ГОСУДАРСТВО И ПРАВО, 2016, № 3, с. 66–77

ПРАВО И ИНФОРМАТИКА

НА ПУТИ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ПРОБЛЕМЫ ФОРМИРОВАНИЯ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ ПОЛИТИКИ И СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

© 2016 г. Иллария Лаврентьевна Бачило[1],
Татьяна Анатольевна Полякова[2]

В статье освещены проблемы формирования государственной информационной политики и совершенствования законодательства. Отмечается, что концепции, доктрины, стратегии обеспечения информационной безопасности обозначают масштаб возможных и реальных угроз для интересов и условий жизни государства, человека, общества.

In the article problems of formation of state information policy and improvement of legislation. It is noted that the concepts, doctrines, strategies of information security indicate the scope of possible governmental and real threats to the interests and conditions of life of the state, man and society.

Ключевые слова: *государственная информационная политика, законодательство, информационная безопасность, государство, инфокоммуникационные технологии.*

Key words: *public information policy, legislation, information security, government, information and communication technologies.*

1. Роль и значение информационной безопасности в развитии общества

Информационная безопасность осознается как социально значимая проблема по мере развития самого общества, смены технологической основы связи, передачи и использования информации. Приобретение опыта, знаний, передача их новым поколениям, охрана от соперников и врагов в борьбе за жизнь сопровождают всю историю человека и разных форм его ассоциаций (род, племя, семья; секреты производства, обмена, торговли, различных видов государственной власти).

Начало современного понимания проблем информационной безопасности коренится в этапах технического прогресса XIX–XX вв. от первых шагов в использовании электричества, телеграфа, телефона, радио, телевидения. Перелом произошел с момента создания и использования ЭВМ. Технологии сбора, обработки информации позволили осознать и использовать ее как особый объект социального, экономического, политического значения и как объект, используемый как продукт, формирующий свою специфику потребления и сегмент рынка. В середине XX в. на первом плане – конкуренция и защита от внешнего проникновения к сведениям их систем, о новых видах связи. Постепенное осознание самой информации как объекта обработки и потребления способствовало *постановке вопроса о праве на информацию, введении права на информацию в состав прав человека и гражданина в международных правовых актах и в национальном законодательстве государств*. Информация становится важнейшей частью свобод человека, защищаемых и гарантируемых конституционно. Как все более значимая часть современной экономики весь комплекс проблем инфокоммуникационного развития и сама информация становятся объектом потребления и составной частью рынка, особенно рынка интеллектуальной собственности и технологий.

Длительное время инфокоммуникационные технологии (ИКТ) и информация как ресурс обработки и спроса были объектом охраны и защиты техническими (физическими) средствами, что нашло отражение в законодательных актах. На их основе формировалось право на информацию,

[1] Главный научный сотрудник сектора информационного права Института государства и права РАН, доктор юридических наук, профессор, заслуженный юрист РФ (E-mail: inform@igpran.ru).
Illariya Bachilo, chief researcher of the information law Institute of state and law of RAS, Doctor of Law, Professor, honored lawyer of the Russian Federation (E-mail: inform@igpran.ru).

[2] Заведующая сектором информационного права Института государства и права РАН, доктор юридических наук, заслуженный юрист РФ (E-mail: inform@igpran.ru).
Tatiana Polyakova, head of sector of the information law Institute of state and law of RAS, Doctor of Law, honored lawyer of the Russian Federation (E-mail: inform@igpran.ru).

а в России и ряде других государств это стало предметом информационного права. Аналогом является законодательство о свободе информации англоязычных и других государств.

Осознание важности и широты изменений в области использования информации как знаний и источника развития всех направлений жизни социума, его зависимости от степени владения информационными, теле-, радио-, аудио-, спутниковыми и прочими технологиями сформулировало такие концепты, как "информационное общество", "электронное государство", "электронное правительство" (управление), "электронный гражданин", "электронное или компьютерное пространство", Интернет, киберпреступность и т.д. Рождение этих не сразу усваиваемых терминов отражает неуклонно развивающийся глобальный процесс сетевого оснащения планеты новыми технологиями и методами работы с информационными ресурсами. *Это – процесс информатизации общества и формирования нового этапа цивилизации, который именуется как "цифровая эпоха".*

В этих условиях общество приобретает новые глобальные характеристики и качества, становясь информационным обществом. Правовая наука информационного права определяет информационное общество как *"общество, создающее и использующее такой уровень инфокоммуникационных технологий, которые становятся самостоятельным социально-технологическим ресурсом жизнедеятельности и развития социума, существенно влияют на парадигмы смены его цивилизационной характеристики".* В этом направлении особенно активно работают такие международные акты, как Окинавская хартия глобального информационного общества, Орхудская конвенция о доступе к информации и др. Проблемы доступа к публичной информации обсуждаются во всем мире.

Опыт научных исследований, включая и проводимый в Институте государства и права РАН (ИГП РАН), подтверждает, что проблемы доступа к информации влекут за собой постановку вопроса *о расширении понятия гражданского общества при ориентации на главную роль человека в системе отношений организаций, граждан и органов государственной власти.* Такие тенденции сегодня отмечаются в целом ряде зарубежных государств. Так, Франция живет в условиях ориентации на "цифровую администрацию", в Германии вопрос об Интернете занимает первую строку в повестке дня во внутренней политике. В августе 2014 г. федеральный Кабинет министров Германии принял "Цифровую повестку дня 2014–2017". В России в 2008 г. также принята и действует Стратегия развития информационного общества до 2020 г. В ИГП РАН проблемы современного понимания и развития гражданского общества получили отражение в ряде публикаций и постоянно учитываются в работах по проблематике информационного общества[3].

