Развитие законодательства в области обеспечения информационной безопасности: тенденции и основные проблемы

Т.А. Полякова

профессор Российского государственного университета правосудия, заведующая сектором информационного права Института государства и права РАН, доктор юридических наук, заслуженный юрист Российской Федерации. Адрес: 117418, Российская Федерация, Москва, Новочерёмушкинская ул., 69. E-mail: polyakova_ta@mail.ru

Е.В. Акулова

аспирантка кафедры информационного права, информатики и математики Всероссийского государственного университета юстиции. Адрес: 117638, Российская Федерация, Москва, ул. Азовская, 2/1. E-mail: akulova_ev@rambler.ru

Аннотация

Предметом исследования является процесс формирования правовой системы обеспечения международной информационной безопасности, а также системы информационной безопасности в рамках законодательства Российской Федерации. Актуальность указанной темы обусловлена высокими темпами развития глобального информационного пространства и информатизации всех сфер жизнедеятельности общества, а также непростой политической ситуацией, сложившейся на мировой арене. Все это в совокупности способствует появлению новых вызовов и угроз информационной безопасности, проблему предотвращения которых можно отнести к числу наиболее серьезных вопросов как национальной, так и международной безопасности. Неуклонное нарастание таких угроз вызывает необходимость построения эффективной системы МИБ, совершенствования национального законодательства в данной области, проведения научных исследований. В связи с этим авторы анализируют тенденции развития законодательства и государственной политики в области обеспечения информационной безопасности, а также обозначают наиболее актуальные проблемы и вопросы, подлежащие научному исследованию. Целью данного научного исследования является формирование практических и теоретических предложений при построений правовой системы МИБ и модернизации правовой системы информационной безопасности Российской Федерации. Достижению поставленной цели способствовали: проведение анализа формирования и развития правовой системы МИБ в современных политических условиях, анализ развития национального законодательства Российской Федерации в области информационной безопасности, выявление правовых проблем и неопределенностей, оказывающих влияние на успешное формирование системы МИБ и модернизации законодательства Российской Федерации в области информационной безопасности, а также формулировка на основе проведенного анализа ряда предложений, способствующих успешной реализации государственной политики Российской Федерации в области МИБ. Методологическую основу исследования составляют общенаучный метод познания, дедуктивный, сравнительно-правовой, формально-юридический методы и метод системного анализа. Одним из основных выводов научной статьи является необходимость расширения договорно-правовой базы межгосударственного сотрудничества, а также разработки общих правил применения норм в информационной сфере, создание единого для участников межгосударственных образований подхода в области правового регулирования — гармонизация и унификация законодательства государств-членов союзных государств, интеграция в законодательство Российской Федерации рекомендаций, закрепленных в международных документах.

Ключевые слова

национальная безопасность, информационное пространство, информационное общество, информационные технологии, международная информационная безопасность, критическая информационная инфраструктура, государственная политика Российской Федерации, персональные данные, облачные технологии.

Библиографическое описание: Полякова Т.А., Акулова Е.В. Развитие законодательства в области обеспечения информационной безопасности: тенденции и основные проблемы // Право. Журнал Высшей школы экономики. 2015. № 3. С. 4–17.

JEL: K 10; УДК: 349

Интенсивность развития информационных технологий при переходе человечества на кардинально новую стадию развития — эпоху глобального информационного общества, внедрение во все сферы жизнедеятельности человека такого феноменального изобретения как Интернет, приводит к возникновению новых вызовов и угроз, связанных с противоправным использованием достижений в области информационных технологий. В связи с этим актуальность проблем обеспечения информационной безопасности как на национальном уровне в рамках отдельных государств, так и международной информационной безопасности (далее — МИБ), в настоящее время признается всем мировым сообществом. В условиях глобализации и информационного развития общества, как справедливо отмечает И.Л. Бачило, усиливаются импульсы активизации международного права. Крепнет идея формирования планетарного права — выработки и обязательности соблюдения всеобщих правовых норм[1].

Кроме того, глобализация и широко раскинувшиеся по всему миру сети «паутины-Интернета» размывают государственные границы. Информационное пространство сегодня не ограничено территорией только одного государства, объединений государств и даже целых континентов, что вызывает необходимость выработки кардинально новых подходов к правовому регулированию общественных отношений, возникающих в настоящее время во всех сферах жизнедеятельности.

В Российской Федерации государственная политика в области обеспечения международной информационной безопасности нашла отражение в документе стратегического характера, в котором определены основные угрозы в области МИБ, цели, задачи и приоритетные направления государственной политики в указанной сфере. Таким документом стратегического планирования являются Основы государственной политики в области обеспечения международной информационной безопасности до 2020 года[2] (далее — Основы государственной политики).

Учитывая многоаспектность и глобальность понятия МИБ, важно определить, что оно в себя включает. В указанном документе содержится понятие МИБ — это состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

[1] *Бачило И.Л.* Информационное право: Учебник для магистров. М. : Изд-во Юрайт, 2013. 564 с.

[2] Утв. Президентом Российской Федерации 24 июля 2013 г. № Пр-1753 // СПС КонсультантПлюс.

