Макаров, Р.М. Юсупов, И.Л. Бачило, М.А. Вус // Власть. – № 11. – 2015. – С. 5–9.

26. Полякова, Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России : автореф. дис. … д-ра юрид. наук :

12.00.14 / Т.А. Полякова ; Рос. правовая акад. М-ва юстиции Рос. Федерации. – М., 2008. – 39 с.

27. Мороз, Н.О. Подходы к определению термина «информационная безопасность» в контексте международного сотрудничества / Н.О. Мороз // Право.by. – № 4 (72). – 2021. – С. 120–126.

28. Макаров, О.С. Об одном методологическом подходе к оценке состояния информационного законодательства государств – участников Содружества Независимых Государств / О.С. Макаров // Актуальные проблемы рос. права. – № 2 (51). – 2015. – С. 59–63.

УДК 341.21

ЦИФРОВЫЕ ТРАНСНАЦИОНАЛЬНЫЕ КОРПОРАЦИИ: ПРАВОВОЙ СТАТУС И ОСОБЕННОСТИ ПРИВЛЕЧЕНИЯ К ОТВЕТСТВЕННОСТИ В СЛУЧАЕ НАРУШЕНИЯ ПРАВ ЧЕЛОВЕКА

Е.В. Ребицкая

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье рассмотрены основные формы влияния цифровых транснациональных корпораций на права человека в киберпространстве, а также проанализированы имеющиеся способы привлечения транснациональных корпораций к ответственности за нарушение прав человека. Автор приходит к выводу о необходимости пересмотра статуса цифровых транснациональных корпораций на международной арене, а также наделения их функциональной правосубъектностью в случаях нарушения прав человека с целью привлечения к международно-правовой ответственности.

Ключевые слова: цифровые транснациональные корпорации, права человека, правосубъектность, киберпреступность.

DIGITAL TRANSNATIONAL CORPORATIONS: LEGAL STATUS AND PECULIARITIES OF BRINGING THEM TO RESPONSIBILITY IN CASE OF HUMAN RIGHTS VIOLATION

E.V. Rebitskaya

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article discusses the main forms of influence of digital transnational corportions on human rights in cyberspace, and also analyzes the available ways to hold transnational corporations accountable for human rights violations. The author comes to the conclusion that it is necessary to review the status of digital transnational corporations in the international arena, as well as to give them a functional legal personality in cases of human rights violations in order to bring them to international legal responsibility.

Keywords: digital transnational corporations, human rights, legal personality, cybercrime.

Цифровая трансформация всех процессов в мире, в особенности рост популярности различных социальных сетей, предоставили отдельным лицам и группам лиц неограниченное пространство для реализации своих прав и свобод. Но в тоже время появились новые проблемы, связанными с использованием цифровых технологий в преступных целях, нарушением прав

человека в киберпространстве, а также использование цифровых площадок для преднамеренного распространения дезинформации и разжигание ненависти в Интернете. За последние 25-30 лет цифровая революция привела к появлению новых субъектов на международном рынке – цифровых транснациональных корпораций (далее – цифровые ТНК) – правовой статус которых на международной арене все еще остается актуальным и дискуссионным вопросом для ученых и юристов всего мира.

Цель исследования – проанализировать влияние деятельности цифровых ТНК на реализацию прав человека в киберпространстве и возможность привлечения ТНК к ответственности за нарушение соответствующих прав и свобод граждан.

В первую очередь необходимо определиться с термином «*цифровые ТНК*». При наиболее общем подходе, выработанном Комиссией ООН по ТНК, под ТНК подразумеваются «фирмы, оперирующие в двух или более странах и управляющие зарубежными подразделениями из единого центра». Под цифровыми ТНК мы будем понимать компании, оперирующие в двух или более странах и управляющие зарубежными подразделениями из единого центра, которые осуществляют свою деятельность в цифровой форме и производят свои продукты, поставляемые в цифровом виде. Согласно классификации цифровых компаний UNCTAD (Конференции Организации Объединенных Наций по торговле и развитию), все цифровые ТНК делятся на две основные группы: фирмы ИКТ (информационно-телекоммуникационные технологии) и истинно цифровые компании. В рамках данного исследования особый интерес для нас представляют истинно цифровые компании – интернет-платформы, компании-поставщики цифровых решений, компании, занятые в электронной торговле, и производители цифрового контента. Первые две из этих групп можно назвать полностью цифровыми компаниями, так как в их бизнес-модели центральная роль принадлежит Интернету, и они полностью работают в цифровой среде. Интернет-платформы включают поисковые системы, социальные сети и другие платформы, например, для совместного использования (Alphabet, Facebook, eBay, Yahoo, Twitter, LinkedIn, Вконтакте, Одноклассники и т.д.) [1, 138].

В настоящее время интернет-платформы выступают основной площадкой нарушения прав человека в киберпространстве. По мнению белорусского ученого, С.А.Трахименко, «деятельность ТНК может стать угрозой мировоззренческого характера, способной порождать различного рода конфликты» [2, 132]. Следует отметить, что нет единого перечня прав человека, нарушение которых возможно по средством деятельности цифровых ТНК. Независимая некоммерческая исследовательская организация RAND Europe в 2021 году провела исследование «Human rights responsibilities in the digital age», в рамках которого определила потенциальную возможность

нарушения следующих прав и свобод человека в киберпространстве: право на частную жизнь; право на свободу выражения мнения; право на свободу мирных собраний и ассоциаций; право на равное участие в политической и общественной жизни государства; право на образование; право на здоровье. Эксперты отмечают, что данный список не является исчерпывающим и лишь иллюстрирует как деятельность цифровых ТНК влияет на различные сферы жизни людей [3].

Так, например, право на свободу мнений и их свободное выражение признается и гарантируется ст. 19 ВДПЧ (а также ст.10 ЕКПЧ) в равной степени защищено и в цифровой среде, поскольку оно применяется независимо от границ и через любые средства массовой информации. Согласно прецедентной практике Европейского суда по правам человека сфера действия права на выражение мнения должна толковаться широко, охватывать не только существо информации и идей, но и значительное разнообразие форм и средств, посредством которых они выражаются, передаются и получаются. Средства выражения включают Интернет и новостные интернет-порталы [4; 828]. Граждане должны иметь возможность распространять мнения и контент, делиться и выражать свои взгляды, а также получать и передавать информацию и идеи в цифровом пространстве без вмешательства со стороны государственных или частных субъектов и независимо от географических границ.

Вместе с тем, реализация вышеописанного права при определенных условиях может стать фундаментом для совершения киберпреступлений. Это побуждает правительствам принимать и осуществлять меры по мониторингу, фильтрации и блокированию распространения вредоносного контента в Интернете или по удалению вредоносного онлайн-контента, а также установления запретов на осуществление деятельности отдельным цифровым ТНК на территории страны. Так, в качестве примера рассмотрим подход «введение налогов на социальные сети» в Уганде. Стремясь ограничить поток призывов граждан к насилию в социальных сетях и укрепить национальную налоговую базу, правительство страны решило ввести налоги на использование популярных социальных сетей (Facebook, Instagram и др.). В правительстве считают, что таким образом граждан можно защитить от экстремистского контента, а также перевести пользователей на импортные мобильные приложения, что должно поспособствовать развитию экономики страны. В тоже время подобная практика, на наш взгляд, непосредственно влияет на осуществление права на свободу мнений и их свободное выражение в эпоху цифровых технологий, а также в перспективе может затронуть права, касающиеся свободы объединения и мирных собраний, а также права на участие в общественной и политической жизни. То есть с одной стороны меры по мониторингу, фильтрации и блокированию распространения

вредоносного контента в Интернете базируются на интересах национальной безопасности, общественного порядка, а также защиты прав и свобод граждан и могут способствовать развитию безопасного киберпространства и, таким образом, поощрению прав человека. Однако, с другой стороны, непропорциональные и всеобъемлющие меры по удалению онлайн-контента могут нанести серьезный ущерб свободе слова и свободе выражения мнений.

Отсюда закономерно возникает вопрос: должны ли цифровые ТНК нести ответственность за нарушение прав человека в киберпространстве и, следовательно, являются ли они субъектами киберпреступлений? В соответствии с Руководящими принципами предпринимательской деятельности в аспекте прав человека (далее – Руководящие принципы) субъекты предпринимательской деятельности (в том числе ТНК) обязаны соблюдать права человека в соответствии с политикой должной осмотрительности [5].

Изучив вышеуказанный международный акт, приходим к выводу, что ТНК не несут прямой ответственности по праву прав человека и в рамках международного права не существует механизма принуждения к исполнению, предусмотренных Руководящими принципами, обязательств (нормы Руководящих принципов носят исключительно рекомендательный характер).

На национальном уровне в законодательстве стран предусмотрены различные подходы по привлечению к ответственности ТНК за нарушение прав человека, (например, в соответствии с чешским Законом об уголовной ответственности юридических лиц, юридические лица могут привлекаться к уголовной ответственности по признаку гражданства, независимо от места совершения правонарушения) [6]. Вопрос привлечения цифровых ТНК к международно-правовой ответственности не урегулирован ни в одном международном акте, т.к. вопрос правосубъектности ТНК на международной арене все еще остается дискуссионным.

Действительно, в настоящее время за ТНК не признан статус субъекта международного права, несмотря на наличие ряда приверженцев расширения круга субъектов международного права и популярности теории «транснационального права» в западной юридической доктрине. Однако не оспоримым остается факт влияния ТНК на процессы, происходящие на международной арене, в том числе и в сфере права прав человека.

Недостаток норм, напрямую связывающих ТНК обязанностями по соблюдению международного права прав человека, является острой проблемой. Разрешение данной проблемы, на наш взгляд, возможно лишь путем пересмотра правового статуса ТНК в международном праве. В отечественной науке международного права широкое распространение получила точка зрения, согласно которой существенная особенность статуса субъекта международного права состоит в том, что он непосредственно участвует в

создании и осуществлении его норм. Второй составляющей, как указывают многие авторы, является такое свойство субъекта международного права, как наличие у него определенных прав и обязанностей [7; 213]. Кроме того, большинство ученых-юристов сходятся на мнение, что все субъекты международного права должны обладать следующими основными признаками:

- иметь права и нести обязанности в соответствии с нормами международного права;
- принимать участие в разработке норм международного права;
- заключать международные договоры.

Однако, в результате обсуждения вопроса о способности заключать международные договоры в 1962 году Комиссия международного права сделала оговорку относительно международных организаций – «способность международных организаций заключать договоры определяется уставом соответствующей организации» [8]. Так, международные организации были наделены функциональной правосубъектностью, т.е. их правосубъектность ограничена целями и задачами международной организации, закреплёнными в её учредительных документах.

На наш взгляд, наделение цифровых ТНК функциональной правосубъектностью (по аналогии с международными организациями) позволит привлекать ТНК к международно-правовой ответственности за нарушение прав человека. Формы и способы привлечения к ответственности требуют последующего детального изучения.

Таким образом, неурегулированный международно-правовой статус цифровых ТНК затрудняет их привлечение к международно-правовой ответственности за совершение киберпреступлений, однако не исключает их ответственности (в том числе и уголовной по национальному законодательству отдельных стран мира). В условиях стремительного развития цифрового общества наблюдается рост нарушения прав человека в киберпространстве. В связи с этим подтверждается необходимость возобновления обсуждения на международной арене вопроса, который касается статуса ТНК на международной арене и возможности привлечения ТНК к международно-правовой ответственности при нарушении норм права прав человека (что возможно, например, наделив ТНК функциональной правосубъектностью).

Библиографический список

1. Ефремов, В.С. Цифровые компании: понятие, масштабы и особенности транснационализации / В.С. Ефремов // Economics: Yesterday, Today and Tomorrow. – М., 2018. – С.137-147.

2. Трахименок, С. А. Безопасность государства. Методолого-правовые аспекты : моногр. / С. А. Трахименок. – Минск : Бел. изд. т-во «Хата», 1997 – 192 с.

3. Human rights responsibilities in the digital age [Electronic resource] : Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK, 2021. – Mode of access: https://www.rand.org/pubs/research_reports/RRA1152-1.html. – Date of access: 31.03.2022.
4. Право Европейской конвенции по правам человека / Харрис, О`Бойл и Уорбик; [пер. с англ. Власихин В.А. и др]. – Науч.изд., 2-е издание, дополн. – М.: Развитие правовых систем, 2018. – 1432 с.
5. Руководящие принципы предпринимательской деятельности в аспекте прав человека [Электронный ресурс]: одобр. резолюцией 17/4 Совета по правам человека от 16 июня 2011 года // Организация Объединенных Наций. – Режим доступа: https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_RU.pdf. – Дата доступа: 31.03.2022.
6. National Action Plans for Business and Human Rights 2017-2022 [Electronic resource]. – Czech Republic, 2017. – Mode of access: https://www.ohchr.org/Documents/Issues/Business/NationalPlans/NationalActionPlanCzechRepublic.pdf. – Date of access: 31.03.2022.
7. Берандзе, М.Р Проблема правосубъектности транснациональных корпораций в доктрине международного права / М.Р. Берандзе // Московский журнал международного права. – М., 2009. – №4 – С. 206-219.
8. Yearbook of the International Law Commission 1962 Volume II [Electronic resource] // United Nations. – Mode of access: https://legal.un.org/ilc/publications/yearbooks/english/ilc_1962_v2.pdf. – Date of access: 31.03.2022.

УДК 341

ДОСТУП К ЦИФРОВОЙ СРЕДЕ: ПРАВО ДЕТЕЙ С ИНВАЛИДНОСТЬЮ?

Н.М. Шевко

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

С распространением информационно-коммуникационных технологий (включая интернет) возникают новые вопросы, связанные с правами детей с инвалидностью в цифровой среде и их защитой. Право на доступ к цифровой среде прямо не закреплено в Конвенции о правах ребенка 1989 г. В свою очередь, ограничение доступа к цифровой среде влечет нарушение фундаментальных прав ребенка с инвалидностью, как в онлайновой, так и в оффлайновой среде.

***Ключевые слова*:** права детей, права детей с инвалидностью, права человека, информационно-коммуникационные технологии, доступ к цифровой среде.

ACCESS TO THE DIGITAL ENVIRONMENT: A RIGHT OF CHILDREN WITH DISABILITIES?

N.M. Shevko

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

With the spread of information and communication technologies (including the Internet), new issues arise related to the rights of children with disabilities in the digital environment and their protection. The right to access to the digital environment is not explicitly enshrined in the 1989 Convention on the Rights of the Child. In turn, restricting access to the digital environment leads to violation of the fundamental rights of a child with disability, both online and offline.

Keywords: children's rights, rights of children with disabilities, human rights, information and communication technologies, access to the digital environment.

Современное общество характеризуется стремительным развитием информационно-коммуникационных технологий (далее ИКТ), включая интернет. Так, благодаря преобладанию смартфонов и планшетов, доступности Wi-Fi и технологий 4G, развитию платформ социальных сетей и приложений, все больше людей получают доступ к интернету. В сложившейся ситуации детство не является исключением. Стоит отметить, что по оценкам ЮНИСЕФ 71 % молодых людей уже находятся в онлайновой среде. Более того, на глобальном уровне каждый третий пользователь интернета является

ребенком (0–18 лет) [1, с. 3]. С одной стороны, благодаря ИКТ у современных детей появляются беспрецедентные возможности в плане общения, установления связей, обучения, обмена информацией и доступа к ней, а также выражения своих взглядов и мнений по вопросам, затрагивающим их жизни и их сообщества. С другой стороны, более широкий и легкий доступ к онлайновым услугам представляет более серьезную угрозу для безопасности детей как в онлайновой среде, так и в реальной жизни: от вопросов неприкосновенности частной жизни, насилия между сверстниками и жестокого и/или не соответствующего возрасту контента до Интернет-мошенничества и преступлений против детей, таких как груминг в онлайновой среде и сексуальные злоупотребления и сексуальная эксплуатация.

В тоже время, правовому положению детей с инвалидностью в цифровой среде уделяется относительно мало внимания в силу того, что и в реальной среде эта группа детей была долгое время «невидима». Находясь в уязвимом положении оффлайн, с большей вероятностью дети с инвалидностью окажутся в том же положении онлайн, что в первую очередь обусловлено их инвалидностью. Вместе с тем, цифровая жизнь детей с инвалидностью во многих отношениях похожа на жизнь детей без инвалидности. Действительно, дети с инвалидностью, как и дети без инвалидности, используют и наслаждаются цифровой средой в целях общения, получения информации, образования, игр и проведения досуга [2, с. 9]. При этом, следует учитывать то, что «дети с инвалидностью не являются однородной группой, и очевидно, что использование ими цифровых медиа и опыт значительно различаются между разными типами инвалидности и внутри них» [2, с. 10]. Так, опыт ребенка с проблемами мобильности во всех материальных отношениях идентичен опыту ребенка без инвалидности. Но ребенок с глубокими физическими недостатками способен взаимодействовать с цифровым миром лишь косвенно и при поддержке других людей [2, с. 10]. Хотя преимущества (социальная интеграция, равенство возможностей, повышение самооценки) от взаимодействия с цифровой средой для детей с инвалидностью очевидны, они находятся в непропорционально невыгодном положении с точки зрения возможности доступа и использования преимуществ цифровых технологий. Среди основных препятствий и ограничений следует выделить следующие:

дискриминация (не только по признаку инвалидности, но и по гендерному признаку (девочки с инвалидностью) - увеличивает гендерный цифровой разрыв;

цифровые барьеры (недоступный формат контента или информации; отсутствие доступа или ограниченный доступ к ИКТ) – увеличивают экономический разрыв;

ограниченный доступ к недорогим ассистивным технологиям (что связано с высокой стоимостью таких технологий) или их отсутствие (например, в школах) – увеличивает неравенство среди детей;

насилие (в частности, сексуальная эксплуатация и сексуальные надругательства) и киберагрессия – увеличивают риски для безопасности, неприкосновенности частной жизни и благополучия детей с инвалидностью.

Вышеуказанные проблемы ограничивают доступ детей с инвалидностью к цифровой среде, что оказывает негативное воздействие на их гражданские, политические, культурные, экономические и социальные права (например: отсутствие ассистивных технологий в школах нарушает право ребенка с инвалидностью на образование на основе равных возможностей (ст. 28 Конвенции о правах ребенка 1989 г.); отсутствие контента в доступном формате нарушает право ребенка с инвалидностью искать, получать и распространять информацию и идеи наравне с другими (ст.21 Конвенции о правах ребенка 1989 г.). Более того, наличие такого рода проблем свидетельствуют о том, что нормативные механизмы, касающиеся цифровой защиты, цифровых возможностей, цифрового управления и цифровой подотчетности, не соответствуют быстро меняющемуся цифровому ландшафту и не учитывают уникальное воздействие цифровых технологий на детей [3, с. 8], включая детей с инвалидностью.

В данном контексте, Комитетом по правам ребенка (далее КПР) было разработано Замечание общего порядка № 25 (2021) о правах детей в связи с цифровой средой (далее Замечание), в рамках которого особый фокус был направлен на детей с инвалидностью. В Замечании особо подчеркивается необходимость «соблюдать, защищать и осуществлять права каждого ребенка в цифровой среде. Инновации в сфере цифровых технологий оказывают на жизнь детей и их права широкомасштабное и взаимозависимое воздействие даже в тех случаях, когда сами дети не имеют доступа к Интернету» [4, п. 4]. Также в Замечании нашли отражение четыре принципа, необходимых для обеспечения реализации прав детей (закрепленных в Конвенции о правах ребенка 1989 г.) в связи с цифровой средой [4, п. 8]: недискриминация, наилучшие интересы ребенка, право на жизнь, выживание и развитие, уважение мнения ребенка. В отношении детей с инвалидностью, право на недискриминацию обеспечивается равным, эффективным и реальным доступом к цифровой среде [4, п. 9]. В частности, Комитет «призывает государства-участники принимать упреждающие меры для предотвращения дискриминации по признаку…инвалидности…» [4, п. 11] и рекомендует «принимать все необходимые меры для преодоления цифровой эксклюзии» [4, п. 9]. В свою очередь, достижение наилучших интересов детей с инвалидностью будет возможно благодаря обеспечению универсальной доступности цифровых продуктов и услуг, с тем чтобы ими могли пользоваться все

дети без исключения и без необходимости адаптации. В этой связи, государствам следует поощрять технологические инновации, отвечающие потребностям детей с различными видами инвалидности и активно привлекать детей с инвалидностью к участию в разработке и реализации мер, продуктов и услуг, которые влияют на осуществление их прав в цифровой среде [4, п. 91]. Так как рискам (включая киберагрессию и сексуальную эксплуатацию и сексуальные надругательства), связанным с возможностями цифровой среды, в большей степени подвержены дети с инвалидности, их право на жизнь, выживание и развитие особо находится под угрозой. В указанных случаях, государствам следует выявлять и устранять такого рода риски и принимать меры по обеспечению безопасности цифровой среды для детей с инвалидностью, борясь при этом с предрассудками, которые могут привести к чрезмерной защите или исключению этой группы детей из жизни общества [4, п. 92]. Применительно к детям с инвалидностью, принцип уважения мнения ребенка в связи с цифровой средой базируется на ключевом принципе в области прав людей с инвалидностью – «ничего о нас без нас». Государствам следует не только прислушиваться к мнениям детей с инвалидностью (а также их родителей и законных представителей) и учитывать их потребности, но и активно привлекать к разработке законодательства, стратегий, программ, услуг и учебных курсов по вопросам прав детей в связи с цифровой средой [4, п. 17]. Повышение осведомленности о цифровых средствах выражения детьми своего мнения и обеспечение доступа к ним, будут способствовать эффективному отстаиванию своих прав детьми с инвалидностью (а также их родителями и законными представителями) как индивидуально, так и в качестве группы [4, п. 16]. Таким образом, как верно отмечает профессор Филип Жаффе из КПР: «Замечание общего порядка ставит права ребенка в центр одного из важнейших достижений человека – развивающейся информационной и технологической революции» [5].

Подводя итоги, стоит отметить, что несмотря на динамичное развитие ИКТ (включая интернет) для многих детей с инвалидностью доступ к ним все еще ограничен или отсутствует, что несомненно связано с существующими барьерами и предрассудками. Более того, открывая перед такой уязвимой группой детей новые возможности, цифровая среда повышает их риски подвергнуться вредному воздействую, которое негативно отразиться на их жизни в реальном мире. Это в свою очередь обуславливает необходимость принятия государствами специальных мер, направленных на защиту прав детей с инвалидностью в цифровой среде. Тем не менее, ИКТ и интернет могут стать мощными инструментами, помогающими выполнить обещание о том, что «никто не будет забыт», сформулированное в Целях в области устойчивого развития (ЦУР), особенно сегодня, когда весь мир

прилагает усилия по осуществлению Повестки дня в области устойчивого развития на период до 2030 года [3, с. 8].

Библиографический список

1. Руководящие указания для отрасли по защите ребенка в онлайновой среде 2020 [Электронный ресурс]. – Режим доступа: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.IND-2020-PDF-R.pdf. – Дата доступа: 20.04.2022.
2. Report on children with disabilities in the digital environment «Two clicks forward and one click back» [Electronic resource]. – Mode of access: https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f. – Date of access: 20.04.2022.
3. Children in a digital world: the state of the world's children 2017 [Electronic resource]. – Mode of access: https://www.unicef.org/media/48601/file. – Date of access: 20.04.2022.
4. General comment No. 25 (2021) on children’s rights in relation to the digitial environment [Electronic resource]. – Mode of access: https://digitallibrary.un.org/record/3906061. – Date of access: 20.04.2022.
5. Новое руководство о правах детей в цифровом мире [Электронный ресурс]. – Режим доступа: https://www.ohchr.org/ru/stories/2021/03/guidance-establishes-childrens-rights-carry-digital-world. – Дата доступа: 20.04.2022.

УДК 321.011

ЗАКОНОДАТЕЛЬНОЕ ЗАКРЕПЛЕНИЕ ЭЛЕМЕНТОВ ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА КАК ОСНОВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Э. Ю. Анциферова

Академия управления при Президенте Республики Беларусь,
ул. Московская 17, Минск, 220089, Беларусь

Статья посвящена вопросам законодательного закрепления элементов информационного суверенитета как основы обеспечения информационной безопасности государства. На основе обобщения делается вывод об обеспеченности информационной безопасности страны лишь при реализация всего комплекса элементов информационного суверенитета. Предложены рекомендации по включению отдельных норм в законодательство Республики Беларусь.

Ключевые слова: информационная безопасность, информационный суверенитет, информация, информационная политика, информатизация, цифровизация.

LEGISLATIVE CONSOLIDATION OF THE ELEMENTS OF INFORMATION SOVEREIGNTY AS A BASIS FOR ENSURING THE INFORMATION SECURITY OF THE STATE

E. Yu. Antsiferova

Academy of Public Administration under the
President of the Republic of Belarus,
17 Moskovskaya street, Minsk, 220089, Belarus

The article is devoted to the issues of legislative consolidation of the elements of information sovereignty as the basis for ensuring the information security of the state. Based on the generalization, it is concluded that the information security of the country is ensured only when the entire complex of elements of information sovereignty is implemented. Recommendations on the inclusion of certain norms in the legislation of the Republic of Belarus are proposed.

Keywords: information security, information sovereignty, information, information policy, informatization, digitalization.

Введение

Стремительное развитие научно-технического прогресса оказывает существенное влияние на все сферы общества, качественно изменяет

общественные процессы, а также модернизирует современное государство. Однако, трансформация общественных процессов порождает новые вызовы и угрозы безопасности личности, общества и государства в целом. Согласно п. 25 Концепции информационной безопасности Республики Беларусь, утвержденной Постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1 «целевой установкой обеспечения информационной безопасности является информационный суверенитет Республики Беларусь» [1]. Конституционное законодательство Республики Беларусь об информационном суверенитете представлено различными видами нормативных правовых актов, среди которых основополагающая роль принадлежит Конституции Республики Беларусь. Преамбула Конституции Республики Беларусь задает вектор развития государства и общества, является ориентиром для дальнейших норм и действий государственных органов. Преамбула Конституции Республики Беларусь содержит положение о «неотъемлемом праве на самоопределение, сохранение национальной самобытности и суверенитета» [2]. Такое закрепление обусловлено стремлением государства сохранить суверенитет и ответом на негативные тенденции глобализации современного мира. Как в конституциях, принятых после II Мировой войны, так и в современных конституциях традиционно закрепляется незыблемость суверенитета государства. Так, во Конституции Франции наблюдается закрепление «приверженности французского народа принципам национального суверенитета» [3]. В свою очередь, Конституция Российской Федерации «возрождая суверенную государственность России утверждает незыблемость ее демократической основы» [4]. В Конституции Казахстана законодатель также указывает на народный суверенитет как ориентир всего населения страны для создания суверенного государства «объединенный общей исторической судьбой, созидая государственность на исконной казахской земле, исходя из своего суверенного права» [5]. Похожее положение закрепляется и в Основном законе Венгрии, в преамбуле которой указывается на «сохранение интеллектуального и духовного единства нации» [6]. Такой подход к выделению суверенитета как одного из основных категорий в конституциях большинства стран в последнее время формируется в процессе глобализации и возникновения новых типов угроз для государства, в том числе и информационных.

Основная часть

Целью обеспечения информационной безопасности согласно Концепции информационной безопасности Республики Беларусь, утвержденной Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 является «достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие» [1].

