ИНФОРМАЦИОННОЕ ПРАВО

№ 1 (59)/2019

НАУЧНО-ПРАКТИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ИЗДАНИЕ. Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций. Рег. ПИ № ФС77-33769 от 17 октября 2008 г. Издается 4 раза в год

Журнал включен в Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук (в редакции от июля 2007 г.)

Учредители:
Республиканский НИИ интеллектуальной собственности (РНИИИС);
ИГ «Юрист»

Адрес редакции:
115184, Москва, ул. Большая Татарская, 35, с. 3. РНИИИС.
Тел./факс: (499) 238-40-83
E-mail: info@rniiis.ru

Главный редактор ИГ «Юрист»
Гриб В.В.

Заместители главного редактора ИГ «Юрист»:
Бабкин А.И., Белых В.С., Ренов Э.Н., Платонова О.Ф., Трунцевский Ю.В.

Центр редакционной подписки:
(495) 617-18-88 – многоканальный

Тел./факс редакции ИГ «Юрист»:
(495) 953-91-08

Адрес издательства/редакции:
115035, г. Москва, Космодамианская наб., д. 26/55, стр. 7
E-mail: avtor@lawinfo.ru

ISSN: 1999–480X

Отпечатано в ООО «Национальная полиграфическая группа», 248031, г. Калуга, ул. Светлая, д. 2, тел. (4842) 70-03-37
Формат 60x90/8. Печать офсетная. Физ. печ. л. 6,0. Усл. печ. л. 6,0. Общий тираж 1 000 экз.
Номер подписан в печать: 26.02.2019.
Номер вышел в свет: 22.05.2019.

Подписка по России:
Объединенный каталог. Пресса России – 91891, а также через www.lawinfo.ru.

Цена свободная.

В НОМЕРЕ:

ТЕОРИЯ И ИСТОРИЯ

Трунцевский Ю.В. Понятие критической информационной инфраструктуры и ее идентификация 4

Шевердяев С.Н., Лаер Е.А. Эволюция концепции открытого правительства в зарубежной правовой доктрине и законодательстве 9

ПРАВО НА ИНФОРМАЦИЮ: ДИСКУССИЯ

Исманжанов А.А. Информация как объект гражданского права в контексте смежных правовых категорий 13

ПРАВО НА ТАЙНУ

Жирнова Н.А. Адвокатская тайна как вид профессиональной тайны: проблемы обеспечения режима конфиденциальности 17

ПРАВОВАЯ ЗАЩИТА

Дремлюга Р.И. Системы искусственного интеллекта как средство совершения преступления 21

ТОЧКА ЗРЕНИЯ

Ковалева Н.Н., Солдаткина О.Л. Запреты в информационном праве 26

ТРИБУНА МОЛОДОГО УЧЕНОГО

Пашнина Т.В. Эволюция права на информацию в России и в мире 31

Полещук Д.Г. Противодействие экстремизму в сети «Интернет»: охранительный аспект 35

ПРЕПОДАВАНИЕ

Вашкевич С.В. Информационно-правовые ресурсы государственной системы правовой информации в образовательном процессе Республики Беларусь 40

КОНФЕРЕНЦИИ

Кибербезопасность и инициативы Сбербанка России 44

Цифровизация городов и информационные технологии 46

INFORMATION LAW

No. 1 (59)/2019

SCIENTIFIC-PRACTICE AND INFORMATION JOURNAL. REGISTERED AT THE MINISTRY OF THE RF OF PRESS, TELECOMMUNICATION AND MASS MEDIA. REG. PI № FC77-33769 of October 17, 2008. Published 4 times a year.

The journal is included in to the List of leading reviewed scientific journals and periodicals where basic results of candidate and doctoral theses shall be published (version as of June, 2007).

Founders:
Republican Scientific Research Institute of Intellectual Property (RNIIIS);
Jurist Publishing Group

Editorial Office Address:
35 bild. 3 Bolshaya Tatarskay Str. (RSRIIP), Moscow, 115184

Tel./fax: (499) 238-40-83

E-mail: info@rniiis.ru

Editor-in-Chief of Jurist Publishing Group
Grib V.V.

Deputy Editors-in-Chief of Jurist Publishing Group:
Babkin A.I., Bely'kh V.S., Renov E'.N., Platonova O.F., Truntsevskij Yu.V.

Editorial Subscription Centre:
(495) 617-18-88 – multichannel

Tel./fax of the Editorial Office of Jurist Publishing Group: (495) 953-91-08.

Address publishers / editors:
Bldg. 7, 26/55 Kosmodamianskaya Emb., Moscow, 115035.
E-mail: avtor@lawinfo.ru

ISSN: 1999–480X

Printed by National Polygraphic Group ltd.
Bldg. 2, street Svetlaya, Kaluga, 248031
Tel. (4842) 70-03-37

Size 60x90/8. Offset printing. Printer's sheet 6,0.
Conventional printing sheet 6,0. Circulation 1 000 copies.
Passed for printing: 26.02.2019.
Issue was published: 22.05.2019.

Subscription in Russia: Unified Catalogue.
Russian Press – 91891,
www.lawinfo.ru

CONTENTS:

THEORY AND HISTORY

Truntsevskiy Yu.V. The Concept and Identification of Critical Information Infrastructure 4

Sheverdyaev S.N., Laer E.A. Evolution of the Open Government Concept in the Foreign Legal Doctrine and Laws 9

THE RIGHT TO INFORMATION: DISCUSSION

Ismanzhanov A.A. Information as a Civil Law Object within the Framework of Related Legal Categories 13

THE RIGHT TO PRIVACY

Zhirnova N.A. The Attorney-Client Privilege as a Type of Professional Secrecy: Issues of Securing the Confidentiality Regime 17

LEGAL PROTECTION

Dremlyuga R.I. Artificial Intelligence Systems as a Means of Crime Committing 21

OPINION

Kovaleva N.N., Soldatkina O.L. Prohibitions in the Information Law 26

YOUNG SCIENTIST'S TRIBUNE

Pashnina T.V. Evolution of the Right to Information in Russia and in the World 31

Poleschuk D.G. Combating Extremism on the Internet: A Protective Aspect 35

TEACHING

Vashkevich S.V. Information Law Resources of the State System of Legal Information in the Educational Process of the Republic of Belarus 40

CONFERENCES

Cybersecurity and Initiatives of Sberbank of Russia 44

Digitization of Cities and Information Technology 46

Требования к материалам, направляемым в журнал «Информационное право»

Уважаемые авторы! При направлении материалов в журнал просим вас соблюдать следующие требования:

1. Редакционный совет и редакция журнала рассматривают материалы, присланные по почте, в том числе по электронной почте, или представленные в журнал на бумажном носителе, в следующих объемах: статья — 7—10 страниц, обзор, рецензия, информация — не более 3 страниц, иные материалы — по согласованию с редакцией.

2. При определении объема материала просим исходить из таких параметров: текст печатается на стандартной бумаге А-4 через 1,5 интервала; размер шрифта основного текста — 13; сноски можно печатать через 1 интервал, размер шрифта 10; поля: слева — 3 см, сверху, справа и снизу — 2 см.

3. При ссылках на авторов в тексте следует указать инициалы и фамилию, в сноске, наоборот, сначала фамилию, затем инициалы автора; обязательно привести название публикации, источник — место, год, номер, страницу.

4. При использовании нормативного акта следует указать в тексте его вид (Федеральный закон, Указ Президента Российской Федерации и т.д.), дату (день принятия — цифрами, месяц — словом, год принятия — четырьмя цифрами, например, 12 декабря 2003 г.), привести в кавычках полное (без сокращений) наименование (в том числе — не РФ, а Российской Федерации). В этом случае в сноске достаточно указать источник публикации. Можно привести в тексте вид, дату и без кавычек сокращенное наименование акта, однако дающее правильное представление о документе. Тогда в сноске надо привести полное название акта и источник публикации.

5. Все сноски размещаются постранично.

6. Настоятельно рекомендуется авторам тщательно проверять перед отправкой в журнал общую орфографию материалов, а также правильность написания соответствующих юридических терминов.

7. С учетом требований включения во всемирные базы данных Web of Science и Scopus, которые являются наиболее значимыми с точки зрения цитирования авторов, в статье на русском и английском языках представляются следующие данные: заглавие статьи, аннотация, ключевые слова, список источников, сведения об авторе: фамилия, имя, отчество, место учебы (университет, специальность, курс), работы (организация, должность), ученая степень, научное звание, адрес электронной почты. В статье сначала следует информация на русском языке, затем на английском языке («Аннотация», затем — Abstract, «Ключевые слова», затем — Key words, после текста статьи «Список источников», затем — References).

Аннотация (Abstract):

— компактная (объем: 200–250 слов);

— информативная (не содержит общих слов);

— оригинальная (не является калькой русскоязычной аннотации с дословным переводом);

— содержательная (отражает основное содержание статьи и результаты исследований);

— структурированная (следует логике описания результатов в статье, содержит следующие пункты: освещение проблемы (Purpose), материалы и методы исследования (Methods), результаты (Results), дискуссия (Discussion));

— написана качественным английским языком;

— необходимо следовать хронологии статьи и использовать ее заголовки в качестве руководства;

— текст должен быть связным, с использованием слов «следовательно», «более того», «например», «в результате» и т.д. (consequently, moreover, for example, the benefits of the study, as a result).

— необходимо использовать активный, а не пассивный залог, т.е. "The study tested", но не "It was tested in this study".

Ключевые слова (Key words)

Количество ключевых слов должно быть не менее 15.

Ключевые слова должны отражать основное содержание статьи, по возможности не повторять термины заглавия и аннотации, использовать термины из текста статьи, а также термины, определяющие предметную область и включающие другие важные понятия, которые позволят облегчить и расширить возможности нахождения статьи средствами информационно-поисковой системы.

Список источников (References)

В Списке источников и References количество источников должно быть не менее 10. При этом в References не включаются документы без авторства (законы, иные нормативные правовые акты, приказы, рекомендации).

Методика, что переводить, что транслитерировать

При ссылках на статью транслитерируется фамилия и имя автора.

Транслитерируется и переводится название журнала.

Название статьи переводится.

Пример ссылки на статью в журнале:

1. Zhbankov V.A. Tamozhenny'e prestupleniya: ponyatie i svoystva [Customs Crimes: Notion and Attributes] / V.A. Zhbankov // Publichnoe i chastnoe pravo — Public and Private Law. 2012. №. 2. S. 77–81.

При ссылках на монографию, книгу транслитерируется название источника, в скобках указывается перевод названия.

Пример ссылки на монографию, книгу:

1. Rolik A.I. Narkoprestupnost: ugolovno-pravovy'e i kriminologicheskie problemy' : monografiya [Drug Crime: Criminal Law and Criminological Issues : monograph] / A.I. Rolik, L.I. Romanova. Vladivostok : Izd-vo Dalnevostochnogo un-ta — Vladivostok : Publishing house of the Far Eastern University, 2016. 448 s.

8. На последней странице в обязательном порядке автор подписывает материал. Здесь же приводятся: фамилия и полные имя, отчество автора; должность и место работы, учебы (с правильным наименованием факультета, вуза, учреждения и т.п.); ученая степень (при наличии); точные контактные данные: адрес — служебный и (или) домашний, с индексом; телефон(ы) и факс (с кодом); адрес электронной почты (при наличии).

9. Материалы аспирантов, соискателей и студентов принимаются при наличии рекомендации соответственно кафедр вузов, отделов, секторов научно-исследовательских учреждений.

10. При несоблюдении перечисленных требований присланные материалы не рассматриваются. Материалы, не принятые к опубликованию, авторам не возвращаются. Об отказе в публикации и его основаниях авторы извещаются.

Вниманию наших авторов!

Отдельные материалы журнала размещаются на сайте журнала «Информационное право».

Понятие критической информационной инфраструктуры и ее идентификация

*Трунцевский Ю.В.**

Цель. *Национальное благополучие зависит от безопасной и устойчивой критической инфраструктуры — тех активов, систем и сетей, которые лежат в основе общества. В России принят Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Защита данных объектов требует определения того, что считать критической инфраструктурой.* ***Методология:*** *диалектика, герменевтика, синергетика, философская концептология.* ***Выводы.*** *Термин «критическая инфраструктура» определен как любой элемент, система или его часть, расположенные в государстве, которое считает необходимым поддержание жизненно важных общественных функций, здоровья, физической неприкосновенности и безопасности, социального и экономического благосостояния. В статье рассматривается два подхода к идентификации критической информационной инфраструктуры (КИИ): государственный и операторский.* ***Научная и практическая значимость.*** *Сформулированные в статье определение критичности, ее критерии для инфраструктуры позволяют составить шкалу критичности (от 5 до 0) с учетом представленных показателей оценки уровня критериев критичности ИИ.*

Ключевые слова: *критическая информационная инфраструктура, информационная безопасность, государство, идентификация, технологии, устойчивость, хакерские атаки, риски, шкала критичности, услуги, сетевые активы, функциональность.*

Purpose. *Russia has adopted Federal Law No. 187-FZ of 26 July 2017 on the Security of the critical information Infrastructure of the Russian Federation. Protecting these objects requires determining what constitutes critical Infrastructure.* ***Methodology:*** *dialectics, hermeneutics, synergetics, philosophical conceptology.* ***Summary.*** *The term «critical Infrastructure» is defined as any element, system or part thereof located in a state that considers it necessary to maintain vital public Functions, Health, physical Integrity and Security, social and economic Well-being. The article considers two approaches to the Identification of critical information Infrastructure (CII): state and operator.* ***Scientific and practical significance.*** *The Definition of criticality formulated in the Article, its criteria for Infrastructure, allow to make a criticality Scale (from 5 to 0) taking into account the presented Indicators of evaluation of the Level of criticality Criteria.***

Keywords: *critical information infrastructure, information security,government, identification, technologies, stability, hacker attacks, risks, criticality scale, services, network assets, functionality.*

Глобализация и связанные с ней процессы (подчас неконтролируемые), ускоряющееся развитие современной цивилизации и научно-технический прогресс как одно из проявлений этой тенденции, расширение сферы науки и объективное возрастание ее роли («саентизация») [1] меняют условия жизни человека, а как следствие — и характер складывающихся общественных отношений.

Один из парадоксов эволюции человечества заключается в том, что создание мощной технологической и информационной сферы параллельно формирует новые угрозы для человека, общества и государства, в том числе связанные с преступной деятельностью людей. На современном этапе характерной особенностью развития цивилизации является возрастание риска ее существования. Прогресс науки и, как производное от него, расширение техносферы создали ряд серьезных вызовов и угроз человеку и среде его обитания [2].

Современная технологическая и информационная сферы, подчас радикально изменяя условия жизни человека, формируют в его окружении большое количество потенциально опасных и одновременно уязвимых (высокорисковых) объектов, обладающих этими характеристиками в силу особенностей технологического процесса, местоположения, размещения на них опасных веществ и материалов (ОВМ), функционального назначения и т.д.

Осуществляемый в нашей стране переход к информационному обществу приводит к тому, что подавляющее большинство бизнес-процессов [3] и систем принятия решений в стратегических отраслях экономики и соответствующей сфере государственного управления реализуются с использованием информационных технологий [4, 5]. В различных информационных системах уже сейчас хранятся и обрабатываются значительные объемы информации, в том числе касающейся вопросов государственной политики и обороны, финансовой и научно-технической сферы, частной жизни граждан. Одновременно информационные технологии повсеместно внедряются при построении автоматизированных систем управления произ-

* **Трунцевский Юрий Владимирович,** ведущий научный сотрудник отдела методологии противодействия коррупции Института законодательства и сравнительного правоведения при Правительстве РФ, профессор кафедры уголовной политики Академии управления МВД России, доктор юридических наук, профессор. E-mail: trunzev@yandex.ru

Рецензент: Лопатин Владимир Николаевич, главный редактор, научный руководитель (директор) РНИИИС, эксперт РАН, доктор юридических наук, профессор, заслуженный деятель науки Российской Федерации.

** **The Concept and Identification of Critical Information Infrastructure**

Truncevski Yu.V., Leading researcher of the Department of Methodology of the Corruption Counteraction of the Institute of Legislation and Comparative Law under the Government of the Russian Federation, Professor of the Department of Criminal Policy of the Academy of Management of MIA of Russia, Doctor of Law, Professor.

Reviewer: Lopatin V.N., Chief Editor, the Scientific Head of the National Research Institute of Intellectual Property (NSRIIP), Expert of the Russian Academy of Sciences, Doctor of Law, Professor, Honored Worker of Science of the Russian Federation.

водственными и технологическими процессами, используемых в топливно-энергетическом, финансовом, транспортном и других секторах критической инфраструктуры Российской Федерации.

Национальное благополучие зависит от безопасной и устойчивой критической инфраструктуры — тех активов, систем и сетей, которые лежат в основе общества. Для достижения этой безопасности и устойчивости критически важные партнеры по инфраструктуре должны коллективно определять приоритеты, формулировать четкие цели, снижать риски, измерять прогресс и адаптироваться на основе обратной связи и меняющейся среды. В России принят Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1].

Преимущества критической информационной инфраструктуры (КИИ) (увеличенное взаимодействие, дистанционный контроль, масштабируемость, надежность, снижение затрат) не всегда одинаково сбалансированы с возможными неблагоприятными последствиями их неисправности. КИИ является «клеем» между и внутри критической инфраструктуры во все более взаимосвязанном мире.

Нанесение ущерба КИИ может привести к катастрофическим последствиям, а учитывая, что она является связующим звеном между другими секторами национальной инфраструктуры, неизбежно нанесет ущерб и этим секторам. Переход информационных и коммуникационных технологий на систему цифровых сигналов упростил и частично автоматизировал управление процессами, но, в то же время, сделал их более уязвимыми перед компьютерными атаками. Вредоносная программа, направленная на внесение изменений в бинарный код программы (алгоритм программы, записанный в двоичной системе исчисления), способна вывести из строя любое оборудование, работающее с использованием бинарного кода. При этом равную опасность могут представлять атаки, совершаемые в преступных, террористических и разведывательных целях со стороны отдельных лиц, сообществ, иностранных специальных служб и организаций [6].

Системы критической энергетической инфраструктуры включают в себя множество различных компаний и организаций, которые связаны друг с другом в электронном виде внутри сектора и с другими секторами критической инфраструктуры посредством информационных сетей. Опора на SCADA-технологии (системы автоматического контроля и сбора информации (SCADA) еще больше увеличивает уязвимость сети. Сбои и электронные атаки делают энергетический сектор в целом высоко уязвимым. Хакерские атаки могут быть запущены для получения или повреждения информации, нарушения работы служб или планирования дальнейших атак на инфраструктуру. Наличие и целостность этих систем и передаваемой информации в значительной степени зависит от хороших физических, личных и технических защитных процедур безопасности.

Критическая инфраструктура особенно уязвима, когда пересекает границы, потому что именно в таких условиях действуют расхождения юрисдикционных норм и стандартов безопасности и вопросы, касающиеся руководства, контроля и подотчетности, являются наиболее неясными.

Сектор КИИ представляет ряд особенностей по сравнению с другими секторами информационной инфраструктуры. Во-первых, можно сказать, что с распространением IT в современном обществе практически каждый человек стал потенциальным слабым звеном информационной безопасности. Следовательно, защита критически важной информационной инфраструктуры является особенно сложной задачей, поскольку в ней участвует почти бесконечное число заинтересованных сторон. Во-вторых, информация — это область, в которой национальные границы не имеют большого значения, а взаимозависимость является нормой. Поэтому в этом секторе в большей степени, чем в других, национальная политика в области защиты должна дополняться совместными многосторонними усилиями.

Защита КИИ требует ряда последовательных шагов:

— во-первых, определить, что считается критической инфраструктурой;

— во-вторых, определить те инфраструктуры, которые подходят под это определение;

— в-третьих, оценить риск этой инфраструктуры и выявить пробелы в ее защите;

— наконец, определение надлежащих мер защиты для снижения данного риска.

Рассмотрим, что считается критической инфраструктурой. Информация и связь были одним из первых секторов, в котором признали необходимость защиты критически важной инфраструктуры от потенциальных угроз.

Информационная инфраструктура — термин, обычно используемый для описания совокупности взаимосвязанных компьютеров и сетей и поток информации через них. Кибер-инфраструктура — это необходимая для предоставления жизненно важных услуг населению безопасность, экономическая стабильность, национальная безопасность, международная стабильность и устойчивость, и восстановление критического киберпространства. Некоторые части этой информационной инфраструктуры могут быть предназначены для управления/контроля других провайдеров инфраструктуры, например — производство электроэнергии, газо-, нефтепроводы, или поддержания экономики, например — банки или телекоммуникации. Вклад услуг этих инфраструктур важен, и удар или сколь угодно неожиданный отказ или их отключение оценивается критично.

Термин «критическая инфраструктура» можно определить как любой элемент, система или его часть, расположенные в государстве, которое считает необходимым поддержание жизненно важных общественных функций, здоровья, физической неприкосновенности и безопасности, социального и экономического благосостояния.

В свою очередь информационная инфраструктура «представляет собой незаменимую «нервную систему», которая позволяет современному обществу работать и жить» [7]. КИИ — это взаимосвязанные коммуникационные инфраструктуры, которые необходимы для поддержания жизненно важных функций (здоровье, безопасность, экономическое или социальное благополучие людей), нарушение или разрушение которых может иметь серьезные последствия.

Критическая информационная инфраструктура — это широкое понятие, обозначающее как саму информацию (поток данных), так и каналы, по которым создается и передается информация (главным образом компьютерные сети). Следовательно, КИИ обычно понимается как включающая защиту данных (включая вопросы конфиденциальности) и защиту информационной инфраструктуры (также называемой «сетевой безопасностью»).

Идентификация КИИ. Можно провести различие между двумя подходами, основанными на том, кто берет на себя ведущую роль в идентификации КИИ:

а) государственный подход, при котором ведущую роль берут на себя правительственные учреждения, уполномоченные выявлять и защищать информационную инфраструктуру (ИИ), в большинстве случаев ответственные министерства;

[1] СЗ РФ. 2017. № 31 (часть I). Ст. 4736.

b) операторский подход, при котором ведущую роль берут на себя операторы важнейших объектов инфраструктуры.

Государственный подход. В случае государство-ориентированного подхода весь процесс определяется государственными органами, которые имеют полномочия по выявлению и защите ИИ. Определившись с критическими секторами, они применяют метод систематического выявления важнейших услуг. Далее они определяют операторов ИИ, участвующих в этой работе. Выявление конкретных активов может осуществляться в сотрудничестве с целью обеспечения эффективности в соответствии с потребностями общества.

В основном уполномоченные организации ИИ определяют перечень фактических критически важных услуг и уведомляют операторов об этих услугах. Таким образом, оператор КИИ отвечает за определение конкретных сетевых активов и соответствующих мер для обеспечения безопасности и доступности подключения. Затем уполномоченные учреждения пересматривают план и периодически обновляют перечень важнейших услуг в связи с постоянно меняющимся ландшафтом угроз.

Подход оператора. В случае оператор-ориентированного подхода ведущая роль отводится операторам КИИ. Государство определяет список операторов (называемых также «жизненно важными операторами»), которые отвечают за определение отдельных важнейших услуг и активов, которые соответствуют ряду анализов рисков и директив по управлению рисками [8]. Затем ответственные министерства рассматривают выбранные услуги и активы вместе с разработанными планами защиты ИИ.

Министерства определяют «жизненно важных операторов» или «жизненно важных поставщиков услуг» в пределах своей собственной зоны ответственности, и эти операторы затем юридически обязаны провести анализ оценки рисков, определить список отдельных критически важных активов и разработать структурированные планы защиты КИИ. При таком подходе определение критических услуг является обязанностью операторов. Типичный пример можно найти во Франции (инструкция 6600/2014) [9]. Это прагматический подход, учитывающий современное состояние идентификации КИИ, поскольку операторы лучше знают свою инфраструктуру. Вместе с тем им делегируется ответственность.

Операторы КИИ должны идентифицировать подробные сетевые активы и пометить их с помощью общей таксономии[2], которая может использоваться для объединения различных представлений.

Независимо от того, какой из двух подходов принимает государство и какая организация должна взять на себя ведущую роль, следует следовать структурированному процессу для определения важнейших услуг. Обычно этот процесс состоит из следующих действий:

а) применение отраслевых критериев для составления краткого перечня потенциальных важнейших услуг;

б) оценка уровня критичности услуг, включенных в шорт-лист.

Следует указать, что критичность — это:

— уровень вклада инфраструктуры в общество в поддержании минимального уровня национального и международного правопорядка, общественной безопасности, экономики, общественного здравоохранения и окружающей среды;

— уровень воздействия на граждан или правительство в результате утраты или разрушения инфраструктуры [10].

«Воздействие» обычно оценивается по трем основным характеристикам:

— область действия или пространственное распределение — географическая область, которая может быть затронута потерей или недоступностью критической инфраструктуры;

— серьезность, интенсивность или масштаб — последствия разрушения или уничтожения той или иной КИИ;

— влияние времени или временного распределения — точка, с которой потеря элемента может иметь серьезные последствия (немедленно, один-два дня, одна неделя и т.п.).

Ряд стран опубликовали критерии критичности [11,12] в целях выявления важнейших активов.

Таблица № 1

Критерии критичности ИИ

Показатель критичности	Значение критичности
Пострадавшее население	Процент населения, пострадавшего от нарушения работы службы
Сосредоточенность	Плотность населения по географическому району, влияющему на обслуживание
Экономическое воздействие	Стоимость прерывания в процентах ВВП
Общественное доверие	Влияние надлежащего функционирования этой службы на доверие населения к правительству

Определить и классифицировать узел как критический можно, если:

— он может оказывать такое влияние на другие узлы, в результате которого может произойти разрушение государственной или общественной инфраструктуры;

— он образует неотъемлемую часть связи узлов, который может воздействовать на них, и неисправность его может привести к серьезным нарушениям.

Предлагаемыми ориентировочными параметрами для идентификации КИИ являются:

— функциональность поддерживаемой системы/информационной инфраструктуры;

— степень взаимодополняемости с другой национальной информационной инфраструктурой;

— связанность с социальными, политическими или стратегическими ценностями.

Итак, идентификация КИИ — это выделение и классификация каждого критического сектора в рамках их инфраструктур на основе функциональности; шкала критичности; степень взаимодополняемости, политического, экономического, социального и стратегического значения; зависимость; чувствительность и т.д. Идентификация КИИ является динамичным процессом и должна периодически пересматриваться всеми заинтересованными сторонами. Идентификация КИИ является частью национальной оценки рисков, которая представляет собой целостное представление обо всех рисках для национальной безопасности.

1. Функциональность — это динамическая концепция, включающая функции и процедуры, связанные с системой или с ее составной частью. Ее можно рас-

[2] Таксоно́мия — учение о принципах и практике классификации и систематизации сложноорганизованных иерархически соотносящихся сущностей. Принципы таксономии применяются во многих научных областях знаний, для упорядочивания объектов географии, геологии, языкознания, этнографии и всего многообразия органического мира.

сматривать на двух уровнях — функциональная уникальность и функциональная зависимость.

2. Шкала критичности — это эвристическое правило для оценки воздействия, основанное на многоаспектном подходе, который включает в себя доступ, завершение основных услуг.

3. Степень взаимодополняемости является отличительной характеристикой ИИ и заключается в том, что она связывает другую информационную инфраструктуру системы вместе. Отказ одной системы может привести к остановке другой КИИ относительно быстро и каскадно.

4. Политические, экономические, социальные и стратегические ценности играют важную роль для политической стабильности, экономического процветания, демократии, единства и целостности государства и общества.

5. Продолжительность времени имеет важное значение для идентификации и категоризации КИИ. Однако одна и та же система может быть/не быть критической в разных случаях при разных обстоятельствах.

Шкалу критичности для информационной инфраструктуры можно охарактеризовать следующим образом.

Таблица № 2

Шкала критичности информационной инфраструктуры

Степень критичности ИИ	Описание критериев критичности ИИ
5	Инфраструктура, потеря которой имела бы катастрофические последствия для государства. Эти активы будут иметь уникальное национальное значение, потери будут иметь национальные долгосрочные последствия в ряде секторов
4	Инфраструктура, имеющая первостепенное значение для различных секторов. Последствия утраты этих активов для основных услуг будут серьезными и могут повлиять на предоставление основных услуг в стране миллионам граждан
3	Инфраструктура, имеющая существенное значение для секторов и основных услуг, утрата которых может затронуть области и многие сотни тысяч людей
2	Инфраструктура, потеря которой окажет существенное влияние на предоставление основных услуг, приводящих к потере или нарушению обслуживания десятков тысяч людей или затрагивающих целые регионы
1	Инфраструктура, потеря которой может привести к умеренному нарушению обслуживания, с высокой степенью локализации, затрагивающая тысячи граждан
0	Инфраструктура, последствия утраты которой будут незначительными в национальном масштабе

Оценка уровня критериев критичности ИИ может включать:

— критерий жертв (потенциальное число погибших или раненых);

— критерий экономического эффекта (значимость потенциальных экономических потерь и/или ухудшения услуги, потенциальные последствия для окружающей среды);

— критерий общественного воздействия (влияние на доверие населения, уровень физических страданий населения, уровень нарушения повседневной жизни);

— критерий зависимости (например, потенциал каскадного воздействия на другие сектора, например, незначительный, умеренный, значительный, уничтожающий);

— сфера охвата критерия воздействия (затрагиваемый район: например, местный, большой район или несколько секторов (частично), общенационального или единого сектора (полностью), международного или нескольких секторов (полностью); затронутое население и/или плотность населения в затронутом районе);

— влияние на услуги (например, время восстановления в днях).

Кроме зависимости внутри страны, можно найти зависимости между национальным ИИ и инфраструктурами соседних стран и регионов. Такие зависимости могут влиять на критичность конкретной национальной инфраструктуры, например, когда национальная экономика в значительной степени зависит от экспорта или импорта.

Зависимость — это отношение между двумя продуктами или услугами, в которых один продукт или услуга необходимы для создания другого продукта или услуги. Взаимозависимость — взаимная зависимость продуктов или услуг. Сектора ИИ и их критически важные услуги зависят от других секторов и их критических сервисов.

Оценка зависимостей. Важным аспектом, который необходимо учитывать при определении важнейших услуг, являются зависимости между различными секторами и подсекторами, а также трансграничные зависимости. Зависимости могут привести к тому, что служба и/или инфраструктура будут определены как критические, не из-за первого порядка сбоев, а из-за каскадных последствий, которые их нарушение может иметь для других служб/инфраструктур. Кроме того, нарушение обслуживания в одной стране может привести к серьезным последствиям в других странах.