При этом особенно важно отметить, что цель государственной политики Российской Федерации заключается в содействии установлению международного правового режима, направленного на создание условий для формирования системы МИБ. Таким образом, очевидна актуальность развития международного информационного права как части системы международного права. Одной из основных задач, способствующих достижению указанной цели, является формирование системы МИБ не только в глобальном масштабе, но и на двустороннем, многостороннем, региональном уровнях на основе применения международно-правовых механизмов и средств.

В целях реализации намеченного в Основах государственной политики курса развития международных отношений в области информационной безопасности в 2014–2015 годах продолжалась активная работа в многостороннем и двустороннем форматах, и несмотря на введение европейскими странами санкционной политики в отношении России, характеризующейся отменой и отложением ряда намеченных консультаций по вопросам информационной безопасности, Россия продолжает активное взаимодействие по вышеназванным направлениям в рамках таких международных организаций, как БРИКС, ШОС, ОДКБ, СНГ.

В условиях сложных политических отношений, складывающихся с США и странами Европы, на первый план выходит необходимость укрепления взаимоотношений в иных международных форматах, а в век высоких технологий, характеризующийся возможностью ведения войны и в киберпространстве, особенное внимание при заключении союзных договоренностей следует уделять вопросу обеспечения МИБ. Например, согласно Концепции участия России в объединении БРИКС, утвержденной Президентом Российской Федерации 9 февраля 2013 г., одной из основных целей сотрудничества с государствами-участниками БРИКС по вопросам международной безопасности является сотрудничество в интересах обеспечения МИБ, а также использование возможностей БРИКС для продвижения инициатив в этом направлении в рамках различных международных форумов и организаций, прежде всего ООН, укрепление в формате БРИКС сотрудничества в области противодействия использованию информационно-коммуникационных технологий в военно-политических, террористических и криминальных целях, а также целях, противоречащих обеспечению мира, стабильности и безопасности[3].

В целях реализации намеченного в Концепции политического курса в июле 2014 г. благодаря инициативе России в Итоговой декларации 6-го саммита БРИКС (г. Форталеза) закреплены два раздела, посвященные вопросам МИБ и интернационализации управления Интернетом. Государства-участники отразили намерение сотрудничать друг с другом в выявлении возможностей для осуществления совместных действий по решению общих проблем безопасности в сфере использования информационно-коммуникационных технологий, а также приняли во внимание и отметили российское предложение о необходимости выработки консолидированной позиции по данному вопросу, совместной разработке соглашения между странами БРИКС о сотрудничестве в области обеспечения международной информационной безопасности. Однако декларативное отражение стремления государств-участников БРИКС заключить международное соглашение по вышеназванному вопросу не должно являться конечной точкой, в связи с чем открывается широкий фронт работ в организационной и правовой сферах по выработке согласованной позиции, которая бы удовлетворяла интересам каждой из сторон соглашения.

[3] Концепция участия Российской Федерации в объединении БРИКС, утв. Президентом Российской Федерации // СПС КонсультантПлюс.

В форматах таких международных организаций как ШОС, ОДКБ, СНГ и др. в разное время были также заключены многосторонние международные соглашения в области обеспечения МИБ (Соглашение между правительствами государств-членов Шанхайской организации о сотрудничестве в области обеспечения международной информационной безопасности[4] (Екатеринбург, 16 июня 2009 г.), Положение о сотрудничестве государств-членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности[5] (Москва, 10 декабря 2010 г.), подписано распоряжение Правительства Российской Федерации от 15 ноября 2013 г. № 2120-р о подписании Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности[6], в 2014 г. велась активная работа по содействию вступлению в силу данного Соглашения, а 4 июня 2015 г. оно вступило в силу для Российской Федерации, Республики Беларусь и Республики Таджикистан.

Еще одним итогом реализации государственной политики в области международной информационной безопасности стало представление на 69-й сессии Генеральной Ассамблеи ООН от имени государств-членов ШОС в качестве официального документа ООН обновленной редакции Правил поведения в области обеспечения международной информационной безопасности (далее — Правила поведения) — документа, являющегося серьезным шагом на пути формирования культуры информационной безопасности, новая редакция которого отличается от концепций, предполагающих регулирование кибервойн, миротворческим характером, нацеленным на предотвращение конфликтов в информационной пространстве.

Обновленная редакция «Правил поведения» отличается от предыдущей расширенным разделом о правах человека, наличием отдельного пункта, посвященного вопросам интернационализации управления сетью Интернет, а также вниманием к проблематике «наращивания потенциала» в сфере информационной безопасности и оказания развивающимся странам содействия в преодолении «цифрового разрыва»[7].

Немаловажным аспектом в вопросе обеспечения информационной безопасности является то, что формирование глобального информационного общества и стремительное развитие интеграции влекут за собой необходимость расширения договорно-правовой базы межгосударственного сотрудничества. Способствовать разработке общих правил применения норм в информационной сфере, в первую очередь, может создание единого для участников межгосударственных образований подхода в области правового регулирования — гармонизация и унификация законодательства государств-членов союзных государств. Подтверждением актуальности такого вопроса является позиция И.Л. Бачило: «…главной задачей при обеспечении отношений и информационного взаимодействия в отдельно взятом государстве, в союзном государстве, в союзе государств или иной форме согласования интересов остается проблема гармонизации законодательства стран-участниц по тем позициям, которые определяют развитие экономики, социальной и культурной жизни, управления общими делами»[8].