В современном мире обеспечить защищенность и безопасность информационной среды государства способно лишь то государство, которое обладает информационным суверенитетом. Суверенитет обеспечивается реализацией основных направлений внутренней и внешней политики государства. Так, Закон Республики Беларусь от 14 ноября 2005 г. №60-З «Об утверждении Основных направлений внутренней и внешней политики Республики Беларусь» выделяет основную задачу внутренней политики – «обеспечение государственного суверенитета и территориальной целостности Республики Беларусь» и основополагающий принцип внешней политики – «повышение эффективности политических, правовых, внешнеэкономических и иных инструментов защиты государственного суверенитета Республики Беларусь и ее национальной экономики в условиях глобализации» [7].

Также стратегической целью государства является защита государственного суверенитета и территориальной целостности Республики Беларусь. В соответствии с п. 31 Концепции информационной безопасности Республики Беларусь «в международных отношениях информационный суверенитет Республики Беларусь обеспечивается в том числе на основе принципа информационного нейтралитета, предусматривающего проведение миролюбивой внешней информационной политики, уважение общепризнанных и общепринятых прав любого государства в данной сфере, исключение инициативы вмешательства в информационную сферу других стран, направленного на дискредитацию или оспаривание их политических, экономических, социальных и духовных стандартов и приоритетов, а также нанесения вреда информационной инфраструктуре каких бы то ни было государств и участия в их информационном противостоянии. При этом Республика Беларусь отстаивает собственные национальные интересы в информационной сфере с использованием всех имеющихся сил и средств» [1].

Подтверждает данную норму и Декларация о недопустимости вмешательства во внутренние дела государств, об ограждении их независимости и суверенитета, принятая резолюцией 2131 (XX) Генеральной Ассамблеи от 21 декабря 1965 г., согласно которой «ни одно государство не может ни применять, ни поощрять применение экономических, политических мер или мер иного характера для принуждения другого государства подчинить осуществление его суверенных прав или для получения от него каких бы то ни было преимуществ» [8]. Считаем необходимым закрепление нормы по обеспечению информационного суверенитета как одной из приоритетных задач внутренней и внешней политики, а также стратегического развития государства в данный момент.

Позиция белорусского законодателя ориентирована на взаимодействие государства в международном пространстве при одновременном законодательном закреплении и урегулировании внутренних вопросов

формирования информационного общества. Согласно стратегии развития информационного общества в Республике Беларусь на период до 2015 года и плане первоочередных мер по реализации Стратегии развития информационного общества в Республике Беларусь на 2010 год, в Республике Беларусь государственная информационная политика реализуется через «деятельность республиканских органов государственного управления, направлена на развитие информационной сферы общества и охватывает всю совокупность общественных отношений, связанных с созданием, накоплением, хранением, обработкой и распространением всех видов информации» [9]. Данные составляющие являются первичными и основными для определения компетенции государственных органов по обеспечению информационной безопасности, а также установлению государственной политики в информационной сфере.

К тому же, в эпоху глобализации и отсутствия информационных границ обеспечение информационной политики и сохранение целостности государства непосредственно связаны с защитой информационного пространства страны от информации, способной дестабилизировать социально-политическую, экономическую, религиозную ситуацию в государстве. Белорусский законодатель в ст. 27 Закона Республики Беларусь «Об информации, информатизации и защите информации» от 10 ноября 2008 г. № 455-З к целям защиты информации относит «обеспечение национальной безопасности, суверенитета Республики Беларусь» [10]. Согласно Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, под информационной безопасностью понимается «состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере» [11]. Таким образом, одним из приоритетных направлений в реализации информационной политики является обеспечение информационной безопасности личности, общества и государства, к которым можно отнести обеспечение прав и свобод граждан в информационном пространстве, материальные и духовные ценности общества и конституционный строй, суверенитет, целостность государства.

Процессы глобализации и информатизации общества, защиты от информационных угроз, формирование и развитие государства нового формата непосредственно связаны с развитием информационных технологий. Технологическое развитие государства и обеспеченность интегрированными цифровыми продуктами прямо влияет на уровень информационного суверенитета в стране, от уровня и качества которых, зависит уровень экономического и социального развития общества, его интеграция в мировую экономическую систему, а также уровень защищенности от угроз информационного характера.

В п. 55 предварительной повестки дня ООН «Информационные и коммуникационные технологии в целях устойчивого развития» указывается на важность развития информационно-коммуникационных технологий, а именно «оказание государствам-членам помощи в построении обществ, в которых знания и технический опыт являются неотъемлемыми элементами развития» [12]. Согласно Указу Президента Республики Беларусь от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь» под информационно-коммуникационными технологиями понимается «совокупность информационных технологий и технологий электросвязи, обеспечивающих сбор, обработку, хранение, распространение, отображение и использование информации в интересах ее пользователей» [13]. Аксиоматично, что информационно-коммуникационные технологии имеют двойное назначение, могут быть источником законных, а также деструктивных целей, компонентами информационного щита, а также меча. Генеральная Ассамблея Организации Объединенных Наций 19 ноября 2018 года приняла резолюцию A73/505 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в которой особо отмечено «стремление международного сообщества к мирному использованию информационно-коммуникационных технологий (далее – ИКТ) в интересах всеобщего блага человечества и дальнейшего устойчивого развития всех стран вне зависимости от их научного и технологического развития» [14]. В Республике Беларусь также принята Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы от 2 февраля 2021 г. № 66 [15]. Государственная программа нацелена на создание, изменение и развитие информационно-коммуникационной инфраструктуры, внедрение цифровых инноваций, а также обеспечение информационной безопасности данных решений. В результате должного развития информационно-коммуникационных технологий, предполагается также и расширение технологий информационного щита, которые способствуют защитной политики от угроз информационного характера.

Следующим компонентом психологической направленности, влияющим на состояние обеспеченности информационного суверенитета, а в перспективе и информационной безопасности страны является уровень информационной культуры гражданского общества. Информационная культура отражает достигнутые уровни организации информационных процессов и эффективности создания, сбора, хранения, обработки, представления и использования информации, обеспечивающих целостное видение мира, его моделирования, предвидения результатов решений, которые принимаются человеком [16, с. 119]. Согласно Кодексу Республики Беларусь об образовании от 13 января 2011 г. «одним из основных составляющих воспитания является гражданское и патриотическое воспитание, направленное на

формирование у обучающихся активной гражданской позиции, патриотизма, правовой, политической и информационной культуры» [17]. Считаем, информационную культуру одним их основных компонентом реализации информационного суверенитета, целью которой является способность обрабатывать, транслировать, оценивать и использовать информацию наиболее эффективным образом. Полагаем, правильно обработанная информация и уровень информационной культуры личности имеет предопределяющий характер действий в информационной среде.

В современном обществе цифровые технологии, проникая во все сферы жизнедеятельности человека, меняют систему реализации общественных отношений в данной среде и требуют системных преобразований правового характера, направленных на упорядочение динамичных и быстрорастущих процессов информатизации общества. Согласно Концепции информационной безопасности Республики Беларусь «информационный суверенитет достигается, прежде всего, путем формирования системы правового регулирования отношений в информационной сфере, обеспечивающей безопасное устойчивое развитие, социальную справедливость и согласие» [1]. Для обеспечения информационного суверенитета страны необходима система гармонизации законодательных актов, быстро адаптированных к изменяющимся условиям в информационном поле.

Также в Решении Конституционного Суда Республики Беларусь от 11 марта 2021 г. № Р-1256/2021 «О состоянии конституционной законности в Республике Беларусь в 2020 году» Конституционным Судом обращено внимание законодателя на то, что «конституционализация формирующегося информационно-цифрового пространства требует доктринального осмысления и эффективного законодательного регулирования. При этом в новых условиях цифровой реальности система права должна гарантировать безопасность реализации прав и свобод человека, стабильность и динамизм в конституционном развитии, сохранение и укрепление национальных фундаментальных ценностей белорусского общества и государства» [18]. Таким образом, цифровой мир нуждается в построении соответствующей модели правового регулирования с компромиссом в защите частной жизни и охраны публичных интересов. Также, Конституционный Суд обращает внимание, что «при установлении нормативно-правового обеспечения процессов в цифровом пространстве следует вырабатывать действенные правовые механизмы обеспечения баланса национальных и наднациональных интересов исходя из верховенства Конституции, конституционных основ государственного устройства, суверенитета Республики Беларусь» [18]. Прежде всего, необходим надлежащий механизм правовой защиты прав и интересов граждан в условиях информатизации и цифровизации общества внутри страны, а также во взаимодействии с зарубежными поставщиками услуг

(вендорами). Невозможно не согласиться с мнением Г. А. Василевича, согласно которому «развитие и совершенствование законодательной базы существенным образом повысит стимулы для точного и полного соблюдения всех правовых норм, регламентирующих деятельность в сфере ИКТ...» [19, с. 12].

Заключение

Информационный суверенитет основывается как на технических, политических и психологических компонентах, так и на законодательных. В современных условиях, для обеспечения информационной безопасности страны необходимо формирование и реализация всего комплекса элементов информационного суверенитета.

Во-первых, информационная безопасность Республики Беларусь существенным образом зависит от обеспечения страны технологическими продуктами и ресурсами, и в ходе технического прогресса эта зависимость будет возрастать. Во-вторых, в результате развитой информационной культуры, формируется предпосылка к защищённости от угроз и негативного психологического воздействия на личность в информационной среде, что способствует формированию информационно развитого населения страны. В-третьих, от уровня развития правового обеспечения формирования информационного общества в стране зависит состояние защищенности национальных интересов в информационной сфере. Следовательно, необходимо принятие концепций развития вышеуказанных элементов с конкретизированными мероприятиями, направленными на обеспечение информационного суверенитета, и, как следствие, информационной безопасности государства.

Библиографический список

1. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета безопасности Республики Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь.. – Минск, 2022.

2. Конституция Республики Беларусь [Электронный ресурс] : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г., 27 фев. 2022 г. // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. [Электронный ресурс]. – Минск, 2022.

3. Конституция Французской Республики, 4 окт. 1958 г. [Электронный ресурс] : офиц. текст : с изм. и доп. от 1 окт. 2008 г. – Коммерческая образовательная библиотека сайт VIVOS VOCO. – 2022. – Режим доступа : http://vivovoco.ibmh.msk.su/VV/LAW/FRANCE_W.HTM. – Дата доступа : 01.06.2022.

4. Конституция Российской Федерации : принята всенар. голосованием 12 дек. 1993 г. : офиц. текст : с изм. от 1 июля 2020 г. // Консультант Плюс. Технология 3000 / ООО «ЮрСпектр». – Минск, 2022.

5. Конституция Казахстана [Электронный ресурс] : принята на республиканском референдуме 30 авг. 1995 г. : офиц. текст : с изм. и доп. от 08.06.2022 г. –Официальный сайт Президента Республики Казахстан. – 2022. – Режим доступа : https://www.akorda.kz/ru/official_documents/constitution. – Дата доступа : 01.06.2022.

6. Основной Закон Венгрии : принят Национальным собранием 25 апр. 2011 г. [Электронный ресурс]. – Сайт национальной бибилиотеки Венгрии. – 2022. – Режим доступа : https://nemzetikonyvtar.kormany.hu/download/3/00/50000/orosznyomda_jav%C3%ADtott.pdf. – Дата доступа : 01.06.2022.

7. Об утверждении основных направлений внутренней и внешней политики Республики Беларусь [Электронный ресурс] : Закон Респ. Беларусь, 14 нояб. 2005 г., № 60-З : в ред. Закона от 4 июня 2015 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

8. Декларация о недопустимости вмешательства во внутренние дела государств, об ограждении их независимости и суверенитета [Электронный ресурс] : принята резолюцией 2131 (XX) Генеральной Ассамблеи, 21 дек. 1965 г. – Официальный сайт Организации Объединенных Наций. – 2022. – Режим доступа : https://www.un.org/ru/documents/decl_conv/declarations/inadmissibility_of_intervention.shtml. – Дата доступа : 01.06.2022.

9. О Стратегии развития информационного общества в Республике Беларусь на период до 2015 года и плане первоочередных мер по реализации Стратегии развития информационного общества в Республике Беларусь на 2010 год : постановление Совета Министров Республики Беларусь, 9 авг. 2010 г., № 1174 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

10. Об информации, информатизации и защите информации : Закон Респ. Беларусь, 10 нояб. 2008, № 455-З : в ред. Закона от 24 мая 2021 г. № 111-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

11. Концепция национальной безопасности Республики Беларусь [Электронный ресурс] : утв. Указом Президента Республики Беларусь, 9 нояб. 2010 г., № 575 : в ред. Указа от 24.01.2014 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

12. Информационные и коммуникационные технологии в целях устойчивого развития [Электронный ресурс] : предварительная повестка дня ООН, г. Париж, 27 марта 2009 г. – Официальный сайт ЮНЕСКО. – 2022. – Режим доступа : https://unesdoc.unesco.org/ark:/48223/pf0000181336_rus. – Дата доступа : 02.06.2022.

13. О некоторых вопросах развития информационного общества в Республике Беларусь [Электронный ресурс] : Указ Президента Респ. Беларусь, 8 нояб. 2011 г., № 515 : в ред. Указа от 16.12.2019. // Эталон – Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

14. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности [Электронный ресурс] : резолюция Генеральной Ассамблеи Организации Объединённых Наций, 19 нояб. 2018 г., № A73/505. – Цифровая библиотека Организации Объединённых Наций. – Режим доступа : https://digitallibrary.un.org. – Дата доступа : 01.06.2022.

15. О государственной программе «Цифровое развитие Беларуси» на 2021–2025 годы [Электронный ресурс] : постановление Совета Министров Республики

Беларусь, 2 февраля 2021 г., № 66 // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». – Минск, 2022.

16. Davenport, T. H. Saving IT's Soul: Human-Centered Information Management / T. H. Davenport // Harvard Business Review. – 1994. – № 72(2). – P. 119–131.

17. Кодекс Республики Беларусь об образовании [Электронный ресурс], 13 янв. 2011 г., № 243-З : в ред. Закона от 14 января 2022 г. // Консультант Плюс: Беларусь. Технология ПРОФ’2012 / ООО «ЮрСпектр», Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2013.

18. О состоянии конституционной законности в Республике Беларусь в 2020 году [Электронный ресурс]: решение Конституционного Суда Респ. Беларусь, 11 марта 2021 г., № Р-1256/2021 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

19. Василевич, Г. А. Белорусский путь развития: правовое обеспечение информационных технологий / Г.А. Василевич // Проблемы упр. – 2006. – № 1. – С. 12.

УДК 341.171

АДВОКАТИРОВАНИЕ КОНКУРЕНЦИИ НА РЫНКЕ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ КАК ОДНО ИЗ НАПРАВЛЕНИЙ ОБЕСПЕЧЕНИЯ ЕГО БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ

П.Г. Черенкевич

Белорусский государственный университет
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье рассматриваются положения международных соглашений в области защиты прав интеллектуальной собственности, которые содержат нормы, регулирующие конкурентные отношения, а также доктринальные источники по данному вопросу, затрагивающие конкуренцию и, в частности, ее адвокатирование. По результатам исследования была выявлена определенная тенденция регулирования конкурентных отношений на рынке интеллектуальной собственности, а также обоснована важность их защиты на указанном рынке посредством адвокатирования.

***Ключевые слова*:** адвокатирование конкуренции, рынок интеллектуальной собственности, защита прав интеллектуальной собственности, конкуренция.

ADVOCATING COMPETITION IN THE INTELLECTUAL PROPERTY MARKET AS ONE OF THE DIRECTIONS TO ENSURE ITS SAFE FUNCTIONING

P.G. Cherenkevich

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article discusses the provisions of international agreements in the field of protection of intellectual property rights, which contain the rules governing competitive relations, as well as doctrinal sources on this issue, affecting competition and, in particular, its advocacy. Based on the results of the study, a certain trend in the regulation of competitive relations in the intellectual property market was identified, and the importance of their protection in this market through advocacy was substantiated.

Keywords: competition advocacy, intellectual property market, protection of intellectual property rights, competition.

Введение

В настоящее время в экономической науке появился термин «новая экономика» или экономика, основанная на знаниях, где результаты

инновационной деятельности, инновации, опыт приобретают особое значение и становятся основными факторами производства, определяют успешность и стабильность экономического развития. Как результат, появляется новый сектор мировой торговли – рынок интеллектуальной собственности (далее – ИС).

Уровень безопасного функционирования рынка ИС становится важнейшим фактором, определяющим включенность государства в мировое сообщество в 21 веке. Неурегулированность вопросов защиты ИС – угроза для нормального развития и функционирования внутреннего рынка и науки, создания инновационных услуг и товаров, взаимодействия с рынками ИС других субъектов международного права.

При этом стоит отметить, что в Глобальном инновационном индексе Всемирной организации ИС (далее – ВОИС) 2021 года Республика Беларусь заняла 62-е место, улучшив свой рейтинг на 2 позиции по сравнению с 2020 годом (64-е место) и на 24 позиции в сравнении с 2018 годом (86-е место) [1]. Так, можно утверждать, что ИС – это фактор, определяющий развитие общества в целом, где содействие в создании и нормальном функционировании рынка ИС становится главной целью законодательной охраны. Вместе с тем инновационное развитие государств, мирового сообщества и их экономик за счет ИС можно обеспечить только посредством конкуренции, а это значит прозрачности в регулировании и защите.

Основная часть

О конкуренции, в том числе на рынке ИС, может идти речь только в случае, если субъекты находятся в определенных отношениях друг с другом, то есть в конкурентных, которые соответствующим образом оформлены с правовой точки зрения [2, с. 21]. Так, для признания участников экономической деятельности конкурентами, то есть участниками конкурентных отношений, должны быть соблюдены такие условия, как состязательность участников конкретного рынка за долю на этом рынке и результатом состязательности является ограничение возможности других участников данного рынка оказывать одностороннее влияние на условия сделок на этом рынке. Следует отметить, что аналогичный по своему содержанию термин «конкуренция» содержится в пункте 8 части 2 статьи 1 Приложения № 19 к Договору о Евразийском экономическом союзе, вместе с тем отсутствует в Договоре о Европейском союзе (далее – ЕС) и Договоре о функционировании ЕС.

Право на конкуренцию закрепляется за его участниками путем выделения общих и специальных пределов осуществления исключительных прав на объекты ИС.

К общим пределам относят сформулированные в качестве основных начал гражданского законодательства требования не нарушать прав и

охраняемых законом интересов других лиц, действовать добросовестно и разумно, осуществлять права в соответствии с их назначением и не допускать злоупотребления правом [3, с. 522-523]. Специальные пределы осуществления исключительных прав на объекты ИС подразделяются на пределы осуществления исключительного права (то есть мера возможного поведения его обладателя в отношении объекта (исчерпание исключительного права правообладателя объектов ИС)) и ограничения исключительного права (то есть мера возможного поведения третьих лиц по использованию данного объекта исключительного права без нарушения такого права) [4, с. 32], [5, с. 136].

В ходе анализа международных соглашений в области охраны прав на объекты ИС, содержащих нормы, посвященные возможным ограничениям исключительных прав, была выявлена тенденция к регулированию конкурентных отношений посредством общих пределов, то есть запретов совершать определенные действия, ограничивающие конкуренцию, со стороны правообладателя и третьих лиц. Среди данных актов следует назвать Договор ВОИС по авторскому праву 1996 г., Международную конвенцию об охране прав исполнителей, производителей, фонограмм и вещательных организаций 1961 г., Парижскую конвенцию по охране промышленной собственности 1883 г., Соглашение по торговым аспектам прав интеллектуальной собственности [6], [7], [8], [9].

Вместе с тем специальные пределы осуществления исключительных прав на объекты ИС, как положительная мера возможного поведения, закреплены только в Бернской конвенции по охране литературных и художественных произведений 1886 г. и частично нашли свое отражение в Договоре ВОИС по исполнениям и фонограммам 1996 г. [10], [11].

Таким образом, представляется, что стабильность и защита прав в отношении объектов ИС, развитие экономики, укрепление и рост экономической безопасности функционирования рынка за счет объектов ИС закрепляется путем установления запретов на нарушение прав и охраняемых законом интересов других лиц и злоупотребление правом самим правообладателям. Вместе с тем идея конкуренции состоит не в ограничении деятельности, а, в первую очередь, в способности к развитию конкурентных отношений, то есть закреплением за участниками конкурентных отношений мер возможного поведения. В противном случае, это противоречит самой сущности конкуренции.

Так, одним из организационных и правовых способов развития конкуренции на объекты ИС в ее правильном понимании («здоровая конкуренция») и безопасным функционированием данного рынка является адвокатирование конкуренции, целями которой являются:

стимулирование рынка ИС к саморегуляции, а не к ущемлению прав участников гражданского оборота посредством установления запретов;

убеждение регулирующих органов не принимать излишне антиконкурентные меры;

повышение уровня осведомленности о преимуществах конкуренции, в частности, на рынке ИС, роли конкурентного права и конкурентной политики среди государственных органов, судебной системы и общества в целом.

Страны ЕС придерживаются определения «адвокатирования конкуренции» данного Рабочей группой по адвокатированию Международной сети по вопросам конкуренции: «адвокатирование конкуренции – набор видов деятельности антимонопольных органов, направленных на укрепление конкурентной среды для экономической деятельности посредством использования механизмов, не являющихся элементами системы принуждения к соблюдению установленных правил и состоящие, главным образом, во влиянии на другие государственные организации и повышении степени понимания широкими кругами общественности выгод конкуренции». Практика ЕС показывает, что необходимость установления продуктивных связей с общественностью, включая политическое лоббирование свободной конкуренции, подталкивает антимонопольные органы ЕС и Европейской комиссии интегрироваться в политические и административные процессы принятия решений [12].

Касаясь ЕАЭС и, в частности, Евразийской экономической комиссии (далее – ЕЭК) стоит отметить, что ЕАЭС были заключены международные соглашения, в которых содержатся положения о сотрудничестве с антимонопольными ведомствами третьих стран. Помимо этого, ЕАЭС и ЕЭК подписали с другими государствами и региональными организациями меморандумы о взаимопонимании, предусматривающие обмен информацией, в том числе с целью развития и совершенствования адвокатирования конкуренции. Согласно экспертному обзору правового регулирования и политики в сфере конкуренции в ЕАЭС, проведенного и опубликованного Организацией экономического сотрудничества и развития 24 декабря 2021 г., ЕЭК еще не представилось возможности предпринять те или иные скоординированные действия в области правоприменения с участием антимонопольного ведомства третьей страны, не проводилось и скоординированной деятельности по адвокатированию [13].

Заключение

На основании вышеизложенного можно прийти к следующим выводам:

1. В международных соглашениях в области охраны прав на объекты ИС, содержащих нормы, посвященные возможной защите от ограничений исключительных прав, и, соответственно, безопасному

функционированию рынка ИС, была выявлена тенденция к регулированию конкурентных отношений на данном рынке посредством установления запретов совершать определенные действия, ограничивающие конкуренцию, со стороны правообладателя и третьих лиц.

2. Установление защиты объектов ИС посредством запретов противоречит самой сущности конкуренции, и, в частности, «здоровой» конкуренции, поскольку идея конкуренции состоит не в ограничении деятельности, а в способности к развитию конкурентных отношений, то есть закреплением за участниками конкурентных отношений мер возможного поведения на рынке ИС.

3. Одним из организационных и правовых способов развития «здоровой» конкуренции, в том числе на вышеуказанном рынке, является адвокатирование конкуренции, цель которой – стимулирование рынка к саморегуляции, а не к ущемлению прав участников гражданского оборота посредством установления запретов; избежание излишних антиконкурентных мер, принимаемых регулирующими органами, повышение уровня осведомленности о преимуществах конкуренции, в том числе на объекты ИС, роли конкурентного права и конкурентной политики, обмен опытом с другими государствами и международными сообществами в части популяризации «здоровой» конкуренции и безопасного функционирования рынка ИС для всех его субъектов.

Библиографический список

1. Беларусь в Глобальном инновационном индексе 2021 года // Постоянное представительство Республики Беларусь при Отделении ООН и других международных организациях в Женеве [Электронный ресурс]. – Режим доступа: https://geneva.mfa.gov.by/ru/embassy/news/b94cb12c0e77c0fe.html#:~:text=20.09.2021%20%D0%B3.,(86%2D%D0%B5%20%D0%BC%D0%B5%D1%81%D1%82%D0%BE). – Дата доступа: 31.05.2022.

2. Конкуренция и антимонопольное регулирование: учеб. пособие для вузов / под ред. А.Г. Цыганова – М.: Логос, 1999.

3. Гражданское право: учебн.: в 3 т. Т. 1 / Е.Н. Абрамова, Н.Н. Аверченко, Ю.В. Богушева [и др.]; под. ред. А.П. Сергеева. – М.: ТК Велби, 2008. – 800 с.

4. Судариков, С.А. Право интеллектуальной собственности / С.А. Судариков. – М.: Проспект, 2016. – 368 с.

5. Лосев, С.С. Исключительные права в системе гражданских прав / С.С. Лосев. – Минск: Бизнесофсет, 2016. – 270 с.

6. Договор Всемирной организации интеллектуальной собственности по авторскому праву от 20 декабря 1996 г. // ЭТАЛОН–ONLINE [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=i09600049&q_id=0. – Дата доступа: 31.05.2022.

7. Международная конвенция об охране прав исполнителей, производителей, фонограмм и вещательных организаций // WIPO LEX [Электронный ресурс]. – Режим доступа: https://wipolex.wipo.int/ru/text/531118. – Дата доступа: 31.05.2022.

8. Парижская конвенция по охране промышленной собственности 1883 года // Электронный фонд правовых и нормативно-технических документов [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1900359 – Дата доступа: 08.02.2022.

9. Соглашение по торговым аспектам прав интеллектуальной собственности (соглашение ТРИПС) // WIPO LEX [Электронный ресурс]. – Режим доступа: https://wipolex.wipo.int/ru/text/379915. – Дата доступа: 31.05.2022.

10. Бернская конвенция по охране литературных и художественных произведений от 9 сентября 1886 г. // Электронный фонд правовых и нормативно-технических документов [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1900493. – Дата доступа: 31.05.2022.

11. Договор Всемирной организации интеллектуальной собственности по исполнениям и фонограммам 1996 г. // WIPO LEX [Электронный ресурс]. – Режим доступа: https://wipolex.wipo.int/ru/text/295480. – Дата доступа: 31.05.2022.

12. Моросанова, А.А, Мелешкина, А.И., Фатихова, А.Ф. Зарубежный опыт адвокатирования конкуренции: цели, методы и результаты // Электронная библиотека РАНХиГС при Президенте РФ [Электронный ресурс]. – Режим доступа: https://archive.econ.msu.ru/sys/raw.php?o=3623&p=attachment#:~:text=%D0%A4%D0%90%D0%A1%20%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8%20%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%8F%D0%B5%D1%82%20%D0%B4%D0%B5%D1%8F%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C%20%D0%B0%D0%B4%D0%B2%D0%BE%D0%BA%D0%B0%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F,%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5%D0%BC%20%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D0%BD%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D1%85%20%D0%BC%D0%B5%D1%85%D0%B0%D0%BD%D0%B8%D0%B7%D0%BC%D0%BE%D0%B2%2C%20%D0%B0%20%D0%BD%D0%B0. – Дата доступа: 31.05.2022.