В этой связи проблема защиты, охраны ИКТ и самой информации как объектов особой важности должна находиться в центре внимания правового регулирования отношений всех категорий и видов субъектов. Это объясняет, почему в системе безопасности *информационная безопасность* есть важная часть международной и государственной (национальной) безопасности. Данный принцип реализуется в государственной политике, находит свое отражение в законодательстве, как в системе государственных функций, так и в системах юридической ответственности. В сфере международных отношений это – один из трудных вопросов реализации государственного суверенитета и сохранения жизнеспособности социума.

2. Сфера и источники информационных угроз; инфраструктура обеспечения информационной безопасности

Концепции, доктрины, стратегии обеспечения информационной безопасности обозначают масштаб возможных и реальных угроз для интересов и условий жизни государства, человека, общества. Все направления противостояния угрозам и формам их реализации имеют системную связь и одновременно требуют учета специфики организационного, технического и правового обеспечения безопасности. На протяжении времени после Второй мировой войны состояние информационной безопасности претерпело существенные изменения.

Не обращаясь к вопросу истории детально, полезно ознакомиться с одной из последних работ политолога и юриста мирового масштаба Г. Киссинджера. В его работе "Мировой порядок", вышедшей в русском переводе в 2015 г.,

[3] См.: *Бачило И.Л.* Государство и право XXI в. Реальное и виртуальное. М., 2012; *Ее же.* Информационное право. Учеб. для магистров. М., 2009, 2013, 2015; Информационное общество и социальное государство / Сост. и отв. ред. И.Л. Бачило. Сб. науч. работ. М., 2011; Право цифровой администрации в России и во Франции. Сб. науч. материалов российско-французской конф., 27–28 февраля 2013 года. М., 2014; Демократические институты в условиях развития информационного общества / Отв. ред. И.Л. Бачило. Сб. науч. работ. М., 2014.

привлекает раздел *"Киберпространства мирового сообщества"*. Интересна глава "Мировой порядок и цифровые технологии" этой книги. Здесь автор рассматривает вопросы *цифровых технологий как фактор формирования нового пространства.* Говоря о процессах усвоения информационных технологий, он отмечает, что «человеческая деятельность становится все более и более цифровой, "квантифицируемой и подлежащей анализу"». И далее делает прогноз, что «к 2020 г. количество устройств, подключенных к Интернету, вырастет до пятидесяти миллиардов. "Всеобщий Интернет" ждет нас впереди. Каждый предмет должен быть подключен к Интернету и запрограммирован на связь с центральным сервером или с другими сетевыми устройствами»[4]. Неизбежны, указывает он, и "последствия этого культурного переворота для отношений между государствами". Г. Киссинджер пишет: "Политик решает множество задач… Он должен в первую очередь проанализировать текущее положение общества. По сути, здесь прошлое встречается с будущим; посему подобный анализ не может не учитывать обоих этих элементов. Затем он должен попытаться понять, куда ведет текущая траектория развития. Нужно устоять перед искушением отождествить политику с проецированием знакомого в будущее, поскольку это путь к стагнации и упадку" (с. 453).

Нельзя пройти и мимо такого его положения: «В эпоху Интернета мировой порядок часто приравнивается к утверждению, что если люди имеют возможность свободно получать и обмениваться информацией, то врожденное человеческое стремление к свободе рано или поздно реализует себя, а история будет двигаться "на автопилоте"» (с. 454). На этом пути немало препятствий. Динамика информационного развития "побуждает политиков ждать, пока проблема возникнет, а не предотвращать ее, воспринимать принятие решений как череду не связанных между собой событий, а не как часть исторического континуума. Когда это происходит, манипулирование информацией заменяет ее осмысление в качестве основного инструмента политики. Интернет лишает общество исторической памяти" (с. 456).

Если ориентироваться на реальную человеческую память, то нельзя забывать, что в отношении государства – победителя в Великой Отечественной войне и во Второй мировой войне – СССР уже в конце войны разрабатывались планы-препятствия нормальному развитию страны, затем готовилась и проводилась "холодная война" – откровенно информационная, но затрагивавшая все стороны национальной безопасности. Не утрачена и память о разрушении СССР и дальнейших планах реализации информационной политики Запада по программам 01 и затем 02 методами так называемой "мягкой силы". Все это уже с помощью использования телекоммуникаций, Интернета и всех доступных форм распространения информации, выгодной для заинтересованной стороны[5].

Планирование и реализация внешних информационных угроз в настоящее время имеют продолжение. Достаточно просмотра новостей в Интернете, не говоря уже о так называемой атаке "санкций" и пропаганды ложных причин их применения. Напомним и о других откровенных заявлениях, например сообщение в апреле 2015 г. в газете "Известия" о том, что на базе чешского офиса "Радио Свободы", финансируемого США, создадут цифровой медиодепартамент, задача которого – «противостояние и дезинформация в российской медиасфере… Планируется деятельность в таких социальных сетях, как Facebook, Twitter, "В контакте" и "Одноклассники". Основным оружием в информборьбе с Россией должны стать оригинальные программы и политическая сатира». В подтверждение такого подхода в разделе "Политика" Интернет-новостей 4 ноября 2015 г. сообщалось: "США увеличат расход на информационную пропаганду против России". Как заявил «заместитель помощника Госсекретаря США по делам Европы и Евразии Зифф на слушаниях в Сенатском комитете по иностранным делам Конгресса США 4 ноября.., "расход на эти цели предусматривает рост на 86 млн долларов"»[6]. Это притом, что в ситуации понимания реальности угроз безопасности Россия придерживается политики не самоизоляции и поиска врагов, а готова к сотрудничеству со всеми, кто отвечает взаимностью. Это еще раз подтверждает важность проблемы толерантности в отношениях правительств разных государств при ориентации на многополярность при решении межгосударственных и глобальных проблем коллективно.