При оценке критичности услуг, инфраструктур и поддерживающих сетевых активов крайне важно рассматривать систему в целом, а не по отдельным компонентам, учитывая, что существует по крайней мере четыре типа зависимостей, которые должны быть приняты во внимание:

— взаимозависимости внутри критического сектора (внутрисекторальные): в секторе телекоммуникаций существуют сильные внутрисекторальные зависимости;

— взаимозависимости между критическими секторами (межсекторальные). Следует учитывать тот факт, что взаимозависимости между инфраструктурами существуют как на логическом, так и на физическом уровне;

— взаимозависимости между активами коммуникационных сетей: сети передачи данных создаются путем связывания компонентов/узлов. Взаимозависимость компонентов является неотъемлемым свойством сети передачи данных: каждый узел сети зависит от других узлов для обмена и пересылки пакетов данных для предоставления услуг связи. Помимо «физической взаимозависимости связности», которая четко отражена в сетевой архитектуре, в современном сетевом ландшафте существует множество типов «логической взаимозависимости связности»;

— взаимозависимости на национальном и международном уровнях (трансграничном), что еще более усложняет задачу оценки риска.

Критическая инфраструктура страны обеспечивает основные услуги, которые лежат в основе российского общества. Упреждающие и скоординированные усилия необходимы для укрепления и поддержания

безопасной, функционирующей и устойчивой критической инфраструктуры, включая активы, сети и системы, которые имеют жизненно важное значение для доверия общественности и безопасности, процветания и благосостояния государства.

Определение критериев критичности инфраструктуры является необходимой мерой построения всей системы защиты КИИ, позволяет оценить риск этой инфраструктуры и выявить пробелы в ее защите. Критическая инфраструктура — это любой элемент, система или его часть, расположенные в государстве, которое считает необходимым поддержание жизненно важных общественных функций, здоровья, физической неприкосновенности и безопасности, социального и экономического благосостояния. КИИ — это взаимосвязанные коммуникационные инфраструктуры, которые необходимы для поддержания жизненно важных функций (здоровье, безопасность, экономическое или социальное благополучие людей), нарушение или разрушение которых может иметь серьезные последствия. Любой из двух подходов (государство-ориентированный и оператор-ориентированный) позволяет составить краткий перечень потенциально важных услуг, где критичность включает: уровень вклада инфраструктуры в общество; уровень воздействия на граждан или правительство (географическая область; серьезность, интенсивность; временное распределение) в результате утраты или разрушения инфраструктуры.

Идентификация КИИ как динамичный процесс периодически пересматривается и включает: выделение и классификацию каждого критического сектора в рамках их инфраструктур на основе функциональности; разработку шкалы критичности; определение степени взаимодополняемости; определение политического, экономического, социального и стратегического значения, зависимости и чувствительности.

Литература

1. Agrawal A. Indigenous knowledge and the politics of classification / A. Agrawal // Intern. Social Science J. 2002. № 173. P. 287–297.

2. Олейников Ю.В. Экологические ограничения развития общества / Ю.В. Олейников // К экологической цивилизации. М., 1993. С. 54–71.

3. Трунцевский Ю.В. Due diligence — правовой аудит хозяйствующих субъектов / Ю.В. Трунцевский, О.Г. Карпович // Безопасность бизнеса. 2013. № 4. С. 22–25.

4. Хабриева Т.Я. Право перед вызовами цифровой реальности / Т.Я. Хабриева // Журнал российского права. 2018. № 9 (261). С. 5–16.

5. Хабриева Т.Я. Право в условиях цифровой реальности / / Т.Я. Хабриева, Н.Н. Черногор // Журнал российского права. 2018. № 1 (253). С. 85–102.

6. Капустин А.Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности / А.Я. Капустин // Журнал зарубежного законодательства и сравнительного правоведения. 2017. № 6. С. 44–51.

7. Colesniuc Dan. Cyberspace and Critical Information Infrastructures / Dan Colesniuc // Informatica Economică vol. 17, №. 4/2013. P. 123–132.

8. Трунцевский Ю.В. О проблемах правового регулирования взаимоотношений государства и бизнеса / Ю.В. Трунцевский // Юридический мир. 2011. № 4. С. 20–25.

9. L'instruction générale interministérielle n° 6600/ SGDSN/PSE/PSN du 7 janvier 2014. URL: http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828

10. Luiijf E. Critical Infrastructure Protection in the Netherlands: A Quick-scan / E. Luiijf; H. Burger & M. Klaver; In U.E. Gattiker (Ed.) // EICAR Conference Best Paper Proceedings. Copenhagen : EICAR, 2003. 19 p.

11. National Infrastructure Protection Plan (NIPP) Security and Resilience Challenge 2018. URL: https://www.dhs.gov/publication/nipp-security-and-resilience-challenge-2018-fact-sheet.

12. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL : https://publications.europa.eu/en/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10/

References

1. Agrawal A. Indigenous Knowledge and the Politics of Classification / A. Agrawal // Intern. Social Science Journal. 2002. № 173. S. 287–297.

2. Oleynikov Yu.V. Ekologicheskie ogranicheniya razvitiya obschestva [Environmental Limitations of the Society Development] / Yu.V. Oleynikov // K ekologicheskoy tsivilizatsii. To the Environmental Civilization. Moskva — Moscow, 1993. S. 54–71.

3. Truntsevskiy Yu.V. Due diligence — pravovoy audit khozyaystvuyuschikh subyektov [Due Diligence: Legal Audit of Business Entities] / Yu.V. Truntsevskiy, O.G. Karpovich // Bezopasnost biznesa — Business Security. 2013. № 4. S. 22–25.

4. Khabrieva T.Ya. Pravo pered vy'zovami tsifrovoy realnosti [Law Facing Digital Reality Challenges] / T.Ya. Khabrieva // Zhurnal rossiyskogo prava — Russian Law Journal. 2018. № 9 (261). S. 5–16.

5. Khabrieva T.Ya. Pravo v usloviyakh tsifrovoy realnosti [Law in Conditions of the Digital Reality] / T.Ya. Khabrieva, N.N. Chernogor // Zhurnal rossiyskogo prava — Russian Law Journal. 2018. № 1 (253). S. 85–102.

6. Kapustin A.Ya. K voprosu o mezhdunarodno-pravovoy kontseptsii ugroz mezhdunarodnoy informatsionnoy bezopasnosti [On the International Law Concept of International Information Security Threats] / A.Ya. Kapustin // Zhurnal zarubezhnogo zakonodatelstva i sravnitelnogo pravovedeniya — Journal of Foreign Law and Comparative Legal Studies. 2017. № 6. S. 44–51.

7. Colesniuc Dan. Cyberspace and Critical Information Infrastructures / Dan Colesniuc // Informatica Economică. Vol. 17. №. 4/2013. S. 123–132.

8. Truntsevskiy Yu.V. O problemakh pravovogo regulirovaniya vzaimootnosheniy gosudarstva i biznesa [On Issues of Legal Regulation of Interrelations between the State and Business] / Yu.V. Truntsevskiy // Yuidicheskiy mir — Legal World. 2011. № 4. S. 20–25.

9. L'instruction générale interministérielle n 6600/ SGDSN/PSE/PSN du 7 janvier 2014. URL: http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828

10. Luiijf E. Critical Infrastructure Protection in the Netherlands: A Quick-Scan / E. Luiijf; H. Burger & M. Klaver; In U.E. Gattiker (ed.) // EICAR Conference Best Paper Proceedings. Copenhagen : EICAR, 2003. 19 s.

11. National Infrastructure Protection Plan (NIPP) Security and Resilience Challenge 2018. URL: https://www.dhs.gov/publication/nipp-security-and-resilience-challenge-2018-fact-sheet

12. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. URL: https://publications.europa.eu/en/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10/

Эволюция концепции открытого правительства в зарубежной правовой доктрине и законодательстве

*Шевердяев С.Н., Лаер Е.А.**

Статья посвящена анализу становления в правовой доктрине западных государств идеи открытости власти. ***Цель.*** *На сравнительно широком материале профильной зарубежной литературы последовательно показать эволюцию основных этапов совершенствования содержания концепта открытого правления и его правовых гарантий как в политико-правовой доктрине, так и в законодательстве зарубежных стран.* ***Методология:*** *в качестве основного средства анализа эволюции взглядов на проблему применен историко-правовой метод, а также используются компаративистские подходы для сопоставления ряда моделей правового регулирования.* ***Результат.*** *Прослежена последовательность основных этапов развития политико-правового мировоззрения западных стран в части идеалов открытости правительства, что позволяет специалистам корректно оценивать проблемные ракурсы аналогичной российской правовой дискуссии.*

Ключевые слова: *открытое правительство, открытость органов власти, открытое общество, конституционные права, право на информацию, право на доступ к информации, гласность, транспарентность, прозрачность.*

The article is devoted to the analysis of the formation of the idea of openness of authority in the legal doctrine of Western States. ***Purpose.*** *To show the evolution of the main stages of improving the concept of open government and its legal guarantees both in the political and legal doctrine and in the legislation of foreign countries on the relatively broad foreign literature.* ***Methodology:*** *the main means of analyzing the evolution of views is the historical-legal method, and comparative approaches are used to compare a number of models of legal regulation.* ***Results.*** *The sequence of the main stages of the development of the political and legal outlook of Western countries in terms of the ideals of openness of the government allows to assess the problematic perspectives of a similar Russian legal debate.***

Keywords: *open government, openness of the authorities, an open society, constitutional rights, right to information, right to access to government information, transparency.*

Появление идеи открытого правительства

Отдельные аспекты идеи открытости власти для граждан при желании можно найти в античной или средневековой истории [1, с. 30]. Однако, если говорить о современном понимании этого концепта, которое связано с возможностью получения гражданами информации о деятельности государственных органов в целях общественного контроля и участия в управлении делами государства, то считается, что первенство постановки вопроса в этом ракурсе принадлежит Швеции, где в 1766 г. был принят соответствующий конституционный акт.

Особый вклад в теорию открытого правительства связан с наследием шведского мыслителя эпохи Просвещения Андерса Чидениуса, который обосновал «принцип гласности» (“offentlighetsprincipen”). Будучи недовольным тем, что у его родной провинции не было доступа к секретным документам, в которых указывалось, какие земли получат экономические выгоды от центрального правительства, он отстаивает идею большей прозрачности экономического регулирования [2, с. 82]. Ему удалось получить место в национальном парламенте, где он продолжил защищать идеи экономической свободы, а также право общественности участвовать в национальных дебатах. Став секретарем комитета по свободе прессы, А. Чидениус смог разработать закон, сочетавший свободу печати и право на доступ к правительственной информации. Хотя этот закон действовал только шесть лет до переворота короля Густава III, он стал одним из первых, который гарантировал открытый доступ к государственным документам [3, с. 11].

Идея открытого правления занимала умы и более именитых мыслителей эпохи Просвещения. К примеру, хорошо известна критика Дж. Локком и Ж.-Ж. Руссо идеи абсолютной монархии, основанной среди прочего на недоступности гражданам сведений о порядке функционирования государственного механизма. Популяризация этой критики и привела в конечном итоге к кардинальным изменениям в политическом строе европейских государств, а разработанный ими аналитический инструментарий помог

* **Шевердяев Станислав Николаевич,** эксперт Проектно-учебной лаборатории антикоррупционной политики НИУ Высшая школа экономики; доцент кафедры конституционного и муниципального права Юридического факультета Московского государственного университета имени М.В. Ломоносова, кандидат юридических наук, директор Научно-образовательного центра конституционализма и местного самоуправления МГУ. E-mail: shevers@rambler.ru
Лаер Елизавета Андреевна, исследователь-аналитик «Томсон Рейтерс». E-mail: yl0407a@student.american.edu
Рецензент: Морозов Андрей Витальевич, член редколлегии, заведующий кафедрой информационного права, информатики и математики Всероссийского государственного университета юстиции (РПА Минюста России), доктор юридических наук, профессор.

** **Evolution of the Open Government Concept in the Foreign Legal Doctrine and Laws**
Sheverdyaev S.N., Expert at the Laboratory for Anti-Corruption Policy at the Higher School of Economics, Associate Professor of the Department of Constitutional and Municipal Law of the Law Faculty of the Lomonosov Moscow State University, Executive Director of the Research and Educational Center for Constitutionalism and Local Self-Governance at the M.V. Lomonosov Moscow State University, Candidate of Legal Sciences.
Layer E.A., Research Analyst at Thomson Reuters.
Reviewer: Morozov A.V., Member of the Editorial Board, Head of the Department of Information Law, Informatics and Mathematics of the All-Russian state University of Justice (RPA of the Ministry of Justice of Russia), Doctor of Law, Professor.

выявить проблемы, возникавшие в обществе из-за повышенной секретности работы правительства [4, с. 4].

Принятая во Франции в 1789 г. Декларация прав человека и гражданина гласит, что «все граждане имеют право устанавливать сами или через своих представителей необходимость государственного обложения... и следить за его расходованием» [5, с. 12]. А уже в 1790 г. был построен и открыт для посетителей Национальный архив Франции, где граждане могли запросить копии правительственных документов [6, с. 20].

Под влиянием этих же идей при написании Конституции США также были частично предусмотрены гарантии защиты права общества на доступ к информации о работе законодательных органов и решениях, принимавшихся в правительстве [7, с. 199]. Понимание того, что доступ к информации является правом граждан, становится теперь более привычным и распространенным.

В первой половине XX века появляется важный теоретический концепт, существенно повлиявший на развитие представлений об открытом правлении. Французский философ Анри Бергсон в 1932 г. описывает концепцию «открытого общества», подразумевая под ним такое общество, которое включает в себя всех своих членов и не пытается приуменьшить значение каждого из них [8, с. 30]. В 1960-х годах Карл Поппер, опираясь на идеи Бергсона, публикует свою эпохальную работу «Открытое общество и его враги», которая перевернула представление об истинном значении категории открытости в современной социальной философии. Поппер указывал, что закрытое общество — это то общество, где общие племенные ритуалы образуют самые важные ценности и не позволяют занять место индивидуальным правам и обязанностям [9, с. 172–173]. А открытое общество — это то общество, где равенство, индивидуализм и вера в разум представляют собой важнейшие идеалы [9, с. 199]. Как полагают многие ученые, современное представление о либеральной демократии без идей Поппера несостоятельно [10, с. 6].

Философская концепция открытого общества закономерно представляет собой более широкое теоретическое понятие, чем идея открытого правления, которое используется в политико-правовой литературе и особенно в нормативных актах для решения более узких задач. Открытое правление можно воспринимать как один из методов, с помощью которых можно добиться подлинной реализации идеи открытого общества. Как заметили гарвардские ученые Арчон Фунг и Дэвид Вил, идея открытого правительства призывает к открытости в органах правительства, не говоря ничего о сфере бизнеса и больших корпорациях, тогда как идея открытого общества призывает к открытости и транспарентности всех учреждений и людей [11, с. 109].

Развитие концепции открытого правительства

Идеалы открытого правления сопровождали историю развития политико-правовых учений со времен античности и даже находили спорадическое отражение в законодательстве. Однако широкое использование в правовой доктрине и появление в законодательстве термина «открытое правительство в его специальном значении» связывается с XX веком.

Исследователи подчеркивают, что в середине прошлого столетия все больше европейцев и американцев выражают недовольство тем, как много военных документов осталось засекреченными и не доступными для общественности [12, с. 2].

В эти годы активно развивается национальная судебная практика, международные нормы и правовая доктрина в этом вопросе. Так, в 1943 г. в США суды объявляют право на доступ к информации неотъемлемым правом человека, а Федеральный конституционный суд Германии устанавливает прямую связь между доверием людей к демократии и наличием прозрачности правительства и прозрачных институционализированных процедур [13, с. 1].

Термин «открытое правительство» начал фигурировать и в разных международных соглашениях. К примеру, в 1946 г. ООН приняла резолюцию (59) 1 «О Созыве международной конференции о свободе информации», в которой говорилось, что «свобода информации является одним из основных прав человека и является краеугольным камнем всех свобод, которые посвящены ООН». При этом восприятие свободы информации в этих документах связывалось не только с деятельностью средств массовой информации. Для свободы расследований у обычных граждан должен быть непосредственный доступ к правительственной информации.

В 1957 г. американский исследователь Уоллес Паркс заметил, что обе основные политические партии в США на последних выборах, пообещали освободить и сделать доступной правительственную информацию, относящуюся к национальному правительству, но эти обещания так и остались не выполненными [14, с. 4]. Для этого автора доступ к информации — один из самых главных примеров применения идеи об открытом правительстве. Без этого доступа у граждан не развивалось ни доверие к правительству, ни желание принимать активное участие в нем.

В 1966 г. в США подписывается эпохальный Закон о свободе информации, который гарантировал доступ граждан к документам федеральных агентств, если эта информация не была защищена одним из девяти исключений, прилагаемых к Закону [15, с. 186–208]. Если государство пыталось отказать в предоставлении информации, то теперь это могло повлечь ответственность, налагаемую в федеральных судах США.

В 1977 г. Даниэль Ивестер описал проблемы организации западных правительств, которые приводят к сокрытию информации от общества. В своей статье «Конституционное право знать», он объяснил, что исполнительная ветвь власти в США становится все сильнее, что вызывает проблемы, так как у президента появляется право решать, что народ должен знать, а что можно от него утаить [16, с. 109]. Это приводит к дисбалансу между тремя ветвями власти и дает президенту больше контроля над той информацией, которую положено знать гражданам.

В 1979 г. Парламентская ассамблея Совета Европы выпустила Рекомендацию № 854, где говорилось, что парламентарная демократия может существовать только если у всех людей есть полный доступ к информации, и было также подчеркнуто, что законы, касающиеся открытого доступа к информации, предоставляют надлежащий контроль над коррупцией и растратой государственных средств. Страны Европы с этого времени включаются в процесс разработки особых законов о доступе к информации и рассекречивания правительственных документов. К 1983 г. в Финляндии, Дании, Франции, Голландии, Норвегии появились законопроекты, похожие на тот, который был подписан в США в 1966 г. [17, с. 13]. Если в США этот закон был встречен первоначально сопротивлением со стороны властей, то в Европе было меньше недовольства со стороны национальных правительств. По свидетельству наблюдателей, это было связано с большей культурой открытости, в особенности в странах Северной Европы.

В договорах, регулирующих функционирование Европейского Союза, также есть конкретные положения о том, что вся информация, касающаяся различных правил и директив, будет доступна для общественности, включая электронные данные. Маастрихтский договор при подписании в 1992 г. вклю-

чал в себя Декларацию № 17 о праве на доступ к информации и рассматривался как способ укрепления демократического характера институтов ЕС и повышения доверия общества к администрации [18, с. 17]. Позже, в 1997 г., Амстердамский договор также закрепил эти права, гарантируя право доступа к документам Европейского парламента, Совета и Комиссии всем физическим и юридическим лицам, проживающим или имеющим зарегистрированный офис в одном из государств, которые являются членами ЕС [18, с. 18].

С 2009 г. правительства США и ряда других стран разработали ряд политических инициатив, которые способствуют раскрытию информации, хранящейся как государственными, так и частными организациями [19, с. 97]. Так, в Директиве открытого правительства, подписанной Бараком Обамой, говорилось, что федеральные агентства должны институционализировать принципы прозрачности в своей деятельности, участие общества в принятии решений агентствами и сотрудничество со всеми заинтересованными сторонами [20, с. 5].

Современный взгляд на «открытое правительство»

В последние годы движение открытого правительства начало набирать силы как среди правительств, так и среди общественных активистов. Больше правительств стали принимать инициативу открытого правительства, основываясь на указанном документе, принятом администрацией Обамы. Исследование реализации принципов открытого правительства в Европейском союзе показало, что на 2015 г. все 28 государств-членов имеют политику, направленную на достижение целей открытого правительства, причем Великобритания считается лидером в этих инициативах [21, с. 13]. Также появилось много международных инициатив, направленных на создание глобальной культуры открытого правительства.

В 2011 г. была создано новая международная организация «Партнерство открытого правительства» (Open Government Partnership), чьи цели заключаются в обеспечении конкретных обязательств стран «содействовать прозрачности, расширять права граждан, бороться с коррупцией и использовать новые технологии для совершенствования управления». Чтобы вступить в это партнерство, страны должны подписать Декларацию открытого правительства, основанную на Всеобщей декларации прав человека и Конвенции ООН против коррупции, после чего государства берут на себя обязательство способствовать созданию глобальной культуры открытого правительства, расширяющей права и возможности граждан и продвигающей идею правительства в XXI веке, которое основано на открытом и активном участии общества.

Дон Тапскотт, специализируйся на воздействии инноваций и технологий на общество, описал открытое правительство как новую, по-настоящему интегрированную организацию, которая сотрудничает со всеми, особенно с гражданами, разделяет ресурсы, которые ранее были тщательно защищены, задействует возможности массового сотрудничества и поощряет прозрачность на протяжении всей своей деятельности [22, с. 16]. Однако в дальнейшем технологическом и организационном развитии концепции открытого правительства появляются и новые опасности. К примеру, это касается практики «электронного правительства», которая внедряется как способ использования технологий в рамках повседневной деятельности, осуществляемой общественными организациями и правительствами (например, предоставление государственных услуг, проведение онлайн-консультаций и выплата денег за ЖКХ), для того чтобы сделать государственные услуги более эффективными и быстрыми [23, с. 2]. Автоматизация некоторых взаимодействий с правительством через вебсайты и онлайн-серверы позволяет этим операциям занимать меньше времени и снижать затраты, которые на них требуются [24, с. 3]. Однако эта практика подвергается критике за то, что оно в основном сосредоточено на совершенствовании государственных услуг, а не трансформации правительства в целом в сторону более широкой демократии, чего хотят добиться активисты открытого правительства [25, с. 541].

Литература

1. Jason Hawke. Writing Authority: Elite Competition and Written Law in Early Greece (DeKalb : Northern Illinois Press, 2011), 171–172 ; James M. Blythe. Ideal Government and the Mixed Constitution in the Middle Ages (Princeton : Princeton University Press, 1992).

2. Thomas S. Blanton. “The Global Openness Movement in 2006: 240 Years after the First Freedom of Information Law, Access to Government Information Now Seen as a Human Right,” in The World’s First Freedom of Information Act: Anders Chydenius’ Legacy Today, eds. Juha Mustonen (Kokkola: Anders Chydenius Foundation, 2006).

3. Richard Chapman and Michael Hunt. Open Government: A Study Of The Prospects Of Open Government Within The Limitations Of The British Political System (London: Croom Helm, 1987).

4. Bo Isenberg. “Critique and Crisis. Reinhart Koselleck’s Thesis of the Genesis of Modernity,” Eurozine — Network of European Cultural Journals (January 2012).

5. National Assembly of France. “The Declaration of the Rights of Man and of the Citizen, 1789” American Bar Association, 2011.

6. Cynthia Warringa van Genderen. “The Right to Know: A Comparative Legal Survey of Access to Official Information in Different Countries,” University of Leiden, (June 2013).

7. David Mitchell Ivester. “The Constitutional Right to Know,” Hastings Constitutional Law Quarterly, vol. 4 (Winter 1977).

8. Henri Bergson, The Two Sources of Morality and Religion (New York: Henry Holt and Company, 1935).

9. Karl Popper. The Open Society and Its Enemies: The Spell of Plato, Vol I, 4th edition (London : Routledge & Kegan Paul, 1962).

10. Mehmet Polat. “Karl Poppper’s ‘Open’ and ‘Closed’ Society in the Context of the EU,” Human Rights Review vol 2, no. 1 (June 2012).

11. Archong Fung and David Weil. “Chapter 8: Open Government and Open Society”, in Open Government: Transparency, Collaboration, and Participation in Practice, eds. Daniel Lanthrop and Laurel Ruma (Sebastopol : O’Reilly Media Inc, 2010).

12. Rodrigo Sandoval-Almazán. “Open Government and Transparency: Building a Conceptual Framework”, Convergencia Revista de Ciencias Sociales (May 2015).

13. Dirk Heckmann. “Open Government — Retooling Democracy for the 21st Century”, University of Passau (2011).

14. Wallace Parks. “The Open Government Principle: Applying the Right to Know under the Constitution”, George Washington Law Review 26, no. 1 (October 1957).

15. Harlan Yu and David G. Robinson. “The New Ambiguity of ‘Open Government’”, UCLA Law Review Discourse (March 2012).

16. Ivester, David Mitchell (1977). The Constitutional Right to Know. Hastings Constitutional Law Quarterly, vol. 4, p. 109–163.

17. Chapman, Richard and Michael Hunt (1987). Open Government: A Study Of The Prospects Of Open

Government Within The Limitations Of The British Political System. London: Croom Helm.

18. Maja Augustyn and Cosimo Monda. “Transparency and Access to Documents in the EU: Ten Years on from the Adoption of Regulation 1049/2001”, European Institute of Public Administration (2011).

19. Jing Zhang, Gabriel Puron-Cid, and Ramon Gil-Garcia. “Creating Public Value Through Open Government: Perspectives, Experiences and Applications”, Information Polity 20 (2015).

20. Dennis Linders and Susan Copeland Wilson. “What is Open Government? One Year After the Directive”, Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, (June 2011), 262 ; “Open Government Directive”, The White House: President Barack Obama, 08 December 2009. URL: https://obamawhitehouse.archives.gov/open/documents/open-government-directive

21. Joan Bremers and Wouter Deleu. “Towards Faster Implementation and Uptake of Open Government”, European Commission (2016).

22. Don Tapscott. “Foreword”, in Open Government: Transparency, Collaboration, and Participation in Practice, eds. Daniel Lanthrop and Laurel Ruma (Sebastopol: O’Reilly Media Inc, 2010).

23. Teresa M. Harrison, Santiago Guerrero, et al. “Open Government and E-Government: Democratic Challenges From a Public Value Perspective”, University of Albany: Center for Technology in Government (June 2011).

24. Richard Heeks. “Understanding e-Governance for Development,” Institute for Development Policy and Management (2001).

25. Karin Hansson, Kheira Belkacem, and Love Ekenberg. “Open Government and Democracy: A Research Review”, Social Science Computer Review 33, no. 5. (2015).

Уважаемые авторы!

Рады сообщить, что вы можете самостоятельно в режиме реального времени получать информацию о статусе статей, направленных для опубликования в Издательскую группу «Юрист». Для этого необходимо отправить с вашего электронного адреса письмо на autor-rq@lawinfo.ru, в теме письма должна быть указана только фамилия, без имени, отчества и др. Обращаем ваше внимание, что адрес для запроса статуса статей отличается от контактного электронного адреса редакции.

Каждый автор может узнать статус только своих статей, направив запрос со своего электронного адреса.

В случае возникновения проблем с получением информации просим обращаться в редакцию по телефону: 8(495) 953-91-08 или по e-mail: avtor@lawinfo.ru.

Информация как объект гражданского права в контексте смежных правовых категорий

Исманжанов А.А. *

Цель. *Исследование нацелено на определение правового режима информации как объекта гражданского права в сравнении со смежными категориями гражданского права (объект исключительного права, ноу-хау, коммерческая тайна, товар). Рассматриваемые категории объектов права и гражданского оборота могут являться информацией. Однако необходимость информации быть ограниченной от общедоступной информации при требованиях к ее конфиденциальности приобретает ключевое значение. Исследование также включает подходы к проблеме из правовой практики ЕС и Великобритании, с учетом популяризации оборота информации в сети Интернет.* ***Методология:*** *сравнительный анализ, системный подход, моделирование.* ***Выводы.*** *Вопрос признания информации как объекта гражданского права связан с ее признанием в качестве объектов исключительных прав и права собственности, а также в качестве товара. Однако признание информации как объекта обязательственных, нежели вещных, прав, а также отсутствие общего режима информации, остается основой для конструктивной критики по отношению к информации как частноправовой категории.* ***Научная и практическая значимость.*** *Исследование занимается изучением информации как объекта гражданского права и предлагает новые подходы к определению правового режима информации, как частно-правовой категории (предложение об охраноспособности более широкой категории информации по признаку относительной конфиденциальности).*

Ключевые слова: *правовой режим информации, информация как объект гражданского права, ноу-хау, коммерческая тайна, товар, исключительное право, право собственности, обязательственное право.*

Purpose. *The study aimed at determining the legal regime of information as an object of civil law in comparison with related categories of civil law (object of exclusive right, know-how, trade secret, goods). Considered categories of objects of Law and civil turnover may be information. The study also includes approaches to the problem from the legal practice of the EU and the UK, taking into account the popularization of civil information exchange on the Internet.* ***Methodology:*** *comparative analysis, system approach, modeling.* ***Results.*** *The issue of recognition of information as an object of civil Law is associated with its recognition as objects of exclusive rights and property rights and goods.* ***Scientific and practical significance.*** *However, the recognition of information as an object of binding rather than proprietary rights, as well as the absence of a general regime of information, remains the basis for constructive criticism of information as a private law category. The Study develops Work on information as an object of Civil Law and offers new approaches to the definition of the legal regime of information as a private legal category (proposal on the protection of a broader category of information on the basis of relative confidentiality).* **

Keywords: *legal regime of information, information as an object of civil law, know-how, trade secret, goods, exclusive right, property, law of obligations.*

Право на информацию приобретает особое значение для юриспруденции в информационном обществе, со специальным интересом к ее значению и содержанию. Субъективное право на информацию входит в ядро юридического содержания правовых отношений в информационной сфере [1, с. 7]. По словам В.А. Дозорцева, право на получение информации относится к публично-правовым правам, а право на ее распространение имеет гражданско-правовое содержание и представляет собой исключительное право» [2, с. 226]. В связи с этим определение значения информации требует уяснения сущности категории исключительное право. Согласно О.А. Русаковой, «Сущность исключительного права состоит в монополии правообладателя на использование прав на охраняемый объект и возможности запрещать или разрешать другим лицам такое использование» [3, с. 86]. В связи с этим напрашивается вопрос: обладает ли обладатель информации монополией на нее? В случае, когда ее пользователи ограничены обязательством конфиденциальности, то ответ, скорее всего, утвердительный.

Однако категория исключительного права в гражданском законодательстве связывается с результатами интеллектуальной деятельности[1],[2]. В то же время, согласно В.А. Дозорцеву, впечатление, что информация регламентирована традиционными исключительными правами, может быть ошибочным, и право на информацию появляется, когда сведения начинают представлять самостоятельную ценность при ее четком обособлении, что позволяет ей участвовать в экономическом обороте [2, с. 226]. Указанный критерий ограниченности в контексте

[1] Гражданский кодекс Российской Федерации от 18 декабря 2006 г., часть 4 // Собрание законодательства Российской Федерации. 2006. № 52. Ст. 5496.