13. ОЭСР (2021), Экспертные обзоры ОЭСР по правовому регулированию и политике в сфере конкуренции: Евразийский Экономический Союз // … [Электронный ресурс]. – Режим доступа: https://www.oecd.org/daf/competition/oecd-peer-reviews-of-competitionlaw-and-policy-eurasian-economic-union-2021.htm. – Дата доступа: 31.05.2022.

УДК 341.1/.8+343.2/.7+347.1

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ ОБОРОТА КРИПТОВАЛЮТ И ТОКЕНОВ В ГОСУДАРСТВАХ-ЧЛЕНАХ ЕВРАЗИЙСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА

И.С. Аземша

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье анализируются угрозы развития рынка криптовалют и токенов, судебная практика, рассматриваются подходы в законодательстве государств-членов Евразийского экономического союза к определению гражданско-правового статуса криптовалют и токенов и криминализации общественно опасных деяний с их использованием. Проводится исследование соответствия их гражданско-правового статуса на предмет соответствии их сущности. Сделан вывод о целесообразности заключения международного договора в форме протокола к Договору о Евразийском экономическом союзе «О развитии и защите рынка цифровых финансовых активов», предусматривающего рекомендации по уголовно-правовой охране криптовалют и токенов в Евразийском экономическом союзе и определению их гражданско-правового статуса. Выработаны предложения по содержанию соответствующих разделов международного договора.

Ключевые слова: криптовалюты, токены, уголовное право, право ЕАЭС.

CRIMINAL LEGAL ASPECTS OF REGULATION OF CRYPTOCURRENCIES AND TOKENS TRAFFIC IN THE EURASIAN ECONOMIC UNION MEMBER STATES

I.S. Azemsha

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article analyzes the threats to the development of the market of cryptocurrencies and tokens, judicial practice, approaches in the legislation of the Eurasian Economic Union member states to determining the civil law status of cryptocurrencies and tokens and criminalizing socially dangerous acts with their use. A study of the compliance of their civil law status is being carried out for the purpose of compliance with their essence. The author concludes on the expediency of concluding an international treaty in the form of a protocol to the Treaty on the Eurasian Economic Union "On the Development and Protection of the Digital Financial Assets Market", which provides recommendations on the criminal law protection of cryptocurrencies and tokens in the Eurasian Economic Union and the determination of their civil law status. Proposals have been developed on the content of the relevant sections of such international treaty.

Keywords: cryptocurrencies, tokens, criminal law, law of the Eurasian Economic Union.

Введение

Актуальность исследования уголовно-правовых аспектов регулирования оборота криптовалют и токенов в государства-членах Евразийского экономического союза (далее – ЕАЭС) обусловлена возрастающим развитием рынка криптовалют и токенов, наличием различных подходов к правовому регулированию криптовалют и токенов в ЕАЭС и, как следствием, различными подходами к рассмотрению криптовалют и токенов в качестве предметов и средств совершения преступлений в уголовном законодательстве государств-членов ЕАЭС.

Цель исследования заключается в выработке на основе анализа законодательства государств-членов ЕАЭС и теоретических трудов ученых пути совершенствования уголовного и гражданского законодательства государств-членов ЕАЭС с целью закрепления эффективных методов защиты экономик государств-членов ЕАЭС.

Вышеизложенное обуславливает актуальность и новизну исследования.

Основная часть

Одной из проблем отсутствия эффективного уголовно-правового инструментария в сфере осуществления охраны правоотношений, связанных с оборотом криптовалют и токенов, является отсутствие криминализации общественно опасных деяний, предполагающих использование криптовалют и токенов, в силу отсутствия их рассмотрения в качестве предметов и средств совершения общественно опасных деяний, что обусловлено отсутствием четкого закрепления их гражданско-правового статуса.

На необходимость рассмотрения, например, криптовалют в качестве предмета преступления указывалось Генеральным прокурором Российской Федерации И.В. Красновым [1].

Одной из опасностей, которую влечет развитие рынка криптовалют и токенов, является создание условий для легализации доходов, полученных преступным путем. Именно наличие барьеров, защищающих денежно-финансовую систему от легализации преступных доходов, является важным условием борьбы с теневой экономикой.

Ученые выделяют следующие риски, связанные с оборотом криптовалют и токенов: затрудненность отслеживания быстрых транзакций, неконтролируемые переводы криптовалют с одного виртуального счета на другой; конвертация криптовалют и других цифровых активов друг в друга и практическое отсутствие данных о таких операциях; анонимность пользователей систем криптовалют и сложности в установлении фактов их активности; большая запутанность моделей транзакций в реально

действующих схемах отмывания денег и технологические сложности в отделении легальных трансакций от нелегальных [2].

Наиболее латентными являются операции с криптовалютой по легализации доходов, полученных преступным путем.

Отметим, что этому способствуют технологии, позволяющие совершать анонимные транзакции с криптовалютами.

Так, российские исследователи отмечают полномасштабное развитие сервисов для конвертации криптовалюты и обналичивания фиатных средств. Как правило, эти транзакции имеют характер P2P (от человека к человеку) с использованием криптоматов. По информации сервиса Coin ATM Radar, в настоящее время в мире установлено больше тысячи таких устройств. За комиссию в размере 15 % сервис обеспечивает бесперебойность перевода и анонимность клиента. Другой способ легализации – использование «программ-смесителей». Они предлагают клиентам запутать историю транзакций либо отмыть доходы, купив для другого лица товары в Интернете за «грязные» деньги. Покупатель компенсирует расходы клиента, за исключением суммы комиссии. В итоге клиент сервиса получает «чистые» деньги, а покупатель — дисконт на товар. Но особое внимание следует обратить на нелегальные сервисы по конвертации криптовалюты. Самые большие объемы отмываемых таким образом средств проходят через офшоры, где финансовый контроль за денежными потоками традиционно более слабый. Новым и популярным способом легализации криминальных доходов является их отмывание через сайты азартных игр. Именно через эти сервисы отмывается около трех четвертей всех грязных виртуальных денег [3].

Отметим, что криптовалюты и токены позволяют совершать дробные транзакции, осуществляя тем самым их размещение. Кроме того, процесс транзакции с криптовалютами, как было указано выше, затрудняет установление ее сторон. Стадия наслоения, интеграции и инвестирования в случае использования криптовалют и токенов более скрытны, что обусловлено возможностью дробления токенизированных акций и высокой волатильностью криптовалют.

Следовательно, общественно опасные деяния, где предметом и средствами совершения деяний могут выступать криптовалют и токены, являются наиболее опасными для стабильности денежно-финансовой системы государства.

Другой угрозой использования криптовалют и токенов является риск осуществления финансирования терроризма и экстремистской деятельности.

В настоящее время в Российской Федерации фиксируются факты финансирования терроризма. Как отмечают специалисты, самыми

популярными криптовалютами, используемыми в России в преступных целях, включая финансирование терроризма являются Bitcoin, Ethereum и Monero [4].

Имеются факты хищения криптовалют. К примеру, на протяжении 2015-2019 гг. М., житель г. Минска, с использованием компьютерной программы осуществил кибератаки на интернет-ресурсы, что позволило ему завладеть конфиденциальной информацией (логины и пароли для доступа к учетным записям и счета к ним), посредством которой он мог неправомерно получать доступ к счетам иностранных граждан, на которых хранилась криптовалюта. Такой преступный механизм позволял злоумышленнику производить незаконные транзакции и похищать криптовалюту. После прохождения цепочки транзакций похищенная криптовалюта переводилась на подконтрольные М. и его соучастникам счета в платежных системах, после чего они получали с использованием банковских платежных карточек наличные денежные средства [5, с. 87–89].

В судебной практике Республики Беларусь существует пример совершения мошенничества, где предметом преступления являлась криптовалют.

Так приговором суда Ленинского района г. Минска от 13 декабря 2021 г. было установлено, что «Д. совершил преступление – завладение имуществом путем обмана (мошенничество), а именно: он, имея умысел на умышленное противоправное безвозмездное завладение чужим имуществом, путем обмана, посредством достоверно неустановленных ресурсов глобальной компьютерной сети Интернет, в том числе приложения Т. посредством переписки с Г., под предлогом предоставления (продажи) невзаимозаменяемых 6 токенов (электронных картинок), создав видимость реальности намерений по их предоставлению, в действительности не намереваясь выполнять принятые на себя обязательства, убедил последнего перевести на его электронный кошелек *** криптовалюту Solana (SOL), в результате чего посредством достоверно неустановленной компьютерной техники, в том числе персонального компьютера, на котором установлена оперативная система W., имеющий доступ в глобальную сеть Интернет, используя неустановленные ресурсы глобальной компьютерной сети Интернет, в том числе виртуальную платформу S., путем мошенничества завладел одной монетой криптовалюты Solana (SOL) ценой 164,59 долларов С., что по курсу белорусского рубля по отношению к иностранной валюте, устанавливаемого Национальным банком Республики Беларусь, на момент совершения преступления, из расчета 2,5146 рубля за 1 доллар С., составило 413 рублей 88 копеек, принадлежащей Г., которую последний перевел на вышеуказанный электронный кошелек, а также одной монетой криптовалюты Solana (SOL) ценой 164,59 долларов С., что по курсу белорусского рубля по отношению к иностранной валюте, устанавливаемого Национальным банком

Республики Беларусь, на момент совершения преступления, из расчета 2,5146 рубля за 1 доллар С., составило 413 рублей 88 копеек, принадлежащей Ш., и одной монетой криптовалюты Solana (SOL) ценой 164,59 долларов С., что по курсу белорусского рубля по отношению к иностранной валюте, устанавливаемого Национальным банком Республики Беларусь, на момент совершения преступления, из расчета 2,5146 рубля за 1 доллар С., составило 413 рублей 88 копеек, принадлежащей Л., которые последний, по предложению Г., перевел на вышеуказанный электронный кошелек, принадлежащий Д., а всего путем мошенничества завладел имуществом потерпевших Г., Ш., Л. на общую сумму 1 241 рубль 64 копейки, похищенным распорядился по своему усмотрению» [6].

В этой связи важным является рассмотрение сущности и гражданско-правового статуса криптовалют и токенов как предметов преступлений и средств совершения преступлений.

В рамках ЕАЭС существует три подхода к рассмотрению криптовалют и токенов в качестве объектов гражданских прав:

1) признание токенов в качестве самостоятельного вида объектов гражданских прав (разновидности имущественных прав) и отсутствие закрепления в качестве объекта гражданских прав криптовалют (Российская Федерация) [7];

2) признание токенов и криптовалют в качестве самостоятельного вида объектов гражданских прав (разновидности имущественных прав) (Республика Казахстан) [8];

3) отсутствие законодательного закрепления в качестве объекта гражданских прав или вида криптовалют и токенов (Республика Беларусь, Кыргызская Республика, Республика Армения) [9], [10], [11].

Отметим, что указание в Декрете Президента Республики Беларусь «О развитии цифровой экономики» от 21 декабря 2017 г. № 8 на то, что цифровой знак (токен) удостоверяет наличие прав владельца на объекты гражданских прав [12] не позволяет вести речь о возможности рассмотрения их в качестве объектов гражданских прав в силу отсутствия прямого закрепления в гражданском законодательстве.

В то же время отметим, что, по-нашему мнению, указанные подходы не в полной мере соответствуют сущности криптовалют и токенов.

Криптовалюты следует рассматривать как отдельный объект граждански прав в силу их роли как платежного средства, которое обладает оборотоспособностью и имеет определенный стоимостный эквивалент, но в то же время не является имуществом в силу нематериального характера и отсутствия обеспеченности конкретным материальным активом.

Токен, исходя из анализа его технический природы, представляет собой запись в блокчейне (распределенном реестре) или в иной информационной

системе, которая является единицей учета в форме цифрового финансового актива, который 1) предоставляет в будущем доступ к продукту либо услуге проекта; 2) обеспечена материальным активом, удостоверяет право собственности на ценные бумаги и предоставляет возможность получения дивидендов; 3) стоимость которого обеспечена стоимостью денежных средств, ценными бумагами и товарами, криптовалютами; 4) представляет собой цифровой объект и удостоверяет право собственности на него.

По нашему мнению, токены удостоверяют обязательственные, вещные права, а также права на результаты интеллектуальной деятельности, поскольку основная функция токенов заключается в том, что они удостоверяют наличие права собственности на вещи, ценные бумаги, результаты интеллектуальной деятельности.

Считаем, что один из видов токенов – стабильные монеты – имеет схожие черты с производными ценные бумагами (деривативами), поскольку удостоверяет право на получение базисного актива (актив, которым обеспечивается стоимость стабильных монет) в зафиксированной стоимости.

Следовательно, полагаем целесообразным выделить рассматривать криптовалюту как отдельный объект гражданских прав, а токены в качестве разновидности имущественных прав.

В то же время, исходя из анализа признаков криптовалют и токенов, предлагается рассматривать криптовалюты и токены в системе цифровых валют как подвиды виртуальных валют, объединенные понятием цифровые финансовые активы.

В Республике Беларусь уголовное законодательство на примере ст. 212 (устанавливает ответственность за совершение хищения путем использования компьютерной техники,) ст. 235 (устанавливается ответственность за легализацию средств, полученных преступным путем), ст. 290-1, ст. 361-2 (устанавливают уголовную ответственность за финансирование террористической деятельность или деятельности экстремистского формирования) Уголовного кодекса Республики Беларусь не предполагает рассмотрение криптовалют и токенов как предметов преступления и средств совершения преступления [13], что обусловлено отсутствием рассмотрения криптовалют и токенов как видов объектов гражданских прав.

Таким образом, ст. 174 (предусматривается уголовная ответственность за совершение финансовых операций и других сделок с денежными средствами или иным имуществом, заведомо приобретенными другими лицами преступным путем, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом), ст. 174-1 (закрепляется уголовная ответственность за совершение финансовых операций и других сделок с денежными средствами или иным имуществом, приобретенными лицом в результате совершения им

преступления, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом), ст. 159-6 (устанавливает уголовную ответственность за мошенничество в сфере компьютерной информации) Уголовного кодекса Российской Федерации предусматривают в качестве предмета и средства совершения преступления, в том числе, только цифровые права (токены) как разновидность имущественных прав.

Однако ст. 282-3 (устанавливает ответственность за финансирование экстремистской деятельности) и ч. 1.1 ст. 205-1 (устанавливает ответственность за финансирование террористической деятельности) Уголовного кодекса Российской Федерации не предусматривают возможность отнесения цифровых прав (токенов) к средству совершения преступления в силу неясности формулировки содержания данного признака [14].

Уголовный кодекс Республики Казахстан в ст. 218 (предусматривает ответственность за легализацию доходов, полученных преступным путем) и ст. 258 (устанавливает уголовную ответственность за финансирование террористической или экстремистской деятельности и иное пособничество терроризму либо экстремизму) Уголовного кодекса Республики Казахстан предусматривает цифровые актив как предмет преступления и средство совершения преступления [15].

Таким образом в силу положений гражданского и уголовного законодательства Республики Казахстан криптовалюты и токены, определенные как цифровые активы, являются предметами и средствами преступного посягательства в рассмотренных выше нормах.

Исходя из анализа главы 7 и главы 8 Гражданского кодекса Республики Армения, можно сделать вывод о том, что криптовалюта не признается имуществом [11], что не позволяет отнести к предмету и средству совершения преступления, предусмотренных, к примеру, ст. 177 (устанавливает ответственность за совершение кражи) и ст. 190 («Легализация доходов, полученных незаконным путем») Уголовного кодекса Республики Армения [16]. Таким образом, криптовалюты и токены не признаются предметами и средствами совершения преступления.

В Кыргызской Республике на сегодняшний день отсутствует правовое регулирование криптовалют и токенов. В главе 3 Гражданского кодекса Кыргызской Республики («Объекты гражданских права») криптовалюты и токены не рассматриваются в качестве имущества [10]. В то же время предметом и средством совершения преступления признается только имущество на примере ст. 215 (устанавливает уголовную ответственность за легализацию доходов, полученных преступным путем) Уголовного кодекса Кыргызской Республики [17].

Таким образом, можно сделать вывод об отсутствии гармонизации законодательств государств-членов ЕАЭС и выделить несколько подходов к криминализации изучаемой категории преступных деяний в тех государствах-членах ЕАЭС, где криптовалюты и токены рассматриваются в качестве видов объектов гражданских прав (Российская Федерация и Республика Казахстан):

1. Криминализация деяний, совершаемых с использованием криптовалют и токенов (Республика Казахстан).
2. Криминализация деяний, совершаемых с использованием токенов (Российская Федерация).

Вышесказанное указывает на необходимость трансформации гражданского законодательства посредством определения соответствующего гражданско-правового статуса, определив криптовалюту как отдельный объект гражданских прав, а токены в качестве разновидности имущественных прав.

Заключение

Отутствие единого подхода государств-членов ЕАЭС к определению гражданско-правового статуса криптовалют и токенов влечет отсутствие эффективных уголовно-правовых средств борьбы с общественно опасными деяниями (хищения, легализация дохода, полученного преступным путем, финансирование терроризма и экстремистской деятельность и др.).

Для решение указанной проблемы необходимо принятие согласованных мер государствами-членами ЕАЭС.

В этой связи считаем целесообразным заключение международного договора в форме протокола к Договору о ЕАЭС «О развитии и защите рынка цифровых финансовых активов», определяющего основные начала правового регулирования оборота криптовалют и токенов на территории ЕАЭС, включающего свою структуру разделы «Гражданско-правовой статус цифровых финансовых активов в законодательстве государств-членов ЕАЭС» и «Уголовно-правовая охрана цифровых финансовых активов в законодательстве государств-членов ЕАЭС».

В разделе «Гражданско-правовой статус цифровых финансовых активов в законодательстве государств-членов ЕАЭС» предлагается в рекомендациях выработать предложение закрепить криптовалюту как отдельный объект гражданских прав, а токены – как разновидность имущественных прав.

В разделе «Уголовно-правовая охрана цифровых финансовых активов в законодательстве государств-членов ЕАЭС» следует внести рекомендации о необходимости внесения изменений в примечания к составам преступлений в уголовном законодательстве государств-членов ЕАЭС, где в качестве предмета и средства совершения преступления закрепить криптовалюты и

токены посредством выделения криптовалюты как самостоятельного объекта гражданских прав, а токенов как вида имущественных прав.

Библиографический список

1. Генпрокурор Краснов предложил признать криптовалюты предметом преступных посягательств // Интерфакс [Электронный ресурс]. – Режим доступа: https://www.interfax.ru/business/837941. – Дата доступа: 26.04.2022.
2. Колесова, И.В., Стась, Т.А. Криптовалюта: возможности и угрозы // Cyberleninka.ru [Электронный ресурс]. – 2018. – Режим доступа: https://cyberleninka.ru/article/n/kriptovalyuta-vozmozhnosti-i-ugrozy. – Дата доступа: 18.04.2022.
3. Иванцов, С.В. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С.В. Иванцов, Э.Л. Сидоренко, Б.А. Спасенников, Ю.М. Березкин, Я.А. Суходолов // Cyberleninka.ru [Электронный ресурс]. – 2019. – Режим доступа: https://cyberleninka.ru/article/n/prestupleniya-svyazannye-s-ispolzovaniem-kriptovalyuty-osnovnye-kriminologicheskie-tendentsii/viewer. – Дата доступа: 15.04.2022.
4. Росфинмониторинг фиксирует факты финансирования терроризма с использованием криптовалют // ТАСС [Электронный ресурс]. – Режим доступа: https://tass.ru/ekonomika/10978989. – Дата доступа: 15.04.2022.
5. Гамко, С.Л. Разоблачение преступной схемы хищения криптовалюты / С.Л. Гамко // Предварительное расследование. – 2019. - № 2. – С. 87–90.
6. Приговор суда Ленинского района г. Минска от 13 декабря 2021 г. // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/pravovaya-informatsiya/bank-sudebnykh-resheniy/document/159123. – Дата доступа: 24.04.2022.
7. Гражданский кодекс Российской Федерации // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142/. – Дата доступа: 10.04.2022.
8. Гражданский кодекс Республики Казахстан (Общая часть), принят Верховным Советом Республики Казахстан 27 декабря 1994 года (с изменениями и дополнениями по состоянию на 12.01.2022 г.) // Юрист [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/document/?doc_id=1006061. – Дата доступа: 10.04.2022.
9. Гражданский кодекс Республики Беларусь № 218-З от 7 декабря 1998 г. // ЭТАЛОН-ONLINE [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=hk9800218. – Дата доступа: 10.04.2022.
10. Гражданский кодекс Кыргызской Республики от 8 мая 1996 года № 15 (Часть I) (с изменениями и дополнениями по состоянию на 18.01.2022 г.) // Юрист [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/Document/?doc_id=30212538&pos=119;-60#pos=119;-60. – Дата доступа: 10.04.2022.
11. Гражданский кодекс Республики Армения // Национальное Собрание Республики Армения [Электронный ресурс]. – Режим доступа: http://www.parliament.am/law_docs/050598HO239rus.html. – Дата доступа: 10.04.2022.
12. Декрет Президента Республики Беларусь от 21 декабря 2017 г. №8 «О развитии цифровой экономики» // ЭТАЛОН-ONLINE [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=PD1700008. – Дата доступа: 09.04.2022.

13. Уголовный кодекс Республики Беларусь № 275-З от 9 июля 1999 г. // ЭТАЛОН-ONLINE [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=hk9900275&q_id=3215843. – Дата доступа: 13.04.2022.

14. Уголовный кодекс Российской Федерации // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/. – Дата доступа: 13.04.2022.

15. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 02.03.2022 г.) // Юрист [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/document/?doc_id=31575252. – Дата доступа: 13.04.2022.

16. Уголовный кодекс Республики Армения // Национальное Собрание Республики Армения [Электронный ресурс]. – Режим доступа: http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=rus. – Дата доступа: 13.04.2022.

17. Уголовный Кодекс Кыргызской Республики от 28 октября 2021 года № 127 (с изменениями и дополнениями по состоянию на 01.04.2022 г.) // Юрист [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/m/document?doc_id=34350840. – Дата доступа: 13.04.2022.

УДК 351

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ В ДАНИИ: ФАКТОРЫ УСПЕХА

А. И. Анищенко
В. С. Соколовский

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье рассмотрен пример Дании как лидера в области цифровой трансформации сферы государственного управления. Содержание работы отражает ключевые факторы успеха и национальные особенности реализации стратегий по цифровому развитию Дании. В статье также проводится демонстрирование различия подходов к реформированию системы государственного управления.

Ключевые слова: электронное правительство, государственные электронные услуги, реформирование системы государственного управления.

THE DIGITAL TRANSFORMATION OF PUBLIC ADMINISTRATION IN DENMARK: SUCCESS FACTORS

A.I. Anischenko
U.S. Sakalouski

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article considers the example of Denmark as a leader in the digital transformation of the sphere of public administration. The content of the article reflects the key success factors and national peculiarities of the implementation of the Danish digital development strategies. The article also demonstrates the differences in approaches to public administration reform.

Keywords: e-government, government e-services, the process of reforming the system of public administration.

Переход к полноценному стабильно и эффективно функционирующему электронному правительству предполагает сложный инновационный процесс адаптации сложившейся модели государственного управления и взаимодействия между правительством и обществом к новым условиям на основе использования современных информационных и коммуникационных технологий (ИКТ). Речь идет о фундаментальных преобразованиях, требующих комплексного подхода и ориентированных, в первую очередь,

на интересы и потребности населения. При этом важно обеспечить баланс государственных и частных интересов, минимизировав риски, сопутствующие цифровизации.

Признанным мировым лидером в области использования цифровых технологий в государственном секторе, последовательно реализующим именно такой подход, является Дания, которая уже традиционно занимает первое место в рейтинге стран, охваченных исследованием Организации Объединенных Наций по вопросам электронного правительства [1]. Ранжирование данного рейтинга происходит на основании системного анализа трех компонентов с точки зрения качества и количества показателей 1) электронных (цифровых) услуг (e-Government Development Index, EGDI и иных онлайн-сервисов), 2) ИКТ-инфраструктуры и 3) человеческого капитала [2, с. 166]. В качестве впечатляющих достижений датского государства в сфере цифровой трансформации государственного управления можно упомянуть: полный отказ от традиционного делопроизводства и бумажного документооборота и автоматизация работы государственного сектора, для чего в Дании был создан целый ряд порталов и онлайн-ресурсов, упрощающих взаимодействие как между чиновниками, так и общение органов государственного управления с обычными гражданами: «Virk.dk», «Digital Post», «Sikkerdigital.dk» и др.; внедрение цифрового ключа – «NemID» (дат. «*ПростоID*»), который обеспечивает простой, удобный и безопасный доступ к широкому спектру публичных и частных сервисов в сети Интернет, включая интернет-банкинг, налоговые формы, службы страхования и пенсионные фонды, с использованием единого идентификатора пользователя и пароля доступа; эффективное вертикальное и горизонтальное (межведомственное) взаимодействие государственных органов и должностных лиц на всех уровнях государственного управления (муниципальный, региональный и общегосударственный), которое опирается на централизованную инфраструктуру ИКТ, связывающую национальные правительственные учреждения, местные органы власти и муниципалитеты. Компетентные представители каждого из этих трех уровней принимают непосредственное участие в выработке, согласовывании и реализации единой стратегии цифровой трансформации государственного сектора. При этом, что интересно, основная нагрузка по имплементации стратегических инициатив правительства ложится как раз на муниципальные и региональные органы власти.

Не останавливаясь на достигнутом, Дания полна решимости оставаться лидером по развитию электронного правительства в мире, о чем свидетельствует реализуемая в настоящее время шестая цифровая стратегия на 2022-2025 годы [3]. Сформулированные в ней долгосрочные приоритеты сфокусированы на подготовке электронного правительства Дании к будущим вызовам посредством укрепления партнерских отношений между

государственным и частным сектором в области инноваций; внедрения технологий искусственного интеллекта[4] и новой системы кибербезопасности; защиты данных и обеспечения равного доступа к ним, дальнейшей цифровизации компаний и развития цифровых навыков граждан.

Используемые датским правительством меры финансового стимулирования включают, среди прочего, налоговые вычеты для предприятий, приобретающих оборудование ИКТ (например, робототехнику и 3D-принтеры) а также инвестирующих в исследования и разработки в области робототехники и беспилотных технологий; гранты для оплаты специализированных консультаций по вопросам экспорта электронных товаров и услуг; финансирование улучшения широкополосной связи, внедрения новых технологий и цифровых решений в секторе здравоохранения [4].

Принимая во внимание, что Республика Беларусь в 2022 году оказалось на 58-м месте из 193 государств-участников вышеупомянутого рейтинга ООН, опустившись на 18 позиций по сравнению с итогами рейтинга 2020 года и на 20 позиций по сравнению с 2018 годом, для развития отечественной системы электронного правительства и совершенствования правового регулирования государственных услуг в Республике Беларусь представляется полезным выявление и анализ ключевых факторов успеха датской модели. При этом необходимо отметить, что успешная реализация такого сложного комплексного проекта как цифровая трансформация зависит от большого количества самых разнообразных (от сугубо технологических до социокультурных) и при этом взаимосвязанных факторов. И с этой точки зрения первостепенной является «увязка» этого многообразия в единую стратегию цифровой трансформации государства, которая должна реалистично учитывать как локальные национальные особенности, имеющуюся технологическую платформу и доступные финансовые ресурсы, так и универсальные актуальные общемировые тренды. Дания как раз являет собой отличный пример такого системного, стратегического подхода к цифровой трансформации, начавшейся в 2001 года и продолжающейся до сих пор. Каждые четыре года общенациональная цифровая стратегия Дании подвергается всесторонней публичной ревизии и ее приоритеты обновляются сообразно достигнутым результатам и вызовам времени.