Если вернуться к работе Г. Киссинджера, то в разделе "Куда мы идем?" автор ведет речь о поиске достижения равновесия сил государств. Он подчеркивает, что исторический смысл проис-

[4] *Киссинджер Г.* Мировой порядок / Пер. с англ. В. Желнинова, А. Милюкова. М., 2015. С. 445, 446. Ссылки на эту работу даны в тексте статьи.

[5] См.: Глобальная безопасность: инновационные методы анализа конфликтов / Под общ. ред. А.И. Смирнова. М., 2011.

[6] Alternat o org\etent\alt\iten\47114 – США увеличивают расходы на антироссийскую пропаганду.

ходящего "заключается в том, чтобы обнаружить его, а не декларировать" (с. 486). Однако при этом Г. Киссинджер продолжает ориентироваться на определяющее место в этом процессе США, которым надлежит играть ответственную роль в развитии мирового порядка XXI в. «Америка – как решительно выражающая в современном мире стремление человека к свободе и как незаменимая геополитическая сила для отстаивания ценностей гуманизма – должна не терять чувства направления… Целью нашей эры должно быть достижение равновесия при одновременном сдерживании "псов войны"» (с. 484, 485). Слова громкие. Однако автор уже отвлекся от своих мыслей о том, что "в отношениях между государствами – и во многих других областях – информацию, чтобы она оказалась действительно полезной, нужно помещать в широкий контекст истории и опыта, дабы она превращалась в фактические сведения. И повезло тому обществу, чьи лидеры хотя бы иногда поднимались до мудрости" (с. 455). Можно сказать, что здесь Г. Киссинджер проявляет себя как научный исследователь. *Но очевиден совсем иной акцент, когда автор этого весьма полезного труда выступает как политик и политолог.* Роль США в эстафете мирового лидерства – лейтмотив всей книги – он подчеркивает уже в предисловии к своей работе, говоря о том, что все человечество переживает очень сложный период перехода от уже упрочившихся самоаттестаций лидеров некоторых государств к новым горизонтам развития социума планеты в цифровую эпоху. В этой связи можно напомнить книгу другого наблюдателя за изменениями в современной истории – П. Смита. В своей работе "Времени больше нет. Американцы после американского века" он анализирует процессы больших сдвигов в обществе и факты неизбежных перемен в соотношении сил основных игроков XX в.[7]

Уделяя внимание внешним факторам в области реальных угроз информационной безопасности, нельзя забывать о противоречиях, упущениях, конфликтах во внутренних проблемах, порождающих обострение состояния информационной безопасности. В этом направлении специалистами по информационному праву и информатизации осуществляется работа в области упорядочения организационных и правовых механизмов обеспечения более высокого уровня информационной безопасности в Российской Федерации и в области межгосударственных отношений в условиях развития информационного общества.

3. Правовые проблемы обеспечения информационной безопасности

В процессе выявления и учета объективных условий глобального развития первых десятилетий XXI в. первостепенное значение имеет осознание значения феномена "информационное пространство". Инфокоммуникационные технологии вывели мышление и общение людей за пределы границ территории отдельного государства. Информационное общение трансгранично во всем его объеме. В этих условиях системы защиты и охраны информации и информационных технологий требуют *расширения фронта и содержания обеспечения информационной безопасности индивида, общества и всех механизмов управления в целях безопасности государства.* Все институты социума ориентированы на консолидацию в условиях, когда социум становится информационным обществом.

Инфраструктура обеспечения информационной безопасности начала XXI в. выстраивается с учетом: 1) специфики внутригосударственных (национальных) условий развития информационного общества; 2) состояния глобальных международных проблем безопасности и сохранения мира в масштабах планеты, 3) формирования межгосударственных механизмов региональных союзов и содружеств государств как способа формирования реальных задач в процессе продвижения в решении глобальных международных проблем безопасности информационной сферы планеты.

3.1. О состоянии правового регулирования в области обеспечения информационной безопасности Российской Федерации

Национальная безопасность страны в целом включает информационную безопасность – и не только как отдельное направление, но как универсальное условие обеспечения безопасности по всем другим направлениям. Это определено Стратегией национальной безопасности Российской Федерации до 2020 г.[8] Вместе с тем в сфере информационной безопасности основным политико-правовым документом, представляющим совокупность официальных взглядов на цели, задачи, принципы и направления обеспечения информационной безопасности, остается Доктрина информационной безопасности Российской Федерации[9]. Курс на формирование и развитие информационного общества определен, как известно, в

[7] См.: *Смит П.* Времени больше нет. Американцы после американского века / Пер. с англ. И.Д. Гольбиной. М., 2015.

[8] Утверждена Указом Президента РФ 12 мая 2009 г. № 537 (см.: СПС "КонсультантПлюс").

[9] Утверждена Президентом РФ 9 сентября 2000 г. № Пр-1895 (см.: Росс. газ. 2000. № 187).