[2] Гражданский кодекс Республики Узбекистан : принят 21 декабря 1995 г., часть I // Собрание законодательства Республики Узбекистан. 2004. № 25. Ст. 287.

* **Исманжанов Акбар Анваржанович,** старший преподаватель отделения «Коммерческое право» Международного Вестминстерского университета в Ташкенте (МВУТ). E-mail: aismanjanov@wiut.uz
Рецензент: Лопатин Владимир Николаевич, главный редактор, научный руководитель (директор) РНИИИС, эксперт РАН, доктор юридических наук, профессор, заслуженный деятель науки Российской Федерации.

** **Information as a Civil Law Object within the Framework of Related Legal Categories**
Ismanzhanov A.A., Senior Lecturer at the Commercial Law Department of Westminster International University in Tashkent.
Reviewer: Lopatin V.N., Chief Editor, the Scientific Head of the National Research Institute of Intellectual Property (NSRIIP), Expert of the Russian Academy of Sciences, Doctor of Law, Professor, Honored Worker of Science of the Russian Federation.

информации определенно требует быть разграниченным от информации в общественном доступе. Здесь в качестве соответствующего критерию объекта напрашивается коммерческая тайна. Однако конфиденциальная информация, представляющая коммерческую ценность, помимо коммерческой тайны также может быть отделима от общедоступной. Даже при коммерческой передаче информации, при наличии договоров о конфиденциальности, вместе со своевременными действиями правообладателя по изъятию попадающих в общественный доступ копий объекта, ее изоляция от общедоступной информации возможна.

Существует позиция, согласно которой информация может быть введена в гражданский оборот после ее овеществления или объективизации [4]. Однако даже при овеществлении информация отделима от материального носителя, и существует риск того, что третьи лица могут приобрести объект и передавать саму информацию, указывая на то, что защищаемой являлась информация с материальным носителем, нежели сама информация. Для этого важным представляется признание правового режима информации независимо от носителя, в силу объективной независимости ее от материального носителя. По мнению К. Рида, одним из наиболее фундаментальных качеств информации является возможность ее передачи в «чистом состоянии», нежели быть записанной на таких носителях, как книги или диски [5, с. 5].

Одним из отличий информации от объектов авторского права является отсутствие четкого понятия автора, как создателя информации, и замена его обладателем информации. Так, применительно к конфиденциальной информации, являющейся коммерческой тайной, также не существует понятия автора коммерческой тайны. Хотя теоретически возможно, что по отношению к конфиденциальной информации может существовать одновременно автор и обладатель информации.

В связи с научно-техническим прогрессом и рыночными отношениями О. Окюлов свидетельствует о рассмотрении информации как товара и предмета гражданско-правовых сделок [6, с. 41]. По мнению А.Г. Каштаряна, «фактор товарности или нетоварности того или иного явления является определяющим для гражданского права» [7, с. 19]. В соответствии с этим автор конструирует товарность ноу-хау как деловой информации и нетоварность деловой информации, составляющей коммерческую тайну, где требования о конфиденциальности ограничивают ее товарность. Соответственно, по мнению автора, это требует разграничения режима защиты деловой информации и ноу-хау в гражданском законодательстве [8, с. 19].

Однако, на наш взгляд, нет объективной причины выводить из правового режима один из объектов, ноу-хау и деловую информацию при их фактическом гражданском обороте, тогда как оба этих объекта сфокусированы на мерах конфиденциальности, базирующихся на действиях правообладателя. Сфера режима конфиденциальной информации может быть намного шире, а круг информации как объекта гражданского права — еще пространнее. Это возможно в связи с тем, что защита может базироваться не на определенных типах информации, а четко очерченных критериях, построенных на объективных факторах. Одним из таких критериев однозначно является конфиденциальность.

Электронная коммерция существенно расширяет товарность информации. Согласно ст. 3 Закона Республики Узбекистан «Об электронной коммерции», электронная коммерция связывается с предпринимательской деятельностью по продаже товаров, выполнению работ и оказанию услуг с использованием информационных систем[3]. Информационные объекты являются наиболее ранними и в данный момент массовыми объектами электронной торговли. Деятельность множества компаний целиком основана на электронной торговле — Cognizant, Thomson Reuters, Netflix и др. Также традиционные компании утилизируют возможность трансформации объектов в цифровую форму, как, например, Amazon по продаже книг с проектом Kindle для электронных книг.

Применительно к зарубежной правовой практике определения товаров А.А. Тедеев указывает на применение по отношению к информационным продуктам и программному обеспечению термина soft товаров, что связано с возможностью их передачи посредством сети Интернет [8, с. 218]. Это создает преимущества для информации как товара, при способности не только быть выполненным электронным путем как в стадии заключения договора, так и его исполнения. Также категория товар является достаточно широко конструированной в международной правовой практике. В законодательстве Европейского Союза категория товар определяется достаточно широко, с указанием на принцип ее определения. В судебном решении Italian Art (1868) товары должны оцениваться в деньгах и быть объектами коммерческой сделки [9]. Это позволило включить информационные объекты в электронной форме в объект правового регулирования в качестве товаров.

Отмечая, что не всякая информация, даже научно-техническая, может быть объектом интеллектуальной собственности, О. Окюлов указывает на то, что информация не имеет единого правового режима. Автор также представляет суждения по поводу принятия закона о научно-технической информации, правовых основах ее хранения, использования и передачи [6, с. 42]. Это позволяет судить об охране разновидностей информации, нежели общей категории информации. Такой же позиции придерживается информационное законодательство Узбекистана, признавая право собственности на информационные ресурсы и системы [9, с. 452]. Как отмечает Х.Т. Маматов, режим информационных ресурсов предоставляет его собственнику право распоряжаться ими по своему усмотрению: предоставлять в пользование другим лицам, дарить, менять, получать прибыль от использования, устанавливать ограничения по использованию [9, с. 44].

По отношению к признанию права собственности на информацию в научном сообществе имеется заметная критика. Как отмечает А.Г. Каштарян, «Поскольку информация имеет нематериальную сущность, заключающуюся в известной независимости информации от материального носителя, невозможно закрепление права собственности (вещного права) на информацию или на некие информационные ресурсы. Следовательно, информация в гражданском праве может быть объектом только обязательственных, исключительных либо корпоративных правоотношений» [7, с. 7]. Данная позиция не беспочвенна и подтверждается зависимостью права на информацию от наличия конфиденциальности на нее, что выражается в практическом применении по отношению к информации лицензионного договора, нежели договора купли-продажи.

[3] Закон Республики Узбекистан «Об электронной коммерции» : принят 22 мая 2015 г. // Собрание законодательства Республики Узбекистан. 2004. № 20 Ст. 132.

С позиции права собственности, как указывает Д.А. Чиниев, существование срока права собственности несовместимо с ее сущностью, если владелец-несобственник не обладает субъективным правом собственности, в основе его притязаний лежат право залога; право аренды и т.д. [10, с. 9]. Тогда как право на информацию существует на основе лицензионного договора, последний может предусматривать срок пользования информацией, что свидетельствует об отсутствии права собственности на информацию и наличии вместо этого права пользования информацией. Об этом также говорит неприменимость по отношению к информации такого способа защиты права собственности как виндикационный иск, как «вещно-правовой способ защиты права собственности, направленный на восстановление владения вещью, который устанавливает общие последствия незаконной передачи и нахождения вещи во владении третьих лиц» [10, с. 16]. Это связано тем, что в большинстве случаев истребование информации у незаконного владельца не способно прекратить нарушение уже распространенной информации.

Вместе с тем в международной юриспруденции с разнообразием объектов права режим права собственности строго не ограничивается вещами и эволюционирует применительно к требованиям времени. Э. Мюррей указывает на решение суда КНР по реституции виртуальных объектов сетевой игры в пользу правообладателя, которые были незаконно получены хакером на основе права собственности, что говорит, по мнению Э. Мюррея, о начале правового признания виртуальной собственности [8, с. 102]. Причем действие по восстановлению виртуального объекта совершено администратором сетевой игры, т.е. частным посредником в правоотношении между правообладателем, нарушителем и государством. Учитывая восстанавливаемость электронной информации, роль контролера системы, или так называемого «гейткипера», приобретает особое значение. Однако если разглашение информации произошло по вине пользователя, налицо нарушение лицензионного соглашения, которое может повлечь ответственность пользователя. Вместе с тем международная практика ответственности ординарных пользователей информации по поводу информации имеет тенденцию к уменьшению, если только речь не идет о распространении информации в коммерческих целях. В судебном решении по делу International Federation of the Phonographic Industry v. Olsson суд Швеции счел действия подростка по установлению ссылки на незаконную копию произведения не противоречащими праву [12, с. 413].

Пользователи сети Интернет должны быть осмотрительны, так как веб-сайты, имеющие информационные ресурсы в открытом доступе, могут не гарантировать нахождение их в общественном достоянии [13, с. 147]. Однако с увеличением объема информации в сети Интернет и увеличивающейся сетевой историей деятельности людей, становится все труднее определить владельцев информации для получения лицензии на пользование. Обсуждаемое на данный момент в Великобритании законодательство позволит получать неисключительную лицензию у государства на работы, правообладатели которых неизвестны (orphan works). Причем акт будет действовать независимо от того, существует авторское право на указанные работы или нет [14, с. 363]. Применение лицензии по отношению к информации, не являющейся объектом авторского права, свидетельствует в пользу информации как объекта гражданского права, по критерию ее оборотоспособности, или способности быть объектом гражданско-правовой сделки.

По мнению К. Рида, на современном этапе становится возможным производителям информации вводить ее в оборот частями без производства массивов информации для достижения рыночной цены [5, с. 5]. Такая фрагментация наглядна в продуктах Kluwer, которые детально структурированы. Таким образом, вопрос об обороте информационных ресурсов становится не только вопросом оборота информационных продуктов, но также вопросом оборота частей продукта. Такая фрагментация также может быть способом защиты всего продукта, тогда как по отдельности она будет представлять ценность лишь для определенной узкой категории потребителей. Рассматриваемую форму защиты можно назвать некой персонификацией информации, изготовленной по потребностям определенного потребителя, которая будет представлять мало ценности для широкого круга пользователей. Это снижает рыночные запросы на объект как один из ключевых факторов компьютерного пиратства.

Литература

1. Оторова Б.К. Правовое регулирование информационно-правовых отношений в Кыргызской Республике : автореф. дис. … канд. юрид. наук / Б.К. Оторова. Бишкек : КНУ, 2012. 23 с.

2. Дозорцев В.А. Интеллектуальные права: Понятие; Система; Задачи кодификации : сборник статей / В.А. Дозорцев; Исследовательский центр частного права. М. : Статут, 2003. 416 с.

3. Русакова О.А. Договоры на создание результатов интеллектуальной деятельности и распоряжении / О.А. Русакова. М. : Проспект, 2016. 134 с.

4. Колобанов Д.В. Информация как объект гражданского права / Д.В. Колобанов. URL: http://www.yurclub.ru/docs/civil/article112.html

5. Chris Reed, Internet Law (CUP 2004). 374 p.

6. Окюлов О. Правовой статус интеллектуальной собственности : автореф. дис. … докт. юрид. наук / О. Окюлов. Т. : ТГЮИ, 2000. 55 с.

7. Каштарян А.Г. Гражданско-правовой режим коммерческой информации : автореф. дис. … канд. юрид. наук / А.Г. Каштарян. М. : МГУ, 2007. 26 с.

8. Тедеев А.А. Информационное право : учебник / А.А. Тедеев. М. : Изд-во Эксмо, 2005. 464 с.

9. Case 7/68 Commission v Italy (Art Treasures) [1968].

10. Маматов Х.Т. Узбекистон Республикасида фукароларнинг ахборотга булган хукукларини амалга оширишнинг конституциявий-хукукий асослари : дис. … канд. юрид. наук / Х.Т. Маматов. Т. : ТДЮИ, 2009. 164 с.

11. Чиниев Д.А. Гаранитии осуществления права собственности в республике Узбекистан : автореф. дис. … канд. юрид. наук / Д.А. Чиниев. Т. : ТГЮИ, 2010. 26 с.

12. Murray A. Information Technology Law. 2nd edn. / A. Murray. UK : Oxford University Press, 602 p.

13. International Federation of the Phonographic Industry v. Olsson, SSC 2000 B 413-00.

14. CyberLaw: Texts and Cases, 3rd edn. / ed. by Gerald R. Ferrera, Margo E.K. Reder, Robert C. Bird et al. USA : South-Western Cengage Learning, 2011. 568 p.

15. Lloyd I. Information Technology Law. 8th edn UK : Oxford University Press, 2017. 537 p.

References

1. Otorova B.K. Pravovoe regulirovanie informatsionno-pravovy'kh otnosheniy v Ky'rgy'zskoy Respublike : avtoref. dis. … kand. yurid. nauk [Legal Regulation of Information Law Relationships in the Kyrgyz Republic :

author's abstract of thesis of ... Candidate of Legal Sciences] / B.K. Otorova. Bishkek : KNU — Bishkek : Kyrgyz National University, 2012. 23 s.

2. Dozortsev V.A. Intellektualny'e prava: Ponyatie; Sistema; Zadachi kodifikatsii : sbornik statey [Intellectual Rights: The Concept; System; Codification Tasks : collection of articles] / V.A. Dozortsev // Issledovatelskiy tsentr chastnogo prava. Research Center of Private Law. Moskva : Statut — Moscow : Statute, 2003. 416 s.

3. Rusakova O.A. Dogovory' na sozdanie rezultatov intellektualnoy deyatelnosti i rasporyazhenii [Agreements on Creation and Disposal of Intellectual Property] / O.A. Rusakova. Moskva : Prospekt — Moscow : Prospect, 2016. 134 s.

4. Kolobanov D.V. Informatsiya kak obyekt grazhdanskogo prava [Information as a Civil Law Object] / D.V. Kolobanov. URL: http://www.yurclub.ru/docs/civil/article112.html

5. Reed Chris. Internet Law (CUP 2004). 374 s.

6. Okyulov O. Pravovoy status intellektualnoy sobstvennosti : avtoref. dis. ... dok. yurid. nauk [The Legal Status of Intellectual Property : author's abstract of thesis of ... Doctor of Law] / O. Okyulov. Tashkent : TGYUI — Tashkent : Tashkent State Institute of Law, 2000. 55 s.

7. Kashtaryan A.G. Grazhdansko-pravovoy rezhim kommercheskoy informatsii : avtoref. dis. ... kand. yurid. nauk [The Civil Law Regime of Commercial Information : author's abstract of thesis of ... Candidate of Legal Sciences] / A.G. Kashtaryan. Moskva : MGU — Moscow : MSU, 2007. 26 s.

8. Tedeev A.A. Informatsionnoe pravo : uchebnik [Information Law : textbook] / A.A. Tedeev. Moskva : Izdvo Eksmo — Moscow : Eksmo publishing house, 2005. 464 s.

9. Case 7/68 Commission v Italy (Art Treasures) [1968].

10. Mamatov Kh.T. Узбекистон Республикасида фукароларнинг ахборотга булган хукукларини амалга оширишнинг конституциявий-хукукий асослари : dis. ... kand. yurid. nauk [thesis of ... Candidate of Legal Sciences] / Kh.T. Mamatov. Tashkent : TDYUI — Tashkent : Tashkent State Institute of Law, 2009. 164 s.

11. Chiniev D.A. Garantii osuschestvleniya prava sobstvennosti v respublike Uzbekistan : avtoref. dis. ... kand. yurid. nauk [Proprietary Right Exercising Guarantees in the Republic of Uzbekistan : author's abstract of thesis of ... Candidate of Legal Sciences] / D.A. Chiniev. Tashkent : TGYUI — Tashkent : Tashkent State Institute of Law, 2010. 26 s.

12. Murray A. Information Technology Law. 2nd edn. / A. Murray. UK : Oxford University Press, 602 s.

13. International Federation of the Phonographic Industry v. Olsson, SSC 2000 B 413-00.

14. CyberLaw: Texts and Cases, 3rd edn. / ed. by Gerald R. Ferrera, Margo E.K. Reder, Robert C. Bird et al. USA : South-Western Cengage Learning, 2011. 568 s.

15. Lloyd I. Information Technology Law. 8th edn UK : Oxford University Press, 2017. 537 s.

Адвокатская тайна как вид профессиональной тайны: проблемы обеспечения режима конфиденциальности

*Жирнова Н.А.**

Цель. *Статья посвящена исследованию проблем современного состояния правового регулирования общественных отношений, связанных с адвокатской тайной, в Российской Федерации.* ***Методы:*** *формально-юридический, сравнительно-правовой, анализ.* ***Результаты.*** *В статье проанализированы признаки адвокатской тайны как одного из видов информации с ограниченным доступом, а именно ее соотношение с банковской, налоговой тайнами, тайной связи. Высказаны предложения по преодолению существующих проблем правового регулирования в данной сфере. Автор, рассматривая данный вопрос, исходит из необходимости обеспечения абсолютного характера данного вида информации с ограниченным доступом. В статье обосновывается положение о том, что именно такой подход способствует наиболее полной и всесторонней реализации прав и свобод человека и гражданина в современном правовом и демократическом государстве в условиях существования гражданского общества. Особое внимание уделено позиции Конституционного Суда Российской Федерации по данному вопросу, проанализированы его позиции по вопросам соотношения правового режима адвокатской тайны с режимами других видов конфиденциальной информации. Затронута проблема влияния «закона Озерова-Яровой» на обеспечение охраны и защиты адвокатской тайны в Российской Федерации. Автор предлагает на законодательном уровне признать приоритет адвокатской тайны над банковской, налоговой и другими видами тайн, а также однозначно установить ее абсолютный характер.*

Ключевые слова: *информация, информация с ограниченным доступом, конфиденциальная информация, тайна, профессиональная тайна, адвокатская тайна, банковская тайна, тайна связи, налоговая тайна, права человека и гражданина, доступ к информации, гражданское общество, правовое государство.*

Purpose. *The article devoted the problems of the current state of legal regulation of public relations related to attorney-client privilege in the Russian Federation.* ***Methodology:*** *formal legal, comparative legal, analysis.* ***Results.*** *The article analyzes the features of attorney-client privilege as one of the types of information with limited access, namely its relation with banking, tax secrets, secret communication. Suggestions were made to overcome the existing problems of legal regulation in this area. The author proceeds from the need to ensure the absolute nature of this type of information with limited access. The article substantiates the position that this approach contributes to the most complete and comprehensive implementation of human and civil rights and freedoms in the modern legal and democratic state in the conditions of existence of civil society. Particular attention is paid to the position of the constitutional court of the Russian Federation on this issue, analyzed its position on the relation of the legal regime of attorney-client privilege with the regimes of other types of confidential information. The problem of the influence of the "Ozerov-Yarovaya law" on the protection and protection of attorney-client privilege in the Russian Federation is touched upon. The author suggests at the legislative level should recognize the priority of attorney-client privilege over banking, tax and other types of secrets, as well as clearly establish its absolute nature.***

Keywords: *information, restricted information, confidential information, secret, professional secret, attorney-client privilege, bank secret, communication secret, tax secret, human and civil rights, access to information, civil society, legal state.*

Сегодня по-настоящему независимая адвокатура является одним из показателей развитости правового и демократического государства, свидетельством признания и обеспечения им прав и свобод человека и гражданина. Это также один из главнейших атрибутов гражданского общества. Федеральный закон «Об адвокатской деятельности и адвокатуре в Российской Федерации» гласит, что целью адвокатской деятельности в нашей стране является защита прав, свобод и интересов доверителей[1]. Адвокатскую деятельность осуществляют лица, обладающие статусом адвоката, важнейшим аспектом деятельности которых является конфиденциальность, т.е. одной из основных обязанностей адвоката выступает обязанность соблюдения профессиональной тайны, точнее — одного из ее видов, а именно — тайны адвокатской [1, с. 539–543; 2, с. 299–301; 3, с. 546; и др.]. Профессиональная тайна — это информация, ставшая известной лицу или организации исключительно в силу исполнения ими

[1] Федеральный закон от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации (ред. от 17 июля 2017 г.) // Собрание законодательства Российской Федерации. 2002. № 23. Ст. 2102; 2017. № 2017. № 31 (ч. 1). Ст. 4818.

* **Жирнова Наталья Александровна,** доцент кафедры административного и муниципального права ФГБОУ ВО «Саратовская государственная юридическая академия», кандидат юридических наук. E-mail: NatalyaZhirnova79@mail.ru

Рецензент: Морозов Андрей Витальевич, член редколлегии, заведующий кафедрой информационного права, информатики и математики Всероссийского государственного университета юстиции (РПА Минюста России), доктор юридических наук, профессор.

** **The Attorney-Client Privilege as a Type of Professional Secrecy: Issues of Securing the Confidentiality Regime**
Zhirnova N.A., Associate Professor of the Department of Administrative and Municipal Law, of Saratov State Law Academy, Candidate of Legal Sciences.

Reviewer: Morozov A.V., Member of the Editorial Board, Head of the Department of Information Law, Informatics and Mathematics of the All-Russian state University of Justice (RPA of the Ministry of Justice of Russia), Doctor of Law, Professor.

своих профессиональных обязанностей или определенных видов деятельности, не связанных с государственной или муниципальной службой, незаконное получение или распространение которой может повлечь за собой вред правам и законным интересам другого лица [4, с. 35].

Информация может считаться профессиональной тайной, если она отвечает следующим требованиям (критерии охраноспособности):

— доверена или стала известна лицу лишь в силу исполнения им своих профессиональных обязанностей;

— лицо, которому доверена информация, не состоит на государственной или муниципальной службе (в противном случае информация считается служебной тайной);

— запрет на распространение доверенной или ставшей известной информации, которое может нанести ущерб правам и законным интересам доверителя, установлен федеральным законом;

— информация не относится к сведениям, составляющим государственную тайну [1, с. 538].

Адвокатская тайна обладает всеми вышеперечисленными признаками. Кроме того, хотелось бы выделить еще ряд признаков, присущих именно тайне адвокатской. Во-первых, наличие специфического правового статуса у держателя этих сведений (статуса адвоката). Основания, условия и порядок приобретения данного статуса детально регламентированы в законодательстве[2]. Во-вторых, в качестве признака, присущего именно адвокатской тайне, следует выделить цель предоставления адвокату данных сведений. Доверитель это осуществляет в целях получения квалифицированной юридической помощи для защиты своих прав и законных интересов, а также для получения доступа к правосудию. В-третьих, признаком адвокатской тайны следует считать то, что вторая сторона конфиденциальных отношений, возникающих между адвокатом с одной стороны, и его клиентом с другой, именуется по тексту закона «доверитель». То есть здесь налицо специальные наименования субъектов возникающих правоотношений. В-четвертых, признаком адвокатской тайны следует признать ее абсолютный характер. Легальное определение адвокатской тайны содержится в ст. 8 Федерального закона «Об адвокатской деятельности и адвокатуре в Российской Федерации», в соответствии с положениями которой адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю[3]. Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием. Проведение оперативно-розыскных мероприятий и следственных действий в отношении адвоката (в том числе в жилых и служебных помещениях, используемых им для осуществления адвокатской деятельности) допускается только на основании судебного решения.

Проблемы правового регулирования адвокатской тайны всегда были предметом внимания ученых-юристов: и до 1917 г. [5, с. 23–27], и в советский период [6, 7, 8], и в настоящее время.

Такая правовая природа адвокатской тайны основывается, в свою очередь, на нормах Конституции РФ, устанавливающих право любого гражданина на получение квалифицированной юридической помощи. Очевидно, что оказание такой помощи адвокатом не представляется возможным без обеспечения правовой защиты сведений, которые доверитель сообщает защитнику. Данные правовые положения развиты далее и в отраслевом законодательстве[4]. Кроме того, Кодекс профессиональной этики адвоката устанавливает, что «доверия к адвокату не может быть без уверенности в сохранении профессиональной тайны... Адвокат не может быть освобожден от обязанности хранить профессиональную тайну никем, кроме доверителя. Без согласия доверителя адвокат вправе использовать сообщенные ему доверителем сведения в объеме, который адвокат считает разумно необходимым для обоснования своей позиции при рассмотрении гражданского спора между ним и доверителем или для своей защиты по возбужденному против него дисциплинарному производству или уголовному делу»[5]. Однако развитие общественных отношений и прежде всего необходимость усиления правовых мер борьбы с терроризмом, коррупцией и тому подобными деструктивными явлениями социальной жизни диктует необходимость несколько пересмотреть так называемый абсолютный характер адвокатской тайны. В 2015 г. Конституционный Суд РФ указал, что применительно к отношениям подозреваемых, обвиняемых со своими адвокатами (защитниками), вмешательство органов государственной власти во взаимоотношения подозреваемого, обвиняемого с избранным им адвокатом (защитником), в том числе путем доступа к материалам, включающим сведения о характере и содержании этих взаимоотношений, может иметь место в исключительных случаях — при наличии обоснованных подозрений в злоупотреблении правом со стороны адвоката и в злонамеренном его использовании со стороны лица, которому оказывается юридическая помощь [9]. Из всего вышесказанного следует однозначный вывод о том, что говорить о так называемом абсолютном характере [2, с. 301; 10, с. 145–147; 11, с. 28; и др.] адвокатской тайны, к сожалению, уже не приходится.

Таким образом, в настоящее время, по мнению Конституционного Суда РФ, возможны как обыск, выемка, так и иные следственные действия с целью изъятия предметов и документов у адвоката, правда, при условии, что представители органов власти (предварительного следствия) должны обладать достаточными на то основаниями. По мнению ряда исследователей, такое положение свидетельствует о наличии преимуществ у стороны обвинения [12, с. 142–143], с которым представляется возможным согласиться. Во-первых, четко не очерчены пределы действий представителей органов предварительного расследования в отношении адвоката. Во-вторых, отмечается отсутствие у судебных органов разработанного механизма проверки обоснованности доводов следователя. В-третьих, сама нечеткость таких понятий, например, как «злоупотребление правом адвоката», «злонамеренное использование» и т.п.

Несмотря на то, что Конституционный Суд РФ акцентирует внимание на важности судебного контроля при принятии решения о производстве следственных действий в отношении адвокатов, не следует забывать, что при принятии соответствующего решения суд выслушивает лишь доводы одной из сторон (стороны обвинения), а адвокат лишен возможности даже присутствия при этом. Таким образом, следует признать, что вышеуказанное определение Конституционного суда весьма спорно. На это обращает внимание в своем особом мнении судья Конституционного Суда РФ К.В. Арановский, который указывает на следую-

[2] Федеральный закон от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации (ред. от 17 июля 2017 г.) // Собрание законодательства Российской Федерации. 2002. № 23. Ст. 2102; 2017. № 2017. № 31 (ч. 1). Ст. 4818.

[3] Там же.

[4] Уголовный процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (в ред. от 27 декабря 2018 г.) // Собрание законодательства Российской Федерации. 2001. № 52 (ч. 1). Ст. 4921; 2018. № 53. (ч. 1). Ст. 8478.

[5] Кодекс профессиональной этики адвоката : принят Первым Всероссийским съездом адвокатов 31 января 2003 г. Ст. 6. URL: http://fparf.ru/documents/normative_acts/1059/ (дата обращения: 31.12.2018).

щее: «Конституция Российской Федерации ставит под защиту презумпцию невиновности, право не свидетельствовать против себя и своих близких и подобные иммунитеты, включая врачебную, адвокатскую тайну, которая в цивилизованном правопорядке так же бесспорна, как, например, тайна исповеди. Следствию и обвинению, если они согласны оставаться в конституционном правопорядке, полагается терпеть связанные с этим ограничения и запреты, какие бы государственные интересы ни имели в виду следователи, дознаватели и обвинители. Нельзя жертвовать конституционными правами лишь потому, что следствие в чем-то уверено и решило твердо стоять на своем, тем более из досады, когда не хватает законных средств, чтобы доказать подозрения. Конституционные иммунитеты нельзя ставить под угрозу ради начальстволюбия и азарта с претензиями на непогрешимость следствия, где его «полноту, всесторонность» и прочие успехи овеществляют обвинительный результат и похвальная отчетность»[6].

Какими же средствами в данных обстоятельствах адвокат может защитить себя и, в частности, сохранить в тайне сведения, ставшие ему известными в ходе оказания юридической помощи доверителю? Разрешение данной непростой ситуации видится, во-первых, в четкой и однозначной регламентации получения судебного согласия на производство следственных действий в отношении адвокатов и адвокатских образований, с обязательным присутствием данных субъектов (либо их представителей) при этой процедуре. Представляется необходимым принятие специального нормативного акта, в котором были бы детально описаны все этапы данной процедуры. Это позволило бы осуществлять должный контроль за соблюдением адвокатской тайны в нашей стране. Во-вторых, в соответствии с нормами действующего законодательства (глава 16 УПК РФ) адвокат вправе обжаловать рассматриваемые действия органов следствия. В-третьих, не следует забывать и о роли адвокатских сообществ, которые должны реагировать на каждый подобный случай. Данные сообщества должны стать теми субъектами общественных отношений, которые обязаны предавать гласности, четко публично выражать свою позицию по каждой подобной ситуации, акцентируя внимание именно на незыблемости абсолютного характера адвокатской тайны, так как безусловное и последовательное соблюдение данного принципа свидетельствует о высоком уровне развития правового и демократического государства.

Кроме вышесказанного, следует обратить внимание на следующий аспект: существует опасность незаконного разглашения сведений, составляющих адвокатскую тайну, вследствие доступа сотрудников кредитных организаций к сведениям об операциях клиентов-адвокатов. В данном случае имеет место трансформация адвокатской тайны в банковскую, которая, исходя из положений ст. 26 Закона «О банках и банковской деятельности», абсолютным характером не обладает[7]. Так как законодательством не предусмотрены процедуры обмена сведениями, составляющими банковскую тайну, между сотрудниками банков, то обязанность по контролю за соблюдением конфиденциальности этих сведений должна выполняться самими кредитными организациями, т.е. именно они должны создать соответствующую систему, гарантирующую сохранность данных сведений в тайне.

Налоговые органы вправе требовать от адвокатов информацию, необходимую для оценки налоговых последствий сделок с их доверителями. Данный вопрос был предметом рассмотрения в Конституционном суде Российской Федерации, который определил, что «предоставление налогоплательщиками-адвокатами и адвокатскими образованиями по требованию налогового органа документов, необходимых для исчисления и уплаты налогов, сами по себе не могут расцениваться как нарушающие конституционные права заявителей» [13]. Здесь также налицо переход конфиденциальной информации из одного режима в другой, а именно адвокатской тайны в налоговую. В таких случаях налоговые органы должны обеспечить сохранность данных сведений в режиме конфиденциальности. Необходимо в действующем законодательстве установить все этапы процедуры получения данных сведений от налогоплательщиков-адвокатов, а также ответственность за незаконное разглашение или представление этой информации сотрудниками органов ФНС [14, с. 10–14].