Основополагающим *институциональным* аспектом, без которого любую, даже самую выверенную и удачную стратегию можно «загубить» в бюрократической «междуусобице» и межведомственной прокрастинации

[4] Следуя передовым трендам в сфере ИТ, Дания уже в 2021 году приступила к реализации национальной стратегии искусственного интеллекта. В рамках этой стратегии предусмотрено создание специального инвестиционного фонда с целью финансового стимулирования и обеспечения реализации проектов, способствующих достижению цифрового благополучия при помощи использования технологий машинного обучения и искусственного интеллекта. Такие проекты предполагается реализовать в области здравоохранения, социальной сферы и занятости населения.

является наличие единого государственного органа, ответственного за реализацию цифровой стратегии и наделенного необходимыми для этого полномочиями. В Дании эту функцию с 2010 года выполняет Датское агентство по цифровизации (дат. Digitaliseringsstyrelsen[5]), созданное путем слияния нескольких государственных органов, ранее вовлеченных в эту работу. К его компетенции отнесены как выработка общего видения, стратегии, дорожных карт ее реализации, так и ежедневная координация всех стратегических инициатив на всех уровнях государственного управления [5, с. 457].

Далее, для успешной практической реализации выработанных стратегических замыслов Дании потребовалось обеспечить всеобщий доступ граждан к сети Интернет и их осведомленность о механизмах получения государственных электронных услуг. Как следствие страна занимает лидирующие позиции в мире по показателю доступа граждан к сети Интернет (94% домохозяйств подключены к сетям с очень высокой пропускной способностью (VHCNs) и 70,1% к оптоволоконным сетям [4], обладает одним из самых высоких в Европе покрытий своей территории мобильной широкополосной связью 5G (доступна в более 80% населенных пунктов).

Хорошее технологическое обеспечение подкреплено развитием человеческого капитала и наличием у населения «цифровых» компетенций (71 % датчан имеют навыки работы с цифровыми технологиями, из них почти 50 % имеют навыки выше базовых) [2, с.161]. Этого удалось достичь благодаря реализации в рамках стратегии цифрового развития на 2016-2020 годы общенациональной программы по обучению цифровым основам граждан, которые не обладали базовыми навыками использования интернет ресурсов. Еще одним важным фактором датского успеха стало эффективное сотрудничество между государственным и частным сектором, стимулирующее взаимное доверие между правительством, гражданами и бизнесом.

Так, весной 2021 года правительство Дании запустило общенациональный проект «Партнерство по цифровизации» [6]. Эта инициатива предполагает стимулирование инклюзивного диалога о проблемах и перспективах использования цифровых технологий для дальнейшего совершенствования электронного правительства в Дании с участием представителей датского бизнеса, академических кругов, гражданского общества, профсоюзов и конечно же органов власти на всех уровнях государственного управления в Дании. В рамках партнерства предполагается укрепить понимание положительного влияния эффективно функционирующего электронного правительства не только на рост национального благосостояния и экономическое развитие, но и на укрепление равенства возможностей и социальной защищенности населения Дании.

[5] https://digst.dk/

Положительную роль в датском успехе сыграла и проактивная модель международного сотрудничества в области электронного правительства, особенно с другими странами Северной Европы. Наглядным примером такого сотрудничества является портал «Nordisk-eTax»[6], который уже много лет успешно используют налоговые органы Норвегии, Дании, Исландии, Финляндии и Швеции.

В завершение отметим, что в переходе от «аналогового» к «электронному» правительству критической ошибкой может стать сведение процесса реформирования к сугубо утилитарной «*цифровизации*» (англ. "*digitization*") отдельных административно-распорядительных функций государственного аппарата и банальному упрощению бюрократических процедур, преимущественно в интересах чиновников. Повторение же датского успеха возможно только при условии полноценной «*цифровой трансформации*» (англ. "*digital transformation*") всей системы государственного управления, то есть осуществления системных *организационных* преобразований посредством эффективного использования современных цифровых технологий с целью принципиального улучшения качества работы государственного аппарата при соблюдении баланса интересов государства, бизнеса и граждан, включая наименее социально защищенные слои населения.

Библиографический список

1. United Nations E-Government Survey 2022: The Future of Digital Government. [Электронный ресурс]. – Режим доступа: https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf – Дата доступа: 15.10.2022.
2. Холодная, Е. В. Цифровизация Дании: опыт лидера по реализации проекта "электронное правительство" / Е. В. Холодная // Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций : Сборник научных трудов по материалам I Международной научно-практической конференции, Саратов, 17–18 октября 2019 года / Под редакцией Н.Н. Ковалевой. – Саратов: Саратовская государственная юридическая академия, 2019. – С. 165-167.
3. The Joint Government Digital Strategy. [Электронный ресурс]. – Mode of access: https://en.digst.dk/strategy/the-joint-government-digital-strategy/ – Date of access: 15.10.2022.
4. Digital Economy and Society Index (DESI) 2021. Country report. Denmark. [Электронный ресурс] – Mode of access: https://digital-strategy.ec.europa.eu/en/policies/desi-denmark. – Date of access: 15.10.2022.
5. Nielsen Morten Meyerhoff. Governance lessons from Denmark's digital transformation. [Электронный ресурс]. – Mode of access: https://digital-strategy.ec.europa.eu/en/policies/desi-denmark. – Date of access: 15.10.2022.
6. The Danish Government Digitisation Partnership. [Электронный ресурс]. – Mode of access: https://en.digst.dk/strategy/the-danish-government-digitisation-partnership/ – Date of access: 15.10.2022.

[6] https://www.nordisketax.net/language/

УДК 004.056.5

К ВОПРОСУ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ФИЗИЧЕСКИХ ЛИЦ, ИСПОЛЬЗУЮЩИХ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ

О. В. Босько

Институт информационных технологий УО «Белорусский государственный университет информатики и радиоэлектроники»,
ул. Петруся Бровки 6, Минск, 220013, Беларусь

Статья посвящена анализу и систематизации рисков, которым подвергаются участники информационного обмена, а также вопросу обеспечения безопасности персональных данных физических лиц, использующих информационную инфраструктуру в личных целях.

Ключевые слова: информационная инфраструктура, информационный обмен, персональные данные, безопасность, риски.

TO THE QUESTION OF ENSURING THE SECURITY OF PERSONAL DATA OF INDIVIDUALS USING INFORMATION INFRASTRUCTURE

O. V. Bosko

Institute of Information Technologies
Belarusian State University of Informatics and Radioelectronics,
6 Petrusya Brovki street, Minsk, 220013, Belarus

The article is devoted to the analysis and systematization of the risks to which the participants of information exchange are exposed, as well as the issue of ensuring the security of personal data of individuals using the information infrastructure for personal purposes.

Keywords: information infrastructure, information exchange, personal data, security, risks.

Использование информационной инфраструктуры для информационного обмена имеет неоспоримые преимущества, среди которых экономия, функциональность, эффективность и целый ряд других. Однако помимо положительных сторон есть риски, которым подвергается как информация, так и сами участники информационного обмена.

Для передаваемой информации существует угроза перехвата, изменения либо подделки и утери информации. В связи с этим основными целями информационной безопасности является сохранение:

- конфиденциальности информации (ее доступности только ограниченному кругу пользователей информационной системы);

- целостности информации (обеспечения защиты от случайного или преднамеренного искажения или разрушения);

- доступности информации.

Опасность перехвата данных особенно велика при использовании сети Интернет. Интернет является открытой системой, предназначенной для свободного обмена информацией. Злоумышленники часто предпринимают попытки несанкционированного доступа к информации. Их действия представляет постоянную угрозу, в том числе для сетей, подсоединенных к Интернету.

При информационном обмене существует риск, что канал обмена данными может быть использован для проведения кибератак. Участник обмена не может в полной мере быть уверен в защищенности других сторон взаимодействия и безопасности передаваемой ими информации. Файлы могут содержать компьютерные вирусы любого типа, червя, троянскую программу или вредоносную программу другого типа, которые могут нанести серьезный урон, привести к повреждению или даже полной утрате информации, содержащейся на компьютере получателя. Еще одним риском для участников информационного обмена является угроза безопасности их персональных данных. В соответствии с Законом Республики Беларусь «О защите персональных данных» персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано [1].

Таким образом, исходя из определения, которое дает закон, персональные данные, – это любая информация, с помощью которой можно прямо или косвенно идентифицировать человека. К такой информации можно отнести паспортные данные (ФИО, пол, дата рождения, серия и номер паспорта, личный номер, адрес регистрации и проживания); биометрические данные (отпечатки пальцев, ладоней, радужная оболочка глаза, характеристики лица и его изображение, описание внешности); генетические данные (ДНК, группа крови); специальные персональные данные (расовая либо национальная принадлежность, политические взгляды, членство в профсоюзах, религиозные или другие убеждения, здоровье, привлечение к административной или уголовной ответственности) и т.д.

Закон Республики Беларусь «О защите персональных данных» регулирует отношения, связанные с защитой персональных данных при их обработке, и не распространяется на отношения, касающиеся случаев обработки персональных данных физическими лицами в процессе исключительно личного, семейного, домашнего и иного подобного их использования, не связанного с профессиональной или предпринимательской деятельностью.

В связи с тем, что физические лица часто используют информационную инфраструктуру и становятся участниками информационного обмена в личных целях, безопасность их персональных данных не всегда может быть обеспечена в процессе таких коммуникаций.

Если рассматривать информацию в качестве объекта, который может быть уничтожен, изменен или похищен, то граждане чаще всего подвергаются следующим видам атак [2]: а) вирусы, трояны, иные вредоносные программы, наносящие урон целостности компьютерных систем; б) программы-вымогатели, занимающие весь экран устройства и не исчезающие до выплаты мошенникам определенной суммы; в) фишинг или хищение информации о банковских картах и счетах путем социальной инженерии, когда физическое лицо добровольно выдает мошеннику, представившемуся сотрудником банка, требуемую информацию, или путем подмены сайта магазина или кредитного учреждения на его подобие; г) кража персональных данных для последующего использования с целью получения каких-либо преференций от имени пострадавшего.

Персональные данные физических лиц, полученные в процессе личного информационного обмена, могут быть использованы злоумышленниками для иных целей (побуждение к совершению преступлений, вовлечение в экстремистскую деятельность и др.).

Таким образом, в результате проведенного анализа определены риски, которые возникают в процессе информационного обмена и использования информационной инфраструктуры: риски для конфиденциальности, целостности и доступности информации (как передаваемой, так и содержащейся на компьютерах участников информационного обмена), а также риски для сохранности персональных данных участников информационного обмена.

В связи с тем, что персональные данные физических лиц могут быть использованы для противоправной деятельности, обосновано разработать комплекс мер, направленных на обеспечение безопасности персональных данных физических лиц, использующих информационную инфраструктуру в рамках информационного обмена, осуществляемого в личных целях.

Библиографический список

1. О защите персональных данных [Электронный ресурс] : Закон Респ. Беларусь, 7 мая 2021 г., № 99-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Свойства безопасности информации [Электронный ресурс] // Информационная безопасность. – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/svojstva-bezopasnosti-informatsii/. – Дата доступа: 04.10.2022.

УДК 347

НЕКОТОРЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВИЗАЦИИ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

С. М. Глебко

Открытое акционерное общество «Минский тракторный завод»,
ул. Долгобродская 29, Минск, 220009, Беларусь

В статье рассматриваются некоторые вопросы правового регулирования новых субъектов и объектов цифровизации. Констатируется переход от мягкого права и саморегулирования к установлению в национальных юрисдикциях обязательных требований к правообладателям цифровых платформ, агрегаторов, маркетплейсов и мер экономического воздействия в случае их неисполнения. Исследуются проблемы регламентации правовых режимов новых цифровых объектов гражданских правоотношений. Предлагается объединить права на некоторые такие объекты в новую (третью) группу имущественных прав, носящих абсолютный характер.

Ключевые слова: цифровизация, новые цифровые субъекты, новые цифровые объекты, особенности, правовой режим.

SOME PROBLEMS OF LEGAL REGULATION OF DIGITALIZATION OF ECONOMIC ACTIVITY

S. M. Glebko

Open Joint Stock Company «Minsk Tractor Works»,
29 Dolgobrodskaya street, Minsk, 220009, Belarus

The article discusses some issues of legal regulation of new subjects and objects of digitalization. The transition from soft law and self-regulation to the establishment in national jurisdictions of mandatory requirements for copyright holders of digital platforms, aggregators, marketplaces and measures of economic impact in case of their non-fulfillment is stated. The problems of regulation of legal regimes of new digital objects of civil legal relations are investigated. It is proposed to combine the rights to some such objects into a new (third) group of property rights that are of an absolute nature.

Keywords: digitalization, new digital subjects, new digital objects, features, legal regime.

В Беларуси легализованное определение термина «цифровизация» содержится в государственном стандарте Республики Беларусь «Цифровая трансформация. Термины и определения: СТБ 2583-2020», согласно которому цифровизация – новый этап автоматизации и информатизации экономической деятельности и государственного управления, процесс перехода

на цифровые технологии, в основе которого лежит не только использование для решения задач производства или управления информационно-коммуникационных технологий, но также накопление и анализ с их помощью больших данных в целях прогнозирования ситуации, оптимизации процессов и затрат, привлечения новых контрагентов и т.д. [1]. Таким образом цифровизация экономической деятельности связана с государственным управлением и является одним из наиболее важных глобальных трендов, необратимым процессом, требующим, в первую очередь, своевременного и эффективного участия государства на всех уровнях власти. Важнейшим направлением такого участия, в частности, является разработка и принятие нормативных правовых актов, издаваемых с целью усиления защиты экономических интересов государства и ликвидации законодательных пробелов. При этом цифровизация привела к возникновению новых субъектов и объектов. На правое регулирование отношений между ними должны быть направлены соответствующие нормативные правовые акты.

Относительно новых субъектов, это в первую очередь, правообладатели цифровых платформ (ЦП), а также агрегаторов и маркетплейсов. ЦП – это основной создатель цифровой экосистемы. К их числу в настоящее время можно отнести, к примеру, поисково-информационные системы (Google, Yandex), площадки электронной торговли (AliExpress, Europages), социальные сети (Facebook, Instagram), мессенджеры (Viber, Telegram. WhatsApp), платежно-расчетные сервисы (Alibaba) и мн. др. Доходы наиболее известных ЦП сопоставимы с бюджетами отдельных небольших государств. ЦП максимально извлекают свою выгоду из отсутствия границ в сети Интернет. В результате национальные государства, юридические и физические лица столкнулись со следующими вызовами со стороны ЦП: 1) сверхприбыли без налоговых обязательств; 2) отсутствие прозрачности в отношении использования генерируемых ЦП персональных данных и доступа к ним; 3) проблемы, связанные с навязыванием пользователям цифровых продуктов, установлением несправедливых условий для доступа к важным пользовательским базам данных; 4) неравенство ЦП и пользователя; 5) уход ЦП от юрисдикции государств; 6) монополия ЦП на рынке цифровых услуг и данных; 7) привилегированное положение правообладателя ЦП по отношению к пользователям, которое, как правило, отражено в соответствующих договорах (пользовательских условиях, соглашениях); 7) проблемы обеспечения качества товаров и услуг, продаваемых на ЦП и маркетплейсах, защиты прав потребителей. В данном вопросе защита слабой стороны и национальных интересов являются приоритетом любого государства. При этом слабой стороной здесь выступает не только потребитель, но и отечественные хозяйствующие субъекты, которые несут большую регуляторную нагрузку, чем иностранный аналогичный бизнес, но не имеют никаких

юрисдикционных привилегий.

В правовом регулировании ЦП долгое время отсутствовало понимание необходимости такого регулирования и, тем более, сам его механизм. Но в 2021 г. стало очевидно, что зарубежные государства, даже те, которые больше всех заявляли о саморегулировании этой сферы, начинают устанавливать на уровне нормативных правовых актов требования к ЦП для обеспечения интересов пользователей, государства, общества, национального бизнеса, и разрабатывают меры принуждения их исполнения (в том числе экономические). Как пример – принятие в июле 2022 г. Европейским парламентом двух законов, которые будут регулировать информационно-технологический сектор в ЕС: закон о цифровых рынках (Digital Markets Act) и закон о цифровых услугах (Digital Services Act) [2]. В целом, законы определяют более жесткое регулирование деятельности крупных технологических корпораций и борьбу с их монополизмом. Им могут быть назначены крупные штрафы (до 10% мирового оборота за первое нарушение и до 20% – за повторное). Но это относится только к так называемым интернет-гигантам (компаниям с капитализацией от 75 млрд. Евро или с годовым оборотом в ЕС от 7,5 млрд. Евро, с не менее 45 млн. ежемесячно активных пользователей, и не менее 10 тыс. бизнес-пользователей из стран ЕС). Ясно, что регулирование закона направлено на ЦП и корпорации типа Google, Amazon, Apple, Microsoft, Alibaba. То есть такие ЦП, чье доминирующее положение в киберпространстве «делает сложным для потребителя избежать их использования». От таких ЦП данный закон требует соблюдения, в числе прочего, следующих норм: предоставлять возможность пользователям отписываться от ключевых сервисов платформы так, чтобы во всех остальных отношениях у них были те же условия, что и у тех, кто подписался на такие сервисы; не требовать по умолчанию при установке операционной системы установки важного программного обеспечения (например, браузеров) от этой же платформы; обеспечить справедливый доступ разных разработчиков приложений к таким функциям смартфонов, как NFC-чипы; предоставить продавцам доступ к данным по эффективности маркетинга и рекламы на платформе; обеспечить совместимость разных сервисов обмена сообщениями и др. При этом, компаниям, подпадающим под действие закона, запрещается: делать преференции товарам и услугам, которые предоставляет сама интернет-платформа; устанавливать несправедливые условия для бизнес-пользователей; требовать от разработчиков, которые хотят добавить свой продукт в магазины приложений, использовать определенные сервисы, например, платежные и др. [3].

Также в Евросоюзе достигнуто принципиальное соглашение по новому законопроекту о рынке цифровых услуг (Digital Services Act). Закон обозначил принцип: «что является незаконным в офлайне, является незаконным и

в онлайне» и включает в себя такие меры по борьбе против нелегальных товаров, как: механизмы, в соответствии с которыми пользователи смогут легко и оперативно сообщать о таких товарах на каких-либо цифровых платформах; более эффективное отслеживание и проверка добросовестности продавцов на онлайн-маркетплейсах; запрет введения пользователя в заблуждение; меры по увеличению прозрачности работы интернет-платформ по ряду параметров, включая алгоритмы рекомендаций контента или продуктов для пользователей и др., а также многочисленные положения по защите персональных данных пользователей [2].

В России с 1 июля 2021 г. вступил в силу Федеральный закон № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети Интернет на территории Российской Федерации» [4]. В соответствии с ним иностранные платформы, охватывающие более 500 000 российских пользователей, обязаны открывать на территории Российской Федерации представительства и встать на налоговый учет. Рассмотренные примеры правового регулирования ЦП в Европейском союзе и Российской Федерации, свидетельствуют о переходе от мягкого права и саморегулирования к установлению в национальных юрисдикциях обязательных требований к их правообладателям (в том числе иностранным) и мер жесткого экономического воздействия в случае их неисполнения. На данном этапе аналогичная деятельность ЦП в Республике Беларусь остается не урегулированной.

Следующей проблемой является необходимость регламентации правовых режимов новых цифровых объектов гражданских правоотношений. Это обусловлено объективными потребностями в стабильности и предсказуемости актов гражданского оборота. Обеспеченная нормативным порядком универсальность и ясность правовых последствий принадлежности и оборота новых цифровых объектов гражданских правоотношений не только расширяет границы имущественного статуса лиц, но и единообразно определяет режим их оборотоспособности.

Предусмотренные ст. 128 Гражданского кодекса Беларуси «Виды объектов гражданских прав» в настоящее время требуют дополнения и упорядочивания. Классические цивилистические подходы в объекту гражданских правоотношений методологически организованы в соответствии с теми представлениями, что объект правоотношения имеет материальную форму. В тоже время процессы цифровизации гражданского оборота привели к появлению цифровых объектов гражданских правоотношений, которые часто не имеют такой формы. Это порождает возникновение проблемы их определения, выявления правовой природы и особенностей установления их правового режима, способов защиты прав на них. Анализ доктринальных представлений о цифровых объектах позволяет сделать вывод о том, что в числе прочего, они должны вписываться в уже существующую систему

объектов с учетом присущих им особенностей.

С нашей точки зрения, на данном этапе, к новым цифровым объектам гражданских правоотношений, применительно к цифровой экономике, можно отнести: криптовалюты; индивидуально определенные токены (NFT); большие данные; доменные имена; смарт-контракты; исключительно электронные формы обязательственных либо корпоративных прав (корпоративные ценные бумаги); национальная цифровая валюта; цифровые модели продукта; новые нематериальные объекты, существующие исключительно в цифровой форме; цифровые платформы, агрегаторы, маркетплейсы; роботы и другие машины, наделенные искусственным интеллектом; различные базы данных.

Если произвести имплементацию поименованных новых цифровых объектов гражданских правоотношений в приведенные в ст. 128 ГК Республики Беларусь виды, то с учетом многочисленных исследований данного вопроса, криптовалюту можно отнести к иному имуществу; большие данные – к базам данных как к объектам авторского права; доменные имена, используемые в коммерческих целях – к имущественным правам; смарт – контракты – компьютерная программа как объект авторского права; исключительно цифровые формы обязательственных либо корпоративных прав (корпоративные ценные бумаги) – ценные бумаги (бездокументарная форма); цифровые модели продукта – объекты права промышленной собственности (полезные модели в объемно-пространственной форме); цифровые платформы, агрегаторы, маркетплейсы – компьютерная программа или база данных как объект авторского права; роботы и другие машины, наделенные искусственным интеллектом – имущество; различные базы данных – базы данных как объекты авторского права.

Относительно национальной цифровой валюты, несмотря на отсутствие на данном этапе ее обращения в Республике Беларусь, можно уже сейчас дополнить такой вид имущества как «деньги» таким их типом как национальная денежная единица в цифровой форме.

Относительно новых нематериальных объектов, существующих исключительно в цифровой форме. В настоящее время к ним, к примеру, можно отнести: стикеры в социальных сетях, месенджерах (viber, WhatsApp, skype и др.); приложения для компьютеров, смартфонов, планшетов; одежда, и другие товары, существующие исключительно в цифровой форме и др. Имущественные права на такие нематериальные объекты не могут быть отнесены к категории вещных прав. Так как согласно постулату гражданского права объектом права собственности может выступать только индивидуально-определенная вещь (материальный предмет). Не могут права на такие объекты рассматриваться и как относящиеся к интеллектуальной собственности, так как они не отвечают установленным законом условиям

охраноспособности. То есть необходимо объединить права на такие объекты в новую (третью) группу имущественных прав, носящих абсолютный характер. И наконец индивидуально определенные токены (NFT), с нашей точки зрения, исключительно по аналогии с криптовалютой, можно отнести к такому виду объектов гражданских прав как иное имущество.

Библиографический список

1. Цифровая трансформация. Термины и определения: СТБ 2583-2020. – Введ. 2021–03–01. – Минск: Госстандарт, 2020. – 16 с.

2. В ЕС одобрены фундаментальные законы о «беспрецедентных стандартах ответственности» онлайн-платформ // [Электронный ресурс]. Режим доступа: https://d-russia.ru/v-es-odobreny-fundamentalnye-zakony-o-besprecedentnyh-standartah-otvetstvennosti-onlajn-platform.html. Дата доступа: 10.10.2022.

3. На интернет-контролеров нашли управу // [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/5280299. Дата доступа: 10.10.2022.

4. О деятельности иностранных лиц в информационно-телекоммуникационной сети Интернет на территории Российской Федерации» [Электронный ресурс]: Федеральный закон, 1 июля 2021 N 236-ФЗ // КонсультантПлюс / ООО «ЮрСпектр» – М., 2022.

УДК 32.01+32:002:004.8

ПОЛИТИЧЕСКАЯ ТЕОРИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Е. М. Ильина

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье раскрыты политологические основания искусственного интеллекта, выявлены его особенности и потенциал для современной политической теории и практики государственного управления в условиях цифровой трансформации.

Ключевые слова: политическая теория искусственного интеллекта, предиктивная аналитика больших данных, метавселенная, цифровое профилирование, интеллектуальный бот, дипфейк.

POLITICAL THEORY OF ARTIFICIAL INTELLIGENCE UNDER CONDITIONS OF DIGITAL TRANSFORMATION OF PUBLIC ADMINISTRATION

E. M. Ilyina

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The political science foundations of artificial intelligence, its features and potential for modern political theory and public administration practice under conditions of digital transformation are revealed in the article.

Keywords: political theory of artificial intelligence, big data predictive analytics, metaverse, digital profiling; intelligent bot, deepfake.

Термин «искусственный интеллект» (далее – ИИ) был введен в научный оборот в 1956 г., что стало официальной точкой отсчета изучения ИИ как экспериментального в своей основе междисциплинарного научного направления, связанного с проектированием интеллектуальных компьютерных систем, позволяющих имитировать когнитивные функции человека.

Под воздействием технологий ИИ из внешней среды на «вход» политической системы неизбежно поступают вызовы с вариативными и неопределенными последствиями, кардинально преобразующие систему

государственного управления в целом или ее отдельные подсистемы и функции. Применение технологий ИИ в политике и государственном управлении предопределено множеством существенных преимуществ и широких возможностей при полной государственной поддержке перспективных цифровых технологий в условиях конструктивного сотрудничества по линии «государство – частный сектор», региональной и международной кооперации. Использование ИИ для анализа больших данных в политико-управленческой практике позволяет значительно упростить процесс принятия решений в условиях неопределенности, что тесно связано с концепцией Data-Driven Political Campaign (применение больших данных, преимущественно в электоральных кампаниях, включающее стадии сбора и алгоритмического анализа массива информации для выстраивания психограмм избирателей, сегментирования аудитории и политического микротаргетинга) и парадигмой Data-Driven Government (принятие управленческих решений институтами государственной власти с помощью интеллектуальных систем поддержки принятия решений на основе технологий и методов анализа больших данных).

В контексте предиктивной аналитики больших данных интересен многолетний опыт представителей Пермской научной школы искусственного интеллекта по проектированию, обучению и тестированию нейросетевых математических моделей для выявления закономерностей и прогнозирования результатов президентских и парламентских выборов и разработки рекомендаций по улучшению рейтинга политических лидеров. В частности, пермскими учеными за полтора года до президентских выборов 2008 г. в России была спрогнозирована победа Д. А. Медведева, когда его личность как политика была еще мало известна.

ИИ и машинное обучение, расширяя предиктивный потенциал технологии моделирования цифровых двойников (от англ. digital twin) – виртуальных аналогов любых физических объектов или процессов, становятся ядром системы «интеллектуальных двойников» (Intelligent Twins) – новой открытой архитектуры для интеллектуальной трансформации государственных органов и городских служб (интеллектуальный двойник города), отраслей промышленности (интеллектуальный двойник промышленности) и предприятий (интеллектуальный двойник бизнеса).