Стратегии развития информационного общества Российской Федерации[10]. Эти документы развиваются в ряде так называемых "дорожных карт": "Повышение качества регуляторной среды для бизнеса" от 11 июня 2013 г. (в ред. от 17 августа 2013 г.), "Развитие отрасли информационных технологий" от 20 июля 2013 г. и др., в которых также отражены актуальные организационно-правовые вопросы, связанные с обеспечением информационной безопасности, которые были утверждены в 2013 г. распоряжениями Правительства РФ. В апреле 2014 г. впервые не распоряжением, а постановлением Правительства РФ от 15 апреля 2014 г. № 313 утверждена новая редакция Государственной программы "Информационное общество"[11], в которой особое внимание уделено вопросам безопасности в информационном обществе и информационном государстве.

Указом Президента РФ от 22 мая 2015 г. № 260[12] в целях противодействия угрозам информационной безопасности России при использовании информационно-телекоммуникационной сети Интернет предписано *преобразовать сегмент международной компьютерной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.* Эта область деятельности находится в ведении ФСО. В российский государственный сегмент сети Интернет, обеспечивающий подключение к глобальной сети Интернет, включаются: предназначенные для взаимодействия в Сети государственных информационных систем и информационно-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[13]. На решение данной проблемы направлены вступившие с 1 июля 2015 г. в силу изменения в ст. 13, 14 Федерального закона "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г.[14], согласно которым технические средства информационных систем, используемых государственными органами власти, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или учреждениями, должны размещаться на территории Российской Федерации. С 1 сентября 2015 г. вступили в силу изменения в Федеральный закон "О персональных данных" от 27 июля 2006 г.[15], предусматривающие, что запись, накопление и хранение персональных данных россиян разрешаются только на территории Российской Федерации. Принятие указанных актов свидетельствует об особом внимании к качеству программного обеспечения парка ИКТ России с учетом того, что Интернет-среда все более насыщается информацией, опасной для человека и используемой в целях массового поражения.

Сегодня среди угроз международной информационной безопасности значительное место занимают информационные преступления, *IT*-преступления, или киберпреступления. Несмотря на различия в терминологии, это не просто противоправные деяния, а именно деяния преступного характера, которые находятся в одном ряду с такими угрозами, как использование ИКТ в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности, в террористических целях, а также для вмешательства во внутренние дела суверенных государств.

Понятие "киберпреступность" применяется широко, хотя и не носит достаточно определенного характера. Нечеткими являются также понятия *"IT-crime"*, "*e-crime"*, "*high-tech crime"*. Приме-

[10] Утверждена Президентом РФ 7 февраля 2008 г. № Пр-212 (см.: там же. 2008. № 34).

[11] См.: Официальный интернет-портал правовой информации // http://www.pravo.gov.ru (Дата обращения: 24.04. 2014 г.).

[12] См.: Собрание законодательства РФ. 2015. № 21. Ст. 3092.

[13] См.: Пояснительная записка «К проекту федерального закона "О внесении изменений в отдельные законодательные акты Российской Федерации"» // СПС "КонсультантПлюс".

[14] См.: Росс. газ. 2006. № 165.

[15] См.: там же.

няемые в различных государствах, они отличаются не только названиями, но и, безусловно, по своему содержанию. В условиях динамичного развития информационного общества неизбежно возникает проблема защиты общества от их использования в преступных целях. Преступность в сфере высоких технологий не имеет границ и составляет угрозу международной информационной безопасности.

Профилактика и сдерживание киберпреступности и кибертерроризма – это комплексная проблема. Законы должны соответствовать требованиям, предъявляемым современным уровнем развития технологий, в связи с чем необходимы унификация и совершенствование национальных законодательств, регулирующих распространение информации в телекоммуникационных сетях общего пользования. К приоритетным направлениям относятся также организация взаимодействия и координации усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой.

В России обычно применяется термин "информационные преступления" или "компьютерные преступления", так даже называется гл. 28 УК РФ, предусматривающая уголовную ответственность за компьютерные преступления. Информация, информационные ресурсы, информационные технологии все чаще становятся предметом и целью преступных посягательств.

Отличительными чертами информационной преступности являются массовость атак и нацеленность на обычных пользователей. Основная цель злоумышленников – получение прямой финансовой выгоды. Банковские троянцы, кликеры, ботнеты, вымогатели, мобильные угрозы и т.п. – все это составляет сегодня более 90% от общего количества современных угроз. Атакующие обычно достаточно узко специализируются либо под конкретную цель, либо под конкретного заказчика. А такой целью нередко выступают кража информации, интеллектуальной собственности, неправомерный доступ к ней, модификация и т.д. Непосредственная финансовая выгода часто не есть прямая цель атакующих. В эту же группу целесообразно включать различные виды вредоносных программ, создаваемых некоторыми компаниями по заказу правоохранительных органов разных стран и практически открыто предлагаемых на продажу (например, разработки компаний *Gamma Group*, *Hacking Team SRL*). Источником этой угрозы являются лица или организации, осуществляющие неправомерное использование информационных ресурсов или несанкционированное вмешательство в такие ресурсы в преступных целях.

Как средство или способ совершения преступления, а также средство связи глобальные компьютерные сети могут использоваться при подготовке и совершении преступлений, предусмотренных УК РФ (ст. 206, 208, 211, 272–274, 277 и др.).

Для расследования террористической и экстремистской деятельности, осуществляемой с применением ИТК, применяются положения Будапештской конвенции о киберпреступности (не подписана Россией в связи с положениями п. *b* ст. 32), которые могут причинить ущерб суверенитету и безопасности государств – участников Конвенции и правам их граждан. Этот пункт гласит, что "сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему". Между тем Конвенция вступила в силу 1 июля 2004 г. Кроме того, 28 января 2003 г. ряд государств подписали Дополнительный протокол к указанной Конвенции, цель которого – введение уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем. В нем отмечается, что нормы как международного, так и национального права должны обеспечивать адекватные и законные ответные меры в борьбе против пропаганды расизма и ксенофобии, проводимой посредством компьютерных систем.