Еще одним «щекотливым» моментом в рассматриваемом вопросе является соотношение адвокатской тайны и тайны связи. Тайна связи в самом общем виде определяется как конфиденциальность переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и гарантируется Конституцией Российской Федерации[8]. Ограничение данного права возможно только на основании судебного разрешения. В ходе оперативно-розыскных мероприятий могут, например, прослушиваться все телефонные разговоры подозреваемых, в том числе и с адвокатами по вопросам оказания юридической помощи. Очевидно, что такие доказательства по уголовному делу не могут быть признаны законными и допустимыми. Еще одна грань данной проблемы появилась в связи с принятием так называемого пакета Озерова-Яровой[9]. Нормы данного документа предписывают операторам связи и организаторам распространения информации в сети Интернет хранить информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи в течение трех лет с момента окончания осуществления таких действий, а сами текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи — до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. При этом какого-нибудь механизма защиты сведений, составляющих адвокатскую тайну (которая в данном случае трансформируется в тайну связи), при осуществлении данных мероприятий не предусмотрено.

Таким образом, резюмируя все вышесказанное, следует отметить необходимость всесторонней охраны и защиты сведений, составляющих адвокатскую тайну. Это является одной из главнейших обязанностей правового и демократического государства

---

[6] Постановление Конституционного Суда РФ от 17 декабря 2015 г. № 33-П «По делу о проверке конституционности пункта 7 части второй статьи 29, части четвертой статьи 165 и части первой статьи 182 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой граждан А.В. Баляна, М.С. Дзюбы и других» // Вестник Конституционного Суда РФ. 2016. № 2.

[7] Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» (ред. от 27 декабря 2018 г.) // Собрание законодательства Российской Федерации. 1996. № 6. Ст. 492; 2018. № 53 (ч. 1). Ст. 8440.

[8] Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 5 февраля 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ) // Собрание законодательства Российской Федерации. 2014. № 31. Ст. 4398.

[9] Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства Российской Федерации. 2016. № 28. Ст. 4558.

и развитого гражданского общества. Для достижения данной цели на законодательном уровне следует признать приоритет адвокатской тайны над банковской, налоговой и другими видами тайн, а также однозначно установить ее абсолютный характер.

Литература

1. Лопатин В.Н. Профессиональная тайна / Бачило И.Л., Лопатин В.Н., Федотов М.А. // Информационное право : учебник. Институт государства и права РАН, Академический правовой университет. СПб. : Юридический центр Пресс, 2001. С. 535–549.

2. Пшукова А.М. Профессиональная тайна адвоката как одно из основных требований адвокатской этики / А.М. Пшукова // Бизнес в законе. 2008. № 2. С. 299–301.

3. Шульга Л.В. Специфические черты адвокатской тайны в структуре института профессиональной тайны / Л.В. Шульга // Современные проблемы науки и образования. 2013. № 2. С. 544–548.

4. Лопатин В.Н. Концепция развития законодательства в сфере обеспечения информационной безопасности Российской Федерации / В.Н. Лопатин. М. : Издание Государственной Думы, 1998. 159 с.

5. Барщевский М.Ю. Из истории русской адвокатуры / М.Ю. Барщевский // Вестник Гильдии российских адвокатов. 1998. № 2. С. 23–27.

6. Антимонов Б.С. Адвокат в советском гражданском процессе / Б.С. Антимонов, С.А. Герзон. М. : Госюриздат, 1954. 259 с.

7. Дубков Е.П. Демократические основы организации советской адвокатуры : автореф. дис. ... канд. юрид. наук / Е.П. Дубков. М., 1964.

8. Цыпкин А.Л. Адвокатская тайна / А.Л. Цыпкин. Саратов : Изд-во СГЮИ, 1947. 53 с.

9. Определение Конституционного Суда РФ от 6 июня 2016 г. № 1232-О «Об отказе в принятии к рассмотрению жалобы гражданина Плетнева Дмитрия Александровича на нарушение его конституционных прав частями второй и третьей статьи 56 Уголовно-процессуального кодекса Российской Федерации» // Вестник Конституционного Суда РФ. 2017. № 1.

10. Ботнев В.К. Адвокатская тайна / В.К. Ботнев // Бизнес в законе. 2010. № 4. С. 145–147.

11. Пилипенко Ю.С. Адвокатская тайна: теория и практика реализации : автореф. дисс. ... канд. юрид. наук / Ю.С. Пилипенко. М., 2009.

12. Астафьев Ю.В., Мардасова Л.И. Границы адвокатской тайны / Ю.В. Астафьев, Л.И. Мардасова // Судебная власть и уголовный процесс. 2017. № 1. С. 141–146.

13. Определение Конституционного Суда Российской Федерации по жалобе гражданина Карелина Михаила Юрьевича на нарушение его конституционных прав положениями подпункта 6 пункта 1 статьи 23 и пункта 1 статьи 93 Налогового кодекса Российской Федерации, пункта 1 статьи 8 и пункта 3 статьи 18 Федерального закона «Об адвокатской деятельности и адвокатуре в Российской Федерации» от 17 июня 2008 года № 451-О-П // Вестник Конституционного Суда РФ. 2009. № 1.

14. Андрианов Н. Адвокатская тайна и тайна налоговая / Н. Андрианов // Адвокатские вести. Информационно-аналитический журнал. 2006. № 10 (72). С. 10–14.

References

1. Lopatin V.N. Professionalnaya tayna [Professional Secrecy] / Bachilo I.L., Lopatin V.N., Fedotov M.A. // Informatsionnoe pravo : uchebnik. Institut gosudarstva i prava RAN, Akademicheskiy pravovoy universitet. Sankt-Peterburg : Yuridicheskiy tsentr Press — Information Law : textbook. Institute of State and Law of RAS, Academic Law University. Saint Petersburg : Legal Center Press, 2001. S. 535–549.

2. Pshukova A.M. Professionalnaya tayna advokata kak odno iz osnovny'kh trebovaniy advokatskoy etiki [The Attorney-Client Privilege as One of the Main Requirements of Legal Ethics] / A.M. Pshukova // Biznes v zakone — Business in Law. 2008. № 2. S. 299–301.

3. Shulga L.V. Spetsificheskie cherty' advokatskoy tayny' v strukture instituta professionalnoy tayny' [Peculiar Features of the Attorney-Client Privilege in the Structure of the Professional Secrecy Institution] / L.V. Shulga // Sovremenny'e problemy' nauki i obrazovaniya — Modern Issues of Science and Education. 2013. № 2. S. 544–548.

4. Lopatin V.N. Kontseptsiya razvitiya zakonodatelstva v sfere obespecheniya informatsionnoy bezopasnosti Rossiyskoy Federatsii [The Concept of Development of Laws on Assurance of Information Security of the Russian Federation] / V.N. Lopatin. Moskva : Izdanie Gosudarstvennoy Dumy' — Moscow : Publishing house of the State Duma, 1998. 159 s.

5. Barschevskiy M.Yu. Iz istorii russkoy advokatury' [From the History of the Russian Advocacy] / M.Yu. Barschevskiy // Vestnik Gildii rossiyskikh advokatov — Bulletin of the Guild of Russian Attorneys. 1998. № 2. S. 23–27.

6. Antimonov B.S. Advokat v sovetskom grazhdanskom protsesse [An Attorney in the Soviet Civil Procedure] / B.S. Antimonov, S.A. Gerzon. Moskva : Gosyurizdat — Moscow : State Publishing House of Legal Literature, 1954. 259 s.

7. Dubkov E.P. Demokraticheskie osnovy' organizatsii sovetskoy advokatury' : avtoref. dis. ... kand. yurid. nauk [Democratic Bases of the Establishment of the Soviet Advocacy : author's abstract of thesis of ... Candidate of Legal Sciences] / E.P. Dubkov. Moskva — Moscow, 1964.

8. Tsypkin A.L. Advokatskaya tayna [The Attorney-Client Privilege] / A.L. Tsypkin. Saratov : Izd-vo SGYUI — Saratov : Publishing house of the Saratov State Law Institute, 1947. 53 s.

9. Opredelenie Konstitutsionnogo Suda RF ot 6 iyunya 2016 g. № 1232-O «Ob otkaze v prinyatii k rassmotreniyu zhaloby' grazhdanina Pletneva Dmitriya Aleksandrovicha na narushenie ego konstitutsionny'kh prav chastyami vtoroy i tretey statyi 56 Ugolovno-protsessualnogo kodeksa Rossiyskoy Federatsii» // Vestnik Konstitutsionnogo Suda RF. 2017. № 1.

10. Botnev V.K. Advokatskaya tayna [The Attorney-Client Privilege] / V.K. Botnev // Biznes v zakone — Business in Law. 2010. № 4. S. 145–147.

11. Pilipenko Yu.S. Advokatskaya tayna: teoriya i praktika realizatsii : avtoref. diss. ... kand. yurid. nauk [The Attorney-Client Privilege : The Implementation Theory and Practice : author's abstract of thesis of ... Candidate of Legal Sciences] / Yu.S. Pilipenko. Moskva — Moscow, 2009.

12. Astafyev Yu.V., Mardasova L.I. Granitsy' advokatskoy tayny' [Limits of the Attorney-Client Privilege] / Yu.V. Astafyev, L.I. Mardasova // Sudebnaya vlast i ugolovny'y protsess — The Judiciary and Criminal Procedure. 2017. № 1. S. 141–146.

13. Opredelenie Konstitutsionnogo Suda Rossiyskoy Federatsii po zhalobe grazhdanina Karelina Mikhaila Yuryevicha na narushenie ego konstitutsionny'kh prav polozheniyami podpunkta 6 punkta 1 statyi 23 i punkta 1 statyi 93 Nalogovogo kodeksa Rossiyskoy Federatsii, punkta 1 statyi 8 i punkta 3 statyi 18 Federalnogo zakona «Ob advokatskoy deyatelnosti i advokature v Rossiyskoy Federatsii» ot 17 iyunya 2008 goda № 451-O-P // Vestnik Konstitutsionnogo Suda RF. 2009. № 1.

14. Andrianov N. Advokatskaya tayna i tayna nalogovaya [The Attorney-Client Privilege and Tax Secrecy] / N. Andrianov // Advokatskie vesti. Informatsionno-analiticheskiy zhurnal — Attorney News. Information and analytics journal. 2006. № 10 (72). S. 10–14.

Системы искусственного интеллекта как средство совершения преступления*

*Дремлюга Р.И.***

Цель. *Искусственный интеллект — наиболее многообещающая и обсуждаемая технология в последнее время, тем не менее не так много исследований посвящено преступному его использованию. Так как интеллектуальные системы полностью изменят существующее социальное устройство, предполагается, что это кардинальным образом повлияет на преступный мир. Искусственный интеллект рассматривается как средство совершения преступления, где главный вопрос, который задает автор: увеличит ли использование этой технологии общественную опасность совершаемых преступлений. Отвечая на этот вопрос, в работе автор определяет, чем же является искусственный интеллект, по сути, выделяя его характеристики, значимые с точки зрения права.* ***Методология:*** *диалектика, абстрагирование, анализ, синтез, дедукция, формально-юридический метод.* ***Выводы.*** *Искусственный интеллект относится к компьютерным программам или системам, и поэтому он унаследовал все «чисто компьютерные» признаки. Уникальными свойствами интеллектуальных систем являются: способность имитировать интеллектуальное поведение человека, более высокая самодетерминированность и, зачастую, способность к обучению. В общем автор приходит к выводу, что искусственной интеллект как способ совершения преступления не повышает общественную опасность преступных деяний. Исключением являются преступления, где интеллектуальные системы могут быть использованы в целях более эффективного обмана больших групп лиц с целью завладения их денежными средствами и имуществом.* ***Научная и практическая значимость.*** *Проведенное исследование является первым исследованием, посвященным уголовно-правовой характеристике преступлений, где системы искусственного интеллекта используются как средство совершения преступного деяния. Статья подробно разбирает отличие искусственного интеллекта от других технологий и как его использование влияет на общественную опасность совершенного преступления.*

Ключевые слова: *искусственный интеллект, интеллектуальные системы, киберпреступления, интернет-преступления, право кибербезопасности, средства совершения преступлений, общественная опасность, квалифицирующие признаки.*

Purpose. *Artificial intelligence is the most promising and discussed technology in recent times, however, there are not so many studies are devoted to AI criminal use. Since intelligent systems completely change the existing society, it is assumed that this will radically affect the criminal sphere. In paper Artificial intelligence is considered as a tool of committing a crime, where the main question that the author asks is whether the use of this technology will increase the public danger of committing offences. Answering this question, the article determines what is artificial intelligence, in fact, highlighting its characteristics which are significant from the legal point of view.* ***Methodology:*** *dialectics, abstraction, analysis, synthesis, deduction, formal-legal method.* ***Results.*** *Artificial intelligence refers to computer programs or systems, and it implies that AI inherites all "purely computer" features. Unique properties of intelligent systems are: the ability to imitate human intellectual behavior, higher self-determination and, often, the ability to learn. In general, the author comes to the conclusion that artificial intelligence as a method of committing a crime does not increase the public danger of criminal acts. Exceptions are crimes where intellectual systems can be used to more effectively deceive large groups of people in order to acquire their money and property.* ***Scientific and practical significance.*** *The study is the first study devoted to the criminal law description of crimes, where artificial intelligence systems are used as a tool of committing a criminal act. The article makes clear the difference between artificial intelligence and other technologies and how it affects the public danger of the AI crime.****

Keywords: *artificial intelligence, intellectual systems, cybercrime, Internet crime, cybersecurity, means of committing crimes, public danger, specific aggravating circumstances.*

Год от года информационные технологии меняют социальную действительность до неузнаваемости, человечество все больше и больше зависит от достижений прогресса. До последнего времени компьютер использовался в основном для рутинных задач, пусть даже и в области фундаментальной науки или современной техники. Человек оставлял за собой мыслительные функции, право принимать

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16129.

** **Дремлюга Роман Игоревич,** заместитель директора Юридической школы Дальневосточного федерального университета, кандидат юридических наук. E-mail: dremliuga.ri@dvfu.ru

Рецензент: Дорошков Владимир Васильевич, член редколлегии, член-корреспондент Российской академии образования, главный научный сотрудник РНИИИС, профессор кафедры уголовного права, уголовного процесса и криминалистики МГИМО МИД РФ, доктор юридических наук, профессор, заслуженный юрист Российской Федерации.

The reported study was funded by RFBR according to the research project № 18-29-16129.

***Artificial Intelligence Systems as a Means of Crime Committing**

Dremlyuga R.I., Deputy Director of the Law School of the Far Eastern Federal University, PhD in Law.

Reviewer: Doroshkov V.V., Member of the Editorial Board, Corresponding Member of the Russian Academy of Education, Chief Researcher of the National Research Institute of Intellectual Property (NSRIIP), Professor of the Department of Criminal Law, Criminal Procedure and Criminology of MGIMO of the Russian Ministry of Foreign Affairs, Doctor of Law, Professor, Honored Lawyer of the Russian Federation.

решения или творческую деятельность. С появлением систем искусственного интеллекта перечисленные чисто человеческие сферы деятельности также стали доступны компьютеру.

Искусственный интеллект уже пишет песни [4; 3] и стихи [16], которые трудноотличимы от произведений, созданных человеком. Ему подвластно принятие сложных даже для человека финансовых и бизнес-решений [12]. Компьютерные системы, способные принимать решения самостоятельно, без участия человека, устанавливаются на автомобили и другой транспорт [13]. Кроме очевидных плюсов и помощи в решении многих проблем, стоявших перед человечеством ранее, искусственный интеллект сам создает новые вызовы для современного общества и государства.

Один из самых обсуждаемых вызовов — это полная замена ручного человеческого труда на производстве и во многих других сферах и, как следствие, массовая безработица невиданных за всю историю масштабов [18]. Например, по некоторым прогнозам, беспилотный автотранспорт будет преобладать на дорогах в развитых странах уже через десять лет, что означает миллионы безработных водителей по всему миру.

Искусственный интеллект способен существенно повысить возможности человека, его использующего, и логично, что его все больше будут задействовать в совершении преступлений. Искусственный интеллект, по факту являющийся компьютерной программой, может выступать средством совершения преступлений. Об использовании компьютерной техники и отдельных ее видов как средства совершения преступлений было написано немало работ [1; 5; 6; 9], свидетельствующих о том, что вовлечение определенных компьютерных технологий может или должно в том числе влиять на квалификацию преступных деяний.

К примеру, использование Интернета в качестве средства совершения преступления закреплено как квалифицирующий признак в ряде составов Уголовного кодекса Российской Федерации (ст. 110 ч. 2 п. «д», ст. 110.2 ч. 2, ст. 151.2 ч. 2, ст. 205.2 ч. 2, ст. 228.1 ч. 2 и др.). Это связано с тем, что при совершении общественно опасного деяния посредством Интернета изменяются его качественные характеристики. За счет того, что глобальная сеть обладает уникальными возможностями, изменяются свойства преступления, что не может не отразиться на степени его общественной опасности [2].

Интернет выделяется из других компьютерных средств совершения преступлений и, в криминологическом смысле, образует новый класс преступных деяний, которые требуют особых мер выявления, борьбы и предупреждения. Поэтому по всему миру создаются специальные подразделения по борьбе с интернет-преступностью.

Искусственный интеллект также является уникальной компьютерной технологией, которая имеет существенное влияние на общественные отношения уже сейчас и, судя по всему, коренным образом преобразует все социальное устройство в будущем. Логично предположить, что технология, которая так кардинально повлияет на общество, изменит и преступную сферу, может повысить общественную опасность преступных деяний, совершаемых с ее помощью.

Для того, чтобы разобраться в поставленном вопросе, необходимо понять, чем по сути является интеллектуальная система и какие особенности выделяют данную компьютерную технологию на фоне других. Существует множество определений искусственного интеллекта. Так, некоторые зарубежные исследователи определяют искусственный интеллект как способность машины (технического средства) имитировать интеллектуальное поведение (англ. AI is the capability of a machine to imitate intelligent behavior) [19, с. 23]. Речь о поведении, до этого приписываемом только человеку, от распознавания сложных образов до творчества.

Отдельные российские авторы подчеркивают, что «интеллектуальной называется система, способная целеустремленно, в зависимости от состояния информационных входов, изменять не только параметры функционирования, но и сам способ своего поведения, причем способ поведения зависит не только от текущего состояния информационных входов, но также и от предыдущих состояний системы» [10]. Данное определение выделяет еще одно отличие систем искусственного интеллекта от других компьютерных систем. Интеллектуальные системы более самодетерминированы и менее зависят от входных параметров, чем другие компьютерные системы.

Иногда подобные системы настолько самодетерминированы, что зарубежными исследователями-юристами предлагается признать искусственный интеллект субъектом уголовного права по аналогии с юридическими лицами [14]. Интеллектуальные системы даже способны лишить человека жизни без прямого указания или команды преступника. К примеру, 37-летний японский сотрудник мотоциклетной фабрики был убит роботом, работающим рядом с ним. Робот ошибочно идентифицировал сотрудника как угрозу для своей миссии и подсчитал, что наиболее эффективным способом устранения этой угрозы было использовать свой мощный гидравлический рычаг. Робот бросил удивленного рабочего на операционную машину, убив его мгновенно [15, с. 171–172].

Часть систем искусственного интеллекта способна к обучению, и их поведение и функционирование не подлежит прогнозированию разработчиками, их проектировавшими. Яркой иллюстрацией этого свойства является пример системы «Тай», разработанной для общения в Интернете. Экспериментальная версия данной системы, которая может учиться у своих собеседников, была создана для общения в Твиттере и запущена в открытом доступе 23 марта 2016 г. Менее чем через день после запуска пользователи сети были удивлены некоторым высказываниям искусственного интеллекта. Среди прочих оскорбительных заявлений Тай высказывался в поддержку геноцида и выражал свое согласие с политикой Гитлера [8]. Компания разработчик не предполагала такого поведения системы на этапе разработки и тестирования, а сами высказывания появились как реакция на не связанный с темой нацизма вопрос [20]. Кто в этом случае будет отвечать за пропаганду расизма и нацизма — остается без ответа.

Из приведенного примера видно, что интеллектуальную систему, изначально не предназначенную для совершения противоправных и преступных действий, можно научить такому поведению. В таком случае преступником, скорее всего, будет являться лицо, обучившее искусственный интеллект подобному поведению и использовавшее его как средство для совершения своего преступного деяния. Хотя в указанном выше примере можно предположить, что гипотетические преступники просто общались с системой или друг другом и высказывали свое мнение, не предвидя, что система в дальнейшем будет себя противоправно вести.

Если обобщить вышесказанное, получается, что *система искусственного интеллекта — это компьютерная система или программа, имитирующая один или несколько аспектов интеллектуального поведения, обладающая более высокой по сравнению с другими компьютерными системами или программами степенью самодетерминированности и независимости от воли разработчика или пользователя. Некоторые интеллектуальные системы способны к обучению и самообучению.*

В отличие от, например, пистолета, где дееспособному человеку понятны последствия нажатия на курок, при использовании интеллектуальных систем преступником результат может существенно отличаться от охватываемого умыслом, при этом как в сторону увеличения негативного социального эффекта, так и в сторону уменьшения. С этой точки зрения вряд ли можно говорить о том, что использование искусственного интеллекта как средства повышает общественную опасность преступного деяния и может быть в будущем использовано в уголовном кодексе как отягчающее обстоятельство.

Являясь компьютерной программой или системой, искусственный интеллект может унаследовать свойства других видов компьютерных программ, которые закреплены в уголовном кодексе. Так, программа искусственного интеллекта может быть заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, т.е. быть компьютерным вирусом. В этом случае использование такой программы как средства совершения преступления в корыстных целях будет квалифицировано по ст. 273 ч. 2 УК РФ.

Интеллектуальная компьютерная программа может быть разработана для ее использования в сети Интернет, в этом случае использование такой программы для распространения информации в Интернете будет квалифицирующим признаком для целого ряда статей составов, закрепленных в Уголовном кодексе РФ (ст. 110 ч. 2 п. «д», ст. 110.2 ч. 2, ст. 151.2 ч. 2, ст. 205.2 ч. 2, ст. 228.1 ч. 2, ст. 280 ч. 2 и др.). Предложенные примеры свидетельствует о том, что использование искусственного интеллекта как средства совершения преступлений лишь в частных случаях может рассматриваться как фактор, увеличивающий общественную опасность преступного деяния. Эти варианты использования интеллектуальных систем уже охватываются и выделяются признаками составов преступлений, закрепленных в Уголовном кодексе РФ.

Пожалуй, единственным случаем, не охватывающимся существующим УК РФ, является использование искусственного интеллекта мошенниками, которые активно задействуют Интернет для того, чтобы обмануть доверчивых пользователей по всему миру. Делается это с помощью рассылки электронных сообщений, в которой под тем или иным предлогом просят перевести деньги, например, в целях благотворительности или последующего обогащения. Эффективность такой неадресной рассылки не очень высока, и преступный результат достигается за счет большого охвата потенциальных жертв. В свою очередь искусственный интеллект в последнее время может выявлять те или иные поведенческие и психологические особенности человека по данным, находящимся в открытом доступе (например, социальные сети или странички сотрудников коммерческих организаций).

Вот несколько небольших примеров. Одна из интеллектуальных систем может с высокой степенью достоверности установить сексуальную ориентацию по фотографии человека [21]. Другая способна распознать политические убеждения и уровень интеллекта [22]. Одна из систем может удаленно установить пользователя по колебаниям и движениям компьютерной мыши [11]. Получается, что мошенник с помощью интеллектуальной системы сможет организовать массовую рассылку с целью получения чужих денежных средств обманом, учитывая слабости и предпочтения конкретных людей.

Эта способность систем искусственного интеллекта уже несколько лет используется в легальных целях крупными интернет-компаниями для повышения эффективности интернет-рекламы [17]. Реклама носит адресный характер, и ее содержание и представление для конкретного интернет-пользователя зависит от анализа с помощью интеллектуальных систем его сетевой активности, профилей в социальных сетях и другой открытой информации. Такой подход позволяет в разы увеличить эффективность интернет-рекламы.

Интеллектуальные системы существенно повышают общественную опасность деяний, в которых преступник пытается манипулировать или обманывать потенциальную жертву. К таким преступлениям относятся: мошенничество (ст. 159 УК РФ), вымогательство (ст. 163 УК РФ), причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ) и т.д. Использование искусственного интеллекта позволяет охватить большое количество потенциальных жертв, при этом учитывая их индивидуальные особенности.

К примеру, известный способ мошенничества — так называемые «нигерийские письма», когда преступник рассылает одно и то же сообщение, предлагая под тем или иным предлогом перевести на счет мошенника деньги. «Как правило, мошенники просят у получателя письма помощи во многомиллионных денежных операциях, обещая солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманиваются крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам, а потом и штрафы» [7]. Эффективность рассылки одного и того же или похожих писем достаточно низка: во-первых, о появлении новой «легенды» для отъема денег быстро становится известно общественности, а во-вторых, текст не адаптирован под конкретную культуру, язык и психологические особенности возможной жертвы.

В свою очередь искусственный интеллект в рассылке в социальных сетях сможет понять из профиля слабые места того или иного человека и выдать сообщение мошеннического характера, которое будет более эффективно. Например, для любителя собак будет просить деньги на помощь собакам, а для людей с нетрадиционной ориентацией на помощь себе подобным. При этом интеллектуальная система может даже адаптировать стилистку и обучаться с каждым отказом или удачей.

Подводя итоги, следует сказать, что в целом искусственный интеллект следует рассматривать как средство совершения преступления, не влияющее на общественную опасность деяний. Несмотря на предполагаемый рост вовлечения интеллектуальных систем в совершение преступлений, лишь в некоторых случаях можно говорить о рассмотрении вопроса повышения мер ответственности при вовлечении искусственного интеллекта. Речь идет об описанных в статье видах преступных деяний, где интеллектуальные системы могут быть использованы в целях более эффективного обмана больших групп лиц с целью завладения их денежными средствами и имуществом.

Литература

1. Дремлюга Р.И. Интернет как способ и средство совершения преступления / Р.И. Дремлюга // Информационное право. 2008. № 4. С. 27–31.

2. Дремлюга Р.И. Интернет-преступность : монография / Р.И. Дремлюга; М-во образования и науки Российской Федерации, Федеральное агентство по образованию, Дальневосточный гос. ун-т. Владивосток, 2008. 240 с.

3. Искусственный интеллект научился сочинять музыку, совсем как человек // Информационный портал RUBASE. URL: https://rb.ru/story/ai-composer/

4. Искусственный интеллект Google написал свою первую песню // Сайт Вести.ru. URL:http://hi-tech.vesti.ru/article/626384/

5. Поляков В.В. Средства совершения компьютерных преступлений / В.В. Поляков, С.А. Лапин // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2 (32). С. 162–166.

6. Смолин С. Уголовно-правовая борьба с высокотехнологичными способами и средствами совершения преступлений / С. Смолин // Уголовное право. 2014. № 4. С. 62–68.

7. Фадина Ю.П. Уголовно-правовая характеристика мошенничества в сети интернет / Ю.П. Фадина // Вестник Югорского государственного университета. 2017. № 1–2 (44). С. 117–121.

8. Чат-бот от Microsoft за сутки научился ругаться и стал расистом // Официальный сайт информационного агентства Интерфакс. URL: http://www.interfax.ru/world/500152

9. Чекунов И.Г. Понятие и отличительные особенности киберпреступности / И.Г. Чекунов // Российский следователь. 2014. № 18. С. 53–56 (доступно в СПС «КонсультантПлюс»).

10. Якушев Д.И. Об определении искусственного интеллекта / Д.И. Якушев // Региональная информатика и информационная безопасность : сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 67–69.

11. Are you lying about your identity? Artificial intelligence can tell by how you use your mouse // Официальный сайт журнала Science. URL: http://www.sciencemag.org/news/2017/06/are-you-lying-about-your-identity-artificial-intelligence-can-tell-how-you-use-your

12. Baur A.W. How pricing of business intelligence and analytics SaaS applications can catch up with their technology / A.W. Baur, J. Bühler, M. Bick // Journal of Systems and Information Technology. 2015. 17(3). P. 229–246.

13. Chen X.-M. Driving Rule Acquisition and Decision Algorithm to nmanned Vehicle in Urban Traffic / X.-M. Chen, G. Tian, Y.-S. Miao, J.-W. Gong // Beijing Ligong Daxue Xuebao/Transaction of Beijing Institute of Technology, 2017. 37(5). P. 491–496.

14. Hallevy G. When Robots kill: Artificial intelligence under criminal law (Book) / G. Hallevy. Publisher. Northeastern University, 2013. 244 p.

15. Hallevy G. The criminal liability of artificial intelligence entities — from science fiction to legal social control / G. Hallevy // Akron Intellectual Property Journal. 2010. 4. P. 171–172.

16. I want to talk to you: See the creepy, romantic poetry that came out of a Google AI system // Информационный портал Кварц. URL: https://qz.com/682814/i-want-to-talk-to-you-see-the-creepy-romantic-poetry-that-came-out-of-a-google-ai-system/

17. Jordan M.I. Machine learning: Trends, perspectives, and prospects / M.I. Jordan, T.M. Mitchell // Science. 2015. 349 (6245). P. 255–260.

18. Makridakis S. The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms / S. Makridakis // Futures. 2017. Volume 90, June 2017. P. 46–60.

19. Padhy N.P. Artificial intelligence and intelligent systems 3 / N.P. Padhy. Oxford University Press, 2005.

20. Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter // Официальный сайт издательства Гардиан. URL: https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter?CMP=twt_a-technology_b-gdntech

21. New AI can guess whether you're gay or straight from a photograph // Официальный сайт издательства Гардиан. URL: https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph

22. Face-reading AI will be able to detect your politics and IQ, professor says // Официальный сайт издательства Гардиан. URL: https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski

References

1. Dremlyuga R.I. Internet kak sposob i sredstvo sovershеniya prestupleniya [Internet as a Method and Means of Crime Committing] / R.I. Dremlyuga // Informatsionnoe pravo — Information Law. 2008. № 4. S. 27–31.

2. Dremlyuga R.I. Internet-prestupnost : monografiya [Internet Crime : monograph] / R.I. Dremlyuga; M-vo obrazovaniya i nauki Rossiyskoy Federatsii, Federalnoe agentstvo po obrazovaniyu, Dalnevostochny'y gos. un-t. Vladivostok — Ministry of Education and Science of the Russian Federation, Federal Education Agency, Far Eastern State University. Vladivostok, 2008. 240 s.