---

[4] Бюллетень международных договоров. 2012. № 1. С. 13–21.

[5] Решение о Положении о сотрудничестве государств-членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности // СПС КонсультантПлюс.

[6] Официальный Интернет-портал правовой информации // http://www.pravo.gov.ru (дата обращения: 01.07.2015)

[7] Официальный сайт Министерства иностранных дел Российской Федерации // http://www.mid.ru (дата обращения: 01.07.2015)

[8] *Бачило И.Л.* Указ.соч.

Осознавая потребность приведения к единообразию законодательных баз союзных государств в рамках организации СНГ на 38-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ 23 ноября 2012 г. были приняты Рекомендации по совершенствованию и гармонизации национального законодательства государств-участников СНГ в сфере обеспечения информационной безопасности[9]. Целью Рекомендаций является установление общих подходов государств-участников СНГ к правовому регулированию обеспечения информационной безопасности, укреплению и обеспечению сбалансированности национальных правовых систем в условиях информатизации общества, а также направленные на развитие международного информационного обмена, обеспечение безопасности информационных условий экономического и таможенного сотрудничества, на стимулирование использования информационно-коммуникационных технологий в социальной и культурной сфере.

Постановлением Парламентской Ассамблеи Организации Договора о коллективной безопасности от 27 ноября 2014 г. № 7-6 (Санкт-Петербург) были приняты аналогичные вышеуказанным Рекомендации по сближению и гармонизации законодательства государств-членов ОДКБ.

Принятие данных актов свидетельствует, что в эпоху формирования глобального информационного общества государствам следует развивать свой правовой потенциал в области обеспечения информационной безопасности ориентируясь на достижения и успехи более развитых в этой области стран, а государствам, состоящим в союзных организациях, также следует приводить национальную законодательную базу к общему знаменателю, упрощая тем самым сотрудничество и взаимодействие в информационной сфере на трансграничном уровне. По нашему мнению, верным является утверждение, что в современных странах первоочередное значение приобретает интеграция национального и международного информационного законодательства, поскольку применение правовых норм только своей страны может привести к частичной или полной изоляции государства на международной арене[10]. В связи с этим полагаем, что упомянутые Рекомендации должны учитываться при разработке новых документов стратегического планирования в области информационной безопасности в РФ, поскольку действующая в настоящее время Доктрина информационной безопасности была утверждена 9 сентября 2000 г.

Важным шагом международно-правового сотрудничества в области формирования общих подходов к проблематике МИБ стали заключенные между Правительством Российской Федерации и Правительством Республики Куба двустороннее Соглашение о сотрудничестве в области обеспечения МИБ[11] (Гавана, 11 июля 2014 г.), вступившее в силу 2 января 2015 г., а также аналогичное Соглашение с Правительством Республики Беларусь[12] (Москва, 25 декабря 2013 г.), вступившее в силу 27 февраля 2015 г. Государствами-участниками обозначены основные угрозы МИБ, определены основные направления, общие принципы, формы и механизмы сотрудничества, что, несомненно, выводит на

[9] Информационный бюллетень. Межпарламентская Ассамблея государств-участников СНГ. 2013. № 57 (часть 2). С. 162–179.

[10] *Булгакова Е.С, Акимов В.С.* Материалы международной научно-практической конференции «Актуальные вопросы правового регулирования использования информационных ресурсов в сети «Интернет». М.: РПА Минюста России, 2014. С. 68.

[11] Официальный Интернет-портал правовой информации // http://pravo.gov.ru (дата обращения: 14.01.2015)

[12] Там же.

новый уровень отношения государств в данной сфере и вместе с тем создает нормативно-правовую базу для практического взаимодействия.

Но особенно следует отметить важность развития международно-правовых отношений в данной сфере с КНР. 8 мая 2015 г., руководствуясь положениями Договора о добрососедстве, дружбе и сотрудничестве между Российской Федерацией и Китайской Народной Республикой[13] от 16 июля 2001 г., подписанного в Москве, между Правительствами Российской Федерации и Китайской Народной Республики также заключено Соглашение о сотрудничестве в области МИБ[14], которое вступит в силу после соблюдения всех необходимых процедур, предусмотренных данным Соглашением.

В вышеуказанном Соглашении государства определили особое значение совместной работы в рамках ШОС, а также необходимость дальнейшего углубления доверия и развития взаимодействия в области использования информационно-коммуникационных технологий, отметили стремление формировать многостороннюю, демократическую и прозрачную международную систему управления информационно-коммуникационной сетью Интернет в целях реальной интернационализации управления сетью Интернет и обеспечения равных прав государств на участие в этом процессе, включая демократическое управление основными ресурсами информационно-коммуникационной сети Интернет и их справедливое распределение. Как справедливо отмечает М. Касенова, сегодня Интернет интегрирует материальные, финансовые, интеллектуальные, социальные и иные ресурсы, влияет на национальные и международные процессы и обеспечивает коммуникационные связи в планетарном масштабе, в связи с чем вопросы управления Интернетом не могут рассматриваться и решаться вне глобального контекста[15].