В условиях конвергенции физической и искусственной реальности ИИ является одним из главных факторов развития концепции «олицетворенного» Интернета / Web 3.0 – метавселенной (от греч. meta – за пределами, вне; от англ. metaverse), которую в политологическом ракурсе можно представить как новый трехмерный виртуально-реальный интерфейс политической системы, децентрализованно управляемый множеством индивидуальных и коллективных цифровых политических акторов (цифровые

персональные копии реальных людей / аватары, боты, виртуальные политические институты и др.) посредством формальных и неформальных форм цифровых политических практик (блокчейн-демократия, цифровая политическая изоляция, цифровая гражданственность, онлайн-митинги, цифровые GR-технологии и др.) [1, с. 248].

Активное внедрение технологий ИИ, включая компьютерное зрение, распознавание и синтез речи, обработку естественного языка, интеллектуальную поддержку принятия решений, способствует развитию систем цифрового профилирования физических и юридических лиц. Такие системы применяются как для управления государственными данными посредством сбора, алгоритмической обработки, анализа и предоставления персональных, в том числе биометрических, сведений, образующих цифровой профиль, с согласия человека или организации по запросу органа власти через соответствующие электронные платформы, так и для социального скоринга (от англ. score – оценка) – алгоритмического оценивания и рейтингования индивидуальных и коллективных субъектов на основе социальных характеристик, полученных в результате мониторинга поведенческих офлайн- и онлайн-активностей, позволяющих прогнозировать их поведение.

Сравнительно новыми ИИ-решениями в политическом и государственном секторах являются интеллектуальные боты (от англ. bot, сокращение от robot) – автоматизированные самообучающиеся алгоритмы, имитирующие поведение реальных политических акторов в новых социальных сетевых медиа для конструирования политической реальности и оказания влияния на общественное мнение или на платформах электронных государственных услуг для быстрой обработки запросов граждан, сбора необходимой информации, виртуальной помощи в решении различных проблем и оптимизации работы государственных структур.

Новым универсальным и эффективным медиаинструментом политики постправды и «мягкой силы» в условиях информационного противоборства становятся дипфейки (от англ. deep learning – глубокое обучение и fake – подделка) – медиаконтент на основе ИИ, синтетически создаваемый посредством генерирования нейронными сетями по генеративно-состязательному принципу новых изображений, видеороликов, аудиофайлов из исходных наборов данных. В политологическом ракурсе наиболее показательны следующие направления применения дипфейк-технологии: конструктивная практика привлечения электората и продвижения политического имиджа кандидата, в том числе среди молодежи; дезинформация, манипулирование избирателями в политических кампаниях, провокация, дискредитация, шантаж и кибербуллинг политических оппонентов; делегитимация институтов государственной власти и дестабилизация политической системы,

деструктивное информационное воздействие и искажение глобального информационного поля, дискредитация государства.

Со стороны государственного сектора увеличивается спрос на беспилотные летательные аппараты и комплексы, оснащенные системами управления на основе ИИ, применяемые как для поисково-спасательных работ, строительства, логистики, мониторинга и охраны природных объектов и городской инфраструктуры, так и для выполнения военных задач в контексте новой парадигмы ведения боевых действий и интеллектуализации вооружения. Интенсивно развивается рынок беспилотной сельскохозяйственной, карьерной, горнодобывающей техники и пассажирских перевозок в условиях развертывания беспилотных технологий на базе ИИ, 5G-сетей и периферийных вычислений.

С каждым годом появляется все больше ИИ-решений в сфере автоматизации политической журналистики, которые не только облегчают выполнение ряда рутинных задач журналистского труда (мониторинг и анализ новостной повестки дня политики, определение инфоповодов, проверка фактов и поиск источников политической информации), но и берут на себя часть работ по непосредственному созданию политического контента. Трудно переоценить потенциал алгоритмов ИИ для политического спичрайтинга.

Таким образом в условиях цифровой трансформации государственного управления формируется *политическая теория ИИ* как относительно автономная специфическая система политического знания, отражающая, объясняющая, оценивающая и прогнозирующая политические феномены в контексте аналитики больших политико-управленческих данных, моделирования трехмерного виртуально-реального интерфейса политической системы Web 3.0 и интеллектуальных двойников политических институтов, автоматизации и интеллектуализации управленческой деятельности и политических практик, проактивного принятия политических решений и предоставления государственных услуг, цифрового профилирования и социального скоринга физических и юридических лиц, новых дипфейк-инструментов политики постправды и «мягкой силы» в условиях информационного противоборства и новой парадигмы «мозаичных» боевых действий. При этом в рамках данной теории любой политический феномен не может обладать однажды выработанной универсальной трактовкой, поскольку детерминирован и темпорально измеряется доминирующей исторической общественно-политической парадигмой, развивается в рамках ее понятийно-категориального аппарата.

Следует отметить, что сильные стороны и возможности ИИ могут легко трансформироваться в его слабые стороны и риски, которые следует учитывать при принятии стратегических решений о внедрении ИИ в

систему государственного управления в условиях неопределенности современной геополитической ситуации и санкционных ограничений.

Библиографический список

1. Ильина, Е. М. Политика в сфере цифровой трансформации: метавселенная / Е. М. Ильина // Современная политическая наука о траекториях развития государства, бизнеса и гражданского общества (Мир в постковидную эпоху: от разобщенности к единству) : сб. статей II Междунар. науч.-практ. конф., Минск, 15–16 дек. 2021 г.) / Белорус. гос. экономический ун-т. ; редкол.: Н. Ю. Веремеев (гл. ред.) [и др.]. – Минск : Колорград, 2021. – С. 246–248.

УДК 340.1

ПРАВОВОЙ РЕЖИМ ИНФОРМАЦИОННЫХ РЕСУРСОВ ЕВРАЗИЙСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

А. А. Каспирович-Шумак

Администрация Президента Республики Беларусь,
ул. Карла Маркса 38, Минск, 220016, Беларусь

В статье рассматриваются вопросы правовых режимов информационных ресурсов Евразийского экономического союза. На основании проведенного анализа Правового портала Евразийского экономического союза, как одного из основных информационных ресурсов в области права, автор делает вывод о том, что исходя из категории доступа рассматриваемый ресурс имеет общий правовой режим.

Ключевые слова: правовой режим, информация, информационные ресурсы, правовой портал Евразийского экономического союза, цифровизация.

LEGAL REGIME OF INFORMATION RESOURCES OF THE EURASIAN ECONOMIC UNION IN THE CONTEXT OF DIGITALIZATION

A.A.Kaspirovich-Shumak

Administration of the President of the Republic of Belarus,
Karl Marx street 38, Minsk 220016, Belarus

The article deals with the issues of legal regimes of information resources of the Eurasian Economic Union. Based on the analysis of the Eurasian Economic Union Legal Portal, as one of the main information resources in the field of law, the author concludes that, based on the category of access, the resource in question has a general legal regime.

Keywords: legal regime, information, information resources, legal portal of the Eurasian Economic Union, digitalization.

На сегодняшний день современный мир характеризуется динамически развивающейся цифровизацией, протекающей параллельно с внедрением инновационных решений. Ученые, исследователи в различных отраслях права отмечают, что в условиях дальнейшего развития информационного общества «формируются особые вызовы и риски, требующие научного осмысления и формирования решения правовых проблем современности» [1, с. 148].

Согласимся с мнением российского ученого Г.С. Беляевой, отмечающей важность правовых режимов. Вместе с тем, особенностью большинства современных работ, посвященных исследованию правовых режимов, можно считать то, что правовой режим в них рассматривается фрагментарно, иногда исключительно с точки зрения объектов правового регулирования: информации (С.Н. Братановский, Л.К. Терещенко), недвижимого имущества (М.А. Димитриев, Н.М. Кавельникова, Л.К. Терещенко); специальных субъектов: субъектов малого предпринимательства или видов деятельности, к примеру, обеспечения таможенного дела [2, с. 5]. Убедительной звучит точка зрения А.А. Чеботарева, который отмечает, что «основной подход к классификации информационных ресурсов – это критерий доступа к ним пользователей. Итак, по категории доступа информационные ресурсы могут быть открытыми (общедоступными) или с ограниченным доступом. Общедоступная информация предоставляется свободно в силу прямого указания закона в случаях реализации гражданином своих конституционных и иных, предоставленных законом прав» [3, с. 56].

Поддерживаем позицию Л.К.Терещенко о разделении правового режима на: общий правовой режим, выражающий общие, исходные способы правового регулирования, и специальные правовые режимы. Автор обосновывает вывод о том, что в основе как общего правового режима, так и специальных правовых режимов лежат конституционные нормы [4, с. 17]. На основе изучения норм автор приходит к выводу, что общим правовым режимом информации является режим открытой информации. Общий правовой режим информации характеризуется открытостью, доступностью информации как для физических, так и для юридических лиц. Исключения из общего режима информации могут устанавливаться только законом, что и составляет специальный правовой режим. Согласимся с мнением Э.В. Талапиной, что при обращении к действующему законодательству основное разделение информации на категории выстраивается именно в зависимости от возможности доступа к ней: общедоступная информация и информация ограниченного доступа. Общедоступная информация – это общеизвестные сведения и иная информация, доступ к которой не ограничен [5, с. 8].

Переходя к вопросу правового режима информационных ресурсов ЕАЭС, напомним, что государствами – членами ЕАЭС являются Республика Беларусь, Республика Казахстан, Российская Федерация, Республика Армения и Кыргызская Республика. Специальные нормы, касающиеся информационного обмена и взаимодействия в области информационных ресурсов закреплены в некоторых документах ЕАЭС. В качестве примера можно привести Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза, содержащемся в приложении 3 к Договору, закреплены

понятия информационного ресурса и общего информационного ресурса: «информационный ресурс» – упорядоченная совокупность документированной информации (базы данных, другие массивы информации), содержащейся в информационных системах; «общий информационный ресурс» – информационный ресурс Комиссии, формируемый путем централизованного ведения либо на основе информационного взаимодействия государств-членов.

Представляет интерес вопрос о формировании информационных ресурсов в государствах – членах ЕАЭС. Основным правовым порталом ЕАЭС выступает правовой портал ЕАЭС – https://docs.eaeunion.org/ru-ru [6]. Данный ресурс содержит в себе информационно-правововые ресурсы органов ЕАЭС с доступом к: Правовому порталу Республики Армении, Правовому порталу Республики Беларусь, Правовой портал Республики Казахстан, Правовой портал Российской Федерации и сайту Правительства Кыргызской Республики.

Как отмечалось выше, Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза закрепляет понятие общего информационного ресурса, основными путями формирования которого является формирование информационного ресурса централизованно либо формирование информационного ресурса на основе взаимодействия.

Несмотря на закрепление термина общий информационный ресурс, представляет интерес термин «централизованное ведение». В Договоре о ЕАЭС определение данного термина не закреплено, несмотря на то, что он употребляется. Исходя из содержания правового портала ЕАЭС можно отметить, что портал не содержит централизованного (единого) ресурса, включающего базы данных с поисковой системой каждой из государств-участниц ЕАЭС. Сформированный ресурс лишь предлагает перейти на конкретный правовой портал каждого из участников ЕАЭС и предлагает правовые акты, принятые в рамках ЕАЭС.

Отметим, что на сегодняшний день в рамках работы информационно-поисковой системы «ЭТАЛОН» функционирует тематический банк данных «Евразийская экономическая интеграция» [7], который содержит систематизированную по тематическим разделам подборку международных правовых актов и нормативных правовых актов Республики Беларусь регулирующих правовые и финансовые аспекты деятельности ЕАЭС и направленных на дальнейшее развитие Евразийской экономической интеграции. По состоянию на 1 сентября 2022 г. в ТБД «Евразийская экономическая интеграция» включено 2913 правовых акта. Также отметим, что в соответствии с постановлением Совета Министров Республики Беларусь от 30 июня 2012 г. № 616 «Об опубликовании решений некоторых межгосударственных

образований и их органов» [8] решения Евразийского межправительственного совета, Евразийской экономической комиссии и Высшего Евразийского экономического совета, за исключением документов ограниченного распространения, размещаются на Национальном правовом Интернет-портале Республики Беларусь. Эти решения размещаются Национальным центром правовой информации Республики Беларусь с указанием даты их официального опубликования и даты вступления в силу.

Анализ международных договоров ЕАЭС позволяет отметить, что на данном этапе развития Евразийского экономического союза вопросы информационно-правового обеспечения и построения единого информационного пространства находятся на стадии развития. В основном документы касаются общих процессов в рамках союза, к примеру: формирование, ведение и использование единой базы данных о клинических исследованиях, формирование, ведение и использование единого таможенного реестра объектов интеллектуальной собственности государств – членов Евразийского экономического союза, формирование, ведение и использование единого реестра медицинских изделий, зарегистрированных в рамках Евразийского экономического союза.

Представляет интерес точка зрения Д.М. Демичева, который отмечает: «обеспечение единства правового пространства в ЕАЭС заключается в обеспечении принципа конституционности. Составной частью правового пространства является единое информационно-правовое пространство государства либо межгосударственных образований, которое можно рассматривать как совокупность всех форм юридического бытия общества, основанную на Конституции как основе правотворчества и правоприменения, а также в которую встроен единый информационно-правовой ресурс, а также единые технологии и стандарты его функционирования; это совокупность баз и банков данных, содержащих правовую информацию, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим стандартам создания, предоставления, обработки, организации и доступа к данной информации» [9, с. 17]. Автор также дает определение информационно-правового пространства ЕАЭС, под которым понимает «совокупность информационно-правовых ресурсов и информационной инфраструктуры, обеспечивающих максимально полное удовлетворение информационных потребностей субъектов Союза – Евразийской экономической комиссии и иных органов ЕАЭС, правительств и контролирующих органов государств, представителей бизнес-сообщества, иных – в правовой информации на основании предоставления доступа к праву ЕАЭС и национальному законодательству всех государств-членов этого объединения».

Правовой портал ЕАЭС, выступая в качестве основного информационно-правового ресурса ЕАЭС, как было отмечено выше, содержит лишь международные договоры ЕАЭС в актуальном состоянии. В целях повышения доступности правовой информации ЕАЭС представляется перспективным создание банка данных документов Союза, содержащего в актуальном состоянии правовые акты Высшего Евразийского экономического совета, Евразийского межправительственного совета, Евразийской экономической комиссии, решения Суда ЕАЭС и иные документы, касающиеся деятельности Союза, для дальнейшего его размещения на его официальном сайте. Все это позволит представить правовые акты в актуальном состоянии с возможностью просмотра истории всех внесенных в них изменений и (или) дополнений, а также обеспечить взаимосвязь между правовыми актами и получить доступ к тематически связанным документам посредством размещаемых гиперссылок. Анализ Правового портала ЕАЭС как информационного ресурса в области предоставления правовой информации позволяет говорить о том, что исходя из категории доступа рассматриваемый ресурс имеет общий правовой режим, поскольку реализует право свободно получать размещаемую информацию, передавать и распространять.

Библиографический список

1. Камалова, Г. Г. Правовые аспекты обеспечения доступности и достоверности информации в цифровую эпоху в условиях пандемии COVID-19 / Г. Г. Камалова // Аграрное и земельное право. 2021. – № 10. –С. 148–150.

2. Беляева, Г. С. Правовой режим: общетеоретическое исследование : автореф. дис. … докт. юр. наук : 12.00.01 / Г. С. Беляева. – Курск, 2008. – 44 с.

3. Чеботарева, А. А. Информационное право : учеб. пособие / А. А. Чеботарева. – М. : Юридический институт МИИТа, 2014. – 160 с.

4. Терещенко, Л. К. Правовой режим информации : автореф. дис. … докт. юр. наук : 12.00.14 / Л. К. Терещенко. – Москва, 2011. – 54 с.

5. Константинов, Ю. Н. Парадоксы рынка: информационный дефицит // Информационные ресурсы России. – 1997. – № 1. – С. 36.

6. Правовой портал ЕАЭС [Электронный ресурс]. – Режим доступа: https://docs.eaeunion.org/ru-ru. – Дата доступа: 30.08.2022.

7. Евразийская экономическая интеграция [Электронный ресурс]. Режим доступа: http://www.base.spinform.ru/index.fwx. – Дата доступа: 30.08.2022.

8. Об опубликовании решений некоторых межгосударственных образований и их органов [Электронный ресурс] : постановление Совета Министров Респ. Беларусь, 30 июня 2012 г., № 616 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

9. Демичев, Д. М. Информационно-правовое пространство: теория и практика / Д. М. Демичев // Научно-практический журнал «Право.by». – 2018. – № 2. – С. 16–20.

УДК 342

ОБ ОТДЕЛЬНЫХ НАПРАВЛЕНИЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ОРГАНОВ РЕСПУБЛИКИ БЕЛАРУСЬ

И.И. Костян

Национальный центр законодательства и правовых исследований Республики Беларусь,
ул. Берсона 1а, г. Минск, 220030, Беларусь

В условиях стремительного научно-технического прогресса, активной цифровизации белорусского общества, активизации информационного противоборства резко возрастает количество угроз и вызовов в сфере информационной безопасности, в том числе для системы государственных органов, являющейся одним из наиболее уязвимых сегментов в данном контексте. Проведенный в рамках исследования анализ действующего законодательства Республики Беларусь и международных документов позволяет выделить ряд основных направлений по формированию механизма обеспечения информационной безопасности функционирования государственных органов на современном этапе, что в свою очередь создает платформу для нормативного закрепления соответствующих правоотношений.

Ключевые слова: государственные органы, информационная безопасность, цифровизация, информационная общество, киберпреступность.

CERTAIN DIRECTIONS OF ENSURING INFORMATION SECURITY OF STATE BODIES OF THE REPUBLIC OF BELARUS

I.I. Kostyan

Legal Research Institute of the National Center for Legislation and Legal Research of the Republic of Belarus,
1a Bersona street, Minsk, 220030, Belarus

In the conditions of rapid scientific and technological progress, active digitalization of the Belarusian society, activation of information confrontation, the number of threats and challenges in the field of information security is sharply increasing, including one of the most vulnerable segments - the system of state bodies. The analysis of the current legislation of the Republic of Belarus and international documents carried out within the framework of the study allows to identify a number of main directions for the formation of a mechanism for ensuring information security of state bodies at the present stage, which in turn creates a platform for the normative consolidation of relevant legal relations.

Keywords: state bodies, information security, digitalization, information society, cybercrime.

В условиях активной цифровизации белорусского общества, находящегося в авангарде развития сферы информационных технологий, государство должно быть готово к появлению новых угроз в информационном пространстве.

Государственный аппарат, ввиду важности возложенных на него общественных функций, объема концентрируемой там информации является одним из наиболее уязвимых сегментов с точки зрения обеспечения информационной безопасности всего белорусского общества.

Вызовы и угрозы, сопровождающие формирование информационного общества в Республике Беларусь, переопределяют необходимость формирования надежного механизма обеспечения информационной безопасности государственных органов является залогом стабильного развития общества в политической, экономической, социальной и других сферах. Определение основных тенденций в области обеспечения информационной безопасности государственных органов позволят предопределить конкретные меры необходимые для защиты государства от внешних угроз в условиях формирования постиндустриального общества, а также сформировать доктринальную базу для нормативного закрепления информационной безопасности государственного сегмента.

На значимость сферы информационных технологий и важность регламентации происходящих в ней процессов указывает ряд международных и национальных стратегических документов.

В соответствии с ч.1 п.2 Стратегии сотрудничества государств – участников Содружества независимых государств в построении и развитии информационного общества на период до 2025 года, утвержденной Решением Совета глав правительств Содружества независимых государств от 28 октября 2016 г. использование информационно-коммуникационных технологий является одним из приоритетов и необходимым условием повышения качества жизни граждан, развития экономической, социально-политической и культурной сфер жизни общества, а также совершенствования системы государственного управления [1].

Согласно п.п.1, 2 Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. №1 (далее – Концепция) на нынешнем этапе мирового развития информационная сфера приобретает ключевое значение для современного человека, общества, государства и оказывает всеобъемлющее влияние на происходящие экономические, политические и социальные процессы в странах и регионах. Вместе с тем трансформация социума в информационное общество порождает новые риски, вызовы и угрозы, которые напрямую затрагивают вопросы обеспечения национальной безопасности, в том числе защищенность информационного

пространства, информационной инфраструктуры, информационных систем и ресурсов [2]. От правильного понимания таких угроз зависит эффективность механизма обеспечения информационной безопасности государства и общества.

Проблематика угроз информационной безопасности нашла отражение уже в Концепции сотрудничества государств - участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, утвержденной Решением Совета глав государств Содружества Независимых Государств от 10 октября 2008 г., согласно п.4.1 которой угрозы информационной безопасности могут иметь объективный и субъективный характер, выражаться в явлениях, процессах и действиях (или их совокупности), исходить от внешних и внутренних источников [3]. В общих чертах такие угрозы можно поделить на семь ключевых структур, которые задают направления в области обеспечения информационной безопасности государства: нежелательный контент; несанкционированный доступ; утечки информации; потеря данных; мошенничество; кибервойны; кибертерроризм [4, с. 187].

Согласно п.15 Концепции целью обеспечения информационной безопасности является достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие [2]. Мы солидарны с мнением И. В. Днепровской, что системообразующим элементом модели комплекса национальных интересов по мнению является именно государственная составляющая, так как государство представляет собой центральное организационное, регулирующее и контролирующее учреждение общества [5, с. 30]. При этом, государство – это абстрактное, обезличенное понятие. Оно действует опосредованно через уполномоченные органы государственной власти и должностные лица, которые реализуют его волю [6, с. 97].

Таким образом, именно государственный орган является важнейшим структурным элементом государственного механизма. В процессе осуществления возложенных на них законом полномочий государственные органы непрерывно подвержены всем угрозам, вызванным стремительным развитием информационно-технической сферы, что переопределяет необходимость принятия мер по обеспечению информационной безопасности их функционирования. Анализ положений законодательства позволяет выделить несколько направлений, складывающихся в контексте принятия таких мер.

а) Выявление угроз информационной безопасности. На государственном уровне осуществляются мониторинг, анализ и оценка состояния информационной безопасности, применяются индикаторы оценки ее состояния

(п.16 Концепции) [1]. Именно систематическое изучение окружающего государственные структуры информационного пространства позволяет выделить границы их информационной безопасности.

б) Защита персональных данных и обеспечение конфиденциальности личной информации. Обязанность государства по созданию условий для защиты персональных данных и безопасности личности и общества при их использовании закреплена в ч.2 ст.28 Конституции Республики Беларусь [9]. Государством обеспечивается конституционное право граждан на тайну личной жизни и иную охраняемую законом тайну, защиту персональных данных и авторских прав, а также соблюдение баланса прав с ограничениями, связанными с обеспечением национальной безопасности (п.17 Концепции) [2]. Согласно ч.2 ст.4 Закона Республики Беларусь «О защите персональных данных» от 7 мая 2021 г. №99-З обработка персональных данных должна быть соразмерна заявленным целям их обработки и обеспечивать на всех этапах такой обработки справедливое соотношение интересов всех заинтересованных лиц [10]. Анализ нормативных положений обозначенной тенденции позволяет выделить в ней два направления: 1) обеспечение защиты персональных данных, тайны личной жизни должностных лиц государственных органов, осуществляющих в рамках своей профессиональной деятельности функционал по представлению интересов государства; 2) выделение исключительных ситуаций получения государственными органами в рамках их деятельности личных (конфиденциальных) данных граждан при строгом соблюдении баланса прав граждан и интересов национальной безопасности (в том числе информационной безопасности самого государственного элемента).

в) Контроль за обеспечением безопасности в сфере деятельности средств массовой информации. Формируются правовые, организационные и технологические условия для безопасности функционирования национальных средств массовой информации (далее – СМИ), осуществляется государственный и общественный контроль их деятельности (п.17 Концепции) [2]. Работа государственных органов, всегда привлекает внимание СМИ, и от того, насколько объективно в них отражается деятельность государственных органов, зависит восприятие государства обществом, вырабатывается отношение граждан к власти и их доверие к государственным структурам. Кроме того, в условиях сложной геополитической обстановки на формирование общественного сознания серьезно влияют информационные потоки из вне. Так, в условиях активизации «информационных войн» Законом Республики Беларусь от 24 мая 2021 г. №110-З «Об изменении законов по вопросам средств массовой информации» (далее – Закон №110-З) [11] внесены существенные изменения в Закон Республики Беларусь от 17 июля 2008 г. №427-З «О средствах массовой информации» (далее – Закон о СМИ),

которые выразились в принятии в том числе мер по: минимизации иностранного влияния на средства массовой информации (п. 1.5, 1.6 ст. 15 Закона о СМИ); введению новых ограничений для учредителей средств массовой информации (п. 3.3 ст. 10 Закона о СМИ); дополнению оснований для лишения аккредитации журналистов (п. 2-1 ст. 35 Закона о СМИ); запрету к распространению ряда информации, имеющей деструктивный характер (п.п. 1.4, 1.5 ст.38 Закона о СМИ) и др. [12].

г) Привитие культуры безопасного пользования информационными ресурсами. Повышается осведомленность граждан и общества об угрозах национальной безопасности и государственных мерах по ее обеспечению, их вовлеченность в обеспечение безопасности информационной сферы (п.17 Концепции) [2]. Развитие культуры пользования информационными ресурсами, как профилактика нарушений в данной области, должно осуществляться как путем повышения уровня осведомленности самих работников государственных органов (в том числе технического персонала), так и путем проведения государственными структурами соответствующей разъяснительной работы среди населения.

д) Разработка технических условий информационной безопасности в государственных органах. Государство всесторонне содействует защищенности национальных информационных систем. В целях улучшения устойчивости государственного сектора к информационным рискам осваиваются передовые технологии, внедряются новые средства и способы обеспечения информационной безопасности (п.18 Концепции) [2]. Создаются защищенные системы межведомственного электронного документооборота (абз.8 ч.8 п.4.9 Стратегии) [1]. Наращивается научный потенциал и финансирование работ по исследованию и созданию новых решений в сфере обеспечения информационной безопасности, в том числе технической защиты информации, криптологии, криминологии, криминалистики (п.22 Концепции) [2]. Без технической оснащенности государственных органов не представляется возможным обеспечить соответствие процессов цифровизации государственных структур современному уровню научно-технического прогресса.

е) Совершенствование кадровой политики в сфере информационных технологий. Сегодня уделяется особое внимание кадровому потенциалу в обеспечении информационной безопасности. На современном образовательном и технологичном уровне осуществляется специальная подготовка, переподготовка и повышение профессиональной квалификации лиц, обеспечивающих информационную безопасность, сотрудничество между государственными органами, учреждениями образования и отраслевыми предприятиями в подборе, подготовке и трудоустройстве таких кадров, интегрирование тематики информационной безопасности в образовательные

программы всех уровней обучения. Формируется государственный заказ на подготовку кадров (п.21 Концепции) [2]. Таким образом, технологическому потенциалу государственных органов должен соответствовать надлежащий уровень подготовки работников указанных структур, как специализированных (технических), так и непосредственно, осуществляющих профильный функционал государственного органа. Такой уровень подготовки необходимо поддерживать непрерывным повышением квалификации указанных работников в информационной сфере.