Особенностями информационных или компьютерных преступлений являются не только высокотехнологичность, быстродействие и трансграничность, но также анонимность, которая создает возможность скрыть личность преступника, его местонахождение, а также впечатление безнаказанности, а значит, и поощряет к неблаговидным поступкам и преступным деяниям.

Информация, информационные ресурсы и технологии стали выступать предметом и целью преступных посягательств, средой, в которой совершаются противоправные деяния, а также средством (орудием) преступления, чем объясняется и имеющееся сегодня разнообразие информационной преступности (преступлений), которая прошла достаточно быстрый путь, став одной из серьезнейших угроз не только национальной, но и международной безопасности. Поэтому так важен вопрос правового регулирования в этой сфере.

Проблемы установления ответственности за совершение противоправных деяний в информа-

ционной сфере требуют своего решения в различных отраслях законодательства, поскольку информационное право – комплексная отрасль права. Особенно актуален вопрос ответственности за противоправные деяния, совершаемые в глобальных информационно-телекоммуникационных системах. Важность проблемы противодействия правонарушениям в информационной сфере и ее безопасность объясняются интенсификацией процессов информатизации как в государственных органах, так и в коммерческих структурах, частном секторе. Развитие банковского и страхового бизнеса, крупных коммерческих структур, их выход на международный уровень, широкое использование сети Интернет, развитие информационного общества и многие иные факторы привели к тому, что проблемы обеспечения защиты информации, рост правонарушений в информационной сфере, определение юридической ответственности за их совершение находятся в центре внимания не только специалистов, но и широкого круга пользователей информационных систем. Актуальность проблемы ответственности за правонарушения в информационной сфере обусловлена ростом количества и разнообразием указанных правонарушений, что предопределяет необходимость формирования и развития соответствующего научно-методологического и правового базиса, обеспечивающего эффективное решение данных проблем[16]. Это объясняет, почему происходит переход от ориентации на защиту информационных ресурсов и информационных технологий к более объемной категории – *обеспечению информационной безопасности.*

3.2. О внутренних вызовах к совершенствованию правового обеспечения информационной безопасности

В обеспечении информационной безопасности в процессах развития информационного общества многое зависит от состояния действующей системы законодательного регулирования отношений всех структур государственной власти, гражданского общества, каждого человека в той социальной, экономической, культурной, правовой среде, в которой индивид принимает (или не принимает) участие и в которой ему приходится реализовывать свои природные, профессиональные, общежительные права и отношения, гарантированные Конституцией и иными законами своего государства.

Наличие и активное развитие информационных технологий, раздвигающих пространство действий, поведения и отношений каждого из видов субъектов социума, требуют соответствующей реакции всех организационных и регулирующих механизмов. Основная цель при этом – создать условия адаптации инфраструктуры социальных отношений к новым условиям жизни в глобальном информационном пространстве, усвоить правила и требования законности и толерантности отношений. Здесь на первом плане – проблема правового и нравственного уровней.

При уяснении вопроса о роли и значении правового регулирования отношений в новых условиях общения субъектов очень важно не терять из виду то обстоятельство, что и *сама правовая информация* в совокупности всех законов, других нормативных правовых актов и правовых актов локального характера, обобщение практики законотворчества, правоприменения во всех направлениях жизни общества, судебной практики есть *важнейший вид информации.* Организация и применение правовой информации с позиций информационной безопасности имеют два важных аспекта.

Первый аспект касается того, что этот вид информации, как и все другие виды и формы информационных ресурсов, которые создает и использует общество, подчиняется общим правилам объектов информационного характера. *Правовая информация как ресурс*, организующий поведение и отношения субъектов социума, не рядовой, а относящийся к *объектам общественного достояния*, имеющий режим открытой информации, обеспеченный в этих целях соответствующими информационными технологиями и представляемый в определенных форматах материализации, имеет правила создания, легализации и применения в обществе. Она предназначена для *информирования пользователей* органов государственной власти, органов местного самоуправления, любых организаций и граждан, *имеет свой правовой режим на всех стадиях образования данной информации, обеспечения доступа к ней, ее безопасности. Правила работы с правовой информацией с применением средств ИКТ являются общими для всех элементов правовой системы и составляют область информационного регулирования, которая реализуется средствами и формами информационного права.* Именно эти обстоятельства объясняют, почему информационное право аккумулирует многие проблемы организации и широкого доступа к правовой информации независимо от отрасли законодательства и предметов регулирования, сосредоточиваются в системе информационного законодательства. Унификация этой стороны работы с правовой информацией, в значительной степени гармонизация ее понятийного аппарата, подходов к классификации законодательства и иных источников правового характе-

[16] См.: *Полякова Т.А.* Информационная безопасность в условиях построения информационного общества в России. М., 2007.

ра находятся в области обеспечения безопасности правовой информации. Эти вопросы как бы формируют организационную инфраструктуру правовой информации и ее безопасности.