Вопрос об интернационализации управления Интернетом уже давно обсуждается, носит дискуссионный характер и по-разному воспринимается — от полного неприятия до всесторонней поддержки. В связи с этим следует отметить особое значение продвижения инициатив России, связанных с принятием в ООН проекта Конвенции об обеспечении МИБ, концепция которой стала результатом многолетней работы российских экспертов в области МИБ во взаимодействии с нашими зарубежными коллегами. В современных политических условиях необходимо закрепить в международном правовом акте положения концепции Конвенции, определяющие правила поведения в киберпространстве, а также касающиеся интернационализации системы управления Интернетом. Требует международно-правового закрепления принцип невмешательства в информационное пространство друг друга и право каждого государства устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством, обязанность государств защищать свободу слова в Интернете[16].

Представляется, что не только указанные международные правовые документы свидетельствуют об определенных шагах, направленных на реализацию государственной политики в данной области, но и развитие национального законодательства в Россий-

---

[13] Бюллетень международных договоров. 2002. № 8. С. 56–62.

[14] Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // СПС КонсультантПлюс.

[15] *Касенова М.Б.* Трансграничное управление Интернетом: основные термины и понятия // Юридический мир. 2014. № 2 С. 58–63.

[16] Официальный сайт Совета Безопасности Российской Федерации // http://www.scrf.gov.ru/documents/6/112.html (дата обращения: 01.07.2015)

ской Федерации, в котором в 2014–2015 гг. уже произошли значительные изменения, направленные на его модернизацию.

Сегодня в России базовым документом по планированию развития системы обеспечения национальной безопасности, в котором излагаются порядок действий и меры по обеспечению национальной безопасности, определяющим, что национальная безопасность страны существенным образом зависит в том числе и от обеспечения информационной безопасности, является Стратегия национальной безопасности Российской Федерации до 2020 года[17]. Вместе с тем в сфере информационной безопасности основным политико-правовым документом, представляющим совокупность официальных взглядов на цели, задачи, принципы и направления обеспечения информационной безопасности России, как уже отмечалось, остается Доктрина информационной безопасности Российской Федерации[18]. В настоящее время реализуется курс на формирование и развитие информационного общества, определенный в Стратегии развития информационного общества Российской Федерации[19].

В 2013 г. распоряжениями Правительства России утверждены планы мероприятий, так называемые «дорожные карты» «Повышение качества регуляторной среды для бизнеса» (11.06.2013 № 953-р (в ред. от 17.08.2013)) и «Развитие отрасли информационных технологий» 20.07.2013 № 1268-р, в которых также отражены актуальные организационно-правовые вопросы, связанные с обеспечением информационной безопасности. Следует отметить, что впервые не распоряжением, а постановлением Правительства России от 15 апреля 2014 г. № 313 была утверждена новая редакция государственной программы «Информационное общество»[20], в которой особое внимание уделено вопросам безопасности в информационном обществе.

Сегодня уже не вызывает сомнения и актуальность реализации мероприятий по созданию отечественных операционных систем, защищенных технологий хранения и обработки информации. Очевидно, что ужесточение геополитического противоборства вызывает серьезные угрозы и в сфере информационной безопасности. В настоящее время в государственных органах власти активно обсуждаются вопросы снижения зависимости функционирования сети Интернет от элементов его инфраструктуры, которые находятся под управлением зарубежных компаний и обусловлены проводимой ими политикой.

В целях противодействия угрозам информационной безопасности России при использовании информационно-телекоммуникационной сети Интернет Указом Президента Российской Федерации от 22 мая 2015 г. № 260[21] предписано преобразовать сегмент международной компьютерной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении Федеральной службы охраны, в российский государственный сегмент сети Интернет, обеспечивающей подключение к сети Интернет предназначенных для взаимодействия с ней государственных информационных систем и информацион-

[17] Утв. Указом Президента Российской Федерации 12 мая 2009 г. № 537 // СПС КонсультантПлюс.

[18] Утв. Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895 // Российская газета. 2000. № 187.

[19] Утв. Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 // Российская газета. 2008. № 34.

[20] Утв. постановлением Правительства Российской Федерации от 15.04.14 № 313 / Официальный Интернет-портал правовой информации // http://www.pravo.gov.ru (дата обращения: 24.04.2014)

[21] СЗ РФ. 2015. № 21. Ст. 3092.

но-телекоммуникационных сетей государственных органов, а также информационных систем и информационно-телекоммуникационных сетей организаций, созданных для выполнения задач, поставленных перед федеральными государственными органами. Данным Указом также утверждается порядок подключения информационных систем и информационно-телекоммуникационных сетей к Интернету и размещения (публикации) в ней информации через российский государственный сегмент Интернета.