ж) Взаимодействие государства по вопросам информационной безопасности с международным сообществом и общественными институтами. Предпринимаются усилия по повышению действенности международного права и соблюдению моральных норм ответственного поведения в информационном пространстве, оказывается содействие разработке и внедрению мер по укреплению доверия в информационном пространстве. (п.23 Концепции) [2]. В рамках Содружества независимых государств ведется обмен информацией и техническими средствами борьбы с нарушениями против информационной безопасности (абз.11 ч.8 п.4.9 Стратегии) [1]. Развивается взаимодействие государства, общественности, бизнес-сообщества, СМИ в целях своевременного обнаружения рисков и вызовов информационной безопасности, воспрепятствования кибератакам и акциям деструктивного информационного воздействия, повышения эффективности правоохранительной деятельности (п.20 Концепции) [2]. Информационная защищенность государственных органов не должна отождествляться с их изолированностью от всех информационных процессов, в том числе на международном уровне.

е) Регламентация ответственности в сфере информационной безопасности. Деяния, причиняющие существенный вред правоохраняемым интересам в информационной сфере или создающие опасность его причинения, криминализируются в уголовном законе в соответствии с существующими мировыми подходами. Осуществляется выявление и привлечение к установленной законом ответственности лиц, наносящих вред государственным информационным системам, обеспечивается государственная защита интересов граждан и организаций вне зависимости от форм собственности (п.19 Концепции) [2]. Так, глава 23 Кодекса Республики Беларусь об административных правонарушениях (далее – КоАП) предусматривает административную ответственность за совершение административных правонарушений в области связи и информации: несанкционированный доступ к компьютерной информации (ст.23.4 КоАП), нарушение законодательства о защите персональных данных (ст.23.7 КоАП) и др. [13]. Главой 31 Уголовного кодекса Республики Беларусь (далее – УК) регламентирована уголовная ответственность за совершение преступлений против информационной безопасности:

несанкционированный доступ к компьютерной информации (ст.349 УК), уничтожение, блокирование или модификация компьютерной информации (ст.350 УК) и др. [14]. Не меньшее значение для обеспечения безопасного функционирования государственных органов сегодня имеет регламентация гражданско-правовой ответственности в информационной сфере.

Деятельность государственного аппарата, находящегося в эпицентре общественной жизни, нуждается в непрерывном обеспечении информационной безопасности в условиях цифровизации.

Трансформация общественных отношений в современном мире, развивающемся в направлении формирования информационного общества, порождает ряд факторов и явлений, представляющих опасность для функционирования государственных органов.

Принятие государством мер по противостоянию указанным угрозам складывается в ряд тенденций по обеспечению информационной безопасности. Выделение указанных тенденций на основе анализа действующего законодательства Республики Беларусь позволяет выделить ряд основных направлений по формированию механизма обеспечения информационной безопасности функционирования государственных органов на современном этапе, что в свою очередь создает платформу для нормативного закрепления основ информационной безопасности процесса функционирования государственных органов.

Библиографический список

1. Стратегия сотрудничества государств - участников Содружества независимых государств в построении и развитии информационного общества на период до 2025 года [Электронный ресурс] : утв. решением Совета глав правительств Содружества независимых государств от 28 октября 2016 г. // ЭТАЛОН. / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
2. Концепция информационной безопасности Республики Беларусь [Электронный ресурс] : утв. постановлением Совета Безопасности Республики Беларусь, 18 марта 2019 г., №1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
3. Концепция сотрудничества государств - участников Содружества Независимых Государств в сфере обеспечения информационной безопасности [Электронный ресурс] : утв. решением Совета глав правительств Содружества независимых государств от 10 октября 2008 г. // ЭТАЛОН. / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
4. Наскидашвили, К. А. Информационная безопасность. Виды угроз информационной безопасности / К. А. Наскидашвили // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университете». – 2020. – Т. 1. – № 12. – С. 187–189.
5. Днепровская, И. В. Государственная составляющая в модели комплекса национальных интересов страны / И. В. Днепровская // Современная экономика: проблемы и решения. – 2010. – № 8. – С. 30-39.

6. Романова, В. В. Понятие органа государственной власти / В. В. Романова // Вектор науки Тольятинского государственного университета. – 2009. – № 5(8). – С. 97-99.

7. Марченко, М. Н. Теория государства и права: учебник. – 2-е издание / М.Н. Марченко – М. : Проспект, 2019. – 640 с.

8. О государственной службе [Электронный ресурс] : Закон Респ. Беларусь, от 1 июня 2022 г., №175-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

9. Конституция Республики Беларусь [Электронный ресурс] : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г. и 17 окт. 2004 г., в ред. Закона Республики Беларусь от 12 окт. 2021 г. N 124-З, Решения республиканского референдума от 4 марта 2022 г. утв. постановлением Совета Безопасности Республики Беларусь // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

10. О защите персональных данных : Закон Респ. Беларусь, от 7 мая 2021 г., №99-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

11. Об изменении законов по вопросам средств массовой информации : Закон Респ. Беларусь, от 24 мая 2021 г., №110-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

12. О средствах массовой информации : Закон Респ. Беларусь, от 17 июля 2008 г., №427-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

13. Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс] : 6 января 2021 г., N 91-З, : принят Палатой представителей 18 декабря 2020 г. : одобр. Советом Респ. 18 декабря 2020 г. : в ред. Закона Респ. Беларусь от 04.01.2022 N 144-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

14. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 12.05.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

УДК 340.13

ТЕНДЕНЦИИ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА О НАУЧНОЙ, НАУЧНО-ТЕХНИЧЕСКОЙ И ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Н.С. Минько

ГНУ «Институт экономики Национальной академии наук Беларуси»,
ул. Сурганова, 1, корп. 2, 220072, Минск, Республика Беларусь

Статья посвящена анализу особенностей развития законодательства о научной, научно-технической и инновационной деятельности в современных условиях. Автором дается оценка возможности формирования на национальном уровне ряда специфических отраслей, подотраслей, институтов (право науки, цифровое право, Интернет-право и др.).

Ключевые слова: право науки, право новых технологий, законодательство о научной, научно-технической и инновационной деятельности, цифровое право (право цифровой среды), Интернет право, платформенное право.

TRENDS IN THE DEVELOPMENT OF LEGISLATION ON SCIENTIFIC, SCIENTIFIC AND TECHNICAL AND INNOVATIVE ACTIVITIES

N. S. Minko

State Scientific Institution
«Institute of Economics of the National Academy of Sciences of Belarus»,
Surganova street, 1, bldg. 2, 220072, Minsk, Republic of Belarus

The article is devoted to the analysis of the features of the development of legislation on scientific, scientific, technical and innovative activities in modern conditions. The author assesses the possibility of forming the level of complexity of a number of specific features, subsectors, institutions (jurisprudence, digital law, Internet law, etc.).

Keywords: law of science, law of new technologies, right to scientific activity, scientific, technical and innovative activity, digital law (law of the digital environment), Internet law, platform law.

Научную, научно-техническую и инновационную сферу деятельности следует рассматривать как самостоятельные этапы единого процесса по разработке новшеств и их последующего освоения в производстве. Правовое регулирование отношений в сфере научной деятельности основано на Конституции Республики Беларусь [1] и осуществляется в соответствии с Законом Республики Беларусь от 21.10.1996 № 708-XIII (ред. от 04.01.2021) «О

научной деятельности» (с изм. и доп., вступившими в силу с 08.01.2021) (далее – Закон «О научной деятельности») [2], другими актами законодательства. В целях обеспечения концентрации государственных ресурсов на реализации наиболее важных и значимых направлений научной, научно-технической и инновационной деятельности Указом Президента Республики Беларусь 07.05.2020 № 156 утверждены приоритетные направления научной, научно-технической и инновационной деятельности на 2021 – 2025 годы [3], среди которых цифровые информационно-коммуникационные и междисциплинарные технологии, основанные на них производства, а также обеспечение безопасности человека, общества и государства: социогуманитарная, экономическая и информационная безопасность.

Видится актуальным закрепление приоритетных направлений научной, научно-технической и инновационной деятельности на законодательном уровне.

Положения о формировании государственной инновационной политики (исходя из принципов свободы научного и технического творчества) отвечают таким конституционным требованиям как гарантирование свободы научного и технического творчества, охрана интеллектуальной собственности законом, содействие государства развитию научных и технических исследований на благо общих интересов. К важнейшему научному заделу и результату, полученному в Институте экономики НАН Беларуси, можно отнести монографию «Концептуальные основы совершенствования правового обеспечения научной, научно-технической и инновационной деятельности в Республике Беларусь» (2018 г.) [4]. В ней коллективом авторов раскрывается система законодательства Республики Беларусь о научной, научно-технической и инновационной деятельности; выявлены и охарактеризованы основные проблемы, возникающие при применении законодательства Республики Беларусь о научной, научно-технической и инновационной деятельности; предложена Концепция совершенствования правового регулирования научной, научно-технической и инновационной деятельности в Республике Беларусь, основу которой составляет обоснование необходимости разработки и принятия кодифицированного нормативного правового акта в указанной сфере. Повышение эффективности научной, научно-технической и инновационной деятельности в Республике Беларусь возможно при наличии современной научной Концепции совершенствования правового регулирования научной, научно-технической и инновационной деятельности, построенной на основе системного подхода. Проект данной Концепции представлен в монографии «Концептуальные основы совершенствования правового обеспечения научной, научно-технической и инновационной деятельности в Республике Беларусь» [4].

Предлагается систематизация, в том числе кодификация законодательства о науке. Ряд актуальных проблем формирования и реализации инновационной функции государства и права неоднократно поднимался В.Г. Тихиней [5; 6]. По его мнению, инновационная функция права должна быть закреплена на высшем законодательном уровне – в Конституции Республики Беларусь. Ученым предлагается разработать и принять Инновационный кодекс Республики Беларусь, он может стать основополагающим нормативным правовым актом белорусского государства, комплексно регулирующим отношения в инновационной сфере деятельности.

Право науки («право научных исследований» или «научно-исследовательское право» (research law)) охватывает правовое обеспечение научной деятельности. С учетом новых вызовов праву, современных условий дигитализации, информатизации и глобализации, перехода научных исследований в цифровой мир, в условиях, когда интеллектуальная собственность становится ведущим видом собственности, с фактически сформированным законодательством о научной, научно-технической и инновационной деятельности как межотраслевой законодательный комплекс закономерно начинает формироваться право науки. Предметом правового регулирования права науки выступают общественные отношения, связанные с правовым регламентированием научных исследований в области естественных и технических наук.

Понятие «право науки» (law of science) используется практически как синоним «научно-исследовательского права», но придает этой новой комплексной отрасли права более значимый и самостоятельный характер, связанный с ее особой ролью в научно-технической революции. Философски новое и еще не до конца познанное и признанное понятие science of science («наука о науке») – это максимально философски и практически широкое понятие, включающее в себя как комплекс всех наук, всех отраслей наук, всех технологий, с ней переплетенных, так и всех взаимосвязанных организационных, финансовых и правовых механизмов, используемых для ее понимания, использования и развития [7, с. 20].

Право науки изучает закономерности и возможности применения механизмов государства и права для регулирования общественных отношений между субъектами, связанными с осуществлением научной деятельности и использованием ее результатов на практике. Центральное место в правовом регулировании научной деятельности занимает Закон Республики Беларусь от 21.10.1996 № 708-XIII (ред. от 04.01.2021) «О научной деятельности» (с изм. и доп., вступившими в силу с 08.01.2021). Основными источниками правового регулирования в области научной деятельности выступают Конституция Республики Беларусь [1], Закон «О научной деятельности» [2], Закон Республики Беларусь от 10 июля 2012 г. № 425-З «О государственной

инновационной политике и инновационной деятельности в Республике Беларусь» [8], Закон Республики Беларусь от 19 января 1993 № 2105-XII (в ред. от 04.01.2021) «Об основах государственной научно-технической политики» [9], Кодекс Республики Беларусь об образовании [10], постановление Совета Министров Республики Беларусь от 22.05.2015 № 431 (в ред. от 01.07.2022) «О порядке функционирования единой системы государственной научной и государственной научно-технической экспертиз» [11], постановление Совета Министров Республики Беларусь от 13.08.2003 № 1065 (в ред. от 31.12.2019) «Об утверждении Положения о научно-технических проектах, выполняемых в рамках международных договоров Республики Беларусь» [12], приказ Государственного комитета по науке и технологиям Республики Беларусь от 22.05.2020 № 153 (вместе с Инструкцией о порядке проведения единой государственной научной и государственной научно-технической экспертиз) [13], Указ Президента Республики Беларусь от 27.05.2019 № 197 (в ред. от 07.05.2020) «О научной, научно-технической и инновационной деятельности» [14], а также Указ Президента Республики Беларусь от 04.02.2013 № 59 (в ред. от 18.06.2018) «О коммерциализации результатов научной и научно-технической деятельности, созданных за счет государственных средств» [15], постановление Государственного комитета по науке и технологиям Республики Беларусь от 24.07.2013 № 10 (в ред. от 19.05.2022) «Об утверждении Инструкции о порядке рассмотрения вопросов, связанных с коммерциализацией результатов научной и научно-технической деятельности, созданных за счет государственных средств» [16] и пр.

При выстраивании иерархии законодательства в области права науки, как нам видится, важнейшее значение имеют документы, носящие программный и концептуальный характер: Концепция совершенствования законодательства Республики Беларусь [17], Концепция национальной безопасности Республики Беларусь [18].

Кроме того, следует отметить, что постановлением Совета Министров Республики Беларусь от 26.03.2021 № 173 «О перечнях государственных и региональных научно-технических программ на 2021 – 2025 годы» утверждены перечень государственных научно-технических программ на 2021 – 2025 годы и перечень региональных научно-технических программ на 2021 – 2025 годы [19], действуют Программа социально-экономического развития Республики Беларусь на 2021 – 2025 годы [20], Указ Президента Республики Беларусь от 15.09.2021 № 348 «О Государственной программе инновационного развития Республики Беларусь на 2021 – 2025 годы» [21], а также должны учитываться положения Указа Президента Республики Беларусь от 25.07.2016 № 289 (в ред. от 18.04.2019) «О порядке формирования, финансирования, выполнения и оценки эффективности реализации государственных программ» [22].

Субъектами права науки являются субъекты научной деятельности – физические и юридические лица, объединения физических и (или) юридических лиц, осуществляющие научную деятельность, а также уполномоченные государственные органы. Субъектами научной деятельности выступают физические лица; временные научные коллективы; научные организации; учреждения, обеспечивающие получение высшего и послевузовского образования, повышение квалификации и переподготовку кадров, органы государственного управления научной деятельностью. В перспективе видится возможным говорить формировании права науки Союзного государства с разработкой соответствующего модельного законодательства.

Другое актуальное направление научных исследований в области права – цифровое право (право цифровой среды) и цифровые права. Предметом правого регулирования в данном случае выступают общественные отношения, связанные с сферой цифрового гражданского оборота с участием нематериальных цифровых объектов, обладающих объявленной или действительной коммерческой ценностью (экономическим содержанием), признаваемые законом и основанные на принципах создания и действия комплексных технологий (технологических платформ) распределенного реестра или иных цифровых технологий (искусственный интеллект, виртуальная и дополненная реальность, криптовалюты и токены, облачные вычисления и др.).

Сегодня научные исследования в области цифрового права главным образом сконцентрированы на вопросах правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде, а также аспектам правового регулирования и саморегулирования в развитии цифровых технологий.

В отношении Интернет права также ведется определенная научная дискуссия. Оно регулирует общественные отношения, формирующиеся в процессе электронной деятельности, осуществляемой в информационной среде.

В свою очередь платформенное право представляет собой регулирующий сетевое взаимодействие юридический механизм, регламентирующий внедрение и применение современных информационно-цифровых технологий и встроенного в них искусственного интеллекта, направленный на обеспечение баланса интересов государства, коллективов людей и каждого отдельного человека и достижение эффективности регулируемых социальных отношений. Предмет платформенного права (как института в рамках Интернет права) составляют отношения, связанные с платформами – цифровыми онлайн механизмами, алгоритмы которых созданы для обслуживания организаций и структур экономической и социальной деятельности.

В связи с указанным важной научной и практической проблемой для Республики Беларусь является разработка законодательного акта по вопросам краудфандинга, деятельности краудфандинговых площадок в Республике Беларусь по вопросам о регулировании деятельности юридических и физических лиц, осуществляющих сбор денежных средств с использованием интернет-сервисов (краудфандинговых площадок).

Современное право новых технологий охватывает такие отрасли, подотрасли и институты, как право науки, цифровое право, Интернет право и платформенное право. В рамках права новых технологий изучению подлежат следующие вопросы: правовое регулирование научной деятельности, включая соглашения о передаче технологии, политику лабораторного регулирования и кодексы поведения; проблемы безопасности, конфиденциальности и наблюдения, возникающие и связи с разработкой новых цифровых технологий и алгоритмов; вопросы пересечения биоэтики и права, особенно в отношении фармацевтической практики, медицинских исследований и новых терапевтических методов; использование новых криминалистических методов в качестве доказательств в судопроизводстве; пределы правового регулирования, сорегулирования и саморегулирования в сфере цифровой экономики и другие [23, с. 69].

Право науки и экономика науки должны развиваться сбалансированно в целях оптимизации принимаемых управленческих решений в сфере научной деятельности. К государственным мерам стимулирования научной, научно-технической и инновационной деятельности относятся: 1) финансовые меры стимулирования; 2) предоставление образовательных, информационно-консультационных услуг, в том числе содействие в разработке проектной документации; оказание содействия в правовой охране, защите и управлении правами на результаты интеллектуальной деятельности; 3) формирование спроса на инновационную продукцию, в том числе посредством использования государственных закупок и системы технического регулирования; 4) стимулирование экспорта инновационной продукции, и технологий, прав на результаты интеллектуальной деятельности, полученные при осуществлении научной, научно-технической деятельности, развитие и защита внутреннего рынка, включая рынок инновационной продукции и рынок прав на результаты интеллектуальной деятельности; 5) имущественные меры стимулирования, в том числе стимулирование создания и функционирования объектов инфраструктуры научной, научнотехнической и инновационной деятельности, а также необходимой для лиц, осуществляющих такую деятельность, социальной, прежде всего жилищной, инфраструктуры; 6) государственно-частное партнерство и иные.

Законодательство в сфере науки и инноваций и соответствующий ему механизм формирования и реализации государственной научно-

технической и инновационной политики должны обеспечить условия для осуществления полного инновационного цикла. Структура законодательства в области научной, научно-технической и инновационной деятельности должна определяться с учетом необходимости формирования правовых, экономических и организационных основ государственного регулирования научной, научно-технической и инновационной деятельности, поэтом важна его систематизация.

Библиографический список

1. Конституция Республики Беларусь 1994 года [Электронный ресурс] : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г., 27 февр. 2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
2. О научной деятельности [Электронный ресурс] : Закон Респ. Беларусь, 21 окт. 1996 г., № 708-XIII : в ред. от 04.01.2021, с изм. и доп., вступившими в силу с 08.01.2021 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
3. О приоритетных направлениях научной, научно-технической и инновационной деятельности на 2021 – 2025 годы [Электронный ресурс] : Указ Президента Республики Беларусь от 07.05.2020 № 156 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
4. Концептуальные основы совершенствования правового обеспечения научной, научно-технической и инновационной деятельности в Республике Беларусь / В. И. Бельский [и др.] ; под ред. В. И. Бельского, В. К. Ладутько. – Минск : Беларуская навука, 2019. – 342 с.
5. Тихиня, В. Г. Современное право Беларуси в условиях инновационного развития общества: проблемы и пути их решения / В. Г. Тихиня // Динамика правотворчества и правоприменения в новых условиях развития экономики: сб. науч. трудов. В 2 ч. / Ин-т парламентаризма и предпринимательства ; кафедра права ; под ред. А. А. Квятович [и др.]. – Минск : ИПП, 2012. – Ч II. – 76 с.
6. Тихиня, В. Г. Роль конституционного контроля в реализации инновационной функции права в Беларуси // В. Г. Тихиня // Конституция Республики Беларусь как ценностный выбор: 25 лет свершений и преобразований: сб. материалов респ. науч.-практ. конф., Минск, 4 марта 2019 г. / редкол. : Г.А. Василевич (гл. ред.) [и др.]; Белорус. гос. ун-т; Ин-т экономики НАН Беларуси; Нац. центр законодательства и правовых исслед. Респ. Беларусь; Нац. центр правовых исслед. Респ. Беларусь; Ин-т подготовки, переподготовки и повышения квалификации судей, работников прокуратуры, судов и учреждений юстиции. – Минск : Право и экономика, 2019. – С. 26–30.
7. Кашкин, С. Ю. Становление права науки как новой комплексной отрасли права / С. Ю. Кашкин // Вестник Ун-та им. О. Е. Кутафина (МГЮА). – 2018. – № 5. – С. 16–27.
8. О государственной инновационной политике и инновационной деятельности [Электронный ресурс]: Закон Республики Беларусь от 10.07.2012 № 425-З : в ред. от 06.01.2022 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
9. Об основах государственной научно-технической политики [Электронный ресурс] : Закон Республики Беларусь от 19.01.1993 № 2105-XII : в ред. от 04.01.2021, с изм.

и доп., вступившими в силу с 08.01.2021 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

10. Кодекс Республики Беларусь об образовании от 13.01.2011 № 243-З (ред. от 23.07.2019) [Электронный ресурс] : Кодекс Республики Беларусь об образовании : с изм. и доп., вступившими в силу с 28.01.2020 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

11. О порядке функционирования единой системы государственной научной и государственной научно-технической экспертиз [Электронный ресурс] : постановление Совета Министров Республики Беларусь от 22.05.2015 № 431 : в ред. от 01.07.2022 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

12. Об утверждении Положения о научно-технических проектах, выполняемых в рамках международных договоров Республики Беларусь : постановление Совета Министров Республики Беларусь от 13.08.2003 № 1065 : в ред. от 31.12.2019 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

13. О единой системе государственной научной и государственной научно-технической экспертиз [Электронный ресурс] : приказ Государственного комитета по науке и технологиям Республики Беларусь от 22.05.2020 № 153 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

14. О научной, научно-технической и инновационной деятельности [Электронный ресурс] : Указ Президента Республики Беларусь от 27.05.2019 № 197 : в ред. от 07.05.2020 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

15. О коммерциализации результатов научной и научно-технической деятельности, созданных за счет государственных средств [Электронный ресурс] : Указ Президента Республики Беларусь от 04.02.2013 № 59 : в ред. от 18.06.2018 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

16. Об утверждении Инструкции о порядке рассмотрения вопросов, связанных с коммерциализацией результатов научной и научно-технической деятельности, созданных за счет государственных средств [Электронный ресурс] : постановление Государственного комитета по науке и технологиям Республики Беларусь от 24.07.2013 № 10 (в ред. от 19.05.2022) // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

17. О Концепции совершенствования законодательства Республики Беларусь [Электронный ресурс] : Указ Президента Республики Беларусь от 10.04.2002 № 205 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

18. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : Указ Президента Республики Беларусь от 09.11.2010 № 575 : в ред. от 24.01.2014 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

19. О перечнях государственных и региональных научно-технических программ на 2021 – 2025 годы [Электронный ресурс] : постановление Совета Министров Республики Беларусь от 26.03.2021 № 173 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

20. Об утверждении Программы социально-экономического развития Республики Беларусь на 2021 – 2025 годы [Электронный ресурс] : Указ Президента Республики Беларусь от 29.07.2021 № 292 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

21. О Государственной программе инновационного развития Республики Беларусь на 2021 - 2025 годы [Электронный ресурс] : Указ Президента Республики Беларусь от 15.09.2021 № 348 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

22. О порядке формирования, финансирования, выполнения и оценки эффективности реализации государственных программ [Электронный ресурс] : Указ Президента Республики Беларусь от 25.07.2016 № 289 : в ред. от 18.04.2019// ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

23. Сатолина, М. Н. Право, наука, техника: проблемы, противоречия и пути их решения / М. Н. Сатолина // Право в современном белорусском обществе: сб. науч. тр. – 2020. – Вып. 15. – С. 64–73.

УДК 316.77

ОТКРЫТЫЕ ДАННЫЕ ДЛЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

П. Н. Орлов

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

Статья посвящена анализу проблем, связанных с внедрением концепции открытых данных в Республике Беларусь. Обосновывается тезис, что позиционирование Беларуси как высокоразвитого государства невозможно представить без открытости органов власти и управления. На основе анализа функционирования национального портала открытых данных, опросов общественного мнения, опыта других стран автор приходит к выводу о расхождении в декларируемых целях и реальной практикой реализации проекта. Предложены концептуальные механизмы выхода из сложившейся ситуации.

Ключевые слова: открытые данные, цифровизация, экономика знаний, государственные услуги, государственное управление, бизнес.

OPEN DATA FOR THE PUBLIC ADMINISTRATION OF THE REPUBLIC OF BELARUS

P. N. Orlov

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article is devoted to the analysis of the problems associated with the implementation of the concept of open data in the Republic of Belarus. The thesis is substantiated that the positioning of Belarus as a highly developed state cannot be imagined without the openness of the authorities and administration. Based on the analysis of the functioning of the national open data portal, public opinion polls, and the experience of other countries, the author comes to the conclusion that there is a discrepancy between the declared goals and the actual practice of project implementation. Conceptual mechanisms for getting out of this situation are proposed.

Keywords: open data, digitalization, knowledge economy, public services, public administration, business.

В 2013 году страны-участники саммита «Большой восьмерки» приняли исторический документ – Хартию открытых данных, которая предусматривает публичное раскрытие информации государственных органов в сети Интернет. Поставить свою подпись под Хартией были приглашены и страны,

не входящие в состав «Большой восьмерки», что придало инициативе глобальный характер.

Главные принципы, прописанные в Хартии: открытость данных по умолчанию, своевременная их публикация в машиночитаемом виде, прозрачность и обязательство обеспечивать условия, в которых разработчики будут создавать приложения на основе открытых данных.

Концепция открытых данных предполагает свободный доступ к данным органов государственной власти, которые раскрывают их деятельность в рамках исполнения ими своих функций. Однако, чтобы считаться открытыми, данные должны соответствовать ряду принципов, которые сводятся к юридической (лицензионная чистота), технической (пригодность для автоматической обработки) и организационной открытости (наличие стратегии и необходимой инфраструктуры.

Информатизация органов государственного управления – один из приоритетов внутренней политики Республики Беларусь. Выступая 20 апреля 2013 года с Посланием белорусскому народу и Национальному собранию, Президент Республики Беларусь А. Г. Лукашенко подчеркнул, что «информатизация способна обеспечить стране ряд стратегических прорывов» [1].

От себя заметим, что позиционирование Республики Беларусь как высокоразвитого государства, ориентированного на стимулирование деловой инициативы и развитие предпринимательства, невозможно представить без открытости органов государственной власти и управления. Решить эту задачу предстоит проекту национального портала открытых данных, который можно рассматривать в качестве катализатора инновационной деятельности в сфере государственного управления, а также повышение ее эффективности [2, с. 96].

Нельзя здесь не привести слова из выступления экс-министра связи и информатизации Республики Беларусь С. А. Попкова на республиканском семинаре по цифровой экономике: «Создание национального портала открытых данных позиционирует наше государство как высокоразвитое и ориентированное на деловую инициативу. Его цель – движение к "прозрачности" государственного управления и содействие развитию предпринимательства» [3, с. 399].