Второй аспект касается безопасности общества от состояния и применения правовой информации. Он затрагивает функционально-целевую роль законодательства, включая и информационное, в плане его соответствия вызовам самого общества в *новых условиях его информационной жизни*. Это требует глубокого мониторинга и анализа состояния правовой информации и всей правовой системы с позиций качества и роли в организации общественных отношений с учетом культуры использования инфокоммуникационных ресурсов государства. Ошибки, поспешность в принятии новых правовых актов или их непрерывные корректировки в зависимости от ситуаций и инцидентов, под влиянием интересов лоббирующих сторон, а не комплексной, системной оценки невольно создают условия для формирования конфликтов и угроз в самом составе правовой информации. Они снижают оценку состояния и возможность прогнозирования модернизации механизмов правового регулирования общественных отношений, формируют внутренний фронт информационной опасности не только законодательства, но и влияют на факторы безопасности государства и личности каждого конкретного лица (физического, юридического, публичного).

В настоящее время все большее значение приобретает *проблема обеспечения безопасности системы государственного управления в условиях глобальной информатизации общества.* Здесь имеют место два аспекта проблемы. Один касается состояния информационной среды, внешней и внутренней, в которой работают органы власти и местного самоуправления, состояния и степени развитости гражданского общества, а также влияния внешних факторов на политику, акценты внимания с учетом их значимости, часто требующих экстренного реагирования и смены курса.

Другой аспект касается качества состояния самой системы органов государственной власти и их функциональной инфраструктуры. Особенно это заметно в области государственного управления, деятельности органов исполнительной власти – администрации всех уровней и форм. В этом срезе проблем безопасности государства и человека важнейшее значение имеет проблема системного построения структуры функций государства, федеральных органов исполнительной власти, органов субъектов Федерации, органов местного самоуправления. Феномен и концепты функций конкретных субъектов в системе управления, реализующих предметную сторону деятельности субъектов, *показывающие, ЧТО должен и делает субъект в своей сфере ведения,* находятся в синхронной связи с таким феноменом и концептами, как *полномочия органа государственной власти*. Эта синхронность и баланс двух инструментов управления определяют качество, а следовательно, и безопасность государственного управления.

В данной области правового регулирования и организационной деятельности органов исполнительной власти к настоящему времени накопилось немало упущений, которые не позволяют качественно и эффективно использовать ИТ. По этой причине все возможные ожидания модернизации государственного управления в условиях информатизации пробуксовывают. Как выражается американский политолог относительно общей ситуации в мире цифровой эпохи, “распространение сетевых коммуникаций в социальном, финансовом, промышленном и военном секторах сулит немалые плюсы, но этот же процесс сопровождается уязвимостью социума. В этом смысле технологическое превосходство *обернулось геополитической импотенцией*” (Курсив наш. – *Авт.*) (с. 438). При всех преимуществах Интернет “сужает поле зрения. Информация легко доступна, коммуникации мгновенны, а потому утрачивается внимание к значению, теряется то, что имеет значение”[17] (с. 456).

На современном этапе в области организации государственного управления несколько активизировано внимание к решению проблем административной реформы в Российской Федерации. Поставлены вопросы об усилении информационного инструментария в этой области: разработка и синхронизация реестров функций и полномочий, предложена модель многомерных классификаторов взаимодействия этих определяющих концептов организации аппарата управления. Это требует основательного пересмотра состава функций и полномочий органов исполнительной власти, создания правильного алгоритма их связи и реализации. Осуществляется работа в области систематизации групп функций отраслевых и ведомственных систем управления, обоснован выход за пределы модели четырех основных функций, предусмотренных решениями 2004 г., установившей первое место в их перечне за “функцией” подготовки и принятия нормативных правовых актов, а также позволяющей руководствоваться выделением проблемы предоставления публич-

[17] См. также: *Бачило И.Л.* Читая Генри Киссинджера. Информационное общество, Интернет как факторы формирования мирового порядка // Евразийский юрид. журнал. 2015. № 7. С. 232–235.

ных услуг как воплощением всех функций управления развитием социальной сферы общества.

В соответствии с предложенной системой функций отраслевого государственного управления выделены восемь групп функций по предметному признаку деятельности государственного аппарата управления, в числе которых – группа функций 01. "Организация структуры и деятельности органа управления" обеспечивает необходимый уровень организации информационных ресурсов и информационного взаимодействия всех внутренних структур органа и его контактов с другими органами исполнительной власти, а также институтами и структурами гражданского общества. В предложенной классификации функций находит свое место и функция предоставления государственных услуг. Нельзя не отметить, что в процессе исследования состояния системы функциональной инфраструктуры органов исполнительной власти обнаруживается такая область информационного обеспечения их деятельности, как провал упорядочения информации, представляемой в форме государственных реестров, регистров, и их кодирования. Являясь исходным базовым информационным ресурсом в процессе организации деятельности органов исполнительной власти, этот участок информационного обеспечения самоорганизации государственного аппарата с 2001 г. по сей день не имеет окончательного структурного порядка. Решения Росстандарта и министерств, которым перепоручена эта область работы, пока не обрели завершения. Общероссийские классификаторы видов экономической деятельности (ОКВЭД или КДЕС), в которых фрагментарно затронуты вопросы классификации системы государственного управления и их деятельности, можно сказать, отсутствуют. Введение КДЕС планируется на 2016 г.