Одной из проблем обеспечения информационной безопасности до недавнего времени оставалось размещение на зарубежных серверах сайтов государственных органов и учреждений, муниципальных образований, что в свою очередь не исключает вероятности уничтожения, блокировки, изменения информации на официальных сайтах, которые не могут быть оперативно устранены и останутся фактически безнаказанными[22]. На решение указанной проблемы направлены вступившие с 1 июля 2015 г. в силу изменения в ст. 13, 14 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[23] (далее — Федеральный закон № 149-ФЗ), согласно которым технические средства информационных систем, используемых государственными органами власти, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или учреждениями, должны размещаться на территории России. С 1 сентября 2015 г. вступают в силу изменения в Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[24], предусматривающие, что запись, накопление и хранение персональных данных россиян разрешаются только на территории Российской Федерации.

Также пристального внимания в целях обеспечения информационной безопасности заслуживают вопросы импортозамещения. В условиях риска введения масштабных санкций, которые могут быть связаны с остановкой предоставления услуг по поддержке программного обеспечения, используемого в Российской Федерации, Минкомсвязи России утвердил План импортозамещения программного обеспечения[25], в соответствии с которым отечественному программному обеспечению при осуществлении закупок за государственный счет предполагается предоставление преференций. Однако наряду с созданием отечественных аналогов западной продукции, по нашему мнению, особенного внимания заслуживают вопросы разработки и создания нового и перспективного программного обеспечения на основе имеющегося научно-технического потенциала страны, и обеспечения конкурентоспособности отечественных разработок на мировом рынке, что возможно при непосредственном участии России в разработке международных стандартов, а также на основе кооперации с зарубежными ИТ-компаниями союзных государств БРИКС и ШОС.

Одним из приоритетных направлений российской государственной политики в области обеспечения информационной безопасности, связанных с преодолением негативных последствий санкционной политики в отношении России, является создание национальной системы платежных карт (далее — НСПК). Новым импульсом для продвижения и реализации этого проекта послужил инцидент, произошедший в финансово-кредитной сфере в марте 2014 г. и связанный с блокировкой без предварительного

[22] Пояснительная записка «К проекту Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации // СПС КонсультантПлюс.

[23] Российская газета. 2006. № 165.

[24] Там же.

[25] Утв. Приказом Минкомсвязи России от 1 апреля 2015 г. № 96 // СПС КонсультантПлюс.

уведомления международными платежными системами VISA и MasterCard расчетов по картам четырех российских банков. Уже в феврале 2015 г. НСПК начала работу, обозначенную подключением к ней пяти первых операторов. Несмотря на то, что имеются определенные проблемы, которые требуют дальнейшей проработки (преимущественная доля программного обеспечения импортного производства, отсутствие ряда положений по реализации мер по борьбе с киберпреступностью), нельзя не отметить наметившуюся в связи с принятием Федерального закона от 27 июня 2006 г. № 161-ФЗ «О национальной платежной системе»[26] позитивную тенденцию в области обеспечения информационной безопасности банковской сферы.

Важно отметить, что Центральный банк России наряду с федеральными органами исполнительной власти, осуществляющими управление в области обеспечения безопасности, указанным Федеральным законом наделен правом нормативного регулирования в области информационной безопасности. Банком России, в свою очередь, на этапе построения НСПК были предъявлены особые требования к информационной безопасности национальной платежной системы (предъявление определенных условий при использовании иностранного оборудования), поскольку в информационной платежной системе ЦБ России, а также информационных платежных системах кредитно-финансовых организаций хранятся и обрабатываются значительные объемы информации, прекращение или нарушение функционирования которых может повлечь негативные последствия для государства и общества. Безусловно, совокупность таких систем можно отнести к критической информационной инфраструктуре.

В связи с этим особенного внимания заслуживает разработка и принятие законопроекта «О безопасности критической информационной инфраструктуры», направленного на создание правового фундамента для регулирования этого вопроса, что будет способствовать защите критической информационной инфраструктуры от ущерба, который может повлечь за собой серьезные и даже катастрофические последствия.

С 2014 г. в нормотворческой деятельности по реализации государственной политики в области обеспечения информационной безопасности наметились и другие положительные тенденции, такие как внесение изменений в отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей. Так, в 2014 г. в Федеральный закон № 149-ФЗ внесены в качестве дополнения новые статьи 10.1, 10.2 и 15.4, в соответствии с которыми определяются перечень обязанностей организатора распространения информации в сети Интернет, особенности распространения блогером общедоступной информации, а также порядок ограничения доступа к информационному ресурсу организатора распространения информации в сети Интернет, что в свою очередь способствует обеспечению информационной безопасности пользователей Интернета[27].

Кроме того, согласно статье 15.1 Закона об информации в целях ограничения доступа к сайтам в сети Интернет, содержащим информацию, распространение которой в России запрещено, создана 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». В указанный реестр в соответствии с критериями и правилами, утвержденным Правительством России, включаются домен-

[26] Российская газета. 2011. № 139.

[27] СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448.

ные имена и (или) указатели страниц сайтов в сети Интернет, содержащие информацию, распространение которой в России запрещено, а также сетевые адреса, позволяющие идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в России запрещено. Полномочия по созданию, формированию и ведению реестра сегодня возложены на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций — Роскомнадзор.

Важно отметить, что с 1 мая 2015 г. вступила в силу ст. 15.6, определяющая порядок ограничения доступа к сайтам в сети Интернет, на которых неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет. С 1 сентября 2015 г. начинает действовать ст. 15.5 указанного Федерального закона, устанавливающая порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства России в области персональных данных. Редакцией этой статьи предусматривается введение ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, а также создание Роскомнадзором автоматизированной информационной системы «Реестр нарушителей прав субъектов персональных данных».