С 11 по 20 мая 2019 г. Министерством связи и информатизации Республики Беларусь было организовано общественное обсуждение проекта постановления «О функционировании национального портала открытых данных на базе единого портала электронных услуг». Проект был опубликован на интернет-сайте правового форума Республики Беларусь. В обсуждении законопроекта приняло участие 3 человека. Этот факт наглядным образом демонстрирует крайнюю незаинтересованность как отдельных граждан, так и

представителей бизнес-сообщества, некоммерческих организаций в обсуждении выносимого проекта документа.

Как говорит нам обоснование необходимости принятия постановления Совета Министров Республики Беларусь «О функционировании национального портала открытых данных на базе единого портала электронных услуг» основной целью создания портала является обеспечение высокого уровня доступности информации о деятельности государственных органов и организаций, о политической, экономической, культурной и международной жизни, состоянии окружающей среды и другой информации в виде открытых данных для физических и юридических лиц [4].

При введении запроса в поисковой системе Google сайт оказался доступен в сети Интернет по адресу: https://data.gov.by. Несмотря на наличие соответствующей информационной инфраструктуры, международные рейтинги говорят о том, что стране предстоит еще долгий путь в части развития этого направления. Так, по итогам четвертой волны исследования Open Data Barometer (Барометр Открытых данных) Республика Беларусь оказалась на 92 месте среди стран, использующих платформу открытых данных [5].

Резонным остается вопрос об экономических эффектах использования открытых данных. Приведем здесь следующие цифры: на портале открытых данных Соединенных Штатов Америки размещено почти 88,4 тыс. наборов данных, на портале Великобритании − 17,8 тыс. В настоящее время экономический потенциал открытых данных в этих странах оценивается в 50 млрд евро ежегодно [6].

По состоянию на май 2021 года на национальном портале открытых данных удалось зафиксировать за 2022 год всего 101 набор данных.

Сообщество «Открытые данные. Беларусь» совместно с компанией Light Well Organization, разработчиком концепции и технического задания для государственного портала открытых данных, провели онлайн-исследование спроса на открытые данные в Республике Беларусь.

На вопрос «Какие открытые данные могли бы помочь вам в работе?» большинство респондентов ответило, что для них наибольший интерес представляют данные из сфер экономики и финансов, данные о государственных расходах и населении. Среди государственных органов, данные которых востребованы, лидируют Министерство экономики, Министерство финансов и местные органы власти. Респонденты также отметили ряд трудностей в работе с открытыми данными: недостаточная частота обновления, неясность методологии сбора, а также недоступность данных в машиночитаемом формате [7].

Исходя из вышеизложенного можно констатировать ряд проблем, стоящих на пути развития темы открытых данных в Республике Беларусь. Среди них: неактуальность и неполнота открытых данных, фатальное

отставание в вопросах открытости власти от развитых государств, отсутствие площадок для взаимодействия с организациями гражданского общества.

В то же время, использование потенциала открытых данных могло бы способствовать:

- использованию их для граждан и бизнеса для подготовки различной аналитики, создания различных бизнес-сервисов и стимулирования создания новых коммерческих продуктов;

- принятие управленческих решений на основе анализа актуальных и достоверных данных;

- повышение уровня подотчетности и прозрачности государственных органов. В разрезе секторального анализа данных, являются данные государственных финансовых потоков, которые позволяют оценивать эффективность использования государственных средств, формируемых из налоговых сборов с обычных граждан.

Какие же актуальные задачи поможет решить более активное внедрение платформы открытых данных в стране?

Во-первых, можно говорить об активизации IT-сектора страны, а также развития «экономики знаний». Разработчики программного обеспечения получат огромное количество информации для разработки информационных сервисов, а бизнес, исследовательские институты и аналитики получат данные, которые впоследствии можно конвертировать в знания. Так, уже упомянутая нами Хартия открытых данных гласит: «Открытые данные являются катализатором инноваций в частном секторе, способствующим созданию новых рынков, коммерческих предприятий и рабочих мест» [8].

Во-вторых, улучшение позиционирования страны среди других государств, разделяющих принципы открытости и свободы информации посредством повышения позиций в международных рейтингах (в т.ч. рейтингах Организации Объединенных Наций).

И в-третьих, укрепление доверия между государством и гражданским обществом. Ведь именно открытые данные сегодня можно квалифицировать в качестве эффективного инструмента государственного управления, сокращения административных затрат, повышения качества обслуживания населения и доверия этого же населения к государственным (политическим) институциям.

В Республике Беларусь сложились определенные предпосылки для развития темы открытых данных. Однако на сегодняшний день необходима скрупулезная и целенаправленная работа по ее дальнейшему развитию и в максимально сжатые сроки устранению всех имеющихся барьеров.

Позволим в заключении рекомендовать всем заинтересованным сторонам ряд основополагающих моментов:

- продолжить работу по регулярному наполнению актуальными открытыми данными национального интернет-портала в соответствии с плановыми показателями;

- разработка национальной стратегии открытости органов государственной власти;

- принятие нормативного правового акта о функционировании национального портала открытых данных с учетом мнений заинтересованной когорты граждан и опираясь на соответствующую правовую базу;

- организация деятельности постоянного действующей коммуникационной площадки между представителями органов государственной власти и компаниями-разработчиками с целью определения первоочередных координирующих мер по развитию направления.

Библиографический список

1. Послание Президента Республики Беларусь А.Г.Лукашенко белорусскому народу и Национальному собранию Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=P013p0001 – Дата доступа: 24.09.2022.
2. Орлов, П.Н. Анализ внедрения и функционирования национального портала открытых данных в Республике Беларусь / Ю.И. Малевич, П.Н. Орлов // Цифровая трансформация финансового сектора экономики: сб. тезисов докладов V Международной научн.-практ. конф. (Одесса, 9–10 апреля 2020 г.) – Одесса: ОНЕО, 2020. – С.96–98.
3. Выступление министра связи и информатизации Республики Беларусь А.С. Попкова на республиканском семинаре по цифровой экономике [Электронный ресурс]. – Режим доступа: https://www.mpt.gov.by/sites/default/files/doklad-ministra.pdf – Дата доступа: 24.09.2022.
4. Проект постановления Совета Министров Республики Беларусь «О функционировании национального портала открытых данных на базе единого портала электронных услуг» [Электронный ресурс]. – Режим доступа: http://forumpravo.by/files/Proekt_postanovlenie_SM_portal_reltingovoj_ocenki_11.05.2019.pdf. – Дата доступа: 24.09.2022.
5. Открытые данные в Беларуси [Электронный ресурс]. – Режим доступа:http://np.aaii.ru/item.php?id=2812&fbclid=IwAR3u3OTE5_5pRoPglqGJM8sVlItq3ZaE9a_jjBpaboBjYZTP_w5152YlFTE − Дата доступа: 24.09.2022.
6. Создание совета по открытым данным при Правительстве Российской Федерации [Электронный ресурс]. – Режим доступа: http://www.echo.msk.ru/programs/svoiglaza/1019306-echo/. − Дата доступа: 24.09.2022.
7. Исследование спроса на открытые данные в Беларуси: что мы узнали [Электронный ресурс]. – Режим доступа: https://opendata.by/open-data-survey − Дата доступа: 24.09.2022.
8. Хартия открытых данных [Электронный ресурс]. – Режим доступа:https://data.gov.ru/sites/default/files/documents/hartiya_otkrytyh_dannyh_gruppy_vosmi.pdf. − Дата доступа: 24.09.2022.

УДК 343.11

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОТПРАВЛЕНИИ ПРАВОСУДИЯ ПО УГОЛОВНЫМ ДЕЛАМ

О.В. Петрова

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

Работа посвящена конкретным направлениям применения информационно-коммуникационных технологий при отправлении правосудия по уголовным делам. Анализируется законодательное закрепление видеоконференцсвязи, веб-конференции, внедрения звуко- и видеозаписи судебного заседания с составлением краткого протокола как основного способа фиксации хода судебного разбирательства. Автор не только отмечает преимущества применения новых технологий, но и определяет сложности, которые привносит цифровизация в отправление правосудия.

Ключевые слова: информационно-коммуникационные технологии, уголовное судопроизводство, видеоконференцсвязь, веб-конференция, звуко- и видеозапись.

APPLICATION OF INFORMATION TECHNOLOGIES IN THE ADMINISTRATION OF CRIMINAL JUSTICE

O. V. Petrova

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The paper deals with specific areas of information and communication technology application in the administration of Criminal Justice. The legal implementation of video conferencing, web conferencing, the introduction of court room audio and video recording with the preparation of a short report as the primary method of trial record are analyzed. The author both notes the benefits of using new technologies and identifies the difficulties that digitalization brings to the administration of justice.

Keywords: information technology, criminal justice, video conferencing, web conferencing, audio video recording.

Современные информационно-коммуникационные технологии (далее – ИКТ) плотно внедряются во все сферы нашей жизни. Развивается их применение и при отправлении правосудия по уголовным делам. Следует отметить, что применение видеотехнических средств в уголовном процессе предполагалось законодателем еще до его системного закрепления. Так реализация мер безопасности в отношении защищаемых субъектов

предполагает возможность допроса участника защищаемого процесса или производства других следственных действий вне визуальной видимости других лиц (ч. 2 ст. 67, ч. 3 ст. 68 Уголовно-процессуального кодекса Республики Беларусь (далее – УПК). Кроме того, предъявление для опознания может проводиться в условиях, исключающих визуальное наблюдение опознаваемым опознающего (ч. 10 ст. 224 УПК). Однако такие возможности не использовались широко в практике.

В настоящее время основными направлениями такого развития являются использование аудио- и видеозаписи и технологии видеоконференцсвязи (веб-конференции) в судебном заседании.

Так, УПК закреплена основная форма фиксации хода и результатов судебного разбирательства посредством звуко- и видеозаписи с составлением краткого протокола судебного заседания (ст. 308). Такой порядок позволяет фактически детально отразить ход судебного заседания, исключает противоречия и неточности в записях показаний и проведения процесса в целом. Стороны также вправе ходатайствовать о получении копии звуко- или видеозаписи хода открытого судебного заседания на предоставленном ими электронном носителе информации (ст. 309 УПК).

Таким образом, с одной стороны повышается уровень правовой защищенности участников уголовного процесса, но, с другой стороны, знакомится со звуко- и видеозаписью многочасового или даже многодневного судебного заседания сложнее, чем с традиционным протоколом. Представляется целесообразным внедрить технологии искусственного интеллекта для автоматической конвертации звуко- и видеозаписи в формат, позволяющий изложить ход процесса на бумажном носителе.

Законом предусмотрено также при рассмотрении уголовного дела в суде апелляционной инстанции исследование дополнительных материалов с использованием аудио- и (или) видеозаписи (ч. 11 ст.385 УПК).

Новеллами Закона Республики Беларусь «Об изменении кодексов по вопросам уголовной ответственности» от 6 января 2021 г. №85-З законодатель включил в УПК в качестве нового источника доказательств звуко- и видеозапись показаний (ч. 2 ст. 88 УПК). Традиционно протоколы допроса и очной ставки не относились к источникам доказательств (ст. 99 УПК). В силу того, что закон исходя принципа непосредственности судебного разбирательства (ст. 286 УПК) предполагает приоритет первоначальных доказательств, представляется, что звуко- и видеозапись не заменяет показаний обвиняемого, подозреваемого, потерпевшего и свидетеля.

Одним из элементов развития применения ИКТ является возможность в силу п. 21 ч. 1 ст. 333 УПК воспроизведения звуко- и видеозаписи показаний, когда потерпевший или свидетель не достигли четырнадцати лет и в материалах уголовного дела имеется звуко- и видеозапись их показаний.

Однако такая возможно не должна исключать в спорных случаях непосредственный допрос свидетеля или потерпевшего в зале суда.

Логичным этапом развития правовой регламентации информатизации уголовно-процессуальной деятельности стало закрепление Законом Республики Беларусь «О внесении изменений и дополнений в некоторые кодексы Республики Беларусь» от 5 января 2016 г. № 356-З применения систем видеоконференцсвязи (далее – ВКС), а с 2021 года – веб-конференции (далее – ВК), при проведении допроса, очной ставки и предъявления для опознания при производстве предварительного расследования (ст. 224^1 УПК), а также проведение допроса, опознания с использованием ВКС (ВК) в судебном разбирательстве (ст. 343^1 УПК).

С точки зрения технический требований закон лишь указывает, что при применении ВКС (ВК) должно обеспечиваться надлежащее качество изображения и звука. Вместе с тем не указываются конкретные технические требования, которые могут быть выработаны лишь практикой. При применении ВКС (ВК), представляется, также должна быть обеспечена также защита данных.

Допрос участников процесса, опознание лиц и/или объектов в ходе судебного разбирательства могут быть произведены с использованием систем ВКС в случаях:

1) невозможности непосредственного присутствия участника процесса в суде по состоянию здоровья и по другим уважительным причинам;

2) необходимости обеспечения безопасности участников процесса и других лиц в соответствии с гл. 8 УПК;

3) проведения допроса несовершеннолетнего участника процесса;

4) необходимости обеспечения наиболее быстрого, всестороннего, полного и объективного исследования обстоятельств уголовного дела.

В целом, допрос по ВКС (ВК) в судебном разбирательстве положительно сказывается на непосредственности судебного разбирательства, в случаях, когда по тем или иным причинам допрос в зале суда невозможен или затруднён. Участники процесса могут задать вопросы допрашиваемому, опровергнуть показания, чего невозможно добиться лишь оглашением показаний в суде или просмотром звукозаписи показаний, видеозаписи или киносъемки допроса.

Допрос участников процесса, опознание лиц и/или объектов с использованием систем видеоконференцсвязи производятся по общим правилам допроса, опознания с соблюдением правил ст. 343^1 УПК.

В помещении, где находится допрашиваемый и/или в котором осуществляется опознание по поручению суда, рассматривающего дело, обязан находится секретарь судебного заседания (секретарь судебного заседания – помощник судьи).

ВКС (ВК) также стала атрибутом судебного заседания в суде апелляционной инстанции. Так, в соответствии с ч. 9 ст. 385 УПК участие обвиняемого, потерпевшего, свидетелей, экспертов, специалистов, представителя умершего обвиняемого, частного обвинителя, гражданского истца, гражданского ответчика и их представителей в заседании суда апелляционной инстанции, а также исследование судом доказательств могут быть обеспечены с использованием систем видеоконференцсвязи (веб-конференции).

Применение видеоконференции позволят сократить сроки предварительного расследования, судебного разбирательства, снизить расходы на обеспечение отправления правосудия (например, на этапирование обвиняемых для их участия в рассмотрении дела судом апелляционной инстанции). Развитие ВКС как информационно-коммуникационной технологии, что позволяет передавать данные в режиме реального времени, становится крайне актуальной в условиях неблагоприятной эпидемиологической ситуации и может быть способствовать цели сохранения общественного здоровья. Пандемия COVID-19 подтолкнула развитие применения ИКТ при отправлении правосудия в большинстве стран мира [1].

Так, допрос свидетеля, находящегося в другом регионе или другой стране, а возможно и в условиях изоляции при COVID-19 при невозможности прибытия участника процесса для производства следственного действия по состоянию здоровья или по другим уважительным причинам (п. 1 ч. 1 ст. 224^1 УПК) становится доступным посредством технологии ВКС или ВК. В противном случае личного допроса лица необходимо было ожидать либо было бы невозможным.

Также указанные ИТ-технологии позволяют обеспечить безопасность участников процесса в тех случаях, когда непосредственный визуальный контакт представляет опасность для его участников (ч. 1 ст. 65 УПК).

При применении в отношении несовершеннолетних технологии позволяют обеспечить безопасную обстановку для производства следственных и иных процессуальных действий. Так, применение ВКС является составляющей допроса в дружественных детям комнатах при допросе несовершеннолетнего (п. 3 ч. 1 ст. 224^1 УПК) позволяет снизить уровень психотравмирующего воздействия процедуры допроса на несовершеннолетнего.

Таким образом, применение ИКТ в уголовном процессе способствует принципу процессуальной экономии и правовой защищенности граждан на всех стадиях уголовного процесса и требует дальнейшего организационно-технического обеспечения.

Вместе с тем применение ВКС (ВК) ставит перед правоприменительной практикой ряд сложностей. Так возникает и вопрос, насколько может компенсировать участие посредством видеоконференцсвязи личное присутствие в зале суда.

Характер судебного разбирательства предполагает не только обеспечение полной передачи изображения и звука, но и обмена документами, а также обозрения происходящего лицом, находящимся в ином помещении, нежели то, где проводится судебное разбирательство, иного участия в исследовании доказательств. Так, УПК представляет возможность предъявления вещественных доказательств сторонам (ст. 337 УПК), использования письменных заметок и документов при даче показаний (ст. 331 УПК).

Закон не дает ответа на вопрос о том, где должен находится педагог (психолог), представитель потерпевшего, адвокат свидетеля, переводчик при применении систем ВКС(ВК) [с.34].

Проведение судебного заседания с применением ВКС (ВК) не решает вопрос, где должен находиться защитник и как организовать конфиденциальное общение обвиняемого и его защитника при рассмотрении дела судом, если защитник находится в зале суда.

Существуют и иные вопросы практической реализации применения ИКТ при оправлении правосудия, которые требуют решения на уровне не только законодательства, но правоприменительной практики.

Библиографический список

1.Качалова, О.В. Работа судов в условиях пандемии: как обеспечить доступ к правосудию / О.В. Качалова, М.В. Беляев// Государство и право в XXI веке: материалы междунар. научн.-практич. конф., посвящ. 95-летию юрид. фак-та Белорус. гос. ун-та, 26–27 ноября 2020 года, г. Минск / БГУ, Юридический фак.; [редкол.: Т. Н. Михалева (гл. ред.) и др.]. – Минск: БГУ, 2021. – С.185-187.

2. Харчейкина, Ю.В. К вопросу о внедрении информационно-коммуникационных технологий в уголовное судопроизводство / Ю.В. Харчейкина // Уголовная юстиция в свете интеграции правовых систем и интернационализации криминальных угроз: сб. науч. тр., приуроч. к 90-летию д-ра юрид. наук проф. И. И. Мартинович / Белорус. гос. ун-т, юрид. фак., каф. уголов. процесса и прокур. надзора ; редкол. : А. А. Данилевич (отв. ред.), О. В. Петрова, В. И. Самарин. – Минск: Изд. центр БГУ, 2017. – С. 32-36.

УДК 349

ВОЗМОЖНОСТЬ ПОДАЧИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ДЛЯ ПОЛУЧЕНИЯ РАЗРЕШЕНИЯ НА ПРИОБРЕТЕНИЕ ОРУЖИЯ

А. О. Сташис

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье рассмотрена возможность получения разрешения на владения гражданским оружием физическим лицом посредством подачи электронной заявки. Проведен комплексный анализ действующего законодательства об основах административных процедур и электронном документообороте. Сформулирован вывод о невозможности перевода в электронный формат административную процедуру, так как подача электронной заявки для получения разрешения на оружие усложняет административно-процедурные действия и способствует формированию самостоятельных групп обязанностей.

Ключевые слова: гражданское оружие, административные процедуры, электронная заявка.

THE POSSIBILITY OF SUBMITTING ELECTRONIC DOCUMENTS TO OBTAIN A PERMIT FOR THE PURCHASE OF WEAPONS

A. O. Stashis

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article considers the possibility of obtaining a permit for the possession of weapons by an individual by submitting an electronic application. A comprehensive analysis of the current legislation on the basics of administrative procedures and electronic document management has been carried out. The conclusion is formulated that it is impossible to transfer an administrative procedure to an electronic format, since filing an electronic application for obtaining a permit for weapons complicates administrative and procedural actions and contributes to the formation of independent groups of responsibilities.

Key words: civil weapons, administrative procedures, electronic application.

При рассмотрении вопроса о возможности подачи электронной заявки на получение оружия физическим лицом, необходимо обратиться к Закону Республики Беларусь « Об основах административных процедур» от 28 октября 2008 г. № 433-З (далее - Закон № 433-З) и Закону Республики Беларусь «Об электронном документообороте и электронной цифровой подписи» от 28 декабря 2009 г. № 113-З (далее в тексте – Закон № 113-З).

Получение разрешение на оружие относится к административной процедуре и в ст. 14 Закона №433-З предусмотрено: «законодательными актами и постановлениями Совета Министров Республики Беларусь наряду с подачей заявления заинтересованного лица в письменной либо устной форме может быть предусмотрена возможность подачи такого заявления в электронной форме» [1]. Заявление, которое подается в электронном формате, оформляется через единый портал электронных услуг и есть несколько вариантов подачи заявления:

- без использования средств идентификации, указанных в абзацах третьем и четвертом ст.14;
- с использованием уникального идентификатора заинтересованного лица (кроме случаев, когда заинтересованным лицом является юридическое лицо). Порядок получения уникального идентификатора устанавливается Советом Министров Республики Беларусь;
- с использованием личного ключа электронной цифровой подписи, сертификат соответствующего открытого ключа которого издан республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

Способ доступа к единому порталу электронных услуг для подачи заявления заинтересованного лица в электронной форме определяется Советом Министров Республики Беларусь в перечне административных процедур, подлежащих осуществлению в электронной форме через единый портал электронных услуг [1].

При рассмотрении заявления заинтересованного лица уполномоченным органом принимается одно из следующих административных решений:

- об отказе в принятии заявления заинтересованного лица;
- об осуществлении административной процедуры;
- об отказе в осуществлении административной процедуры.

В случае отказа в осуществлении административной процедуры возможно обжалование данного решения во внесудебном порядке. В ст. 30 Закона № 433- 3 определено: «административная жалоба направляется в вышестоящий государственный орган (вышестоящую организацию) либо в государственный орган, иную организацию, к компетенции которых в соответствии с законодательными актами и постановлениями Совета Министров Республики Беларусь относится рассмотрение таких жалоб». Срок обжалования установлен один год со дня принятия обжалуемого административного решения.

В случае осуществления уполномоченным органом административной процедуры в Законе 433-3 определен предельный срок осуществления административной процедуры - пятнадцать дней. Исключения составляют

случаи направления уполномоченным органом запроса в другие государственные органы, иные организации, в этом случае предельный срок осуществления административной процедуры не должен превышать одного месяца [1]. Применительно к обороту оружия определено, что максимальный срок осуществления административной процедуры будет один месяц. Исключение составляют административные процедуры, для которых определен предельный срок осуществления административной процедуры 10 дней, а именно:

- *выдача разрешения на хранение и ношение гражданского оружия гражданам Республики Беларусь, иностранным гражданам и лицам без гражданства, постоянно проживающим в Республике Беларусь;*

- *выдача разрешения на хранение и ношение наградного оружия гражданам Республики Беларусь.*

При подаче заявления на оружие в электронной форме необходимо соблюдать требования, установленные для данного вида документа. Основные требования, предъявляемые к электронному документу, определены в ст. 16 Закона № 113-З. Одним из требований является наличие структуры электронного документа, которая состоит из общей части, то есть информации, отражающей содержание электронного документа, и особенной части, которая включает в себя одну или несколько электронно-цифровых подписей (далее - ЭЦП) [2].

Отдельно необходимо обратить внимание на ЭЦП, которая будет удостоверять подлинность электронного документа. В Законе определено, что физические лица могут приобрести ЭЦП. Подписание электронного документа путем проставления ЭЦП представляет собой процедуру выработки электронной цифровой подписи с использованием личного ключа. Личный ключ определен в Законе как: "последовательность символов, принадлежащая определенной организации или физическому лицу и используемая при выработке электронной цифровой подписи";

В соответствии со ст. 25 Закона №113-З владелец личного ключа обязан:

-хранить в тайне личный ключ;

-обеспечивать защиту личного ключа от случайного уничтожения или модификации (изменения);

-не использовать личный ключ, если соответствующий ему открытый ключ отозван или срок действия этого открытого ключа истек;

-отозвать открытый ключ в случае, если тайна соответствующего ему личного ключа нарушена.

При получении физическим лицом ЭЦП одновременно возникает обязанность по сохранности личного ключа. В случае нарушения

вышеуказанных обязанностей, ответственность возлагается в виде возмещения причиненного вреда [2].

Относительно специфики приобретения оружия можно смоделировать следующий пример: у физического лица (далее - гражданина Л.) имеется ЭЦП и собраны все документы для получения разрешения на владение оружием, однако, доступ к ЭЦП гражданина Л. получило иное физическое лицо и от имени гражданина Л. получило разрешение на владение оружием, вред уже будет причинен государственным интересам и гражданин Л. будет нести ответственность. Таким образом, подача электронной заявки для получения разрешения на оружие только усложняет данную процедуру, так как у физического лица в нашем примере существует две самостоятельные группы обязанностей (по сохранности оружия и по сохранности ЭЦП).

Следует отметить, что при получении разрешения на отдельные виды оружия (например, охотничье оружие) необходимо также сдать экзамен в соответствии с Инструкцией о порядке прохождения специального охотничьего экзамена утвержденной постановлением Министерства лесного хозяйства Республики Беларусь от 6 августа 2018 года № 17 (далее - Инструкция). В Инструкции определено обязательно очное присутствие на экзамене, в п.11 указано: претендент допускается к экзамену после удостоверения личности. Электронного варианта сдачи экзамена пока нет, более того, он нецелесообразен по ряду причин. В частности: 1) аутентификация личности, 2) возможность использования сторонней помощи. Таким образом, перевести процедуру получения разрешения на оружие исключительно в электронный формат не представляется возможным [3].

При получении разрешения на приобретение оружия подается не только заявление в органы внутренних дел, а также медицинская справка о состоянии здоровья, в целом для приобретения разных видов оружия предусмотрена подача разных видов документов. При переходе на электронную подачу документов вышеуказанные документы будут подаваться в виде копий. В соответствии с пунктом 64 Инструкции по делопроизводству в государственных органах и иных организациях, утвержденной постановлением Министерства юстиции Республики Беларусь от 19.01.2009 N 4: «для придания копии документа юридической силы она должна быть заверена (засвидетельствована) уполномоченным должностным лицом организации». Таким образом, на лицо, которое желает приобрести оружие, будут возложены дополнительные обязанности [4].

Также для получения электронных документов необходимо наличие определенного программного обеспечения в государственном органе, об этом указанно в «Инструкции о порядке работы с электронными документами в государственных органах, иных организациях» (далее - Инструкция).

Оплате будет подлежать не только внедрение новых систем, но и услуги технической поддержки для обеспечения работы системы [5].

Если рассмотреть законодательство Российской Федерации, то можно отметить, что отсутствует единый законодательный акт, как в сфере регулирования электронного документооборота, так и в сфере регулирования административных процедур. При этом, в рамках получения разрешения на оружие на сайте «Госуслуг» предусмотрена удобная система, в которой определено, что необходимо для получения разрешения на оружие, а именно: какие документы необходимо иметь для получения разрешения на различные виды оружия, на сайте есть возможность через сайт записаться к врачу для получения медицинской справки, также можно на сайте оставить заявку на получения оружия, по результатам рассмотрения оставленной заявки субъекту необходимо лично предоставить оригиналы необходимых документов. Таким образом, в данном случае отправление заявки на сайте «Госуслуг» нельзя рассматривать как подачу электронного документа на получение оружия. Так как при подаче электронного документа субъект рассчитывает на конкретный результат, а именно: получение разрешения на оружие, в данном случае оставление заявки просто укоряет процедуру получения разрешения на оружие.