3. Iskusstvenny'y intellekt nauchilsya sochinyat muzy'ku, sovsem kak chelovek [Artificial Intelligence Has Learned to Compose Music Just Like Human] // Informatsionny'y portal RUSBASE — RUSBASE information portal. URL: https://rb.ru/story/ai-composer/

4. Iskusstvenny'y intellekt Google napisal svoyu pervuyu pesnyu [Google Artificial Intelligence Has Composed Its First Song] // Sayt Vesti.ru — Vesti.ru website. URL: http://hitech.vesti.ru/article/626384/

5. Polyakov V.V. Sredstva sovershеniya kompyuterny'kh prestupleniy [Means of Cybercrime Committing] / V.V. Polyakov, S.A. Lapin // Doklady' Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki — Speeches of the Tomsk State University of Control Systems and Radioelectronics. 2014. № 2 (32). S. 162–166.

6. Smolin S. Ugolovno-pravovaya borba s vy'sokotekhnologichny'mi sposobami i sredstvami sovershеniya prestupleniy [Criminal Law Combating High-Tech Methods and Means of Crime Committing] / S. Smolin // Ugolovnoe pravo — Criminal Law. 2014. № 4. S. 62–68.

7. Fadina Yu.P. Ugolovno-pravovaya kharakteristika moshennichestva v seti internet [Criminal Law Characteristics of Internet Fraud] / Yu.P. Fadina // Vestnik Yugorskogo gosudarstvennogo universiteta — Bulletin of the Yugra State University. 2017. № 1–2 (44). S. 117–121.

8. Chat-bot ot Microsoft za sutki nauchilsya rugatsya i stal rasistom [Microsoft's Chatbot Has Learned to Curse and Became a Racist in a Day] // Ofitsialny'y sayt informatsionnogo agentstva Interfaks — Official website of the Interfax information agency. URL: http://www.interfax.ru/world/500152

9. Chekunov I.G. Ponyatie i otlichitelny'e osobennosti kiberprestupnosti [The Concept and Distinctive Features of Cybercrime] / I.G. Chekunov // Rossiyskiy sledovatel — Russian Investigator. 2014. № 18. S. 53–56 (available in the ConsultantPlus reference legal system).

10. Yakushev D.I. Ob opredelenii iskusstvennogo intellekta [On the Definition of Artificial Intelligence] / D.I. Yakushev // Regionalnaya informatika i informatsionnaya bezopasnost : sbornik trudov. Sankt-Peterburgskoe obschestvo informatiki, vy'chislitelnoy tekhniki, sistem svyazi i upravleniya — Regional Informatics and Information Security : collection of works. St. Petersburg Society of Informatics, Computer Facilities, Communication and Control Systems. 2016. S. 67–69.

11. Are You Lying about Your Identity? Artificial Intelligence Can Tell by How You Use Your Mouse // Ofitsialny'y sayt zhurnala Science — Official website of the Science journal. URL: http://www.sciencemag.org/news/2017/06/are-you-lying-about-your-identity-artificial-intelligence-can-tell-how-you-use-your

12. Baur A.W. How Pricing of Business Intelligence and Analytics SaaS Applications Can Catch up with Their Technology / A.W. Baur, J. Bühler, M. Bick // Journal of Systems and Information Technology. 2015. 17(3). S. 229–246.

13. Chen X.-M. Driving Rule Acquisition and Decision Algorithm to Unmanned Vehicle in Urban Traffic / X.-M. Chen, G. Tian, Y.-S. Miao, J.-W. Gong // Beijing Ligong Daxue Xuebao / Transaction of Beijing Institute of Technology, 2017. 37(5). S. 491–496.

14. Hallevy G. When Robots Kill: Artificial Intelligence under Criminal Law (Book) / G. Hallevy. Publisher. Northeastern University, 2013. 244 s.

15. Hallevy G. The Criminal Liability of Artificial Intelligence Entities — from Science Fiction to Legal Social Control / G. Hallevy // Akron Intellectual Property Journal. 2010. 4. S. 171–172.

16. I Want to Talk to You: See the Creepy, Romantic Poetry that Came out of a Google AI System // Informatsionny'y portal Kvarts — Quartz information portal. URL: https://qz.com/682814/i-want-to-talk-to-you-see-the-creepy-romantic-poetry-that-came-out-of-a-google-ai-system/

17. Jordan M.I. Machine Learning: Trends, Perspectives, and Prospects / M.I. Jordan, T.M. Mitchell // Science. 2015. 349 (6245). S. 255–260.

18. Makridakis S. The Forthcoming Artificial Intelligence (AI) Revolution: Its Impact on Society and Firms / S. Makridakis // Futures. 2017. Volume 90. June 2017. S. 46–60.

19. Padhy N.P. Artificial Intelligence and Intelligent Systems 3 / N.P. Padhy. Oxford University Press, 2005.

20. Tay, Microsoft's AI Chatbot, Gets a Crash Course in Racism from Twitter // Ofitsialny'y sayt izdatelstva Gardian — Official website of the Guardian publishing house. URL: https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter?CMP=twt_a-technology_b-gdntech

21. New AI Can Guess Whether You're Gay or Straight from a Photograph // Ofitsialny'y sayt izdatelstva Gardian — Official website of the Guardian publishing house. URL: https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph

22. Face-Reading AI Will Be Able to Detect Your Politics and IQ, Professor Says // Ofitsialny'y sayt izdatelstva Gardian — Official website of the Guardian publishing house. URL: https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski

Редакционная политика Объединенной редакции «Издательская группа «Юрист» запрещает:

1. Самоплагиат. В случае, если элементы научной статьи ранее были опубликованы, в том числе и в журналах Издательской группы «Юрист», автор обязан сослаться на ранее опубликованную работу. Дословное копирование собственных работ и их перефразирование не допускается, они могут быть использованы только в качестве основы для новых выводов.
2. Дословное копирование более 10 процентов работы другого лица без указания его авторства, ссылки на источник и использования кавычек.
3. Некорректное перефразирование произведения другого лица, при котором было изменено более одного предложения в рамках одного параграфа или раздела текста, либо предложения были расположены в ином порядке без соответствующей ссылки на источник. Существенное некорректное перефразирование (более 10 процентов оригинальной работы) без ссылки на источник приравнивается к дословному копированию.
4. Использование составных частей произведения другого лица без указания авторства, например, абзаца, рисунка или таблицы без указания ссылки на источник или использования кавычек.

Запреты в информационном праве

*Ковалева Н.Н., Солдаткина О.Л.**

Цель. *Статья посвящена вопросам формирования системы запретов в отрасли информационного права. Наибольшее количество запретов, законодательно обусловленных, возникает при обеспечении информационной безопасности, при осуществлении права на информацию, наоборот, возникает большое количество необоснованных запретов.*

Методология: *правовой анализ, совокупность диалектического, формального и системного методов исследования, а также информационный подход. В соответствии с ним при изучении любого объекта, процесса или явления в природе и обществе в первую очередь выявляются и анализируются наиболее характерные для них информационные аспекты, которые существенным образом определяют их состояние и развитие.*

Результаты. *Рассмотрены особенности формирования запретов в информационном праве, в частности: очень тонкая грань между цензурой и запретом на распространение информации, подрывающей основы государственного устройства, а также есть проблемы технологического свойства, возникающие при блокировке сайтов. Следовательно, решение вопроса построения каркаса из запретительных норм в области правового режима, информации, информационных ресурсов, права на доступ к информации и информационной безопасности должно прорабатываться и систематизироваться в соответствии с положениями действующего законодательства. Результатом является также то, что запреты в рамках информационного права политики должны быть не только задекларированы, но и подкреплены соответствующим терминологическим аппаратом и эффективными мерами по их реализации.*

Ключевые слова: *правовые запреты; информационное право; информационная безопасность, право на информацию, правовой режим, информационный ресурс, информационные технологии, коммуникации.*

Purpose. *The article is devoted to the formation of a system of prohibitions in the field of information law. The greatest number of prohibitions, legally conditioned, occurs in the course of information security, in the exercise of the right to information, on the contrary, there is a large number of unjustified prohibitions.*

Methodology: *legal analysis of the categories of «prohibitions» and «legal regime», a set of dialectical, formal and systemic research methods, as well as information approach. In accordance with it, when studying any object, process or phenomenon in nature and society, the most characteristic information aspects are first identified and analyzed, which essentially determine their state and development.*

Results. *The features of the formation of prohibitions in information law, in particular: a very fine line between censorship and the ban on the dissemination of information that undermines the foundations of the state structure, and there are problems of technological properties that arise when blocking sites. Consequently, the solution of the issue of building a framework of prohibitive rules in the field of legal regime, information, information resources, the right of access to information and information security should be worked out and systematized in accordance with the provisions of the current legislation. The result is also that the prohibitions in the information law of policy should not only be declared, but also supported by appropriate terminology and effective measures for their implementation.***

Keywords: *legal prohibitions; information law; information security, the right to information, legal regime, information resources, information technologies, communications.*

Запреты в праве в целом имеют важное регуляционное значение. «В праве запреты носят исходный, фундаментальный характер и выражают самую суть права и правовой регуляции, состоящую в том, чтобы исчерпывающе, четко и прямо запретить все негативное (общественно вредное в действиях и отношениях людей) и таким путем признать и взять под свою защиту все остальное в качестве положительного, общественно не вредного» [1, с. 92]. На балансе запретов и дозволений, как на каркасе, выстраивается весь массив конкретных юридических норм; именно соотношение запретов и дозволений задает разрешительный или дозволительный характер системе правового регулирования. И здесь следует помнить прежде всего о том, насколько важно соблюдать этот баланс — излишнее увлечение запретами как правовым средством так же опасно, как и недостаточное его применение.

Размечая области применения запретов в информационном праве, необходимо помнить об об-

* **Ковалева Наталия Николаевна,** профессор кафедры административного и муниципального права Саратовской государственной юридической академии, доктор юридических наук, профессор. E-mail: kovaleva.natalia@mail.ru
Солдаткина Оксана Леонидовна, доцент кафедры информатики, доцент кафедры административного и муниципального права Саратовской государственной юридической академии, кандидат юридических наук. E-mail: buzum@mail.ru
Рецензент: Морозов Андрей Витальевич, член редколлегии, заведующий кафедрой информационного права, информатики и математики Всероссийского государственного университета юстиции (РПА Минюста России), доктор юридических наук, профессор.

** **Prohibitions in the information Law**
Kovaleva N.N., Professor of the Department of Administrative and Municipal Law Saratov State Law Academy, Doctor of Law, Professor.
Soldatkina O.L., Associate Professor of the Department of Computer Science, Associate Professor of the Department of Administrative and Municipal Law Saratov State Law Academy, PhD in Law.
Reviewer: Morozov A.V., Member of the Editorial Board, Head of the Department of Information Law, Informatics and Mathematics of the All-Russian State University of Justice (RPA of the Ministry of Justice of Russia), Doctor of Law, Professor.

щих свойствах информации. Здесь необдуманное применение запретов, пожалуй как нигде в других сферах правового регулирования, может привести к прямо противоположному эффекту. Так, метод распространения информации в сети Интернет имеет природу слухов, а значит, прямой запрет ее распространения может привести к усилению интереса к данному виду информации и ее более обширному распространению, нежели было до запрета.

Именно поэтому к запретам в информационном праве и информационно-правовой политике надо относиться крайне осторожно. Попробуем далее наметить области правового регулирования информационной сферы, где использование запретительных норм необходимо.

Говоря об информационном праве, исследователи обычно выделяют несколько отдельных институтов, методы и средства правового регулирования внутри которых сильно отличаются друг от друга. Причем в Концепции информационного кодекса РФ [2] часть институтов объединяется в так называемые суперинституты, которых выделяется три:

1. Правовой режим информации, информационных ресурсов, информационных технологий и коммуникаций.
2. Право на информацию.
3. Информационная безопасность.

В то же время, по оценке профессора В.Н. Лопатина, «кроме обозначения некоторых проблемных вопросов сами проблемы и пути их решения в рамках кодификации по каждому из перечисленных институтов авторами концепции, как правило, не раскрываются, а структура «суперинститутов», описанная в трех разделах концепции, имеет различный набор компонентов. В значительной степени связывая решение вопросов систематизации законодательства в рамках первого «суперинститута» с институтами интеллектуальной собственности, авторы при этом выделяют программы для ЭВМ и программное обеспечение информационных систем как самостоятельные объекты правового регулирования при систематизации информационного законодательства, хотя эти нормы уже кодифицированы в рамках части четвертой ГК РФ. …Включение же вопросов защиты информационной системы и защиты информации и документов в информационной системе от несанкционированных изменений или уничтожения в состав первого «суперинститута» (параграф 5.1. концепции) вместо третьего (глава 7 концепции), наряду с другими противоречиями и явными правовыми несуразицами наводит на печальную мысль, что желание выглядеть оригинальным подменило научность и взвешенность выводов» [3, с. 8].

Рассмотрим далее каждый из этих институтов с точки зрения теории запретов.

Правовой режим информации, информационных ресурсов, информационных технологий и коммуникаций

В науке выделяют льготный и ограничительный правовые режимы [4, с. 56]. Для льготного информационного режима характерно возрастание дозволений, убывание запретов и обязываний, для ограничительного режима — возрастание запретов и связываний, убывание дозволений. Законодательный акт «О принципах регулирования информационных отношений в государствах — участниках Межпарламентской Ассамблеи СНГ» от 23 мая 1993 г., носящий рекомендательный характер, определяет правовой режим информации как нормативно установленные правила, определяющие степень открытости, порядок документирования, доступа, хранения, распространения и защиты информации, а также права на информацию[1]. По мнению Л.К. Терещенко, правовой режим информации — это режим объектов права, который вводится законом и позволяет обеспечить комплексное воздействие регулятивными, охранительными, процессуально-процедурными средствами, представляющими собой особую совокупность дозволительных, запрещающих и обязывающих и гарантирующих соблюдение этого режима норм [5, с. 13].

Из этого можно сделать вывод, что запреты в правовом режиме информации, информационных ресурсов, информационных технологий и коммуникаций обусловлены ограничениями доступа и особенностями технологической обработки цифровой информации.

Право на информацию

Право на информацию закрепляется в Российской Федерации на самом высоком уровне — в Конституции РФ. Прежде всего, конечно, речь идет о ст. 29, имеющей основополагающее значение для всего информационного права. В ч. 1 этой статьи говорится: «Каждому гарантируется свобода мысли и слова», в ч. 4 фиксируются общие юридические условия и пределы свободной информационной деятельности: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется Федеральным законом»; в ч. 5 устанавливается следующее положение: «Гарантируется свобода массовой информации» [6]. Однако уже и на уровне Конституции РФ основные информационные права как бы «обрамляются» запретительными нормами. В ч. 2 ст. 29 содержится запрет пропаганды «социального, расового, национального религиозного или языкового превосходства», а в ч. 5 — запрет цензуры.

Свобода поиска информации означает возможность обращения к кому-либо (организации, должностному лицу и др.) с просьбой о предоставлении определенной информации, с волеизъявлением лиц, направленным на ее получение законным способом. Свобода получения информации означает вероятность стать ее обладателем на законных основаниях. Свобода передачи и распространения информации указывает на возможность доведения информации до сведения неограниченного круга лиц.

Свободный поиск и распространение сведений о деятельности государственных и муниципальных органов любым законным способом также содержится и в федеральном законодательстве.

Например, средства массовой информации обязаны предоставлять гражданам оперативные достоверные сведения о деятельности органов власти (под органами власти понимается совокупность государственных и муниципальных органов) и их должностных лиц[2]. При этом редакции средства массовой информации, зарегистрированного надлежащим образом, гарантируется возможность запросить подобную информацию. Гарантом этого

---

[1] Рекомендательный законодательный акт «О принципах регулирования информационных отношений в государствах — участников Межпарламентской Ассамблеи СНГ» : принят постановлением Межпарламентской Ассамблеи государств — участников СНГ от 23 мая 1993 г. URL: //htpp: www.medialaw.ru/exussrlaw/index.htm (дата обращения: 23.11.2018).

[2] Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» // Ведомости СНД РФ и ВС РФ. 1992. № 7. Ст. 300; СЗ РФ. 1995. № 30. Ст. 2870; 2011. № 30, ч. 1. Ст. 4600.

права выступает обязанность руководителей государственных и муниципальных органов, их заместителей, работников пресс-служб либо других уполномоченных лиц предоставить данные сведения, за исключением информации ограниченного доступа.

Кроме того, с 1 января 2010 г. вступила в законную силу норма (ст. 38 Закона РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»), отсылающая к специальному федеральному законодательству, регламентирующему проблемы доступа к информации о деятельности государственных и муниципальных органов и судов, если предоставление государственными и муниципальными органами информации о своей деятельности по запросам редакций не урегулированы нормативными актами о средствах массовой информации.

Действующее законодательство Российской Федерации также предусматривает возможность обращения граждан лично или коллективно в государственные и муниципальные органы с заявлениями, жалобами, обращениями. Однако Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[3] содержит легальное определение права на доступ к информации, а также имеет место противоречие при определении этого понятия в ст. 8 и в п. 6 ст. 2.

Очевидно, что информация о деятельности органов власти регулярно используется гражданами в повседневной жизни. Однако есть граждане, чья профессиональная деятельность так или иначе связана с использованием информации о деятельности органов власти. Согласно исследованию Института развития свободы информации, они составляют 34% от общего числа опрошенных [7]. Это означает, что около трети взрослого населения Российской Федерации с той или иной степенью регулярности специально обращаются к информации о деятельности органов власти и могут быть отнесены к категории «профессиональных пользователей права на доступ к информации». Чем выше уровень образования, тем более вероятно вхождение индивидуума в эту группу. Следует подчеркнуть, что должностные лица государственных и муниципальных органов являются активными пользователями информации о деятельности органов власти, т.е. они не только производят, хранят, распространяют информацию о деятельности органов власти, но и потребляют ее.

Результаты проведенных исследований показали, что реализация и защита права на доступ к информации о деятельности государственных и муниципальных органов власти в нашей стране сопровождается немалыми проблемами.

Основная задача процесса внедрения информационных технологий в работу государственных и муниципальных органов состоит в повышении эффективности их деятельности. Ее решение позволит гражданам беспрепятственно реализовывать право на доступ к информации и оказывать им государственные и муниципальные информационные услуги. Кроме того, технологии электронного государства предоставляют гражданам возможности интерактивного участия в работе демократических институтов, в принятии управленческих решений [8, с. 177–180].

Информационная безопасность

Говоря об информационной безопасности сегодня, мы имеем в виду не только защиту информации или критических объектов информационной инфраструктуры, но и различного рода негативные воздействия информации на человека [9, с. 237–248]. Такое разделение присутствует и в последующих двух Доктринах информационной безопасности (далее — Доктрина). Собственно, именно Доктрина является основным стратегическим документом в данной сфере, задающим каркас для всего сегмента правовой системы (в основном в главе IV «Стратегические цели и основные направления обеспечения информационной безопасности»), поэтому анализ необходимых в данной области запретов начнем именно с ее положений.

Согласно Доктрине, выделяются несколько различных областей, где стратегические цели обеспечения информационной безопасности ставятся отдельно, а именно: оборона страны; государственная и общественная безопасность; экономическая сфера; наука, технологии и образование; стратегическая стабильность и равноправное стратегическое партнерство.

Все перечисленные области и поставленные соответствующие им цели указывают на свой сегмент системы правового регулирования, где уже существует какой-то набор норм права различного вида, в том числе и запретительных. Рассмотрим далее для примера одну из областей, а именно государственную и общественную безопасность.

Пункт 23 Доктрины намечает основные направления обеспечения информационной безопасности в области государственной и общественной безопасности, каждое из которых также достаточно объемно с точки зрения выбранной темы, поэтому далее рассмотрим подробнее в качестве примера только один из них.

Обратим внимание на п. а Доктрины: противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации. Более того, в отечественном законодательстве этот вопрос решается путем установления прямого запрета сразу в нескольких законодательных актах:

1. В ч. 2 ст. 29 Конституции РФ установлен запрет пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду, а также запрет пропаганды социального, расового, национального, религиозного или языкового превосходства.

2. Уголовный кодекс РФ содержит достаточно составов, прямо либо косвенно связанных с запретом таких пропагандистских действий (ст. 205.2, 205.4, 212.1, 354 УК РФ).

3. Запрет на пропаганду недопустимой информации конкретизирует и ряд федеральных законов, в том числе Федеральный закон «Об информации, информационных технологиях и о защите информации» в п. 6 ст. 10 (запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность).

При этом, несмотря на внушительный список нормативных правовых актов, содержащих запрет пропаганды, в этой области существует и ряд проблем, снижающих эффективность данных запретительных норм [10].

Например, Е.Н. Тогузаева обращает внимание на «размытость» понятия «пропаганды» в силу отсут-

[3] СЗ РФ. 2006. № 31, ч. 1. Ст. 3448; 2011. № 30, ч. 1. Ст. 4600.

ствия его формального закрепления в российском законодательстве. Не сложилось единого понимания относительно содержания указанного термина и в научной литературе. Отечественное законодательство достаточно вольно использует термины, не устанавливая их сходства и различия. Касается это и таких понятий как пропаганда, призыв, публичное оправдание, побуждение к совершению противоправных действий. Все это ведет к расширенному толкованию закона, что недопустимо в целях обеспечения единообразия правоприменительной практики [11].

Действительно, даже в законодательстве пропаганда определяется и как процесс распространения сведений (модельный закон о защите детей от информации, причиняющей вред их здоровью и развитию, принят в г. Санкт-Петербурге 3 декабря 2009 г. Постановлением 33-15 на 33-м пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ), и как целенаправленная деятельность, осуществляемая субъектами пропаганды по распространению знаний (приказ МВД РФ от 2 декабря 2003 г. № 930 «Об организации работы Государственной инспекции безопасности дорожного движения Министерства внутренних дел Российской Федерации по пропаганде безопасности дорожного движения»).

Словари и энциклопедии определяют термин «пропаганда» тоже несколько по-разному. С точки зрения закрепления значения этого термина в нормах права, на наш взгляд, интерес представляет дефиниция, данная в новой философской энциклопедии, где пропаганда определяется как распространение и внушение взглядов, идей, мнений с целью позитивно или негативно настроить аудиторию (любого состава — от нескольких человек до масс и даже общества в целом) и стимулировать ее реакции в желательном направлении [12]. Из данного определения сразу следует наличие позитивной и негативной пропаганды. Под запрет должна попадать не вся пропаганда, а только негативная ее часть.

И здесь мы сталкиваемся с еще одной проблемой в данной области — необходимостью субъективной оценки при отнесении информации к негативному ее виду. Грань между цензурой и запретом на распространение информации, подрывающей основы государственного устройства, достаточно тонкая. Между тем Конституция РФ устанавливает прямой запрет цензуры, а демократическое общество в целом подразумевает наличие оппозиции к действующей власти. Поэтому необходимо выработать четкие критерии, по которым информация может быть признана пропагандирующей экстремизм, ксенофобию, подрывающей суверенитет, стабильность, насильственное изменения конституционного строя, нарушение территориальной целостности Российской Федерации.

Вызывают вопросы и меры технического обеспечения реализации данного запрета. Так, одним из самых простых и очевидных способов прекратить правонарушение в сети Интернет является так называемая блокировка [13], используемая традиционно в большинстве стран мира. В том числе и в России.

Статья 9 Федерального закона «Об информации, информационных технологиях и о защите информации» устанавливает возможность ограничения доступа к информации федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. В целях ограничения доступа к сайтам, содержащим информацию, распространение которой в Российской Федерации запрещено, создана единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено» (п. 1 ст. 15). Основанием для включения в реестр сведений, указанных в ч. 2 п. 1 ст. 15 Федерального закона «Об информации, информационных технологиях и о защите информации», является в том числе вступившее в законную силу решение суда о признании информации, распространяемой посредством сети Интернет, информацией, распространение которой в Российской Федерации запрещено.

Однако такой способ реализации запрета негативной пропаганды представляется далеко не самым эффективным. Дело в том, что в большинстве стран процедура блокировки является более или менее произвольной, непрозрачной, не позволяющей гражданам знать, какой контент и по какой причине закрыт [14, с. 194]; несовершенны и имеющиеся сегодня технологии блокирования, в большинстве случаев либо недостаточные, либо избыточные, к тому же в законодательстве они в явном виде не установлены.

Таким образом, мы видим, что каркас из запретительных норм в области правового режима, информации, информационных ресурсов, права на доступ к информации и информационной безопасности должен прорабатываться и систематизироваться в соответствии с положениями действующего законодательства. Кроме того, запреты должны быть не только задекларированы, но и обязательно подкреплены соответствующим терминологическим аппаратом и эффективными мерами по реализации установленных запретов.

Литература

1. Нерсесян В.С. Философия права : учебник для вузов / В.С. Нерсесян. М., 1997. 664 с.

2. Концепция информационного кодекса Российской Федерации / под ред. И.Л. Бачило. М., 2014. 192 с.

3. Лопатин В.Н. Проблемы и перспективы кодификации законодательства в сфере информационного права и интеллектуальной собственности / В.Н.Лопатин//Информационноеправо.2014.№3(39). С. 4–10.

4. Городов О.А. Информационное право : учебник / О.А. Городов. М., 2009. 242 с.

5. Терещенко Л.К. Правовой режим информации : автореф. дис. ... докт. юрид. наук / Л.К. Терещенко. М., 2011. 54 с.

6. Куликова С.А. Перспективы совершенствования правового регулирования СМИ и других источников массовой информации / С.А. Куликова // Информационное право. 2017. № 3. С. 26–33.

7. Отчет по результатам репрезентативного общероссийского опроса на сайте Института Развития Свободы Информации. URL: www.svobodainfo.org (дата обращения: 20.07.2018).

8. Ковалева Н.Н. Административно правовое регулирование использования информационных технологий : дис. ... докт. юрид. наук / Н.Н. Ковалева. Саратов, 2014.

9. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство : монография / В.Н. Лопатин. СПб., 2000. 428 с.

10. Исмаилов С.А. Обеспечение защиты от воздействия информации, разжигающей национальную ненависть и вражду (информационно-правовой

аспект) : дис. ... канд. юрид. наук / С.А. Исмаилов. М. : ИГП РАН, 2003. 169 с.

11. Тогузаева Е.Н. Технико-юридические приемы закрепления запрета деструктивных видов пропаганды в конституционных актах современных государств / Е.Н. Тогузаева. URL: http://www.justicemaker.ru/view-article.php?id=10&art=6018 (дата обращения: 05.03.2018).

12. Новая философская энциклопедия : в 4 т. / под ред. В.С. Степина. М. : Мысль, 2001.

13. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации : утв. Генпрокуратурой России // СПС «КонсультантПлюс».

14. Информационные правоотношения : теоретические аспекты / под ред. И.М. Рассолова. М. : Проспект, 2017. 204 с.

References

1. Nersesyan V.S. Filosofiya prava : uchebnik dlya vuzov [Philosophy of Law : textbook for higher educational institutions] / V.S. Nersesyan. Moskva — Moscow, 1997. 664 s.

2. Kontseptsiya informatsionnogo kodeksa Rossiyskoy Federatsii [The Concept of the Information Code of the Russian Federation] / pod red. I.L. Bachilo. Moskva — Moscow, 2014. 192 s.

3. Lopatin V.N. Problemy i perspektivy kodifikatsii zakonodatelstva v sfere informatsionnogo prava i intellektualnoy sobstvennosti [Issues and Prospects of Codification of Laws in the Sphere of Information Law and Intellectual Property] / V.N. Lopatin // Informatsionnoe pravo — Information Law. 2014. № 3 (39). S. 4–10.

4. Gorodov O.A. Informatsionnoe pravo : uchebnik [Information Law : textbook] / O.A. Gorodov. Moskva — Moscow, 2009. 242 s.

5. Tereschenko L.K. Pravovoy rezhim informatsii : avtoref. dis. ... dokt. yurid. nauk [The Legal Regime of Information : author's abstract of thesis of ... Doctor of Law] / L.K. Tereschenko. Moskva — Moscow, 2011. 54 s.

6. Kulikova S.A. Perspektivy› sovershenstvovaniya pravovogo regulirovaniya SMI i drugikh istochnikov massovoy informatsii [Prospects of Improvement of Legal Regulation of Mass Media and Other Mass Information Sources] / S.A. Kulikova // Informatsionnoe pravo — Information Law. 2017. № 3. S. 26–33.

7. Otchet po rezultatam reprezentativnogo obscherossiyskogo oprosa na sayte Instituta Razvitiya Svobody› Informatsii [A Report on the Results of a Representative All-Russian Survey on the Website of the Information Freedom Development Institute]. URL: www.svobodainfo.org (data of access: July 20, 2018).

8. Kovaleva N.N. Administrativno pravovoe regulirovanie ispolzovaniya informatsionny›kh tekhnologiy : dis. ... dokt. yurid. nauk [Administrative Law Regulation of Information Technology Use : thesis of ... Doctor of Law] / N.N. Kovaleva. Saratov — Saratov, 2014.

9. Lopatin V.N. Informatsionnaya bezopasnost Rossii: Chelovek. Obschestvo. Gosudarstvo : monografiya [Information Security of Russia: Man. Society. State : monograph] / V.N. Lopatin. Sankt-Peterburg — Saint Petersburg, 2000. 428 s.

10. Ismailov S.A. Obespechenie zaschity ot vozdeystviya informatsii, razzhigayuschey natsionalnuyu nenavist i vrazhdu (informatsionno-pravovoy aspekt) : dis. ... kand. yurid. nauk [Assurance Protection against the Influence of Information Fostering National Hatred and Hostility (an Information Law Aspect) : thesis of ... Candidate of Legal Sciences] / S.A. Ismailov. Moskva : IGP RAN — Moscow : ISL RAS, 2003. 169 s.

11. Toguzaeva E.N. Tekhniko-yuridicheskie priemy zakrepleniya zapreta destruktivnykh vidov propagandy v konstitutsionnykh aktakh sovremennykh gosudarstv [Technical Legal Methods of Consolidation of Prohibition against Destructive Types of Propaganda in Constitutional Acts of Modern States] / E.N. Toguzaeva. URL: http://www.justicemaker.ru/view-article.php?id=10&art=6018 (date of access: March 5, 2018).

12. Novaya filosofskaya entsiklopediya : v 4 t. [New Encyclopedia of Philosophy : in 4 vol.] / pod red. V.S. Stepina. Moskva : My›sl — Moscow : Thought, 2001.

