СОДЕРЖАНИЕ

Раздел 3
ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВА ЧЕЛОВЕКА

Раздел 4
ЦИФРОВИЗАЦИЯ ЭКОНОМИЧЕСКИХ ОТНОШЕНИЙ И ПРАВО

Раздел 5
ПРАВО МЕЖДУНАРОДНОЙ ОТВЕТСТВЕННОСТИ ГОСУДАРСТВ В КИБЕРПРОСТРАНСТВЕ И ОТВЕТСТВЕННОСТЬ ГРАЖДАН ЗА ИНФОРМАЦИОННЫЕ ПРЕСТУПЛЕНИЯ

CONTENT

Chapter 3
DIGITAL TECHNOLOGIES AND HUMAN RIGHTS

Chapter 4
DIGITALIZATION OF ECONOMIC RELATIONS AND LAW

Chapter 5
THE RIGHT OF INTERNATIONAL RESPONSIBILITY OF STATES IN CYBERSPACE AND THE RESPONSIBILITY OF CITIZENS FOR INFORMATION CRIMES

ПРЕДИСЛОВИЕ

Мы живем в большом информационном мире, где слова «Интернет», «цифровое государство», «цифровая экономика», «цифровые деньги», «цифровые технологии», «цифровое судопроизводство» и т.п. стали часто употребляемыми. Наука и закон постепенно раскрывают их смысл и значение, практика – погружает в новую реальность. И верно то, что эти явления принципиально изменили ритм нашей жизни, наше мышление, навыки и умение работать, открыли новые горизонты общения и взаимодействия людей, расширили индивидуальную автономию, возможности бизнеса и сотрудничества государств. Но чем больше цифровизации и автоматизации в различных областях жизни общества и государства, конкретного человека, тем сильнее потребность в регулировании «цифровых» отношений и адаптации права к этим технологическим новациям. Однако юридическая точка зрения на цифровое пространство и, главным образом, на Интернет порой сталкивается с «романтическим» взглядом на него ряда пользователей, IT-специалистов и экспертов, утверждающих, что «Интернет является уникальной системой, которую следует оставить для самоуправления, поскольку он слишком обширен и неосязаем, чтобы когда-либо эффективно контролировать его»[1]. Некоторые из правовых проблем, возникающих в этом пространстве, на самом деле, не новы, но обращение к ним часто может оказаться полезным.

Данный сборник, подготовленный правоведами и учеными-специалистами в области информационных технологий ИНИОН РАН и Российского государственного университета правосудия, позволит читателям познакомиться с кругом проблем в области

[1] *Maag C.D.* Legal dilemmas in the digital age // International affairs review. – Washington, 2013. – Vol. 6, N 2. – Mode of access: http://www.inquiriesjournal.com/articles/1205/2/legal-dilemmas-in-the-digital-age

информационно-коммуникативных отношений, возникающих на стыке социальных, в частности юридических, и технических наук. В статьях и аналитических обзорах правовой литературы, международного и национального законодательства авторы сборника раскрывают основные тенденции и проблемы развития государства и права в условиях внедрения новых цифровых технологий в разные сферы жизни социума. В ряде его статей отражена практика реализации Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. и Программы «Цифровая экономика Российской Федерации».

Открывается сборник статьей доктора технических наук, профессора Д.А. Ловцова. В центре его внимания специфика регулирования информационных отношений в инфосфере в связи с переходом к глобальному информационному обществу. Речь идет о концептуально-логическом моделировании систем регулирования информационных отношений в инфосфере (международных, национальных, федеральных, территориальных и др.), так называемых *правовых эргасистемах.* Автор раскрывает понятие этой системы, выделяет и рассматривает три ее базовые функциональные подсистемы: 1) правовую систему (позитивное право, правовые институты, правовая наука); 2) правосознание (индивидуальное, групповое, общественное); 3) правоотношения. Основные информационно-кибернетические контуры целевого регулирования характеризуются как ключевые внешние факторы воздействия на эти подсистемы. Среди них: целевые установки государства и соответствующее правовое и индивидуальное регулирование; правоприменительная практика; информационно-психологические воздействия государственных и иных структур; юридические факты и социальное поведение.

Кроме того, в статье определены направления обеспечения информационной безопасности личности, общества и государства, обусловленной уровнем защищенности содержательной информации, циркулирующей в глобальных и российских телематических сетях, а также наиболее актуальные научные вопросы, требующие первоочередного обсуждения, как то: формирование концептуально-логических моделей систем правового и индивидуального регулирования и информационной сферы общественно-производственной деятельности; определение базиса лингвистического обеспечения правового регулирования; разработка продуктивных концепций проблемно-ориентированного комплексного «информационно-кибернетическо-синергетического» подхода (ИКС-подхода)

к исследованию таких сложных явлений, как информационная безопасность правовой эргасистемы, безопасность привилегированной информации в этой системе; обоснование состава, структуры и места информационно-правового знания в существующей трехкомпонентной системе общественных, естественных и технологических наук.