Самостоятельным участком работы по упорядочению законодательства в области информационных ресурсов является *работа по систематизации и совершенствованию правового обеспечения институтов информационного права.* Разработанная и обсуждаемая Концепция информационного кодекса РФ предлагает упорядочить систему институтов информационного права в целях установления более устойчивого правового регулирования институтов субъектов информационных отношений и их статуса, а также в Общей части Кодекса укрепить институт понятийного аппарата этой отрасли. Эти институты Общей части Кодекса будут способствовать развитию субинститутов Особенной части, которые имеют более сложную структуру и более динамичны в своем развитии. Они касаются проблем развития информационных ресурсов, информационных технологий и коммуникаций; проблем развития и использования институтов права на информацию. Третья область Особенной части Кодекса относится к упорядочению институтов обеспечения информационной безопасности. Многогранность проблем, различных направлений в этой области диктует необходимость выделения вопросов обеспечения информационной безопасности в суперинститут или подотрасль информационного права. Это позволит более основательно систематизировать и увязать в единый комплекс правового регулирования все виды отношений в данной области.

Еще одно направление работы в области упорядочения законодательства и правоприменительной практики – проблема приведения в порядок понятийного аппарата в информационном праве. Здесь накоплен большой материал, который требует специального рассмотрения и анализа. Предстоит обобщить материалы состоявшегося в начале 2015 г. Международного семинара-конференции и завершить подготовку коллективной монографии по указанной теме[18].

4. О проблемах обеспечения международной информационной безопасности и развитии региональных ассоциаций государств в этой области

Неуклонное нарастание угроз и конфликтов вызывает необходимость построения эффективной системы международной информационной безопасности, развития и совершенствования международного законодательства, проведения научных исследований в данной области. В этой связи представляется важным научное исследование тенденций развития законодательства и проблем реализации государственной и согласованной международной политики в решении глобального обеспечения информационной безопасности.

Актуальность проблем обеспечения информационной безопасности как на национальном уровне в рамках отдельных государств, так и международной информационной безопасности в настоящее время признается всем мировым сообществом. В условиях глобализации и информационного развития общества усиливаются импульсы активизации международного права. Крепнет идея формирования планетарного права – выработки и обязательности соблюдения всеобщих правовых норм[19]. Эта идея заслуживает самого пристального внимания. Кроме того, глобализация и широко раскинувшиеся по всему

[18] См.: Понятийный аппарат информационного права / Отв. ред. И.Л. Бачило, Э.В. Талапина. Сб. науч. работ. М., 2015.

[19] См.: *Бачило И.Л.* Информационное право. Учеб. для магистров. Изд. 3-е, перераб. и доп. М., 2013.

миру сети "всемирной паутины" – Интернета размывают государственные границы. Информационное пространство не ограничено территорией только одного государства, объединений государств и даже целых континентов, что вызывает необходимость выработки новых подходов к правовому регулированию межгосударственных и международных отношений.

Как известно, в Российской Федерации государственная политика в области обеспечения международной информационной безопасности нашла отражение в документе стратегического характера, в котором определены основные угрозы в этой области, цели, задачи и приоритетные направления государственной политики в указанной сфере. Это – Основы государственной политики в области обеспечения международной информационной безопасности до 2020 г.[20]

Учитывая многоаспектность и глобальность понятия "международная информационная безопасность", оно определяется как состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры. При этом особенно важно отметить, что цель государственной политики России отвечает ее национальным интересам, связанным с установлением международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности. Очевидна актуальность развития международного информационного права как части системы международного права.

Важнейшей формой организации при решении задач международной информационной безопасности, способствующей достижению указанной цели, является формирование системы международной информационной безопасности не только в глобальном масштабе, но и на многостороннем, региональном, двустороннем уровнях на основе применения международно-правовых механизмов и средств. В сложных политических отношениях, 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, особое внимание при заключении союзных договоренностей следует уделять вопросу обеспечения международной информационной безопасности. Например, согласно Концепции участия России в объединении БРИКС, утвержденной Президентом РФ 9 февраля 2013 г., одной из основных целей сотрудничества с государствами – участниками БРИКС по вопросам международной безопасности является сотрудничество в интересах обеспечения международной информационной безопасности, 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 ИКТ в военно-политических, террористических и криминальных целях, а также в целях, противоречащих обеспечению мира, стабильности и безопасности[21].

В июле 2014 г. благодаря инициативе России в Итоговой декларации 6-го саммита БРИКС в г. Форталеза были закреплены вопросы международной информационной безопасности и интернационализации управления Интернетом. В этой связи открывается широкий фронт работ в организационной и правовой сферах по выработке согласованной позиции, которая удовлетворяла бы интересы каждой из сторон соглашения.

В форматах таких международных организаций, как ШОС, ОДКБ, СНГ и др., в разное время были также заключены многосторонние международные соглашения в области обеспечения международной информационной безопасности *(Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности*[22] *(Екатеринбург, 16 июня 2009 г.), Положение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности*[23] *(Москва, 10 декабря 2010 г.). Подписано распоряжение Правительства РФ от 15 ноября 2013 г. № 2120-р о подписании Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности*[24]*. В 2014 г. велась активная работа по*

[20] Утверждены Президентом РФ 24 июля 2013 г. № Пр-1753 (см.: СПС "КонсультантПлюс").

[21] См.: Концепция участия Российской Федерации в объединении БРИКС (утв. Президентом РФ) // Там же.

[22] См.: Бюллетень международных договоров. 2012. № 1. С. 13–21.

[23] См.: Решение о Положении о сотрудничестве государств – членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности // СПС "КонсультантПлюс".

[24] См.: Официальный интернет-портал правовой информации // http://www.pravo.gov.ru (Дата обращения: 01.07.2015 г.).

содействию вступлению в силу данного Соглашения, а 4 июня 2015 г. оно вступило в силу для Российской Федерации, Республики Беларусь и Республики Таджикистан).

Важным 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 – 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 информационном пространстве[25].