13. Metodicheskie rekomendatsii po osuschestvleniyu prokurorskogo nadzora za ispolneniem zakonov pri rassledovanii prestupleniy v sfere kompyuternoy informatsii : utv. Genprokuraturoy Rossii // SPS «KonsultantPlyus».

14. Informatsionnye pravootnosheniya : teoreticheskie aspekty› [Information Legal Relationships : Theoretical Aspects] / pod red. I.M. Rassolova. Moskva : Prospekt — Moscow : Prospect, 2017. 204 s.

Эволюция права на информацию в России и в мире

*Пашнина Т.В.**

Цель. *В статье дается анализ права на информацию как института права. Изучения генезиса, трансформации и современных тенденций развития права на информацию важно для понимания сущности и направлений развития данного права, приобретшего особую значимость в условиях цифровой среды.*

Методология: *диалектика, анализ, исторический, формально-юридический, сравнительно-правовой.* ***Результаты.*** *Рассмотрен генезис права на информацию в странах Европы в XVII–XIX веках. Констатировано, что впервые термин «информация» в рамках института прав человека был использован во Всеобщей декларации прав человека 1948 г. Приводится перечень иных важнейших международных правовых актов, повлиявших на становление права на информацию. Утверждается, что в данных документах указанное право рассматривалось в качестве элемента свободы слова. Констатировано, что в качестве самостоятельного права право на информацию появилось в 90-х годах прошлого века и понималось как право на доступ к информации. На основании анализа иностранных публикаций утверждается, что современными зарубежными исследователями право на информацию трактуется не как единое право, а как система информационных прав.*

Рассмотрена история и основные тенденции развития права на информацию в современной России. Констатировано, что элементы права на информацию в нашей стране появились в конце XVIII века и почти весь дореволюционный период оно развивалось под давлением цензурного законодательства. Доказано, что отдельные черты права на информацию наблюдаются в конституциях советского периода, однако в качестве самостоятельного право на информацию было закреплено в Декларации прав и свобод человека и гражданина 1991 г. и Конституции Российской Федерации 1993 г. Приведен перечень основных федеральных законов, регулирующих право на информацию в нашей стране. Особое внимание уделено документам стратегического характера, повлиявшим на современное состояние рассмотренного права в Российской Федерации. Констатировано, что российское право на информацию также рассматривается учеными в качестве системы информационных прав. Кроме того, отсутствует единство мнения по поводу понимания сущности права на информацию и определения его места в системе иных прав и свобод. Исследование показало, что формирование права на информацию во всем мире продолжается до сих пор.

Ключевые слова: *информация, свобода мысли и слова, свобода информации, право на информацию, право на доступ к информации, цензура, история конституционного развития, система информационных прав, право на Интернет.*

Purpose. *This paper analyzes the right to information from its inception to the present day. The importance of studying the Genesis, transformation and current trends in the development of the right to information is important for understanding the essence and directions of development of this right, which has acquired special importance in the digital environment.*

Methodology: *dialectics, analysis, historical, formal legal, comparative legal.* ***Results.*** *The Genesis of the right to information in Europe in 17–19 centuries is considered. It is stated that for the first time the term «information» within the framework of the Institute of human rights was used in the universal Declaration of human rights in 1948. A list of other important international legal acts that influenced the formation of the right to information is Given. It is argued that in these documents this right was considered as an element of freedom of speech. It is stated that as an independent right, the right to information appeared in the 90s of the last century and was understood as the right to access to information. Based on the analysis of foreign publications it is stated that modern foreign researchers interpret the right to information not as a single right, but as a system of information rights.*

*The history and main trends of development of the right to information in modern Russia are considered. It is stated that the elements of the right to information in our country appeared in the late 18th century and almost the entire pre-revolutionary period it developed under the pressure of censorship legislation. It is proved that some features of the right to information are observed in the constitutions of the Soviet period, but as an independent right to information was enshrined in the Declaration of human and civil rights and freedoms in 1991 and the Constitution of the Russian Federation in 1993. The list of the main Federal laws regulating the right to information in our country is given. Particular attention is paid to the strategic documents that influenced the current state of the law in the Russian Federation. It is stated that the Russian right to information is also considered by scientists as a system of information rights. In addition, there is a lack of consensus on understanding the essence of the right to information and determining its place in the system of other rights and freedoms. The study showed that the formation of the right to information around the world is still ongoing.***

* **Пашнина Татьяна Викторовна,** преподаватель кафедры государственно-правовых дисциплин Уральского филиала Российского государственного университета правосудия (г. Челябинск), аспирант кафедры теории и истории государства и права, конституционного и административного права Южно-Уральского государственного университета (национального исследовательского университета). E-mail: pashninatv_chel@mail.ru

Рецензент: Минбалеев Алексей Владимирович, ответственный секретарь, ведущий научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права Российской академии наук; ведущий научный сотрудник научно-исследовательского отдела законодательства и сравнительного права интеллектуальной собственности РНИИИС; профессор кафедры теории государства и права, конституционного и административного права Южно-Уральского государственного университета (национального исследовательского университета), доктор юридических наук, доцент.

** **Evolution of the Right to Information in Russia and in the World**

Keywords: *information, freedom of thought and speech, freedom of information, the right to information, the right to access information, censorship, the history of constitutional development, the system of information rights, the right to the Internet.*

Современная цивилизация немыслима без прав человека, а одним из важнейших прав человека XXI века является право на информацию. Данное право имеет свою собственную историю, «вписанную» в историю института прав и свобод человека.

Н.О. Травников отмечает, что в предшествующий появлению государства период истории человеческого общества и в первые моменты формирования государственной власти потребности в специальном регулировании информационных процессов не возникало. После появления института государства был запущен процесс отграничения, сокрытия наиболее важной государственной и религиозной информации. Специальные законы, направленные на защиту интересов государства от утечки секретов, появились уже в Древнем Риме. В Великобритании первый закон о государственной тайне был издан в 1352 г.

Борьба личности против тирании абсолютистского государства привела в XVII–XIX веках к признанию возможности свободно выражать свое мнение, в том числе посредством печати. Отправной точкой законодательного закрепления свободы слова стал английский Билль о правах 1689 г. [1, с. 43–47].

Н.Б. Баранова утверждает, что самым первым европейским законом о праве на информацию считается Акт о свободе печати, принятый в 1766 г. в Швеции. Среди «пионеров» нормативного регулирования информационных прав человека исследователи называют французскую Декларацию прав человека и гражданина 1789 г., Конституцию Бельгии 1831 г., Конституцию Великого Герцогства Люксембург 1868 г., Закон о форме правления в Финляндии 1919 г. [2, с. 27–41].

Термин «информация» в контексте основных прав и свобод человека и гражданина впервые был употреблен во Всеобщей декларации прав человека 1948 г.[1], в ст. 19 провозгласившей правомочие каждого свободно выражать свое мнение. Как констатирует П.У. Кузнецов, именно благодаря данному документу появилось современное понимание «информационной свободы», ставшей синонимом термина «право на информацию» [3, с. 14]. Вскоре аналогичное положение было закреплено в Европейской конвенции о защите прав человека и основных свобод 1950 г.[2], затем — в Международном пакте о гражданских и политических правах 1966 г.[3] Однако, по справедливому утверждению С. Шевердяева, право на информацию в этих документах не является самостоятельным правом, оно рассматривается в качестве части свобод мысли и слова [4].

И.Н. Забара констатирует тот факт, что формирование концепции права на информацию как самостоятельного права на общемировом уровне началось с 90-х годов XX века. Именно с середины 90-х годов начинают говорить о праве на информацию как о гарантированном доступе к информации (или «праве на доступ к информации») [5, с. 3–6].

Данную точку зрения поддерживают и зарубежные исследователи. Как отмечает Кэтлин Дженссен, с 1990-х годов многие страны приняли законы о праве на информацию. В настоящее время около 90 государств имеют законодательство о свободе информации, а еще 50 разрабатывают такие правовые акты [6].

В современных зарубежных исследованиях, касающихся права на информацию в Европе и США, речь идет не о едином праве на информацию, а о системе информационных прав. Например, американский исследователь Черил Энн Бишоп выделяет четыре вида информационных прав: концепцию свободы выражения, концепцию личной информации, концепцию права на здоровую окружающую среду и концепцию права на правду [7, с. 206–207].

Проводятся также исследования о соотношении права на информацию (движение «Right to information», RTI) и движения открытых правительственных данных (движение «Open Government Date», OGD) [6].

При всех неоспоримых плюсах движения открытых правительственных данных зарубежные исследователи обращают внимание на ту опасность, которую оно может представлять для собственно права на информацию. Это связано с подменой качественной (интеллектуальной) оставляющей чисто количественной (технической) стороной, при которой преимущества получает «цифровая элита», а обычные граждане, не владеющие необходимыми навыками и знаниями, не могут извлечь из огромного массива предоставляемых данных необходимые им сведения, следовательно, не получают полный доступ к необходимой им информации [6].

В нашей стране право на информацию имеет не менее богатую и драматичную историю. По мнению исследователей, в России элементы данного права появились при Екатерине II во второй половине XVIII века [8, с. 39].

М.А. Кудрявцев отмечает, что в правление Екатерины II был издан императорский Указ от 15 января 1783 г. «О вольных типографиях», дающий право открывать типографии всем желающим. Дарованная просвещенной императрицей информационная свобода имела недолгую историю, завершившись введением жесткой духовной цензуры, нашедшей законодательное закрепление в Указе 1878 г. «О запрещении в продажу всех книг, до святости касающихся» и Указе 1796 г. «Об ограничении свободы книгопечатания», отменившем Указ «О вольных типографиях». Исследователь отмечает, что новый указ, аналогичный Указу «О вольных типографиях», появился в нашей стране лишь в 1802 г., и вплоть до 1905 г. свобода печати регламентировалась цензурным законодательством.

Элементы законодательного закрепления свободы слова появились в п. 1 Манифеста об усовер-

[1] United nations universal declaration of human rights, 1948. URL: http://www.un.org/en/universal-declaration-human-rights/index.html

[2] European convention on human rights, 1950. URL: http://www.echr.coe.int/Documents/Convention_eng.pdf

[3] International Covenant on Civil and Political Rights, 1966. URL: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

Pashnina T.V., Lecturer of the Department of State and Legal Disciplines of the Russian State University of Justice, the Ural branch, Postgraduate Student of Department of Theory of State and Law, Constitutional and Administrative Law, South Ural State University (National Research University).
Reviewer: Minbaleev A.V., Executive Secretary, Leading Researcher of the Information Law Branch of the Institute of State and Law of the Russian Academy of Sciences; Leading Researcher of the Scientific Research Department of the Legislation and Comparative Law of Intellectual Property of RNIIIS; Professor of the Department of Theory of State and Law, Constitutional and Administrative Law, Deputy Director of the Law Institute of the South Ural State University (National Research University), Doctor of Law, Associate Professor.

шенствовании государственного порядка от 17 октября 1905 г., в ряде Именных высочайших указов Правительствующему Сенату 1905–1906 гг., а после Февральской революции — в Постановлениях Временного правительства 1917 г. («О печати», «Об учреждениях по делам печати»). Также свобода слова и печати нашла свое отражение в каталоге основных прав и свобод российских подданных Высочайше утвержденными Основными государственными законами от 26 апреля 1906 г. (ст. 37) и созданным на их основе Сводом Основных государственных законов 1906 г. (ст. 79) [9, с. 150–151].

Конституция РСФСР 1918 г. в ч. 13, 14 гл. 5 содержала отдельные положения, которые касались свободы мнений и печати (свобода религиозной и антирелигиозной пропаганды, переход печати в руки рабочего класса и крестьянской бедноты). В первой советской Конституции 1924 г. аналогичные положения отсутствовали. В «сталинской Конституции» 1936 г. имелись нормы, касающиеся свободы слова и печати (ст. 125), носившие исключительно декларативный характер.

М.В. Алексеева обращает внимание на тот факт, что в Конституции СССР 1977 г. и в Конституции РСФСР 1978 г. право на информацию не выделялось как самостоятельное, отдельные его элементы были включены в содержание ряда политических прав и свобод (свободы слова и печати, права на тайну переписки, телефонные переговоры и телеграфные сообщения и др.) [10, с. 16–19].

Как самостоятельное право право человека и гражданина на информацию в России впервые было закреплено в Декларации прав и свобод человека и гражданина 1991 г.[4]

Конституция РФ 1993 года — первая конституция страны, закрепившая право на информацию в качестве самостоятельного права. Она гарантирует свободу поиска, получения, передачи, производства и распространения информации любым законным способом[5].

Однако без системы гарантий любая юридическая норма, даже зафиксированная в Основном законе государства, остается декларативной. И одним из важнейших средств механизма реализации норм Конституции РФ является отраслевое законодательство.

Помимо Конституции, в Российской Федерации имеется конкретизирующее законодательство в области права на информацию, которое начало активно формироваться в начале третьего тысячелетия. Начало данному процессу было положено Указом Президента РФ от 31 декабря 1993 г. № 2334 «О дополнительных гарантиях прав граждан на информацию»[6].

Основными нормативными правовыми актами в информационной сфере на настоящий момент являются: Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[7], Федеральный закон от 22 декабря 2008 г. № 262–ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»[8], Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[9] и т.д.

При этом работа над законодательством в области права на информацию в нашей стране продолжается: предлагаются проекты Закона об Интернете, Информационного кодекса и т.д.

Но данные проекты носят перспективный характер, а в настоящее время перед Россией стоят иные задачи, нашедшие отражение в документах стратегического характера: указе Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[10] и Указе Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[11].

Анализ положений данных документов показывает: информационная политика современной России закономерно трансформируется от количественной составляющей права на информацию к акценту на его качественной стороне. Стратегическое значение приобретает право на «объективную, достоверную, безопасную информацию», отражающую национальные и культурные традиции России. Как эти установки будут реализованы на практике — покажет время.

Отметим также, что, как и в зарубежных странах, право на информацию в России трактуется не в качестве единого права, а рассматривается как система информационных прав, классифицируемых по различным основаниям [11]. Особую актуальность в последнее время приобретает выделение «права на доступ в Интернет», теоретическое обоснование которого одним из первых было сделано А.В. Минбалеевым [12, с. 10], к настоящему времени не нашедшее закрепления на законодательном уровне в нашей стране, но получившее признание в среде ученых и имеющее прецедент в зарубежных странах [13, с. 109–123].

Кроме того, в современной науке российского права сложились разные, нередко прямо противоположные трактовки права на информацию. А.В. Минбалеев связывает это с тем, что универсальность и всеобщность права на информацию порождает неоднозначность его толкования исследователями, а также определения места в системе прав и свобод и соотношения с иными правами. При этом по вопросу состава правомочий, входящих в право на информацию, а также его трактовки в юридической науке сегодня сложилось два подхода — узкий и широкий. В рамках первого подхода право на информацию рассматривается только как право на получение (доступ) информации, а в рамках второго подхода к праву на информацию относят все субъективные права, направленные на информацию или действия с ней [14, с. 114–115].

Из вышеперечисленного следует: формирование права на информацию в России и в мире про-

---

[4] Декларация прав и свобод человека и гражданина : принята постановлением ВС РСФСР от 22 ноября 1991 г. № 1920–I // Ведомости СНД РФ и ВС РФ. 1991. № 52. Ст. 1865.

[5] Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. // Российская газета. 1993. 25 декабря.

[6] Указ Президента РФ от 31 декабря 1993 г. № 2334 «О дополнительных гарантиях прав граждан на информацию» // Российская газета. 1994. 10 января.

[7] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. 29 июля.

[8] Федеральный закон от 22 декабря 2008 г. № 262–ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // Собрание законодательства Российской Федерации. 2008. № 52 (ч. 1). Ст. 6217.

[9] Федеральный закон от 9 февраля 2009 г. № 8–ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства Российской Федерации. 2009. № 7. Ст. 776.

[10] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

[11] Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

должается до сих пор. Анализ становления права на информацию, изучение его трансформации и выявление современных тенденций развития необходимы для лучшего уяснения его правовой природы и определения вектора дальнейшего развития в реалиях нового информационного общества.

Литература

1. Травников Н.О. Основные этапы становления прав личности в информационной сфере / Н.О. Травников // Современное право. 2016. № 2. С. 43–47.

2. Баранова Н.Б. Конституционное право граждан на информацию и его реализация в Российской Федерации : дис. ... канд. юрид. наук / Н.Б. Баранова. Пенза, 2005. 196 с.

3. Кузнецов П.У. Основы информационного права : учеб. для бакалавров / П.У. Кузнецов. М. : Проспект, 2015. 312 с.

4. Шевердяев С. Право на доступ к информации в России: Проблемы теории и законодательства / С. Шевердяев. URL: http://old.svobodainfo.org/ru/node/195

5. Забара И.Н. Становление и развитие концепции права на информацию в науке и практике международного права / И. Н. Забара // Информационное право. 2013. № 5. С. 3–6.

6. Janssen Katleen. Open Government Data and the Right to Information: Opportunities and Obstacles / Katleen Janssen // The Journal of Community Informatics. 2012. Vol. 8, No 2.

7. Bishop Cheryl Ann. Internationalizing the right to know: conceptualizations of access to information in human rights law: a dissertation submitted to the faculty of the University of North Carolina at Chapel Hill / Cheryl Ann Bishop. Chapel Hill, 2009. 268 p.

8. Сакулина Л.Л. Механизм административно-правового регулирования права граждан на информацию : дис. ... канд. юрид. наук / Л.Л. Сакулина. М., 2006. 201 с.

9. Кудрявцев М.А. Свобода информации и проблемы обеспечения информационных прав личности / М.А. Кудрявцев // Динамика институтов информационной безопасности. Правовые проблемы : сб. науч. тр. / отв. ред.: Т.А. Полякова, В.Б. Наумов, Э.В. Талапина. М. : ИГП-РАН: Канон-Плюс, 2018. С. 146–170.

10. Алексеева М.В. О проблемных вопросах реализации конституционного права на информацию как одного из основных прав и свобод человека и гражданина / М.В. Алексеева // Конституционное и муниципальное право. 2012. № 7. С. 16–19.

11. Бачило И.Л. Информационное право : учебник. Институт государства и права РАН, Академический правовой университет / Лопатин В.Н., Федотов М.А. СПб. : Юридический центр Пресс, 2001. С. 219–258.

12. Минбалеев А.В. Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества : автореф. дис. ... докт. юрид. наук / А.В. Минбалеев. Челябинск, 2012. 45 с.

13. Хуснутдинов А.И. Право на доступ в Интернет — новое право человека? / А.И. Хуснутдинов // Сравнительное конституционное обозрение. 2017. № 4. С. 109–123.

14. Минбалеев А.В. Система информации: теоретико-правовой анализ : дис. ... канд. юрид. наук / А.В. Минбалеев. Челябинск, 2006. 272 с.

References

1. Travnikov N.O. Osnovny'e etapy' stanovleniya prav lichnosti v informatsionnoy sfere [The Main Stages of Personal Rights Establishment in the Information Sphere] / N.O. Travnikov // Sovremennoe pravo — Modern Law. 2016. № 2. S. 43–47.

2. Baranova N.B. Konstitutsionnoe pravo grazhdan na informatsiyu i ego realizatsiya v Rossiyskoy Federatsii : dis. ... kand. yurid. nauk [The Civil Constitutional Right to Information and Its Exercising in the Russian Federation : thesis of ... Candidate of Legal Sciences] / N.B. Baranova. Penza — Penza, 2005. 196 s.

3. Kuznetsov P.U. Osnovy' informatsionnogo prava : ucheb. dlya bakalavrov [Fundamentals of the Information Law : textbook for bachelors] / P.U. Kuznetsov. Moskva : Prospekt — Moscow : Prospect, 2015. 312 s.

4. Sheverdyaev S. Pravo na dostup k informatsii v Rossii: Problemy' teorii i zakonodatelstva [The Right to Access Information in Russia: Issues of the Theory and Legislation] / S. Sheverdyaev. URL: http://old.svobodainfo.org/ru/node/195

5. Zabara I.N. Stanovlenie i razvitie kontseptsii prava na informatsiyu v nauke i praktike mezhdunarodnogo prava [Establishment and Development of the Concept of the Right to Information in the International Law Science and Practice] / I. N. Zabara // Informatsionnoe pravo — Information Law. 2013. № 5. S. 3–6.

6. Janssen Katleen. Open Government Data and the Right to Information: Opportunities and Obstacles / Katleen Janssen // The Journal of Community Informatics. 2012. Vol. 8. № 2.

7. Bishop Cheryl Ann. Internationalizing the Right to Know: Conceptualizations of Access to Information in Human Rights Law : A dissertation submitted to the Faculty of the University of North Carolina at Chapel Hill / Cheryl Ann Bishop. Chapel Hill, 2009. 268 s.

8. Sakulina L.L. Mekhanizm administrativno-pravovogo regulirovaniya prava grazhdan na informatsiyu : dis. ... kand. yurid. nauk [The Mechanism of Administrative Law Regulation of the Right of Citizens to Information : thesis of ... Candidate of Legal Sciences] / L.L. Sakulina. Moskva — Moscow, 2006. 201 s.

9. Kudryavtsev M.A. Svoboda informatsii i problemy' obespecheniya informatsionny'kh prav lichnosti [The Freedom of Information and Issues of Enforcement of Personal Rights to Information] / M.A. Kudryavtsev // Dinamika institutov informatsionnoy bezopasnosti. Pravovy'e problemy' : sb. nauch. tr. / otv. red. : T.A. Polyakova, V.B. Naumov, E.V. Talapina — Dynamics of Information Security Institutions. Legal Issues : collection of research works / publishing editors : T.A. Polyakova, V.B. Naumov, E.V. Talapina. Moskva : IGP-RAN : Kanon-Plyus — Moscow : ISL RAS : Canon Plus, 2018. S. 146–170.

10. Alekseeva M.V. O problemny'kh voprosakh realizatsii konstitutsionnogo prava na informatsiyu kak odnogo iz osnovny'kh prav i svobod cheloveka i grazhdanina [On Disputable Issues of Exercising of the Constitutional Right to Information as One of the Main Human and Civil Rights and Freedoms] / M.V. Alekseeva // Konstitutsionnoe i munitsipalnoe pravo — Constitutional and Municipal Law. 2012. № 7. S. 16–19.

11. Bachilo I.L. Informatsionnoe pravo : uchebnik. Institut gosudarstva i prava RAN, Akademicheskiy pravovoy universitet [Information Law : textbook. Institute of State and Law of RAS, Academic Law University] / Lopatin V.N., Fedotov M.A. Sankt-Peterburg : Yuridicheskiy tsentr Press — Saint Petersburg : Legal Center Press, 2001. S. 219–258.

12. Minbaleev A.V. Teoreticheskie osnovaniya pravovogo regulirovaniya massovy'kh kommunikatsiy v usloviyakh razvitiya informatsionnogo obschestva : avtoref. dis. ... dokt. yurid. nauk [Theoretical Bases of Legal Regulation of Mass Communications in Conditions of Information Society Development : author's abstract of thesis of ... Doctor of Law] / A.V. Minbaleev. Chelyabinsk — Chelyabinsk, 2012. 45 s.

13. Khusnutdinov A.I. Pravo na dostup v Internet — novoe pravo cheloveka? [The Right to Internet Access: A New Human Right?] / A.I. Khusnutdinov // Sravnitelnoe konstitutsionnoe obozrenie — Comparative Constitutional Overview. 2017. № 4. S. 109–123.

14. Minbaleev A.V. Sistema informatsii: teoretiko-pravovoy analiz : dis. ... kand. yurid. nauk [An Information System: A Theoretical Legal Analysis : thesis of ... Candidate of Legal Sciences] / A.V. Minbaleev. Chelyabinsk — Chelyabinsk, 2006. 272 s.

Противодействие экстремизму в сети «Интернет»: охранительный аспект

*Полещук Д.Г.**

Цель. *Развитие информационных технологий расширяет возможности использования сети Интернет по всему миру. В числе негативных тенденций — его доступность и привлекательность для современных экстремистских организаций. Это обуславливает необходимость защиты информационного пространства государств от противоправных посягательств экстремистской направленности. Одним из ключевых механизмов противодействия экстремизму в сети Интернет и обеспечения информационной безопасности выступает установление превентивных охранительных норм.*

Методология: *сравнительно-правовой метод, метод системного анализа, диалектика, герменевтика.*

Выводы. *Противодействие экстремизму в Интернете средствами охранительного законодательства осуществляется по направлениям обеспечения защиты от информации экстремистского содержания и защиты от воздействия на информационные коммуникации и средства в экстремистских целях. Определение запрещенной информации экстремистского содержания в Республике Беларусь и Российской Федерации имеет некоторые отличия. В этой связи в исследуемой сфере требуется согласование норм материального уголовного права на уровне соответствующих международных соглашений. Следует учитывать возможность установления ответственности за предоставление информации экстремистского содержания конкретным лицам. Применение признака «использования глобальной компьютерной сети Интернет» для описания преступлений, связанных с размещением информации экстремистского содержания в сети Интернет, в уголовных законах Республики Беларусь и Российской Федерации не во всех случаях носит системный характер. В условиях современного развития общества указанный квалифицирующий признак может охватываться основным составом преступлений.*

Научная и практическая значимость. *В статье рассматривается охранительный аспект противодействия экстремизму в сети Интернет в Республике Беларусь и Российской Федерации, выделяются направления противодействия экстремизму в сети Интернет, проводится сравнительный анализ законодательства указанных государств в части защиты общества от информации экстремистского содержания, предлагаются выводы относительно совершенствования действующего законодательства.*

Ключевые слова: *противодействие экстремизму, Интернет, информационная безопасность, информация экстремистского содержания, информационная сфера, угрозы, экстремистская идеология, экстремистская деятельность, информационный экстремизм, распространение информации.*

Purpose. *The development of information technology extends the use of the Internet throughout the world. Its accessibility and attractiveness for modern extremist organizations one of the topical negative trends nowadays. Consequently, this fact makes it necessary to protect the state's information space against illegal encroachments of extremist orientation. Among the key mechanisms for countering extremism in the Internet and ensuring information security is the establishment of preventive protective norms.*

Methodology: *comparative legal method, method of system analysis, dialectic, hermeneutics.*

Results: *countering extremism in the Internet by means of protective legislation is carried out in the areas of providing protection against information of extremist content and protection from the impact on information communications and funds for extremist purposes. The definition of prohibited information of extremist content in the Republic of Belarus and the Russian Federation has some differences. As a result, in the investigation sphere it is necessary to harmonize norms of substantive criminal law by the relevant international agreements. One should take into account the possibility of establishing responsibility for providing information of extremist content to specific individuals. The use of the sign «use of the Internet» to describe crimes related to the placement of information of extremist content on the Internet in the criminal laws of the Republic of Belarus and the Russian Federation is not always systemic. Due to the modern development of society, this qualifying sign can be covered by the main composition of crimes.*

Scientific and practical significance. *The article deals with the protective aspect of countering extremism in the Internet in the Republic of Belarus and the Russian Federation, identifies areas for countering extremism in the Internet, compares the legislation of these states with regard to protecting society from information of extremist content, suggests conclusions on improving legislation.***

Keywords: *countering extremism, the internet, information security, information of extremist content, information sphere, threats, extremist ideology, manifestations of extremism, information impact, extremist activity, information extremism, information dissemination.*

* **Полещук Дмитрий Григорьевич,** аспирант Института правовых исследований Национального центра законодательства и правовых исследований Республики Беларусь, главный специалист Национального центра законодательства и правовых исследований Республики Беларусь, магистр юридических наук. E-mail: Elios.dmp@gmail.com

Рецензент: Лопатин Владимир Николаевич, главный редактор, научный руководитель (директор) РНИИИС, эксперт РАН, доктор юридических наук, профессор, заслуженный деятель науки Российской Федерации.

** **Combating Extremism on the Internet: A Protective Aspect**

Poleshchuk D.G., Postgraduate Student of the Institute for Legal Research of the National Centre of Legislation and Legal Research of the Republic of Belarus, Chief Specialist of the National Centre of Legislation and Legal Research of the Republic of Belarus, Master of Law.

Reviewer: Lopatin V.N., Chief Editor, the Scientific Head of the National Research Institute of Intellectual Property (NSRIIP), Honored Worker of Science of the RF, Expert of the Russian Academy of Sciences, Doctor of Law, Professor.

Противодействие экстремизму в сети Интернет выступает важным направлением обеспечения информационной безопасности личности, общества и государства. Доступность современных информационных технологий, скорость распространения информации и глобализация информационного пространства являются теми факторами, которые непосредственно оказывают влияние на жизнь человека в XXI веке. Вместе с тем далеко не всегда это влияние может иметь положительный характер и приносить пользу современному обществу. В первую очередь, это касается использования глобальной компьютерной сети Интернет в противоправных целях. Одной из таких негативных целей выступает продвижение идеологии экстремизма и его проявлений в рамках мирового информационного пространства, наполненное стремлением охватить как можно большее число людей. Анализ информационной обстановки в сети показывает, что контент основных интернет-ресурсов по продвижению идеологии терроризма носит наступательный, агрессивный характер, отличается хорошей теоретической базой, продуманным спектром методов управляемого информационно-психологического воздействия на пользователей и защищенностью ресурсов [1]. В этой связи транснациональные IT-корпорации внедряют новые интеллектуальные механизмы, призванные противостоять указанным явлениям [2]. Сложившаяся ситуация, обусловленная развитием региональных конфликтов, как правило, на политической, национальной, этнической и религиозной основе, вынуждает современные государства принимать соответствующие меры, в том числе охранительные, направленные на противодействие экстремизму в информационной сфере.

Угрозы информационного характера определяются государствами в нормативных правовых актах, имеющих стратегическое значение для их устойчивого развития. В частности, Стратегия противодействия экстремизму в Российской Федерации до 2025 г., Национальная стратегия кибербезопасности Испании закрепляют приоритетную роль сети “Интернет” при совершении преступлений экстремистской направленности, распространения экстремистской идеологии[1].

В Республике Беларусь отсутствует единый комплексный акт по вопросу противодействия экстремизму в информационной сфере. Отдельные аспекты правового регулирования защиты населения (общества) от информационного воздействия экстремистов и защиты от воздействия на информационные коммуникации и средства находят свое закрепление в программных документах различных уровней и законодательных актах, направленных на регулирование более широкого круга иных общественных отношений (общее регулирование противодействия экстремизму, деятельность СМИ, проведение массовых мероприятий и др.). Так, Концепция национальной безопасности Республики Беларусь в качестве угроз национальной безопасности определяет: проявление социально-политического, религиозного, этнического экстремизма и расовой вражды на территории Республики Беларусь; деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам; нарушение функционирования критически важных объектов информатизации[2].