Во второй статье Д.А. Ловцова, написанной в соавторстве с В.А. Ниесовым, рассматриваются направления и прагматические принципы системной модернизации организационно-правового обеспечения «цифрового» (автоматизированного) судопроизводства. Среди основных задач модернизации цифрового судопроизводства в России авторы выделяют следующие: 1) создание экосистемы цифрового судопроизводства, в которой данные в цифровой форме являются ключевым фактором его комплексного обеспечения; 2) развитие системы российских центров обработки данных, которая обеспечивает предоставление государству, бизнесу и гражданам доступных, безопасных и экономически эффективных услуг по хранению и переработке данных; 3) внедрение цифровых платформ работы с данными; 4) создание эффективной системы сбора, обработки, хранения и предоставления потребителям пространственных данных; 5) обеспечение организационной и правовой защиты информационных ресурсов.

В статье И.А. Алешковой и О.Х. Молокаевой анализируются направления организации и функционирования судебной власти в условиях новой информационной реальности, рассматривается ряд проблем, связанных с внедрением цифровых технологий в судебный процесс в Российской Федерации, опыт некоторых зарубежных стран в этой области.

Об особенностях развития информационного права как отрасли права нового поколения, возникшей под воздействием процесса технократизации, говорится в статье доктора юридических наук, профессора И.А. Умновой (Конюховой). Главное предназначение отраслей права нового поколения – обслуживание новых или преобразованных (расширенных, модифицированных) функций государства. Расширение норм права, регулирующих общественные отношения, обусловленные развитием информационных технологий, предопределило в рамках информационного права формирование новых подсистем – подотраслей, к которым относятся кибернетическое право, интернет-право (сетевое право), цифровое право. Появились такие новые сферы правового регулирования информационных технологий, как биоинженерия, нанотехнологии,

робототехника, искусственный интеллект, многомерная визуализация, новые технологии денежно-финансовых потоков (биткойны, криптовалюта, блокчейны) и др. Одновременно с преобразованием технократического общества возникла тенденция формирования технотронного общества нового поколения. Поднимается также ряд серьезных проблем, связанных с модернизацией информационного и кибернетического права, со злоупотреблениями информацией и нарушениями прав пользователей информации.

Проблемы применимости международно-правовых принципов суверенитета и юрисдикции государств к отношениям, возникающим в связи с использованием информационно-коммуникационных технологий, исследует Д.В. Красиков. Автор сосредоточивает внимание на одном из центральных вопросов современной дискуссии ученых о нормативной архитектуре киберпространства – особенностях реализации в нем международно-правового принципа государственного суверенитета, анализирует позиции ученых и отдельных государств, отмечает отсутствие общепризнанных и четких критериев толкования принципа суверенитета в киберпространстве.

Значительная часть его статьи посвящена рассмотрению особенностей территориального и экстерриториального распространения государствами законодательной, судебной и принудительной (исполнительной) юрисдикции в отношении деятельности в киберпространстве. Для сравнения автор приводит позиции властей КНР, принявших в 2017 г. Стратегию международного сотрудничества в киберпространстве, в которой суверенитету отведена роль одного из четырех основных принципов международного взаимодействия в киберпространстве (наряду с принципами мира, совместного управления и общей пользы). Заслуживает внимания, по мнению данного автора, упомянутое в указанном акте право государств участвовать в управлении международным киберпространством на равных основаниях, которое затрагивает непосредственно связанный с суверенитетом принцип суверенного равенства государств, закрепленный в Уставе ООН. Кроме того, в статье дан анализ практики законодательной юрисдикции государств в отношении транснациональной деятельности в киберпространстве, выделяются основные подходы к решению вопроса о том, какую деятельность в Интернете вправе регулировать конкретное государство.

Вопросы международного взаимодействия государств в сфере информационной безопасности, в том числе государств Азиатско-Тихоокеанского региона и Евросоюза, рассматриваются в статье Т.В. Захарова. Современными достижениями в этой области он

признает: практическую вовлеченность в обсуждение проблем кибербезопасности главных органов ООН и ряда функциональных и вспомогательных органов, специализированных учреждений ООН; закрепление компетенции в данной области за комитетами Генеральной Ассамблеи ООН; создание групп правительственных экспертов ООН по вопросам международной информационной безопасности. Отмечается рост числа государств, инициирующих разработку проектов резолюций органов ООН в данной области. Подобная институциональная основа политического взаимодействия, по мнению Т.В. Захарова, может стать движущей силой появления новых международно-правовых норм. В статье показано разнообразие нормативного решения вопросов международной информационной безопасности, при этом придается особое значение Стратегии кибербезопасности Евросоюза 2013 г.