Библиографический список

1 Об основах административных процедур [Электронный ресурс] : Закон Респ. Беларусь от 28 октября 2008 г. № 433-З: в ред. от 9 января 2017 г. № 17-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2 Об электронном документообороте и электронной цифровой подписи [Электронный ресурс] : Закон Респ. Беларусь от 28 декабря 2009 г. № 113-З : в ред. от 8 ноября 2018 г. № 143-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

3 Инструкция о порядке прохождения специального охотничьего экзамена : утв. М-вом лесного хозяйства Респ. Беларусь 06.08.2018 г. №17 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

4 Инструкция по делопроизводству в государственных органах и иных организациях : утв. М-вом юстиции Респ. Беларусь 19.01.2009 г. № 4 : в ред. от 17 октября 2019 г. № 193 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

5 Инструкция о порядке работы с электронными документами в государственных органах, иных организациях : утв. М-вом юстиции Респ. Беларусь 06.02.2019 г. №19 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

УДК 341:347

ВЗАИМОСВЯЗЬ МЕЖДУНАРОДНОГО И НАЦИОНАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА В ПРАВОВОМ РЕГУЛИРОВАНИИ ЦИФРОВИЗАЦИИ

Т.В. Телятицкая

Белорусский государственный экономический университет,
проспект Рокоссовского, 65, Минск, 220110, Беларусь

В работе анализируются вопросы правового регулирования цифровизации в рамках различных межгосударственных образований. Исследуется связь национального и международного права при регулировании передачи и использования данных. Выявлена корреляция публичного и частного начал в вопросе регламентации цифровизации. Дана оценка отдельных международных актов в области оборота информации. Сформулированы и обоснованы основные проблемы международно-правового регулирования цифровизации. Подчеркивается, что процессы цифровизации на территории ЕАЭС предполагают гармонизированное и сбалансированное правовое регулирование как на национальном, так и наднациональном уровнях, что может быть обеспечено только посредством синхронизации соответствующего регулирования и дальнейшей реализацией всего массива международно-правовых и национальных актов. Сделан вывод, что с точки зрения унификации происходящих процессов в цифровой сфере необходимо развитие правовой базы на уровне ЕАЭС.

Ключевые слова: правовое регулирование, законодательство, цифровизация, цифровая экономика, ЕАЭС.

INTERCONNECTION OF INTERNATIONAL LAW AND NATIONAL LEGISLATION IN REGULATING OF DIGITALIZATION

T. Telyatitskaya

Belarusian State Economic University,
65 Rokossovsky Avenue, Minsk, 220110, Belarus

The paper analyzes the issues of legal regulation of digitalization within various interstate entities. The relationship between national and international law in regulating the transfer and use of data is investigated. The correlation of public and private principles in the issue of regulation of digitalization has been revealed. An assessment of individual international acts in the field of information circulation is given. The main problems of international legal regulation of digitalization are formulated and substantiated. It is emphasized that the processes of digitalization on the territory of the EAEU imply harmonized and balanced legal regulation both at the national and supranational levels, which can only be ensured by synchronizing the relevant regulation and further implementation of the entire array of international legal and

national acts. It is concluded that from the point of view of the unification of ongoing processes in the digital sphere, it is necessary to develop a legal framework at the level of the EAEU.

Keywords: legal regulation, legislation, digitalization, digital economy, EAEU.

Современную жизнь невозможно представить без цифровых технологий, которые широко используются во всех областях жизни. Если прошлые два столетия стали этапами стремительного развития промышленности, то XXI век уверенно можно назвать веком расцвета информационных технологий.

В последние несколько десятилетий коммуникационные связи, скорость получения информации и стиль поведения людей стремительно изменились. Многие исследователи считают, что цифровые технологии будут развиваться и дальше в геометрической прогрессии [1, с. 6].

Происходящая цифровизация экономики, государственного управления, общественной жизни изменяет не только подход к выполнению повседневных задач, но и способствует повышению эффективности управленческих процессов, оказывает влияние на развитие целых стран и регионов.

Понятие цифровизации намного шире, чем использование электронных сервисов. Термин «цифровизация» ввел в употребление в 1995 г. профессор Массачусетского технологического института, основатель и директор Media Lab Николас Негропонте, сформулировавший концепцию Digital Economics [2].

Эксперты предлагаю рассматривать термин «цифровизация» в узком и широком значении, понимая под цифровизацией в узком смысле переход с аналоговой формы передачи информации на цифровую, «преобразование информации в цифровую форму, которое в большинстве случаев ведет к снижению издержек, появлению новых возможностей и т.д.», а под цифровизацией в широком смысле – «современный общемировой тренд развития экономики и общества, который основан на преобразовании информации в цифровую форму и приводит к повышению эффективности экономики и улучшению качества жизни» [3, с. 46].

В условиях глобализации правовое регулирование отношений, связанных с использованием цифровых технологий, больше не является и не может являться прерогативой национального законодательства. Вместе с развитием науки и технологий цифровизация перешагнула границы отдельных государств и вышла на мировой уровень. При всех многообещающих перспективах, связанных с созданием материальных благ, улучшением качества жизни и т.п., в связи со стремительным развитием цифровизации возникает множество проблем, связанных с

защитой прав потребителей, обеспечением безопасности, конфиденциальности и др.

Возникновение повышенного научного интереса к соответствующей тематике во многом обусловлено рядом нормативных документов, определяющих перспективные пути социально-экономического развития Республики Беларусь, а также состояние информационной безопасности и основные информационные угрозы. На международном уровне определение общих путей правового регулирования цифровизации гораздо сложнее из-за ряда как объективных факторов, так и в большей степени субъективных, включая политическую составляющую.

Поэтому сотрудничество государств в рамках международных организаций и межгосударственных интеграционных объединений выступает наиболее подходящей формой для международно-правового регулирования цифровых технологий. Причем именно формат межгосударственных интеграционных объединений представляется наиболее подходящим для этих целей, поскольку там уже сформированы тесные интеграционные связи, созданы и успешно функционируют различные консультативные и иные общие органы, отработаны механизмы разрешения противоречий.

Можно выделить три группы проблем международно-правового регулирования цифровизации:

1) субъективные проблемы разработки международно-правовых актов, выражающиеся в концептуальных противоречиях между различными государствами во взглядах на регулирование цифровых технологий;

2) проблемы, связанные с введением в действие уже разработанных международно-правовых актов в связи со сложностью согласования актов, принятых различными межгосударственными объединениями;

3) неизбежные коллизии принятых международно-правовых актов с национальными законодательствами, неготовность правовых систем отдельных государств к восприятию новых подходов в регулировании цифровизации или, наоборот, отставание международно-правового регулирования от законодательства отдельных государств.

Для решения этих проблем представляется необходимой согласованная передача с национального уровня на международный основных аспектов правового регулирования, отказ от определенных полномочий в пользу наднациональных структур.

Республика Беларусь уже провозгласила курс на построение цифровой экономики и интенсивно разрабатывает дорожные карты ее развития. Предоставление практически всех видов услуг посредством Интернета уже давно стало обыденностью, равно как и необходимость правовой защиты цифровых данных. Тем не менее, как справедливо отмечает В.С. Каменков,

применительно к вопросам правового регулирования цифровых технологий на уровне кодексов можно выявить только правовые нормы об электронной цифровой подписи в Налогом кодексе, в Хозяйственном процессуальном кодексе и в Гражданском кодексе. Среди иных законодательных актов Республики Беларусь, затрагивающих сферу цифровых технологий, можно назвать законы Республики Беларусь «Об электросвязи» (от 19.07.2005 № 45-З), «Об электронном документе и электронной цифровой подписи» (от 28.12.2009 г., № 113-З), а также ряд указов Президента и постановлений Совета министров Республики Беларусь [4].

Конференция ООН по торговле и развитию еще в 2017 г. выделила основные технологии, касающиеся сферы цифровизации. Это: продвинутая робототехника; искусственный интеллект; Интернет вещей; облачные технологии; большие данные; трехмерная печать; цифровые платежные системы [5].

В Декларации о цифровой экономике Организации по безопасности и сотрудничеству в Европе подчеркивается необходимость укрепления международного сотрудничества по следующим направлениям: содействие созданию благоприятных условий для цифровых инноваций в деловом секторе; стимулирование конкуренции в цифровой экономике; продвижение международных трудовых норм; расширение доступа к цифровым технологиям и услугам во всех секторах экономики; обмен опытом в области цифровой трансформации и др. [6].

В Европейском Союзе стратегия единого цифрового рынка базируется на следующих принципах: лучший доступ для потребителей и предприятий к онлайн-товарам и услугам по всей Европе; создание надлежащих условий для развития цифровых сетей и услуг; максимизация потенциала роста европейской цифровой экономики [7].

Вопросы развития цифровой экономики находятся в поле зрения и иных международных структур, не формализованных в формате международных организаций или межгосударственных интеграционных объединений. В частности, Декларация по цифровой экономике была принята в 2018 г. на Конференции G20 на уровне соответствующих министров.

В итоговом документе содержатся предложения по сокращению цифрового гендерного неравенства, трансформации правительств, измерению цифровой экономики и ускорению развития цифровой инфраструктуры. В декларации цифровизация признана мощным стимулом для всеобщего экономического роста. Документ призывает страны G20 лучше понять новые бизнес-модели, чтобы ускорить цифровую экономику. Перечислены также требования к процветающей цифровой экономике – это, в частности, эффективная и высококачественная инфраструктура и среда,

которая поддерживает инновации и даёт им правовое обеспечение, а также способствует свободному распространению информации, знаний и идей [8].

Можно отметить, что Европейский Союз наиболее продвинулся в вопросах правового регулирования цифровизации, хотя до конечного желаемого результата еще очень далеко. Однако многие их наработки вполне могут быть использованы для формирования законодательства Евразийского экономического союза. Например, можно позаимствовать опыт ЕС по отмене неоправданных ограничений на трансграничное перемещение цифрового контента, создать по подобию европейского облачного ресурса свой, евразийский и др. Безусловно, все заимствования должны учитывать специфику ЕАЭС, где достаточно большой массив вопросов в сфере цифровой экономики, в соответствии с Договором о Евразийском экономическом союзе от 29 мая 2014 г., относится к сфере национального правового регулирования государств-членов [9].

Таким образом, государства, входящие в ЕАЭС, самостоятельно определяют свою политику в сфере цифровизации, разрабатывают национальные программные документы в данной сфере, а также нормативные правовые акты. Однако с точки зрения унификации происходящих процессов в цифровой сфере видится необходимым развитие правовой базы именно на уровне ЕАЭС, что предусмотрено в Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года [10].

Таким образом, процессы цифровизации на территории ЕАЭС предполагают гармонизированное и сбалансированное правовое регулирование как на национальном, так и наднациональном уровнях, что может быть обеспечено только посредством синхронизации соответствующего регулирования и дальнейшей реализацией всего массива международно-правовых и национальных актов.

Библиографический список

1. Тесленко, И. Б. Цифровая экономика / И. Б. Тесленко, В. Е. Крылов, О. Б. Дигилина, А. М. Губернаторов. – М: КОРУС, 2023. – 214 с.

2. Negroponte, N. Being Digital / N. Negroponte [Электр. ресурс]. – Режим доступа: https://b-ok.org/book/1188274/ca2aa4/ – Дата доступа: 10.10.2022.

3. Халин, В. Г. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски / В.Г. Халин, Г.В. Чернова // Управленческое консультирование. – 2018. – № 10. – С. 46–63.

4. Каменков, В. С. Профессионально об актуальном: О системе правового регулирования цифровой экономики Республики Беларусь / В.С. Каменков [Электр. ресурс]. – Режим доступа: https://pravo.by/novosti/novosti-pravo-by/2020/january/44419/. – Дата доступа: 16.09.2022.

5. Information Economy Report 2017: Digitalization, Trade and Development [Электр. ресурс]. – Режим доступа: https://unctad.org/en/PublicationsLibrary/ier2017_en.pdf. – Дата доступа: 16.09.2022.

6. Declaration on the Digital Economy as Driver for Promoting Co-operation, Security and Growth [Электр. ресурс]. – Режим доступа: https://www.osce.org/chairmanship/405920?download=true. – Дата доступа: 10.09.2022.

7. Monitoring the Digital Economy and Society 2016-2021 [Электр. ресурс]. – Режим доступа: https://ec.europa.eu/eurostat/documents/341889/725524/Monitoring+the+Digital+Economy+%26+Society+2016-2021/7df02d85-698a-4a87-a6b1-7994df7fbeb7. – Дата доступа: 10.09.2022.

8. Декларация G20 по развитию цифровых экономик [Электр. ресурс]. – Режим доступа: https://ksi.lenobl.ru/ru/news/3260/. – Дата доступа: 09.10.2022.

9. Договор о Евразийском экономическом союзе: ред. от 01.10.2019, с изм. от 31.03.2022 [Электр. ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=f01400176. – Дата доступа: 14.09.2022.

10. Об основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года: решение Высшего Евразийского экономического совета, 11.10.2017, № 12 [Электр. ресурс]. – Режим доступа: https://docs.cntd.ru/document/555625953. – Дата доступа: 15.09.2022.

УДК 349.6

ЦИФРОВИЗАЦИЯ И ЭКОЛОГИЗАЦИЯ ТРАНСПОРТНОЙ ДЕЯТЕЛЬНОСТИ НА ЕВРАЗИЙСКОМ ПРОСТРАНСТВЕ: ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ЭФФЕКТИВНОСТИ

О.А. Хотько

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

Автор отражает проблемные аспекты экологизации транспортного законодательства, отмечает меры цифровизации транспортной деятельности, впервые в юридической науке анализирует взаимосвязь правового обеспечения экологической безопасности при осуществления транспортной деятельности в контексте цифровизации в данной сфере. Исследование вышеуказанных ключевых тенденций на евразийском пространстве с учетом целей устойчивого развития послужило основанием выработки новых подходов реализации принципа экологичности транспортной политики Евразийского экономического союза и осуществления управления в связи с цифровизацией транспорта.

Ключевые слова: экологическая безопасность, экологизация, цифровизация, транспортная деятельность, правовое обеспечение, законодательство, устойчивое развитие.

DIGITALIZATION AND ENVIRONMENTALIZATION OF TRANSPORT ACTIVITIES IN THE EURASIAN SPACE: LEGAL ASPECTS OF ENSURING EFFICIENCY

O. A. Khotsko

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The author reflects the problematic aspects of the environmentalization of transport legislation, notes the measures of digitalization of transport activities, for the first time in legal science it analyzes the relationship of legal support for environmental safety in the implementation of transport activities in the context of digitalization in this area. The study of the above key trends in the Eurasian space, taking into account the goals of sustainable development, served as the basis for developing new approaches to the implementation of the principle of environmental friendliness of the transport policy of the Eurasian Economic Union and the implementation of management in connection with the digitalization of transport.

Keywords: environmental safety, environmentalization, digitalization, transport activities, legal support, legislation, sustainable development.

Вопросам экологической безопасности каждое государство уделяло и уделяет большое внимание на протяжении длительного времени. Процесс осуществления транспортной деятельности представляет одну из серьезных угроз экологической безопасности как составляющей национальной безопасности Республики Беларусь. Особое значение в данном контексте занимает цифровизация транспортной деятельности в условиях интеграционных процессов, что связано с управлением в области охраны окружающей среды и обеспечения экологической безопасности.

Усиливающееся влияние транспорта на состояние окружающей среды и рост цифровых разработок обусловливает необходимость осмысления связанных с этим вопросов эффективного правового обеспечения, совершенствования и систематизация законодательства в области экологической безопасности, определения направлений дальнейшего развития правовых норм в данной сфере в целях достижения защищенности благоприятного состояния окружающей среды, жизни и здоровья граждан. В современных условиях развития общественных отношений, ключевую роль в которых занимает законодательное регулирование при внедрении новых технологий, а также социально-экономические и интеграционные факторы, целесообразным представляется системное формирование норм, касающихся эколого-безопасного развития транспортной деятельности, что окажет существенное влияние при проведении транспортной политики как в Республике Беларусь, так и рамках Евразийского экономического союза (далее – ЕАЭС).

В научной литературе вопросам государственного управления в области охраны окружающей среды, целесообразности реализации стратегии устойчивого развития, государственной экологической политики, создания экологориентированной экономики, правовой интеграции государств и соответствующим направлениям развития государственного управления в Республике Беларусь посвящены работы С.А. Балашенко [1], Н.А. Карпович [2], Е.В. Семашко [3], О.И. Чуприс [4] и иных ученых. Обратим внимание на то, что специалисты в области экономики также обращаются к данного рода проблемам, представляя авторский подход к пониманию экологически ориентированного управления устойчивым развитием транспортного кластера [5]. В то же время лишь в рамках юридической науки при выработке обоснованной системы концептуальных приоритетов в области обеспечения экологической безопасности возможна систематизация законодательства, в процессе которого должна быть достигнута четкость правового регулирования на основе отражения анализа экологических рисков и рисков цифровизации производства в транспортной отрасли.

Развитию сотрудничества государств-членов в транспортной сфере придало импульс подписание актов в рамках ЕАЭС, разрабатываются планы мероприятий, в соответствии с которыми страны реализуют

направления деятельности. Так, полностью подготовлен договор о формировании союзного рынка электрической энергии, формулируются предложения при создании единого газового рынка в рамках Союзного государства, однако данные акты направлены прежде всего на защиту потребителей. Вместе с тем, имеется в этом отношении и взаимосвязь с функционированием транспортной деятельности, что благоприятно может сказаться на экологизации, переходу к «зеленой» экономики в ЕАЭС, внедрении мер, принципов и механизмов, направленных на модернизацию законодательства в области транспорта, что подтверждается данными аналитического доклада, подготовленного Департаментом макроэкономической политики по анализу международного опыта и практики по развитию отраслей и сфер «зеленой» экономики [6]. Данный доклад, включающий концептуальные подходы (предложения) относительно «зеленой» энергетики и «зеленых» технологий в сфере транспорта с учетом вызовов для Евразийского экономического союза выступает промежуточным этапом для разработки Сторонами проекта Концепции по внедрению принципов «зеленой» экономики в ЕАЭС в 2023 году.

Государства-члены ЕАЭС имеют особые масштабные возможности транзитного значения. Стороны утвердили 8 транспортных коридоров, которые «увязаны с международным и коридорами и гармонизируются с «Одним поясом и одним путем» [7]. В свете имеющихся огромных территорий в ЕАЭС, обоснованного развития транслогистического проекта государств-членов Евразийского экономического союза и в перспективе взаимодействия с Шанхайской организацией сотрудничества в настоящее время основным вопросом наряду с обеспечением экологической безопасности развивающихся проектов выступает цифровизация транспортных коридоров. Это позволит перевозчикам оценивать ситуацию по загрузке товаров, владеть информацией о состоянии дорог, знать пункты отдыха и пункты заправок и учитывать иные непредвиденные ситуации, как отмечает председатель коллегии Евразийской экономической комиссии [7].

Республика Беларусь является активным участником в ЕАЭС при формировании международных отношений в рамках координации действий с Китаем. Претворять в жизнь новые инициативы и углублять двустороннее сотрудничество в рамках ЕАЭС целесообразно на прочной правовой основе. Так, определенные шаги в данном направлении предпринимаются на наднациональном уровне (в ЕАЭС приняты решения, распоряжения о поддержке развития электротранспорта, начиная с 2018 года).

Экологичность и цифровизация – основные стратегические направления развития ОАО «БЕЛАЗ» и повышения деятельности горнодобывающей промышленности, что звучало как лейтмотив на форуме при участии специалистов, представителей компаний-партнеров из Российской Федерации и

Республики Беларусь [8]. Тенденции деятельности в данной сфере проявились в разработке совместного проекта вышеуказанных государств – гибридного самосвала, представленного летом 2022 года. Цифровая трансформация, интеллектуальные решения, взаимосвязанные с экологической безопасностью, являются важнейшими ключевыми направлениями вышеотмеченного предприятия и многих иных, которые могут показаться совершенно самостоятельными областями деятельности на первый взгляд. Вместе с тем в рамках научных исследований при проведении международных транспортно-правовых форумов ранее автором показаны проблемы обеспечения экологической безопасности в условиях цифровой трансформации транспортных процессов, отмечено влияние интеллектуальных транспортных систем на экологическую безопасность и правовые аспекты развития в данной сфере общественных отношений [9; 10].

Кроме того, в частности, в рамках развития экономической интеграции рассматриваются вопросы использования навигационных пломб при перевозке грузов не только железнодорожным, но также и автомобильным транспортом, что позволит отслеживать местонахождение товаров при использовании сопроводительных документов в электронном виде и ускорить процесс перевозок. Соответственно, принят законопроект «О ратификации Соглашения о применении в Евразийском экономическом союзе навигационных пломб для отслеживания перевозок», разработанный на основании Соглашения о применении в ЕАЭС навигационных пломб для отслеживания перевозок от 19 апреля 2022 г. Предусматривается, что нововведения об отсутствии необходимости сопровождения некоторых видов грузов, современные геоинформационные и информационные технологии позволят ускорить перемещение товаров между странами ЕАЭС и стимулировать развитие бизнес-процессов [11].

Проведенное исследование позволяет прийти к выводу, что данная деятельность неизбежно должна сопровождаться экологическими инструментами правового механизма охраны окружающей среды и обеспечения экологической безопасности. В литературе их классифицируют на инструменты административного регулирования, экономические и информационные [12]. В науке экологического права должен получить признание такой механизм относительно транспортной деятельности в целях снижения ее вредного воздействия на окружающую среду, отражающий также и цифровизацию производства. Несмотря на то, что в актах ЕАЭС не достаточно полно закреплены требования экологической безопасности, в том числе на уровне технических регламентов относительно деятельности транспорта, что подробно отражено автором в исследовании [13], требуется выработка подходов для развития экологизации транспортного законодательства на национальном уровне, а также принятие согласованного документа в ЕАЭС

(возможно, рекомендаций). Это обусловлено потребностью внедрения мер «зеленой» политики в сфере транспорта и инфраструктуры, стимулирования и продвижения их на наднациональном уровне в рамках ЕАЭС, формированием направлений в области устойчивого развития и сближения позиций государств-членов в части климатической повестки с учетом имеющегося достаточного потенциала для развития принципа экологичности транспортной политики, заложенного в Договоре о Евразийском экономическом союзе от 29 мая 2014 года.

Библиографический список

1. Балашенко, С.А. Государственное управление в области охраны окружающей среды : монография / С.А. Балашенко; Белорус. гос. ун-т. – Минск, БГУ, 2000. – 341 с.

2. Карпович, Н.А. Экологическая политика Республики Беларусь: теоретические и концептуальные основы совершенствования правового обеспечения / Н.А. Карпович // Правовая политика Республики Беларусь : современное состояние и перспективы развития : сб. материалов Междунар. научно-практ. конф. (Минск, 6 дек. 2013 г.) / Нац. центр законодательства и правовых исслед. Респ. Беларусь ; редкол. : В.И. Семенков (гл.ред.) и др. – Минск : Институт радиологии, 2013. – С. 13–21.

3. Семашко, Е.В. Мировоззренческие основы развития национальной правовой системы в контексте правового обеспечения экологической безопасности / Е.В. Семашко // Основы устойчивого развития национальной правовой системы в XXI столетии: методология, теория, практика : колл. монография / В.А. Абрамович [и др.] ; под ред. В.И. Павлова. – Минск : Бизнесофсет, 2016. – С. 205–218.

4. Чуприс, О.И. Правовая интеграция государств и отдельные направления развития государственного управления в Республике Беларусь / О.И.Чуприс // Право. by. – 2017. – № 5. – С. 43–49.

5. Новиков, А.В. Особенности экологически ориентированного управления устойчивым развитием транспортного кластера / А.В. Новиков // Проблемы теории и практики управления. – 2019. – № 3–4. – С. 98–106.

6. О международном опыте разработки и внедрения принципов, мер и механизмов «зелёной» экономики и концептуальных подходах в Евразийском экономическом союзе [Электронный ресурс] // Режим доступа: https://eec.eaeunion.org/upload/medialibrary/939/Doklad_Zelenaya_ekonomika_PDF_sayt.pdf. – Дата доступа: 06.01.2022.

7. О сотрудничестве ЕАЭС и ШОС рассказал Михаил Мясникович [Электронный ресурс] // Режим доступа: https://www.tvr.by/news/ekonomika/o_sotrudnichestve_eaes_i_shos_rasskazal_mikhail_myasnikovich/ . – Дата доступа: 02.10.2022.

8. Экологичность и цифровизация. Гендиректор БЕЛАЗа о стратегических направлениях развития [Электронный ресурс] // Режим доступа: https://www.belta.by/comments/view/ekologichnost-i-tsifrovizatsija-gendirektor-belaza-o-strategicheskih-napravlenijah-razvitija-8375/. – Дата доступа: 30.09.2022.

9. Хотько, О.А. Правовые проблемы обеспечения экологической безопасности в условиях цифровой трансформации транспортных процессов / О.А. Хотько // Правовые аспекты цифровизации международного транспорта и логистики: материалы Второго Международного транспортно-правового форума / под ред. А. А. Чеботаревой, В. Е.

Чеботарева ; вступительное слово Н.А. Духно. – Москва : Изд-во Юридического института МИИТ, 2020. – С. 86–91.

10. Хотько, О.А. Теоретические основания законодательного регулирования интеллектуальных транспортных систем в контексте правового обеспечения экологической безопасности и устойчивого развития государства и общества / О.А. Хотько // Искусственный интеллект и тренды цифровизации: материалы Третьего Междунар. транспортно-правового форума, приуроч. к 125-летию Российск. ун-та транспорта, 10-11 февраля 2021 г. / под ред. А.А. Чеботаревой, В.Е. Чеботарева ; вступ.слово Н.А. Духно. – Москва : Изд-во Юрид. института МИИТ, 2021. – С.127–132.

11. Депутаты ратифицировали соглашение ЕАЭС о навигационных пломбах для отслеживания перевозок [Электронный ресурс] // Режим доступа: https://www.belta.by/economics/view/deputaty-ratifitsirovali-soglashenie-eaes-o-navigatsionnyh-plombah-dlja-otslezhivanija-perevozok-525717-2022/. – Дата доступа: 26.09.2022.

12. Жаворонкова, Н.Г. Правовое обеспечение экологической безопасности в условиях экономической интеграции Российской Федерации / Н.Г. Жаворонкова, Ю.Г. Шпаковский. – М.: Изд-во «Проспект», 2017. – 160 с.

13. Хотько, О.А. Теоретико-методологические проблемы технического регулирования на евразийском пространстве как составляющей правового обеспечения экологической безопасности транспортной деятельности / О.А. Хотько // Журнал заруб. законодательства и сравнительного правоведения. – 2021. – № 3. – С.84–89.

Научное издание

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ И ГОСУДАРСТВА В СОВРЕМЕННОМ МЕЖДУНАРОДНОМ ПРАВЕ

Материалы круглого стола кафедры государственного управления юридического факультета Белорусского государственного университета

Минск, 12 апреля 2022 г.

В авторской редакции

Ответственный за выпуск *В. С. Михайловский*

Художник обложки *И. К. Марченко*

Подписано в печать 25.11.2022. Формат 60×86/16. Бумага офсетная.
Печать цифровая. Усл. печ. л. 17,44. Уч.-изд. л. 18,24.
Тираж экз. Заказ

Белорусский государственный университет.
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий № 1/270 от 03.04.2014.
Пр. Независимости, 4, 220030, Минск.

Отпечатано с оригинал-макета заказчика