В юридической науке вопросы борьбы с экстремизмом или его проявлениями исследовались А.В. Барковым, А.Е. Гучком, Р.Ж. Идрисовым, А.Г. Никитиным, В.К. Потаповым, А.В. Шидловским, Г.И. Юсуповой и другими авторами.

Отдельные проблемы противодействия экстремизму в сети Интернет изучались В.В. Батоевым [3], Н.И. Болычевым [4], Л.А. Бураевой [5], В.В. Гладышевым [6], Е.А. Олейниковой [7], А.В. Петряниным [8], Ю.Н. Троегубовым [9].

Вместе с тем многоаспектность проблемы современного экстремизма, новизна и неизученность вопросов противодействия экстремизму в сети Интернет в части совершенствования охранительного законодательства предопределяет актуальность настоящего исследования.

В рамках противодействия экстремизму в сети Интернет средствами охранительного законодательства, на наш взгляд, следует выделить 2 основных направления: 1) защита от информации, способствующей развитию и укреплению в сознании людей экстремистской идеологии (экстремистских материалов, информации экстремистской направленности), отнесенной профессором В.Н. Лопатиным к разновидности вредной информации [10, с. 237]; 2) защита от проявлений экстремизма в сети Интернет (защита от воздействия на информационные коммуникации и средства в экстремистских целях).

Закон Республики Беларусь «О противодействии экстремизму» в ст. 1, определяя сам термин «экстремизм» (экстремистская деятельность), также относит к нему следующие действия, непосредственно затрагивающие информационную сферу, а именно: разжигание расовой, национальной, религиозной либо иной социальной вражды или розни; пропаганду исключительности, превосходства либо неполноценности граждан по признаку их социальной, расовой, национальной, религиозной или языковой принадлежности; пропаганду и публичное демонстрирование, изготовление и распространение нацистской символики или атрибутики; распространение экстремистских материалов, изготовление, издание, хранение или перевозку в целях распространения таких материалов; публичные призывы к экстремистской деятельности. Часть 1 ст. 14 Закона устанавливает запрет на распространение информационной продукции, содержащей призывы к экстремистской деятельности или пропагандирующей такую деятельность.

В Российской Федерации ст. 1 Федерального закона «О противодействии экстремистской деятельности» в понятие экстремистской деятельности (экстремизма) помимо иных деяний включает: публичное оправдание терроризма; возбуждение социальной, расовой, национальной или религиозной розни; пропаганду исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; пропаганду и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо публичное демонстрирование атрибутики или символики экстремистских организаций; публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения. Как и в Республике Беларусь, на территории Российской Федерации в соответствии с Законом запрещается распространение экстремистских материалов[3].

[1] Стратегия противодействия экстремизму в Российской Федерации до 2025 года : утв. указом Президента Российской Федерации 28 ноября 2014 г. № Пр-2753 // СПС «КонсультантПлюс» ; CODEXTER — Spain Profile on Counter-Terrorist Capacity // Online legislative database. URL: http://www.legislationline.org/topics/country/2/topic/5 (дата обращения: 10.01.2018).

[2] Об утверждении Концепции национальной безопасности Республики Беларусь : Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 // Национальный реестр правовых актов Республики Беларусь. 2010. № 276. 1/12080.

[3] О противодействии экстремистской деятельности : Федеральный закон Российской Федерации от 25 июля 2002 г. // СПС «КонсультантПлюс».

Анализ рассматриваемых актов в части определения компонентов, составляющих экстремизм (экстремистскую деятельность), позволяет сделать вывод о возможности совершения деяний, связанных с размещением запрещенной информации экстремистского содержания в сети Интернет.

Однако сопоставление норм белорусского и российского законодательства относительно содержания такой запрещенной информации указывает на определенные отличия в объеме правового регулирования, которые могут вызывать проблемы в практической деятельности и в рамках международного сотрудничества при применении охранительных норм. Для целей обеспечения системного регулирования противодействия экстремизму в сети Интернет на уровне международного сотрудничества и национального законодательства, опираясь на положения ст. 2 Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г., закрепляющей понятие «информационный терроризм», существуют основания для выделения понятия «информационный экстремизм» с конкретным описанием перечня исследуемых деяний.

За размещение информации экстремистского содержания в сети Интернет в Республике Беларусь и Российской Федерации предусмотрена при наличии соответсвующих признаков административная и уголовная ответственность.

Административная ответственность в указанной сфере с учетом ее охранительного и предупредительного потенциала предусмотрена за общественно вредные деяния в сети Интернет, связанные с пропагандой и (или) публичным демонстрированием нацистской (и сходной с ней) атрибутики или символики (ст. 20.3 Кодекса об административных правонарушениях (далее — КоАП) Российской Федерации), ст. 17.10 КоАП Республики Беларусь); массовым распространением экстремистских материалов (информационной продукции), включенных в соответствующие списки (ст. 20.29 КоАП Российской Федерации; ч. 2 ст. 17.11 КоАП Республики Беларусь); распространением информационной продукции, содержащей призывы к экстремистской деятельности или пропагандирующей такую деятельность, если в этих деяниях нет состава преступления (ч. 1 ст. 17.11 КоАП Республики Беларусь).

Проблемным вопросом является исключение применения мер административной ответственности по ст. 20.29 КоАП Российской Федерации и ст. 17.11 КоАП Республики Беларусь в случае предоставления указанной информации конкретным лицам (например, посредством социальной сети в целях последующей вербовки). При этом информация может распространяться как новостная рассылка от сообщества, в котором состоит пользователь социальной сети, так и непосредственно от пользователя к пользователю, что и обуславливает скорость ее распространения [6]. Тем не менее, на наш взгляд, с учетом расширения масштабов деятельности экстремистских организаций в сети Интернет, законодателям не следует исключать из сферы действия охранительного законодательства факты предоставления запрещенной информации для ознакомления конкретным лицам.

Противодействие размещению информации экстремистского содержания в сети Интернет с помощью уголовно-правовых средств имеет приоритетное значение для обеспечения информационной безопасности государства. Значимость криминализации отдельных деяний, касающихся защиты от такой информации, определяется и на уровне международных актов. В частности, Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем от 28 января 2003 г. (далее — Дополнительный протокол) в ст. 3 устанавливает требование криминализации на национальном уровне распространения расистского и ксенофобского материала или обеспечения доступа к нему для общественности через компьютерные системы, когда это сделано умышленно и противоправно.

Кроме того, ст. 6 Дополнительного протокола ориентирует на установление уголовной ответственности за умышленное и противоправное распространение или обеспечение доступа для общественности через компьютерную систему материала, который полностью отрицает или чрезвычайно умаляет отрицательные последствия, одобряет или оправдывает действия, являющиеся геноцидом или преступлениями против человечества, как определено международным правом и как это признано окончательными и обязательными решениями Международного военного трибунала, образованного в соответствии с Лондонским соглашением от 8 августа 1945 г., или любого другого Международного суда, образованного согласно соответствующим международным документам и юрисдикция которых признана государством[4]. Вместе с тем, несмотря на то, что Республика Беларусь и Российская Федерация не участвуют в указанной Конвенции, уголовные законы предусматривают специальные составы преступлений, обеспечивающие защиту общества от информации экстремистского содержания.

С учетом роли сети Интернет в современных общественных отношениях, вовлечения в ее использование большинства людей, размещение информации экстремистского содержания в рамках виртуального пространства в Республике Беларусь соответствует признакам следующих составов преступлений:

— распространение в любой форме взглядов, идей или призывов с целью вызвать агрессию одной страны против другой — пропаганда войны (ст. 123 Уголовного кодекса (далее — УК) Республики Беларусь);

— умышленные действия, направленные на возбуждение расовой, национальной, религиозной либо иной социальной вражды или розни по признаку расовой, национальной, религиозной, языковой или иной социальной принадлежности (ст. 130 УК Республики Беларусь);

— угроза совершением акта терроризма (ст. 290 УК Республики Беларусь).

Также криминализированы призывы к действиям, направленным на причинение вреда национальной безопасности Республики Беларусь (включая совершение акта терроризма) либо распространение материалов, содержащих такие призывы, совершенные с использованием средств массовой информации или глобальной компьютерной сети Интернет (ч. 3 ст. 361 УК Республики Беларусь).

В УК Российской Федерации применительно к противодействию экстремизму в сети Интернет предусмотрена уголовная ответственность за:

— угрозу совершения террористического акта (ст. 205 УК Российской Федерации);

— публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет» (ст. 205.2 УК Российской Федерации);

— публичные призывы к осуществлению экстремистской деятельности, совершенные с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет» (ч. 2 ст. 280 УК Российской Федерации);

---

[4] Об утверждении Концепции национальной безопасности Республики Беларусь : Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 // Национальный реестр правовых актов Республики Беларусь. 2010. № 276. 1/12080.

— публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») (ч. 2 ст. 280.1 УК Российской Федерации);

— действия, направленные на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично или с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет» (ст. 282 УК Российской Федерации);

— публичные призывы к развязыванию агрессивной войны и те же деяния, совершенные с использованием средств массовой информации (ч. 1 и ч. 2 ст. 354 УК Российской Федерации);

— отрицание фактов, установленных приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран оси, одобрение преступлений, установленных указанным приговором, а равно распространение заведомо ложных сведений о деятельности СССР в годы Второй мировой войны, совершенные публично, а также те же деяния, совершенные с использованием средств массовой информации (ч. 1 и ч. 2 ст. 354.1 УК Российской Федерации);

— угрозу совершения акта международного терроризма (ст. 361 УК Российской Федерации).

Анализ представленных норм об уголовной ответственности за размещение информации экстремистского содержания в сети Интернет позволяет констатировать следующие особенности и правовые проблемы:

1) объем уголовно-правовой охраны общественных отношений, связанных с защитой от информации экстремистского содержания, в Республике Беларусь и Российской Федерации имеет определенные отличия. Так, в уголовном законе Республики Беларусь не криминализировано публичное оправдание терроризма, а также отрицание фактов, установленных приговором Международного военного трибунала, образованного в соответствии с Лондонским соглашением от 8 августа 1945 г., или любого другого Международного суда, образованного согласно соответствующим международным документам. В этой связи несогласованность рассматриваемых норм об уголовной ответственности может вызывать затруднения в практической деятельности при осуществлении международного сотрудничества по вопросам противодействия экстремизму, в том числе в сети Интернет. Учитывая необходимость формирования единых норм материального уголовного права по вопросам противодействия экстремизму в сети Интернет в рамках международного сотрудничества, следует рассмотреть возможность заключения соответствующего международного соглашения в рамках Организации Договора о коллективной безопасности либо дополнить Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. соответствующими положениями;

2) признак «использования глобальной компьютерной сети Интернет» имеет различное описание и не используется в конструкции всех составов преступлений. Принимая во внимание, что указанный признак является квалифицирующим и влечет более строгую ответственность, на наш взгляд, требуется выработка единого подхода к его употреблению в тексте уголовного закона: либо дополнение всех рассматриваемых составов преступлений указанным признаком, либо исключение его из конструкции исследуемых уголовно-правовых норм. По нашему мнению, наличие или отсутствие указанного признака не имеет решающего значения при квалификации соответствующих преступлений, поскольку основной состав исследуемых преступлений уже охватывает указанный признак. В то же время в условиях информатизации общественной жизни, развития информационных технологий и перехода межличностных коммуникаций и исследуемых противоправных деяний в глобальную компьютерную сеть Интернет установление более строгой ответственности только за сам факт ее использования носит дискуссионный характер.

Подводя итог настоящему исследованию, можно сделать следующие выводы.

1. Противодействие экстремизму в сети Интернет средствами охранительного законодательства осуществляется по направлениям обеспечения защиты от информации экстремистского содержания и защиты от воздействия на информационные коммуникации и средства в экстремистских целях.

2. Определение запрещенной информации экстремистского содержания в Республике Беларусь и Российской Федерации имеет некоторые отличия, что может вызывать проблемы в рамках международного сотрудничества при применении охранительных норм. Для системного изложения деяний, связанных с экстремизмом, в сети Интернет на уровне национального законодательства и международных актов можно использовать термин «информационный экстремизм».

3. Имеются определенные основания установления ответственности не только за массовое распространение информации экстремистского содержания, но и за ее предоставление конкретным лицам.

4. Учитывая различный объем уголовно-правовой охраны общественных отношений, связанных с защитой от информации экстремистского содержания в сети Интернет, требуется согласование норм материального уголовного права на уровне соответствующих международных соглашений. При этом в Республике Беларусь можно рассмотреть возможность криминализации оправдания терроризма, а также отрицания фактов, установленных приговором Международного военного трибунала, образованного в соответствии с Лондонским соглашением от 8 августа 1945 г. в сети Интернет.

5. Применение признака «использование глобальной компьютерной сети Интернет» для описания преступлений, связанных с размещением информации экстремистского содержания в сети Интернет, в уголовных законах Республики Беларусь и Российской Федерации не во всех случаях носит системный характер. В условиях современного развития общества указанный квалифицирующий признак может охватываться основным составом исследуемых преступлений.

Литература

1. Противодействие идеологии терроризма в сети «Интернет» // МВД по Республике Коми. URL: https://11.мвд.рф/Protivodejstvie_ideologii_terrorizma_v_s (дата обращения: 20.01.2018).

2. Google ужесточает борьбу с распространением экстремистских видео на YouTube // Информационное агентство России ТАСС. URL: http://tass.ru/obschestvo/4346995 (дата обращения: 20.01.2018).

3. Батоев В.В. Проблемы противодействия экстремистской деятельности, осуществляемой с использованием сети Интернет / В.В. Батоев // Вестник Воронежского института МВД России. 2016. № 2. С. 37–43.

4. Болычев Н.И. О зарубежном опыте правового регулирования противодействия экстремизму в сети Интернет / Н.И. Болычев // Вестник Воронежского института МВД России. 2015. № 3. С. 209–214.

5. Бураева Л.А. Мировой опыт противодействия экстремизму и терроризму в глобальном информационном пространстве / Л.А. Бураева // Теория и практика общественного развития. 2015. № 18. С. 131–134.

6. Гладышев В.В. Социальные сети как инструмент для пропаганды экстремизма / В.В. Гладышев // Национальный антитеррористический комитет Российской

Федерации. 2018. URL: http://nac.gov.ru/publikacii/stati-knigi-broshyury/gladyshev-v-socialnye-seti-kak-instrument-dlya.html (дата обращения: 10.01.2018).

7. Олейникова Е.А. Противодействие экстремизму в сети Интернет / Е.А. Олейникова // Законность. 2016. № 5. С. 6–9.

8. Петрянин А.В. Уголовно-правовые, оперативно-разыскные и криминалистические механизмы противодействия экстремизму в телекоммуникационных сетях и сети «Интернет»: на примере статьи 280 УК РФ / А.В. Петрянин // Вестник Нижегородской академии МВД России. 2016. № 1. С. 158–161.

9. Троегубов Ю.Н. Проблемы противодействия экстремизму в сети Интернет / Ю.Н. Троегубов // Humanitarian vector. 2014. № 3. С. 143–147.

10. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство : монография / В.Н. Лопатин. СПб., 2000. 428 с.

References

1. Protivodeystvie ideologii terrorizma v seti «Internet» [Combating the Terrorism Ideology on the Internet] // MVD po Respublike Komi — Ministry of Internal Affairs for the Komi Republic. URL: https://11.mvd.rf/Protivodejstvie_ideologii_terrorizma_v_s (data of access: January 20, 2018).

2. Google uzhestochaet borbu s rasprostraneniem ekstremistskikh video na YouTube [Google Steps up Combating Extremist Video Distribution on YouTube] // Informatsionnoe agentstvo Rossii TASS — TASS information agency of Russia. URL: http://tass.ru/obschestvo/4346995 (data of access: January 20, 2018).

3. Batoev V.V. Problemy' protivodeystviya ekstremistskoy deyatelnosti, osuschestvlyaemoy s ispolzovaniem seti Internet [Issues of Combating Extremist Activities Carried out Using the Internet] / V.V. Batoev // Vestnik Voronezhskogo instituta MVD Rossii — Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2016. № 2. S. 37–43.

4. Bolychev N.I. O zarubezhnom opy'te pravovogo regulirovaniya protivodeystviya ekstremizmu v seti Internet [On Foreign Experience of Legal Regulation of Combating Extremism on the Internet] / N.I. Bolychev // Vestnik Voronezhskogo instituta MVD Rossii — Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2015. № 3. S. 209–214.

5. Buraeva L.A. Mirovoy opy't protivodeystviya ekstremizmu i terrorizmu v globalnom informatsionnom prostranstve [World Experience of Combating Extremism and Terrorism in the Global Information Space] / L.A. Buraeva // Teoriya i praktika obschestvennogo razvitiya — Social Development Theory and Practice. 2015. № 18. S. 131–134.

6. Gladyshev V.V. Sotsialny'e seti kak instrument dlya propagandy' ekstremizma [Social Networks as a Tool of Extremism Propaganda] / V.V. Gladyshev // Natsionalny'y antiterroristicheskiy komitet Rossiyskoy Federatsii. 2018 — National Antiterrorism Committee of the Russian Federation. 2018. URL: http://nac.gov.ru/publikacii/stati-knigi-broshyury/gladyshev-v-socialnye-seti-kak-instrument-dlya.html (data of access: January 10, 2018).

7. Oleynikova E.A. Protivodeystvie ekstremizmu v seti Internet [Combating Extremism on the Internet] / E.A. Oleynikova // Zakonnost — Legality. 2016. № 5. S. 6–9.

8. Petryanin A.V. Ugolovno-pravovy'e, operativno-razy'skny'e i kriminalisticheskie mekhanizmy' protivodeystviya ekstremizmu v telekommunikatsionny'kh setyakh i seti «Internet»: na primere statyi 280 UK RF [Criminal Law, Intelligence and Criminalistic Mechanisms of Combating Extremism in Telecommunication Networks and on the Internet: On the Example of Article 280 of the Criminal Code of the Russian Federation] / A.V. Petryanin // Vestnik Nizhegorodskoy akademii MVD Rossii — Bulletin of the Nizhniy Novgorod Academy of the Ministry of the Interior of Russia. 2016. № 1. S. 158–161.

9. Troegubov Yu.N. Problemy' protivodeystviya ekstremizmu v seti Internet [Issues of Combating Extremism on the Internet] / Yu.N. Troegubov // Humanitarian Vector. 2014. № 3. S. 143–147.

10. Lopatin V.N. Informatsionnaya bezopasnost Rossii: Chelovek. Obschestvo. Gosudarstvo : monografiya [Russian Information Security: Man. Society. State : monograph] / V.N. Lopatin. Sankt-Peterburg — Saint Petersburg, 2000. 428 s.

Уважаемые авторы!

Просим вас тщательно проверять перед отправлением в редакцию общую орфографию статей, а также правильность написания соответствующих юридических терминов, соблюдение правил научного цитирования и наличие необходимой информации. Обращаем ваше внимание на то, что автор несет личную ответственность за оригинальность текста, а также за достоверность приведенных данных и точность цитируемых текстов.

Информационно-правовые ресурсы государственной системы правовой информации в образовательном процессе Республики Беларусь

*Вашкевич С.В.**

Цель. *Внимание сосредоточено на значимых для Республики Беларусь проектах, реализованных в период деятельности кафедры ЮНЕСКО НЦПИ, направленных на развитие ИКТ и их применение в сфере образования и права, обеспечение свободного доступа граждан к правовой информации и знаниям.*

Материалы и методы исследования. *Изучены документы ЮНЕСКО (Инчхонская Декларация, Декларация Циндао, Рамочная программа действий «Образование-2030», Цели в области устойчивого развития), направленные на совершенствование качества образовательных процессов посредством ИКТ. Использована совокупность общенаучных и частнонаучных методов познания, в том числе абстрагирование, сравнительный анализ и синтез, метод системного анализа, сопоставление, моделирование, терминологический анализ, научный анализ и обобщение. Методологической основой исследования является интегративный подход к используемой совокупности методов.*

Результаты. *Сформулирован вывод в части необходимости дальнейшего участия Кафедры в достижении целей устойчивого развития через реализацию новой концепции образования, которая декларирует необходимость использования ИКТ для укрепления образовательных систем, распространения знаний, обеспечения доступа к информации, качественного и эффективного обучения и более эффективного предоставления услуг.*

Дискуссия. *Автор отмечает возрастающую роль кафедры ЮНЕСКО НЦПИ в рамках национальных процессов, направленных на качественное преобразование юридического образования, правового воспитания и просвещения граждан на основе внедрения информационно-коммуникационных технологий и развитие этих технологий.*

Ключевые слова: *ЮНЕСКО, кафедра ЮНЕСКО НЦПИ, государственная система правовой информации Республики Беларусь, эталонный банк данных правовой информации Республики Беларусь, государственные информационно-правовые ресурсы, Национальный центр правовой информации Республики Беларусь, правовое просвещение граждан, информационные технологии в юридической деятельности, информационное общество, информационно-коммуникационные технологии, правовая информация, информатизация, информатизация правовой сферы, правовая информатизация, доступ к правовой информации.*

Purpose. *Attention is focused on significant for the Republic of Belarus projects, implemented during the period of operation of the UNESCO Chair NCLI, aimed at the development of ICT and their application in the field of education and law, ensuring free access of citizens to legal information and knowledge.*

Methodology: *studied UNESCO documents (the Incheon Declaration, the Qingdao Declaration, the Framework for Action "Education-2030", the goals in the field of sustainable development) aimed at improving the quality of educational processes through ICT. A set of general scientific and private scientific methods of cognition is used, including abstraction, comparative analysis and synthesis, the method of system analysis, comparison, modeling, terminological analysis, scientific analysis and generalization. As the methodological basis of the research, an integrative approach to the set of methods used is laid.*

Results. *The conclusion is drawn regarding the need for further participation of the Chair in achieving the goals of sustainable development through the implementation of the new concept of education, which declares the need for ICTs to strengthen educational systems, disseminate knowledge, provide access to information, provide quality and effective instruction, and provide more effective services.*

Discussion. *The author notes an increasing role of the UNESCO Chair NCLI in national processes, aimed at the qualitative transformation of legal education, legal nurturing and enlightenment of citizens, based on implementation of ICT and the development of these technologies.***

Keywords: *UNESCO, UNESCO Chair NCLI, state system of legal information of the Republic of Belarus, reference databank of legal information of the Republic of Belarus, state information and legal resources, National center of legal information of the Republic of Belarus, legal education of citizens, information technologies in legal activities, information society, information and communication technologies, legal information, informatization, legal sphere informatization, legal informatization. access to legal information.*

* **Вашкевич Светлана Владимировна,** младший научный сотрудник отдела научно-методического обеспечения правовой информатизации управления правовой информатизации Национального центра правовой информации Республики Беларусь. E-mail: vashkevich@ncpi.gov.by

Рецензент: Лопатин Владимир Николаевич, главный редактор, научный руководитель (директор) РНИИИС, эксперт РАН, доктор юридических наук, профессор, заслуженный деятель науки Российской Федерации.

** **Information Law Resources of the State System of Legal Information in the Educational Process of the Republic of Belarus**

Vashkevich S.V., Junior Researcher of the Division of Research and Methodological Support of legal Informatization of the Department of Legal Informatization of the National Center of Legal Information of the Republic of Belarus.

Reviewer: Lopatin V.N., Chief Editor, the Scientific Head of the National Research Institute of Intellectual Property (NSRIIP), Expert of the Russian Academy of Sciences, Doctor of Law, Professor, Honored Worker of Science of the Russian Federation.

Благодаря бурному развитию ИКТ стало возможным обеспечение быстрого и постоянного доступа в режиме реального времени к любым видам информации, что является одним из важнейших условий полноценного развития современного информационного общества. В связи с этим особое внимание мирового образовательного сообщества уделяется использованию ИКТ в рамках новой концепции образования для обеспечения справедливого качественного образования и возможностей обучения на протяжении всей жизни для всех на основе принципов Инчхонской Декларации [1], Декларации Циндао [2], Рамочной программы действий «Образование-2030» [3] и Цели 4 в области устойчивого развития [4].

Необходимость использования ИКТ «для укрепления образовательных систем, распространения знаний, обеспечения доступа к информации, качественного и эффективного обучения и более эффективного предоставления услуг» [1] заявлена в качестве приоритетного направления деятельности ЮНЕСКО в дальнесрочной перспективе как на глобальном уровне, так и на уровне отдельного государства.

В Республике Беларусь при содействии ЮНЕСКО осуществлен целый ряд проектов, направленных на совершенствование качества образовательных процессов посредством ИКТ. Примером тому является почти 15-летняя деятельность кафедры ЮНЕСКО по информационным технологиям и праву НЦПИ (Кафедра), направленная на продвижение и внедрение ИКТ в юридической науке и образовании, а также правовое воспитание и просвещение граждан. Конкретные практики Кафедры осуществляются путем ее участия в разработке современных механизмов образования через использование в учебном процессе возможностей ИКТ, а также посредством расширения сотрудничества с высшими учебными заведениями, государственными структурами, общественными организациями, другими кафедрами ЮНЕСКО.

Основной деятельностью Кафедры ЮНЕСКО НЦПИ является совершенствование юридического образования в Республике Беларусь. Ее активность в этом направлении обусловлена трансформационными процессами в сфере высшего образования, повлекшими актуализацию содержания подготовки юридических кадров в условиях построения информационного общества.

Кафедра инициирует и осуществляет разработку учебно-методических материалов (типовых учебных программ, учебно-методических комплексов и др.) учебных курсов, по вопросам правовой информатизации и ГСПИ. Так, программа специального курса «Основы государственной системы правовой информации и правовой информатизации», разработанная в 2012 г., уже внедрена в образовательный процесс ряда белорусских вузов. На ее базе функционирует инновационная площадка кафедры теории и истории государства и права факультета управления Института управленческих кадров Академии управления при Президенте Республики Беларусь, которая преследует цели повышения качества подготовки юридических кадров за счет усиления практико-ориентированной составляющей образовательного процесса посредством эффективного использования опыта сотрудников НЦПИ и его материально-технической базы, а также потенциала кафедры ЮНЕСКО НЦПИ.

Кроме этого, Кафедра является площадкой для формирования необходимых компетенций, развития умений и навыков по использованию ИКТ в информационно-правовой деятельности будущих юристов. На постоянной основе ее сотрудниками проводятся ознакомительные встречи, экскурсии для студентов и преподавателей учреждений образования с информированием о государственной системе правовой информации Республики Беларусь, информационно-правовых ресурсах, формах и способах доступа граждан к эталонной правовой информации.

С участием Кафедры развиваются формируемые НЦПИ государственные информационно-правовые ресурсы, которые широко используются в национальном образовательном процессе на всех уровнях: от дошкольного и начального школьного до системы переподготовки и повышения квалификации. Среди них: эталонный банк данных правовой информации с информационно-поисковой системой «ЭТАЛОН» и «ЭТАЛОН-ONLINE» (удаленный доступ посредством сети Интернет) [5], Национальный правовой интернет-портал Республики Беларусь (основной государственный информационно-правовой ресурс в сети Интернет, источник официального опубликования правовых актов) [6], Детский правовой сайт (ресурс, представляющий собой адаптированную игровую и информационную правовую среду для детей и подростков) [7], сайт «Правовой форум Беларуси» (интерактивная площадка для общения, получения необходимой информации, обмена опытом и мнениями по вопросам, связанным с правом) [8].

Изданы учебное пособие «Информационные технологии для юристов», коллективная монография «Правовая информатизация Республики Беларусь: становление и перспективы развития». Выпускаемый научно-практический журнал «Право.by» освещает актуальные вопросы развития юридической науки по всем отраслям права, правоприменительной деятельности, а также вопросы юридического образования, правовой информатизации.

Высока активность Кафедры в проведении научно-практических мероприятий: международных конференций, семинаров и других профессиональных форумов, ориентированных на обмен опытом в сфере правовой информатизации между учеными и практиками Республики Беларусь и других стран. Самыми значимыми являются международные научно-практические конференции «Информационные технологии и право (Правовая информатизация)», которые проведены НЦПИ в 2004, 2010 и 2012 и 2015 гг. [9]

Принимая во внимание значимость сохранения историко-культурного наследия белорусской нации, важной частью которой являются памятники истории права, Кафедра на постоянной основе участвует в просветительском проекте «Наследие права», в том числе в формировании коллекции историко-ориентированных ресурсов правовой тематики [10]. В их числе тематические банки данных «Помнікі гісторыі права Беларусі» [11], «Уголовное право Беларуси» [12], «Хозяйственное право Беларуси» [13], «Правовые акты БССР» [14]. Часть этих ресурсов размещена в свободном доступе, что позволяет сделать уникальные правовые акты различных исторических периодов доступными максимально широкому кругу лиц.

Обучение на протяжении всей жизни предусматривает широкий доступ граждан к информации и знаниям, в том числе правовым. В Республике Беларусь достижение указанной цели обеспечивается посредством функционирования публичных центров правовой информации (более 590 ПЦПИ), которые предоставляют возможность доступа любому гражданину к эталонной правовой информации, способствуя тем самым не только формированию

правовой и информационной культуры, но и когнитивных, межличностных и социальных навыков. Также Кафедра участвует в создании центров эталонной правовой информации в стране и за рубежом (всего более 90 ЦЭПИ). Только в 2017 г. 7 новых ЦЭПИ открылись на базе Евразийского национального университета имени Л.Н. Гумилева (Республика Казахстан), на базе Восточно-китайского педагогического университета (Китайская Народная Республика), на базе Кыргызско-Российского Славянского университета (Кыргызская Республика), на базе общественного представительства Белорусской торгово-промышленной палаты в г. Белграде (Республика Сербия), на базе Чешско-Белорусской торгово-промышленной палаты (Чешская Республика), на базе Восточно-Китайского педагогического университета, Шанхайской академии общественных наук (Китайская Народная Республика) [15].

В октябре-декабре 2017 г. НЦПИ с учетом финансовой поддержки ЮНЕСКО, предоставленной в рамках Программы участия на 2016–2017 гг., а также благодаря поддержке Национальной комиссии Республики Беларусь по делам ЮНЕСКО реализован проект «Ознакомление детей и подростков со своими правами посредством адаптированных средств информации». Основной целью проекта являлось воспитание гражданской ответственности, повышение уровня правовой культуры детей и подростков, правовой информированности педагогов по вопросам, связанным с правами детей, посредством развития адаптированной информационной среды — Детского правового сайта, а также других государственных информационно-правовых ресурсов. В рамках проекта было проведено шесть семинаров во всех областных городах Беларуси, в которых приняли участие более 300 специалистов различных организаций, работающих непосредственно с детьми [16].