Такие изменения обусловлены потребностью в обеспечении безопасности персональных данных, используемых в различных информационных системах. Важно отметить, что в России завершена почти семилетняя процедура, связанная с ратификацией одного из актуальнейших международных правовых актов в области защиты прав человека в процессе использования современных информационно-коммуникационных технологий — Конвенции о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.). Таким образом, сделан значительный шаг на пути к полноформатному участию России в усилиях государств-членов Совета Европы по укреплению безопасности человека в киберпространстве и общеевропейском правовом пространстве. Однако процесс модернизации указанной Конвенции, в котором Россия задействована в качестве полноправного участника, все еще продолжается, чем и вызвано динамичное развитие подзаконных актов Правительства России и федеральных органов исполнительной власти.

Еще одной актуальной проблемой в области информационного права является защита авторских и смежных прав. Как верно отмечено в работе Б.Н. Мирошникова, «авторское право, действующее сегодня повсеместно в мировом масштабе (с различными национальными вариациями) складывалось веками в развитых странах, и только-только зарождается в развивающихся. Все бы ничего, но Интернет вывел всех на единый уровень плоскости мирового информационного пространства и явился источником большой мировой проблемы в 21-м веке… Благодаря Интернету убытки правообладателей астрономически огромны — в литературе, музыке, программном обеспечении и так далее»[28].

Вопросы, связанные с попыткой защитить субъектов авторских и смежных с ними прав от незаконного использования результатов их деятельности отражены в новой ст. 15.2 (введена в действие в 2013 г.) Закона об информации, закрепляющей порядок ограничения доступа к информации, распространяемой с нарушением исключительных прав на фильмы, в том числе кинофильмы, телефильмы, согласно которой правооб-

[28] *Мирошников Б.Н.* Сетевой фактор. Интернет и общество. Взгляд. М.: Инфорос, 2012. 208 с.

ладатель в случае обнаружения фильмов (кинофильмов, телефильмов) в информационно-телекоммуникационных сетях, включая сеть Интернет, которые распространяются без его разрешения или иного законного основания, вправе обратиться в Роскомнадзор с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такие фильмы или информацию, на основании вступившего в силу судебного акта. Принятие таких изменений (так называемого «антипиратского закона») получило широкий отклик, а в процессе прохождения процедуры общественного обсуждения данного законопроекта активно вносились предложения по совершенствованию ст. 15.2 Закона об информации и расширению сферы ее действия. С 1 мая 2015 г. вступили в силу изменения, согласно которым ныне действующий порядок ограничения доступа к информации распространяется на все объекты авторских и смежных прав, кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии, а в новой ст. 15.7 Закона об информации предусмотрены внесудебные меры по предотвращению нарушения авторских и (или) смежных прав в информационно-телекоммуникационных сетях, в том числе сети Интернет, принимаемые по заявлению правообладателя.

В рамках данной статьи следует также отметить важность проблемы обеспечения информационной безопасности при использовании облачных вычислений и утверждения необходимых стандартов безопасности облачных сред и инструментов измерения уровня рисков и угроз. Правовые вопросы обеспечения информационной безопасности при использовании «облачных» технологий являются, несомненно, актуальными и, по нашему мнению, которое также поддерживается в монографии А.В. Морозова и Т.А. Поляковой, «заслуживают особого внимания, поскольку использование «облачных» вычислений становится все более популярным и выгодным, а сами «облачные» вычисления уже выделяются в отдельную область рынка информационных технологий. При этом очевидно, что пропорционально стремительному росту возможностей данных технологий и очевидным преимуществам использования данного вида технологий растет также количество новых рисков и угроз информационной безопасности технологического, организационного и правового характера. Это подтверждает и заявление, сделанное в конце 2012 г. экспертами компании *Trend Micro*, одного из лидирующих поставщиков комплексных средств защиты «облаков», что имеющиеся сегодня средства безопасности пока не способны защитить данные в «облачных» инфраструктурах»[29].

Особого внимания заслуживает широкое применение информационно-коммуникационных технологий в судебной системе, в частности, использование «облачных вычислений», что предусмотрено Федеральной целевой программой «Развитие судебной системы России на 2013–2020 годы», утвержденной Правительством России в декабре 2012 г. В настоящее время активно идет реформа судебной системы, готовятся изменения в процессуальное законодательство, связанные с использованием электронных документов и применением электронной подписи (соответствующие изменения внесены Федеральным конституционным законом от 8 июня 2015 г. № 5-ФКЗ «О внесении изменений в Федеральный конституционный закон «О Конституционном Суде Российской Федерации»).

Однако следует признать, что основным сдерживающим фактором при использовании облачных технологий в деятельности государственных органов, а также более широкого их распространения в целом, является недостаточное урегулирование основных правил использования облачных технологий, в частности, касающихся обеспе-

[29] *Морозов А.В., Полякова Т.А.* Организационно-правовое обеспечение информационной безопасности. М.: РПА Минюста России, 2013. 276 с.