Для обеспечения информационной безопасности важны также формирование глобального информационного общества и стремительное развитие интеграции, которая влечет необходимость расширения договорно-правовой базы межгосударственного сотрудничества. Способствовать разработке общих правил применения норм в информационной сфере должно создание единого для участников межгосударственных образований подхода в области правового регулирования – гармонизации и унификации законодательства государств – членов союзных государств. В этой связи актуальной представляется позиция о том, что 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[26]. Представляется важным отметить, что в целях приведения к единообразию законодательства государств в рамках 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[27]. Их цель – установление общих подходов государств – участников СНГ к правовому регулированию обеспечения информационной безопасности, укреплению и обеспечению сбалансированности национальных правовых систем в условиях информатизации общества, направленных на развитие международного информационного обмена, обеспечение безопасности информационных условий экономического и таможенного сотрудничества, на стимулирование использования информационно-коммуникационных технологий в социальной и культурной сферах. Еще пример: Постановлением Парламентской Ассамблеи Организации Договора о коллективной безопасности от 27 ноября 2014 г. № 7-6 (г. Санкт-Петербург) были приняты аналогичные вышеуказанным Рекомендации по сближению и гармонизации законодательства государств – членов ОДКБ. Этот комплекс работ на базе международных правовых актов СНГ завершен в 2014 г. более конкретными материалами. Запланированное изменение Модельного закона "Об информации, информатизации и о защите информации" завершилось разработкой нового Модельного закона "Об информации, информатизации и обеспечении информационной безопасности". Кроме того, разработан Модельный закон "О безопасности критически важных объектов"[28]. Принятие данных актов свидетельствует о том, 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 сфере 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. Положения указанных Рекомендаций должны учитываться при разработке новых документов стратегического планирования в области информационной безопасности в Российской Федерации.

Значительными достижениями в области международно-правового сотрудничества по формированию общих подходов к проблематике между-

[25] См.: Официальный сайт Министерства иностранных дел РФ // http://www.mid.ru (Дата обращения: 01.07.2015 г.). 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".

[26] См.: *Бачило И.Л.* Информационное право. Учеб. для магистров. Изд. 3-е, перераб. и доп.

[27] См.: Информационный бюллетень. Межпарламентская Ассамблея государств – участников СНГ. 2013. № 57 (Ч. 2). С. 162–179.

[28] *Юсупов Р.М., Бачило И.Л., Бондуровский В.В. и др.* Вклад российских и белорусских ученых в разработку информационного законодательства для государств СНГ и ОДКБ // Вопросы правоведения. 2015. № 3.

народной информационной безопасности стали заключенное Россией с Правительством Республики Куба двустороннее Соглашение о сотрудничестве в области обеспечения международной информационной безопасности[29] (г. Гавана, 11 июля 2014 г.), вступившее в силу 2 января 2015 г., а также аналогичное Соглашение с Правительством Республики Беларусь[30] (г. Москва, 25 декабря 2013 г.), вступившее в силу 27 февраля 2015 г.

Следует также отметить значение развития международно-правовых отношений России в данной сфере с Китаем[31]. Отмечаются особое значение совместной работы в рамках ШОС, а также необходимость дальнейшего углубления доверия и развития взаимодействия в области использования информационно-коммуникационных технологий, 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 указывается в научной литературе, "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"[32].

Давно обсуждается проблема интернационализации управления Интернетом, высказываются дискуссионные точки зрения – от полного неприятия до всесторонней поддержки. В этой связи следует отметить важность продвижения инициатив России, связанных с принятием в ООН проекта конвенции об обеспечении международной информационной безопасности, концепция которой стала результатом многолетней работы российских экспертов в области международной информационной безопасности во взаимодействии с нашими зарубежными коллегами. В современных политических условиях необходимо закрепить в международном правовом акте правила поведения в киберпространстве, а также касающиеся интернационализации системы управления Интернетом. Международно-правового закрепления также требуют 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[33].

Указанные проблемы свидетельствуют о необходимости совершенствования как международной, так и национальной систем информационной безопасности в России. Рассмотренные в настоящей статье вопросы представляются не просто актуальными и требующими продолжения соответствующих научных исследований, но и нуждаются в научно обоснованных подходах к формированию соответствующей государственной политики, научной разработанности теории и методологии правового обеспечения информационной безопасности, отражающейся в модернизации законодательства, направленного на обеспечение информационной безопасности. В новой редакции Доктрины информационной безопасности важно определить современный понятийный аппарат в области информационной безопасности, национальные интересы в информационной сфере и принципы их обеспечения, оценку основных угроз информационной безопасности и направлений обеспечения информационной безопасности, а также приоритетные направления правового обеспечения информационной безопасности.

---

[29] См.: Официальный интернет-портал правовой информации // http://pravo.gov.ru (Дата обращения: 14.01.2015 г.).

[30] См.: там же.

[31] См.: Соглашение между Правительством РФ и Правительством КНР о сотрудничестве в области обеспечения международной информационной безопасности // СПС "КонсультантПлюс". 8 мая 2015 г., руководствуясь положениями Договора о добрососедстве, дружбе и сотрудничестве между Российской Федерацией и Китайской Народной Республикой от 16 июля 2001 г., подписанного в Москве между Правительствами Российской Федерации и Китайской Народной Республики, также заключено Соглашение о сотрудничестве в области международной информационной безопасности.

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

[33] См.: Официальный сайт Совета Безопасности РФ // http://www.scrf.gov.ru/documents/6/112.html (Дата обращения: 01.07.2015 г.).