Таким образом, все эти социальные практики являются ярким примером участия Кафедры в достижении целей устойчивого развития через реализацию новой концепции образования, которая декларирует необходимость использования ИКТ для укрепления образовательных систем, распространения знаний, обеспечения доступа к информации, качественного и эффективного обучения и более эффективного предоставления услуг.

Литература

1. Инчхонская декларация «Образование 2030: Обеспечение всеобщего инклюзивного и справедливого качественного образования и обучения на протяжении всей жизни». 2017. URL: http://unesdoc.unesco.org/images/0023/002331/233137r.pdf (дата обращения: 27.10.2017).

2. Декларация Циндао. 2018. URL: https://ictedupolicy.org/resource-library/content/qingdao-declaration-russian-version (дата обращения: 05.03.2018).

3. Рамочная программа действий «Образование-2030». 2018. URL: http://unesdoc.unesco.org/images/0024/002456/245656R.pdf (дата обращения: 05.03.2018).

4. Цель 4 в области устойчивого развития. 2018. URL: http://www.un.org/sustainabledevelopment/ru/issues/people/education/ (дата обращения: 05.03.2018).

5. ЭТАЛОН-ONLINE. 2018. URL: http://etalonline.by/ (дата обращения: 05.03.2018).

6. Национальный правовой Интернет-портал Республики Беларусь. 2018. URL: http://pravo.by/. (дата обращения: 05.03.2018).

7. Детский правовой сайт [Электронный ресурс]. 2018. Режим доступа: http://mir.pravo.by/ (дата обращения: 05.03.2018.

8. Правовой форум Беларуси. 2018. URL: http://forumpravo.by/ (дата обращения: 05.03.2018).

9. Международная научно-практическая конференция «Информационные технологии и право (Правовая информатизация — 2015). 2018. URL: http://pravo.by/conf2015/ (дата обращения: 05.03.2018).

10. Наследие права. 2018. URL: http://pravo.by/pravovaya-informatsiya/nasledie-prava/nauchnye-trudy/sborniki/ (дата обращения: 05.03.2018).

11. Банк данных «Помнікі гісторыі права Беларусі». 2018. URL: http://pravo.by/pravovaya-informatsiya/pomniki-gistoryi-prava-belarusi/kanstytutsyynae-prava-belarusi/agulnyya-zvestki/ (дата обращения: 05.03.2018).

12. Банк данных «Уголовное право Беларуси». 2018. URL: http://pravo.by/pravovaya-informatsiya/pomniki-gistoryi-prava-belarusi/kryminalnae-prava-belarusi/ (дата обращения: 05.03.2018).

13. Банк данных «Хозяйственное право Беларуси». 2018. URL: http://pravo.by/pravovaya-informatsiya/pomniki-gistoryi-prava-belarusi/gaspadarchae-prava-belarusi/ (дата обращения: 05.03.2018).

14. Банк данных «Правовые акты БССР». 2018. URL: http://pravo.by/pravovaya-informatsiya/pravovye-akty-bssr/o-banke-dannykh/ (дата обращения: 05.03.2018).

15. Центры эталонной правовой информации. 2018. URL: http://ncpi.gov.by/publcpi/centri%20etaloninf.aspx (дата обращения: 05.03.2018).

16. Завершен совместный проект Национального центра правовой информации и ЮНЕСКО «Ознакомление детей и подростков со своими правами посредством адаптированных средств информации». 2018. URL: http://www.pravo.by/novosti/novosti-pravo-by/2018/january/27142/ (дата обращения: 12.01.2018).

References

1. Inchkhonskaya deklaratsiya «Obrazovanie 2030: Obespechenie vseobschego inklyuzivnogo i spravedlivogo kachestvennogo obrazovaniya i obucheniya na protyazhenii vsey zhizni». 2017 [The Incheon Declaration Education 2030: Towards Inclusive and Equitable Quality Education and Lifelong Learning for All. 2017]. URL: http://unesdoc.unesco.org/images/0023/002331/233137r.pdf (date of access: October 27, 2017).

2. Deklaratsiya Tsindao. 2018 [The Qingdao Declaration. 2018]. URL: https://ictedupolicy.org/resource-library/content/qingdao-declaration-russian-version (date of access: March 5, 2018).

3. Ramochnaya programma deystviy «Obrazovanie-2030». 2018 [The Framework for Action Education 2030. 2018]. URL: http://unesdoc.unesco.org/images/0024/002456/245656R.pdf (date of access: March 5, 2018).

4. Tsel 4 v oblasti ustoychivogo razvitiya. 2018 [Sustainable Development Goal 4. 2018]. URL: http://www.un.org/sustainabledevelopment/ru/issues/people/education/ (date of access: March 5, 2018).

5. ETALON-ONLINE. 2018 [ETALON-ONLINE. 2018]. URL: http://etalonline.by/ (date of access: March 5, 2018).

6. Natsionalny'y pravovoy Internet-portal Respubliki Belarus. 2018 [The National Legal Internet Portal of the Republic of Belarus. 2018]. URL: http://pravo.by/ (date of access: March 5, 2018).

7. Detskiy pravovoy sayt. 2018 [The Children's Legal Website. 2018. URL: http://mir.pravo.by/ (date of access: March 5, 2018).

8. Pravovoy forum Belarusi. 2018 [The Legal Forum of Belarus. 2018]. URL: http://forumpravo.by/ (date of access: March 5, 2018).

9. Mezhdunarodnaya nauchno-prakticheskaya konferentsiya «Informatsionny'e tekhnologii i pravo (Pravovaya informatizatsiya — 2015)». 2018 [The International Scientific and Practical Conference Information Technology and Law (Legal Informatization 2015). 2018]. URL: http://pravo.by/conf2015/ (date of access: March 5, 2018).

10. Nasledie prava. 2018 [The Heritage of Law. 2018]. URL: http://pravo.by/pravovaya-informatsiya/nasledie-prava/nauchnye-trudy/sborniki/ (date of access: March 5, 2018).

11. Bank danny'kh «Помнікі гісторыі права Беларусі». 2018 [Databank Monuments of the Belarusian Law History. 2018]. URL: http://pravo.by/pravovaya-informatsiya/pomniki-gistoryi-prava-belarusi/kanstytutsyynae-prava-belarusi/agulnyya-zvestki/ (date of access: March 5, 2018).

12. Bank danny'kh «Ugolovnoe pravo Belarusi». 2018 [Databank Criminal Law of Belarus. 2018]. URL: http://pravo.by/pravovaya-informatsiya/pomniki-gistoryi-prava-belarusi/kryminalnae-prava-belarusi/ (date of access: March 5, 2018).

13. Bank danny'kh «Khozyaystvennoe pravo Belarusi». 2018 [Databank Business Law of Belarus. 2018]. URL: http://pravo.by/pravovaya-informatsiya/pomniki-gistoryi-prava-belarusi/gaspadarchae-prava-belarusi/ (date of access: March 5, 2018).

14. Bank danny'kh «Pravovy'e akty' BSSR». 2018 [Databank Legal Acts of the Belarusian Soviet Socialist Republic. 2018]. URL: http://pravo.by/pravovaya-informatsiya/pravovye-akty-bssr/o-banke-dannykh/ (date of access: March 5, 2018).

15. Tsentry' etalonnoy pravovoy informatsii. 2018 [Reference Legal Information Centers. 2018]. URL: http://ncpi.gov.by/publcpi/centri%20etaloninf.aspx (date of access: March 5, 2018).

16. Zavershen sovmestny'y proekt Natsionalnogo tsentra pravovoy informatsii i YUNESKO «Oznakomlenie detey i podrostkov so svoimi pravami posredstvom adaptirovanny'kh sredstv informatsii». 2018 [The Joint Project of the National Legal Information Center and UNESCO Getting Children and Teenagers to Know Their Rights Using Adapted Information Media Is Completed. 2018]. URL: http://www.pravo.by/novosti/novosti-pravo-by/2018/january/27142/ (date of access: January 12, 2018).

В соответствии с Распоряжением Минобрнауки России от 28 декабря 2018 г. № 90-р федеральный научно-практический журнал «Информационное право» включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученых степеней кандидата и доктора наук по научной специальности и соответствующей ей отрасли науки:

12.00.13 — Информационное право (юридические науки).

Кибербезопасность и инициативы Сбербанка России*

В первый день Всемирного экономического форума 22 января 2019 г. на площадке «Русского дома» в Давосе традиционно стартовала деловая программа мероприятий, организованных Росконгрессом. Хотя, в силу прежде всего внешних неурядиц, связанных с санкциями, программа была значительно сокращена как по числу мероприятий, так и по перечню высоких гостей, все сессионные площадки были заполнены, а вечерние залы «Русского дома» казались самыми оживленными на променаде в Давосе, где расположены основные офисы национальных делегаций ВЭФ.

Второй день деловой программы официальной российской резиденции стал основными и открылся рабочей дискуссией Международного конгресса по кибербезопасности. Следует признать важность и полезность инициатив Сбербанка России в постановке этих проблем и их обсуждении на пленарных и сессионных площадках Давосского экономического форума.

Станислав Кузнецов, заместитель председателя правления ПАО «Сбербанк», и ***Дмитрий Самарцев***, директор BI.ZONE, в течение часа вместе с участниками сессии в «Русском доме» активно обсуждали тему «**Частные корпорации vs. киберпреступность: коллаборация как ключ к успеху**». ***Елена Теплицкая***, советник Президента и Председателя Правления ПАО «Сбербанк», успешно продвигала эти инициативы на аналогичной сессии в рамках «Каспийского дома» с участием представителей США и стран ЕС.

К основным выводам по итогам дискуссий можно отнести следующие:

— развитие киберпреступности в мире опережает развитие систем противодействия ей («Ситуация очень печальна: международной системы противодействия киберпреступности на текущий момент нет, и нужно что-то с этим сделать. ...Преступники воруют деньги, данные, подрывают работу корпораций и чувствуют себя неуязвимыми. Это сегодняшняя действительность»);

— киберпреступность, в отличие от систем противодействия киберпреступлениям, не знает государственных границ, имеет экстерриториальный характер («Любой киберпреступник сегодня фактически является глобальным преступником, международным преступником. Он использует инфраструктуру различных стран, он точно и нацелено атакует компании, физические лица, юридические лица в любых странах мира, ему не нужно ограничиваться какими-то национальными границами. А правила борьбы с этими преступниками у нас всегда имеют национальные границы. «CitiGroup» — это банк, который присутствует в порядка 50 странах, и если он попробует выполнить одновременно законодательство всех стран своего присутствия, то, к сожалению, банк надо закрывать»);

— риски мировой экономики, связанные с киберпреступностью, превышают объем ВВП многих стран («Прогноз, который мы делали год назад, составлял 1 трлн долларов убытка мировой экономике. То, что

* Обзор подготовил Лопатин Владимир Николаевич, научный руководитель РНИИИС, генеральный директор Ассоциации интеллектуальной собственности Корпорации РНИИИС, главный редактор журнала «Информационное право», председатель межгосударственного технического комитета по стандартизации МТК 550 «Интеллектуальная собственность», доктор юридических наук, профессор, заслуженный деятель науки Российской Федерации.

Подробная информация о мероприятиях деловой программы размещена в информационно-аналитической системе Росконгресса на сайте https://roscongress.org.

Полная запись сессий, которые шли в режиме прямой интернет-трансляции, представлена по адресу: http://houserussia.com/programme/business-programme/.

эта цифра (1 трлн долларов) состоялась по итогам прошлого года, у нас не вызывает никаких сомнений. К 2022 г. ожидается 8 трлн долларов убытка в мире [от киберпреступности]. В России такой ущерб в 2018 г. составил, по оценкам, более 1 трлн рублей);

— основные объекты — мишени киберпреступников: финансовые институты, коммерческие организации, физические лица («Как правило, во всем мире и у нас в России объектами [киберпреступлений] номер один становятся финансовые институты, кредитные организации, банки. Примерно 96% наших так называемых кибремошенников — это те люди, которые воруют деньги у физических лиц. Всего 3–3,5% — это те самые хакеры, которые атакуют сознательно юридические лица, и всего небольшое количество хакеров — их не более 0,5% — занимаются так называемой разработкой серьезных вирусов, которые нацелены на управление компаниями, воровство больших данных и подобных систем. При этом атаки на население, на физических лиц имеют тенденцию к усилению, увеличению не менее чем на 15–20% в год»);

— киберпреступность уже граничит с кибертерроризмом («Мы имеем примеры, когда хакеры, пытаясь вывести деньги, случайно или неслучайно, попадали в системы по управлению самолетами, в диспетчерские центры аэропортов, мы имеем примеры, когда критическая инфраструктура была под большой угрозой». «Главный врач Тюменской больницы проводил нейрохирургическую операцию, и «благодаря» атаке хакеров отключилось все оборудование. Было ноль шансов продолжать эту операцию. То, с чем мы столкнулись, — это то, насколько в данной больнице отсутствуют правила кибербезопасности»);

— Россия, несмотря на распространенное за рубежом мнение, не является лидером в сфере киберпреступности («Мы посмотрели на структуру хакеров из различных стран мира, и российские хакеры точно не входят в пятерку, может быть даже в десятку лучших. В разные годы структура меняется. Иногда лидируют турки, иногда китайцы, иногда корейцы, иногда украинцы, иногда бразильцы»);

— классическая преступность все больше перемещается в компьютерное пространство. Киберпреступления больше не требуют обязательного наличия компьютерных навыков высокого уровня или больших финансовых затрат («атаки на обычных людей с использованием методов социальной инженерии не стоят ничего. Мошеннику не нужно быть искусным хакером, программистом. Все это можно купить как сервис в теневом интернете. Это может стоит несколько десятков, максимум — сотен долларов. Именно в России сегодня мошенничество с использованием методов социальной инженерии лидирует в мире. Стоимость выхода на этот рынок [киберпреступности] должна быть выше»);

— жертвы киберпреступности, по разным причинам, часто скрывают факт кибератак («По нашей оценке, не менее 80% всех, кто был атакован, скрывают это. По данным Интерпола, менее 1% информируют правоохранителей о том, что были хакнуты, были атакованы». «К сожалению, обучить население планеты кибергигиене — это достаточно сложная задача, на корпоративном уровне ее достаточно сложно решить»);

— существует дефицит международно-правовой базы, механизмов и институтов по борьбе с киберпреступностью («Внедрение GDPR (General Data Protection Regulation — европейский инструмент защиты информации — … привело к тому, что сервис WhoIs перестал работать. Сегодня, чтобы узнать, кто стоит за IP-адресом, нужно обращаться в полицию. Бюрократия международных отношений между полициями занимает месяцы, а в расследовании кибератак счет идет на минуты»);

— низкий уровень профессиональной компетенции в государственных органах, отсутствие единой системы подготовки кадров и недостаточный уровень экспертизы в сфере борьбы с киберпреступностью («Основная проблема сегодня — это то, что вся экспертиза в этой области сосредоточена в корпоративных, крупных игроках — международных. Это банки, технологичные компании, компании, которые являются экспертами в этой предметной области». В России ежегодно выпускается 17 тысяч специалистов по кибербезопасности, но в силу отсутствия единого стандарта их качество оставляет желать лучшего. В Москве в отделениях Сбербанка работает 400 таких специалистов, выпускников 206 вузов, для переподготовки которых создана Академия кибербезопасности, и Сбербанк подписал соглашения с 8 вузами).

В своем выступлении ***Владимир Лопатин,*** научный руководитель РНИИИС, генеральный директор Ассоциации интеллектуальной собственности Корпорации РНИИИС, главный редактор журнала «Информационное право», остановился на ряде проблем, требующих осмысления и решения с правовых позиций при выработке Стратегии, концепций и программ противодействия киберпреступности на корпоративном — государственном — международном уровнях.

Исходя из собственного опыта подготовки концепций и доктрины в сфере информационной безопасности, он предложил на стратегическом уровне на данном этапе поставить две цели: как объединить усилия при межгосударственном и межведомственном взаимодействии и как разделить/дифференцировать объекты защиты от киберугроз.

В частности, признавая позитивную роль инициатив Сбербанка России в постановке и решении проблем в этой сфере, очевидно также, что без государственного участия здесь не обойтись. В то же время любые усилия на национальном и региональном уровнях по противодействию киберпреступности упираются в существующие международные правовые барьеры, отдающие приоритет в защите на национальный уровень. По-видимому, назрела ситуация принятия единого международного договора с исключением из этого правила и обязательного для всех стран по основным процедурам защиты от киберпреступности и привлечения к ответственности лиц, виновных в этом. Роль бизнеса здесь в мотивации национальных правительств и парламентов в подписании и ратификации такого договора.

Необходимость разделения/дифференциации объектов защиты от киберпреступлений также определяется разностью правовых режимов охраны объектов (информация и информационные ресурсы (персональные данные, охраняемая законом тайна, базы данных как объекты интеллектуальной собственности), программное обеспечение и информационные технологии — как объекты интеллектуальной собственности, технические средства — как объекты вещной собственности) и правовых статусов их субъектов (обладатели информации, правообладатели интеллектуальной собственности и собственники). Кроме того, до сих пор остается неясным и различным по решению в разных странах вопрос о соотношении правовых статусов этих субъектов в рамках информационных систем и их операторов.

«Они [корпорации] должны объединяться, создавать глобальные базы данных киберугроз. Это может быть на базе блокчейна», — предложил ***Александр Иванов***, основатель блокчейн-платформы Vostok. «Можно собирать доказательную базу совместными усилиями частных компаний для того, чтобы отдавать эту информацию правоохранительным органам», — заметила ***Светлана Гербель***, генеральный директор ООО «Сименс Здравоохранение».

Подводя итоги дискуссии, ***Станислав Кузнецов***, заместитель председателя правления ПАО «Сбербанк», призвал к объединению усилий: «Этот год должен стать переломным не только для российских, но и для мировых компаний, когда мы должны научиться обмениваться информацией. Мы не должны делать из обмена информацией о киберпреступниках бизнес. Мы должны научиться обмениваться в онлайн-форма-

те с нашими партнерами подобного рода информацией, использовать ее автоматически для того, чтобы обучать наши системы быть эффективней в противодействии киберпреступникам, Нам надо строить мост между правоприменением и частным сектором».

Руководители Сбербанка пригласили всех участников дискуссии к ее продолжению в рамках Международного конгресса кибербезопасности, который организуется Сбербанком и пройдет в Москве 20–21 июня 2019 г.

Цифровизация городов и информационные технологии

Заключительным мероприятием деловой программы второго дня «Русского дома» в Давосе стала сессия, посвященная актуальной теме цифровой трансформации городов, — **«Городская цифровая трансформация: перспективы внедрения искусственного интеллекта в управление муниципальными процессами и процедурами».** В заседании приняли участие как спикеры: председатель фонда «Сколково», президент FIDE ***Аркадий Дворкович***, министр, руководитель департамента внешнеэкономических и международных связей Правительства Москвы и председатель правления делового совета по сотрудничеству с Индией ***Сергей Черёмин***, советник Премьер-Министра по экономическим вопросам Государства Катар ***Али Аль Тани***, президент и генеральный директор Американо-Российского делового совета ***Дэниел Расселл*** и основатель бюро Bernaskoni ***Борис Бернаскони***.

«В Сколково есть все три составляющие, связанные с исследованиями. В рамках Сколтеха идут серьезные исследования, которые будут являться основой будущих технологий, и machinelearning, и искусственного интеллекта применительно к самым разным сферам, от медицины до энергетики. Есть составляющая бизнеса — довольно много стартапов и индустриальных партнеров, которые заинтересованы в развитии этой темы. Третья составляющая — государство. Нужно сделать так, чтобы на новых технологиях можно было зарабатывать деньги, тогда часть этих заработанных денег может идти в бюджет в виде налогов и инвестироваться в оказание новых услуг, создание новых сервисов. Государство это сегодня в целом понимает», — подчеркнул ***Аркадий Дворкович,*** председатель фонда «Сколково». По его словам, «когда задумывали Сколково 10 лет назад, приняли решение, что все новые интересные находки будут опробоваться на «Сколково». Именно этим занимаемся в рамках развития энергоинфраструктуры Сколково: умные сети, умное управление энергетическими системами. То же самое касается транспортной инфраструктуры. В Сколково уже ездит автономный автомобиль «Яндекс» без водителя.

Основное место на сессии было посвящено опыту организации «умных» городов, на примере Москвы. «Москва — локомотив российской экономики. Это примерно 26% ВВП Российской Федерации, в Москву приходят более 50% иностранных инвестиций.... Без цифровых технологий, без использования искусственного интеллекта, без аналитики огромного количества собираемых данных невозможно говорить ни о развитой инфраструктуре, ни о развитом транспорте, здравоохранении, образовании, социальной сфере.

Мы были на перепутье: либо нам модернизировать старые системы и идти по пути brownfield, либо начинать greenfield и внедрять самые современные технологии, которые мы в том числе позаимствовали у наших партнеров, коллег, собирая их по всему миру. Мы пришли к выводу, что где-то можно модернизировать уже имеющиеся платформы, но мы сможем достигнуть революционного движения вперед, только если мы будем идти по пути greenfield». Поэтому для того, чтобы сохранить конкурентоспособность в этом мире и оставаться экономическим лидером, необходимо развивать цифровые технологии в крупных городах, и с 2011 года это — один из приоритетов развития столицы России. Мы работаем над созданием единого интерфейса для обеспечения единой управляемости всех городских процессов», — подчеркнул в ходе сессии ***Сергей Черёмин.***

По его оценке, «умный город» — это человеческий капитал плюс цифровизация всех областей муниципальной деятельности и всех сфер экономики города. Без этого сегодня осуществлять управление гигантским мегаполисом, без цифровых технологий, без использования искусственного интеллекта, без аналитики огромного количества собираемых данных, без того, чтобы отслеживать каждого человека в режиме реального времени, невозможно говорить ни о развитой инфраструктуре, ни о развитом транспорте, здравоохранении, образовании, социальной сфере. В прошлом году ООН поставила Москву на первое место в мире по внедрению информационных технологий в городскую среду. Организация WEGO также поставила Москву в список лидеров по информационным технологиям. PWC поставил Москву в пятерку мегаполисов, которые готовы к принятию самых высокотехнологичных решений в муниципальном хозяйстве. Москва, по рейтингу организации TOM, стала лидером по внедрению информационных технологий в парковочные системы.

Город вкладывает гигантские средства в развитие транспортной инфраструктуры, прежде всего общественного транспорта, и в том числе в его цифровизацию. Московский метрополитен, перевозя от 8 до 10 млн пассажиров в день, управляется с такой эффективностью, что частота движения поездов достигает 80–90 секунд. Таких скоростей нет нигде, за исключением, может быть, Японии и нескольких городов мира. Вы пользуетесь, сами того не замечая, высокоскоростным Wi-Fi в поездах метрополитена — об этом 10 лет назад даже футурологи не могли мечтать. Или о том, что в московских трамваях и автобусах будет существовать Wi-Fi, навигация, что по движению транспорта будут делаться аналитические выводы, как менять транспортные потоки, где открывать новую полосу для движения общественного транспорта, куда развивать метрополитен. За семь лет протяженность метрополитена выросла на 30%, 136 км новых линий, 70 новых станций.

Чемпионат мира прошел удачно в том числе благодаря цифровым технологиям. Системы контроля и паспорт болельщика позволили предотвратить появление на стадионах значительного количества провокаторов. Сейчас в Москве будет запускаться самая современная система видеонаблюдения. В Москве интегрировано более 140 тыс. камер в единую систему видеонаблюдения, больше, чем в Лондоне.

В Москве внедрена уникальная система «Московская электронная школа» — это единая информационная платформа, объединившая всех учеников, учителей, преподавателей, это уникальная библиотека лучших уроков… Такие гигантские инвестиции дают неизмеримый эффект. В прошлом году организация Pisa поставила Москву в список лидеров по начальному образованию. Вошли в пятерку лучших мегаполисов мира по качеству среднего образования.

Все данные, так называемые Bigdata, собираемые аналитическими центрами, — они ложатся в основу принятия решений, в том числе в урбанистике. Все это невозможно без использования цифровых технологий», — подытожил Сергей Черёмин.

С учетом того, что следующий Чемпионат мира по футболу пройдет в Катаре, следующим спикером стал ***Али Аль Тани***, советник Премьер-Министра по экономическим вопросам Катара. По его словам, «проект [Люсиль] абсолютно новый — новый город, который был построен четко с целью создать «умный город». Поэтому вся инфраструктура, все сети создавались извне. В этом проекте использовали централизованный подход к решению целого ряда проблем. Прежде всего — это центр управления городом, в котором соединяется целый ряд муниципальных органов, которые в режиме реального времени мониторят ситуацию в городе и принимают все необходимые меры по управлению транспортом, управлению системой водоснабжения, вывоза и переработки мусора. Еще одно решение касается гражданской обороны и служб эффективной борьбы с пожарами. Если возник пожар в каком-то здании, через наш центр управления мы можем быстро блокировать движение транспорта за счет регулирования светофоров, а также создать зеленый коридор для машин скорой помощи и пожарных. С помощью сети 5G мы сможем оказывать специализированные услуги, связанные с беспилотными автомобилями, таким образом, мы сможем сократить опоздание во времени до миллионной секунды. И, конечно, это служба беспилотных такси. В Дохе была проблема с дождями. За счет проектов по «умным городам» мы смогли эффективно создать топографическую карту дорог в разных городах и смоделировать такую систему дорог, которая позволяет нам аккумулировать воду в каких-то зонах и предотвратить возможные наводнения».

Дэниел Расселл акцентировал свое выступление на взаимосвязи умного города и развития бизнеса: «Исследование Национальной лиги государств говорит о том, что 66% американских городов используют умные технологии в той или иной степени. Эксперты дают три основных комментария. Первый — все истории успеха в США так или иначе связаны с механизмом ГЧП: идеи, прорывные технологии от бизнеса, поддержка от городских властей и госструктур и необходимая инфраструктура. Второй фактор — создание некоей экосистемы, которая будет служить интересам всех участников. Архитектура должна быть открытой, чтобы она могла принимать в себя новые технологии… Бизнесу нужны «умные города». Если мы посмотрим на рост мирового ВВП — именно урбанизированные зоны создают ключевой рост мировой экономики. Поэтому нам важно жить в комфортной среде, и это будет комфортно для бизнеса и в конечном итоге для мирового ВВП.

Свой оригинальный взгляд на проблемы «умного города» предложил ***Борис Бернаскони***, архитектор и автор проекта «Гиперкуб» в Сколково: «Первое здание в Сколково — гиперкуб — было прототипом архитектуры будущего, которая заключалась в очень простой формуле «4Э» — энергоэффективность, экологичность, эргономичность и экономичность, дальше добавили пятый «э» — эмоциональность. Мы, по сути, создали первое бессмертное здание. Сколково можно считать международного рода стартапом в области создания «умного города». Современные «стартапы» не могут подстроиться под уже существующую инфраструктуру, и современным решениям нужна другая инфраструктура».

В завершение сессии свои вопросы ее основным участникам Аркадию Дворковичу и Сергею Черёмину задал в своем выступлении ***Владимир Лопатин*** — научный руководитель РНИИИС, генеральный директор Ассоциации интеллектуальной собственности Корпорации РНИИИС.

За последние 18 лет доля рынка интеллектуальной собственности — «четвертой корзины» в мировой торговле — выросла в 4 раза (до 15% ВВП) и продолжает расти. В цифровой экономике, по экспертным

оценкам, эта доля к 2030 г. вырастет еще в два раза (до 30% ВВП). В то же время в России она составляет, по оценке Президента России, менее 1%, хотя наша страна входит в ТОП-8 стран в мире по затратам на исследования и разработки, публикациям, патентам и патентным заявкам.

В этой связи был задан вопрос С. Черёмину: что планирует делать правительство Москвы, на долю которой приходится четверть российского ВВП, чтобы цифровизация города вела не к обогащению иностранных компаний, а позволяла увеличить добавленную стоимость от коммерциализации отечественной интеллектуальной собственности в национальном ВВП. На этот вопрос министр Правительства Москвы ответил с уверенностью, что «доля добавленной стоимости от коммерциализации интеллектуальной собственности в ВВП и экономике будет расти в ближайшее время в геометрической прогрессии. Наша задача — если не перегнать, то догнать страны ЕС, США и такие развивающиеся страны, как Индия».

Обращаясь к А. Дворковичу, В. Лопатин со ссылкой на собственный опыт отметил, что сейчас его возможности в статусе руководителя Фонда «Сколково» не ограничены рамками государственных должностей и позволяют лучше реализовать свои творческие планы. В рамках повестки дня сессии он предложил руководителю Фонда «Сколково» помочь найти ответ на вопрос для его последующей апробации в «Сколково» и реализации в России и в мире: кому принадлежат права на результаты творчества систем искусственного интеллекта и каковы перспективы получения добавленной стоимости при их коммерциализации в составе товаров/работ, услуг. Вопрос вызвал большое оживление в зале, но, по сути, остался пока без ответа. При этом Аркадий Дворкович в ответе подчеркнул, что коммерциализация интеллектуальной собственности, в том числе искусственного интеллекта — «это мерило нашего успеха, мы нацелены на это».

****

В рамках третьего дня деловой программы «Русского дома» 24 января прошла закрытая встреча членов Консультативного совета по иностранным инвестициям в России. Завершающим мероприятием деловой части программы официальной российской резиденции в Давосе стала панельная сессия «**Экономика России — шаг вперед**». Модератор сессии ***Томас Блэквелл,*** главный исполнительный директор, соучредитель EM, последовательно предложил ее спикерам как лидерам ответить на два вопроса: каковы слагаемые сегодняшнего успеха «чемпионов экономики России» и какие перспективы ожидаются через 5 лет.

На эти вопросы отвечали: ***Максим Орешкин*****,** министр экономического развития Российской Федерации (развивать человеческий капитал через подготовку кадров, и «власть не должна мешать бизнесу»); ***Дмитрий Конов,*** председатель Правления СИБУР Холдинг (главное — это команда, реализующая технологии: производственные (18 тыс. человек) и управленческие (9 тыс. человек); ***Грег Абовский***, операционный директор, финансовый директор «Яндекс» (российская кампания с 1997 г. выросла в экосистему и нацелена на дальнейшее развитие через новые сервисы для пользователей); ***Андрей Дубовсков,*** президент, председатель правления АФК «Система» (мобильные телесистемы универсальны, межотраслевое взаимодействие дает синэнегетический эффект); ***Максим Евдокимов,*** главный цифровой директор «Тинькофф Банк» (надо помочь людям понять свои запросы и правильно организовать свое личное время, чтобы получить хорошие впечатления); ***Дмитрий Алимов,*** основатель Frontier Ventures (нужно менять систему права и снижать бюрократию); и ***Брайан Паллас***, основатель, Председатель Правления и главный исполнительный директор Opportunity Network.