чения безопасности и конфиденциальности информации, передаваемой поставщику облачных услуг (в законодательстве не закреплены нормы, определяющие административную и гражданско-правовую ответственность поставщика облачных услуг, а также ответственность руководителей и работников организаций, оказывающих облачные услуги). Указанные тенденции развития законодательства в области обеспечения информационной безопасности безусловно разнообразны и разноплановы, нередко находятся на стыке различных специальностей как в области права, так и информационных технологий и нуждаются в научных исследованиях, связанных с обеспечением информационной безопасности.

Еще одним серьезным направлением на пути к построению системы обеспечения информационной безопасности является подготовка высококвалифицированных кадров. В связи с этим представляется совершенно верным вывод, изложенный в статье Т.А. Поляковой и А.И. Химченко, что «наиболее целесообразными способами повышения уровня компетенций в Российской Федерации в сфере информационной безопасности являются целенаправленная подготовка высококвалифицированных специалистов в специализированных учебных заведениях, а также непрерывный процесс развития общих навыков грамотности, культуры при обращении со служебной и личной информацией (особое место занимают персональные данные) и трансграничности, а также пропагандой политики безопасности в указанной сфере»[30].

Обеспечение перечисленных приоритетных, по мнению авторов, направлений обеспечения информационной безопасности составляет теоретическую и практическую основу для развития национального и международного информационного права, а также непосредственного формирования системы международной информационной безопасности.

Библиография

Бачило И.Л. Информационное право. 3-е изд.. М.: Юрайт, 2013. 564 с.

Бачило И.Л. Правовая платформа построения электронного государства // Информационное право. 2008. № 4. С. 41–45.

Булгакова Е.С, Акимов В.С. Интеграция национального и международного информационного законодательства // Материалы международной научно-практической конференции «Актуальные вопросы правового регулирования использования информационных ресурсов в сети «Интернет»». М.: РПА Минюста России, 2014. С. 67–71.

Касенова М.Б. Трансграничное управление Интернетом: основные термины и понятия // Юридический мир. 2014. № 2. С. 58–63.

Мирошников Б.Н. Сетевой фактор. Интернет и общество. М.: Инфорос, 2012. 208 с.

Морозов А.В., Полякова Т.А. Организационно-правовое обеспечение информационной безопасности: монография. М.: РПА Минюста России, 2013. 276 с.

Морозов А.В. Правовое обеспечение информационной безопасности. М.: РПА Минюста России, 2012. 346 с.

Полякова Т.А. Совершенствование информационного законодательства в условиях перехода к информационному обществу // Журнал российского права. 2008. № 1. С. 62–69.

Полякова Т.А., Химченко А.И. Актуальные организационно-правовые вопросы трансграничной передачи персональных данных // «Право». Журнал Высшей школы экономики. 2013. № 1. С. 113–122.

[30] *Полякова Т.А., Химченко А.И.* Особенности подготовки кадров в области организационно-правового обеспечения информационной безопасности» // Информационное право. 2013. № 3. С. 21–23.

Полякова Т.А., Химченко А.И. Особенности подготовки кадров в области организационно-правового обеспечения информационной безопасности // Информационное право. 2013. № 3 С. 21–23.

Талимончик В.П. Всемирный саммит по информационному обществу в развитии международного информационного обмена // Информационное право. 2006. № 2. С. 3–6.

Терещенко Л.К. Модернизация информационных отношений и информационного законодательства: монография. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, ИНФРА-М, 2013. 227 с.

Тихомиров Ю.А. Международно-правовые акты: природа и способы влияния // Журнал российского права. 2002. № 1 // http://www.center-bereg.ru/o5845.html (дата обращения: 01.05.2015)

Федеральный справочник «Национальная безопасность России». Т.1. М.: Центр стратегического партнерства, 2014. 566 с.

Шерстюк В.П. Угроза международной информационной безопасности в условиях формирования глобального информационного общества и направления сотрудничества // Право и безопасность. 2010. № 4 (37). http://dpr.ru/pravo/pravo_33_8.htm (дата обращения: 01.05.2015)

The Development of Legislation in the Field of Information Security: Trends and Key Issues

Tat'ana A. Polyakova

Professor, Moscow State University of Justice, Head, Information Law Centre, Institute of State and Law, Doctor of Juridical sciences, Merited Lawyer of the Russian Federation. Address: 69 Novocheremushkinskaya Str., Moscow, 117418, Russian Federation. E-mail: polyakova_ta@mail.ru

Elena V. Akulova

Postgraduate student, Department of Information Law, Informatics and Mathematics, All-Russia State University of Justice. Address: 2/1 Azovskaya Str., Moscow, 117638, Russian Federation. E-mail: akulova_ev@rambler.ru

Abstract

The subject matter of this article is the process of forming legal system of international information security and information security within the framework of the RF legislation. The relevance of this topic is due to the fast development of the global information space and the Information system development in all spheres of society, as well as the challenging political situation in the world, which contributes to the emergence of challenges and threats to information security. The steady increase in such threats is the need to build an effective system of international information security, improvement of national legislation in this field. In this context, the authors examine the trends in the development of legislation, public policy in the field of information security, and identify the most topical problems and issues of scientific research. The purpose of this research is shaping the system of international information security and modernization of Russian law in the field of information security, and making up a number of provisions to facilitate the implementation of public policy of the Russian Federation in the field of information security. The methodological basis of scientific methods of knowledge include: deductive, comparative legal, formal-legal techniques and methods of system analysis. One of the main conclusions of the paper is the need to expand the legal framework of international cooperation as well as the development of common rules of standards in the field of information, creation of a single participants interstate formations approach in the field of legal regulation — harmonization and unification of legislation of the members of union states, integration to the RF legislation of the recommendations set out in international instruments.

Keywords

national security, Information space, information society, information technology, International information security, critical information infrastructure, the state policy of the Russian Federation, personal data, cloud technologies

Citation: Polyakova T.A., Akulova E.V. (2015) The Development of Legislation in the Field of Information Security: Trends and Key Issues. *Pravo. Zhurnal Vysshey shkoly ekonomiki,* no 3, pp. 4–17 (in Russian)

References

Bachilo I.L. (2013) *Informatsionnoe pravo* [Information Law]. Moscow: Yurayt, 564 p. (in Russian)

Bachilo I.L. (2008) Pravovaya platforma postroeniya elektronnogo gosudarstva [Legal Platform to Build Electronic State]. *Informatsionnoe pravo,* no 4, pp. 41–45.

Bulgakova E.S, Akimov V.S. (2014) Integratsiya natsional'nogo i mezhdunarodnogo informatsionnogo zakonodatel'stva. Materialy mezhdunarodnoy konferentsii [The Integration of National and International Information Legislation. Proceedings of the International Research Conference «Problems of Legal Regulation in Applying Information Resources on the Internet»]. Moscow: Russian Legal Academy, pp. 67–71.

Kasenova M.B. (2014) Transgranichnoe upravlenie Internetom: osnovnye terminy i ponyatiya [Transborder Administration of the Internet: Terms and Concepts]. *Yuridicheskiy mi*r, no 2, pp. 58–63.

Miroshnikov B.N. (2012) *Setevoy faktor. Internet i obshchestvo. Vzglyad*. [Net Factor. The Internet and Society. Glance]. Moscow: Inforos, 208 p. (in Russian)

Morozov A.V., Polyakova T.A. (2013) *Organizatsionno-pravovoe obespechenie informatsionnoy bezopasnosti: monografiya* [Organizational and Legal Support of Information Security]. Moscow: Russian Legal Academy, 276 p. (in Russian)

Morozov A.V. (2012) *Pravovoe obespechenie informatsionnoy bezopasnosti : uchebnoye posobie* [Legal Support of Information Security. Manual]. Moscow: Russian Legal Academy, 346 p. (in Russian)

Polyakova T.A. (2008) Sovershenstvovanie informatsionnogo zakonodatel'stva v usloviyakh perekhoda k informatsionnomu obshchestvu [Improving Information Legislation on the Way to Information society]. *Zhurnal rossiyskogo prava*, no 1, pp. 62–69.

Polyakova T.A., Khimchenko A.I. (2013) Aktual'nye organizatsionno-pravovye voprosy transgranichnoy peredachi personal'nykh dannykh [Organizational and Legal Issues of Cross-Border Transfer of Personal Data]. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 1, pp. 113–122.

Polyakova T.A., Khimchenko A.I. (2013) Osobennosti podgotovki kadrov v oblasti organizatsionno-pravovogo obespecheniya informatsionnoy bezopasnosti [Preparing the Personnel for Organizational and Legal support of Information Security]. *Informatsionnoe pravo*, no 3, pp. 21–23.

Talimonchik V.P. (2006) Vsemirnyy sammit po informatsionnomu obshchestvu v razvitii mezhdunarodnogo informatsionnogo obmena [International Summit on Information Society in the Development of the International Information Exchange]. *Informatsionnoe pravo*, no 2, pp. 3–6.

Tereshchenko L.K. (2013) *Modernizatsiya informatsionnykh otnosheniy i informatsionnogo zakonodatel'stva: monografiya* [Modernization of Information Relations and Information Legislation. Monograph]. Moscow: INFRA-M, 227 p. (in Russian)

Tikhomirov Yu.A. (2002) Mezhdunarodno-pravovye akty: priroda i sposoby vliyaniya [International Law Acts: Nature ans Ways of Influence]. *Zhurnal rossiyskogo prava*, no 1. Available at: // http://www.center-bereg.ru/o5845.html (accessed: 01 May 2015).

Federal'nyy spravochnik. Natsional'naya bezopasnost' Rossii. (2014) T. 1 [Federal Reference Book. National Security of Russia. Vol. 1]. Moscow: Tsentr strategicheskogo partnerstva. 566 p. (in Russain)

Sherstyuk V.P. (2010) Ugroza mezhdunarodnoy informatsionnoy bezopasnosti v usloviyakh formirovaniya global'nogo informatsionnogo obshchestva i napravleniya sotrudnichestva [Threat to the International Information Security and shaping Global Information Society]. *Pravo i bezopasnost'*, no 4 (37). Available at: http://dpr.ru/pravo/pravo_33_8.htm (accessed: 01 May 2015)