Изучению проблем защиты прав человека в Интернете, в том числе его права на конфиденциальность персональных данных, а также решений Европейского Суда по правам человека, направленных на защиту частной жизни и права на свободу выражения мнения, посвящены статьи Е.В. Алферовой, А.П. Ивановой и Н.В. Кравчук. Исследование национального законодательства ряда стран в этой области позволяет выделить основные направления поиска оптимального баланса между правом на свободу выражения мнения в Интернете и его ограничением государством в общественных целях. Практика реализации международного и национального законодательств, как и теоретическое обоснование правовых идеалов прав человека в Интернете и их ограничение показывают, что достичь баланса интересов прав человека в Интернете практически очень сложно, что правовое регулирование конфиденциальности не отвечает современным условиям. Авторы считают, что необходимо расширить научную дискуссию по проблеме защиты конфиденциальности. Речь идет о выработке критериев и принципов взаимосвязи права на неприкосновенность частной жизни и свободы слова, свободы выражения мнений; об учете технической точки зрения и сетевых стандартов при разработке правовой политики; о пересмотре роли местоположения, гражданства индивидов в этой политике, поскольку проблема конфиденциальности вышла за пределы государственных границ. Еще одна важная проблема, которая поднимается учеными-правоведами, отражена в аналитическом обзоре А.П. Ивановой – ограничение неправомерного государственного вмешательства – государственного надзора. В этих целях, например, Дж.Д. Скотт излагает

концепцию «публичной приватности», предполагающую ликвидацию массового правительственного контроля над личной информацией пользователей: сведений в социальных сетях, историй поисковых запросов, данных о местонахождении. «Люди беззащитны не только перед угрозой раскрытия данных, но и перед возможностью тотального контроля со стороны правительственных структур, – замечает он. – Это рождает недоверие граждан к власти, о чем свидетельствует изменение общей статистики поисковых запросов пользователей, появление “самоцензуры” в среде современных авторов, изменение настроек конфиденциальности пользователей в социальных сетях»[1].

На конфиденциальность в Сети влияет появление Интернета вещей, которые распространяются с огромной скоростью, как и многообразие самих «умных» вещей. Эти устройства контролируют каждое наше движение, незаметно собирая при помощи датчиков информацию о нас. Помимо привычных нам смартфонов или фитнес-трекеров появляются поистине инновационные и неожиданные разработки, о которых говорится в статье Е.А. Афанасьевой. Они облегчают жизнь людей, однако полностью меняют принятую концепцию конфиденциальности.

В рамках рассмотрения проблем цифровой экономики в сборник включены статьи и аналитические обзоры юридической литературы и законодательства Т.В. Захарова, М.А. Беловой, Н.В. Крысановой, Е.Г. Афанасьевой, А.П. Ивановой, затрагивающие вопросы влияния «больших данных» на конкуренцию и конфиденциальность, на развитие интернет-рынков, а также проблемы правовых стандартов их использования. В центре внимания также правовые аспекты электронных сделок и уберизации. С одной стороны, оцифровывание изменяет экономические и конкурентные условия рынка на различных уровнях, заставляя считаться с новыми цифровыми продуктами и услугами, в особенности с изменением производственной цепочки (индустрия 4.0, машина-машина-общение и т.п.). С другой стороны, современный сбор больших данных сравнивается с цифровым «шпионажем», приводящим к неправомочному раскрытию, хищениям персональных и идентификационных данных, дискриминации при трудоустройстве, предоставлении в наем жилища или финансовых услуг и т.п. Борцы

[1] *Scott D.J.* Social media and government surveillance: Case for better privacy protections for our newest public space // Journal of business & technology law. – Maryland, 2017. – Vol. 12, N 2. – P. 151–164.

за гражданские права стараются привлечь внимание к тому, что большинство потребителей сервисов цифровой экономики и пользователей сети Интернет не осознаёт масштабов генерируемых их действиями данных, которые собираются, анализируются и используются в правительственных и коммерческих целях, пишут ученые. Так, по В. Банголи, следует руководствоваться принципом «ограничения целей» *(purpose limitation)*, закрепленным в п. b ст. 6.1 Директивы Европейского парламента и Совета ЕС от 24 октября 1995 г. «О защите прав частных лиц применительно к обработке персональных данных о свободном движении таких данных». Согласно данному принципу персональные данные должны собираться для объявленных, явных и законных целей. И в дальнейшем они не могут обрабатываться каким-либо образом, не совместимым с этими целями[1]. Большое значение в нормировании использования больших данных в экономических отношениях играют Руководящие принципы предпринимательской деятельности в аспекте прав человека, разработанные ООН и касающиеся средств правовой защиты, особенно в отношении компаний сектора информационных и коммуникационных технологий.

Важные аспекты информационной реальности исследуются в статьях Д.В. Красикова и Е.В. Пискуновой – международно-правовая ответственность государств в киберпространстве и уголовная ответственность граждан за информационные преступления. Внимание Д.В. Красикова сосредоточено на общей характеристике применимости норм права международной ответственности к поведению государств в киберпространстве; особенностях их поведения в этом пространстве, сложностях, возникающих в этом отношении на практике; концепции нарушения международно-правового обязательства как элемента в структуре международно-противоправного деяния в киберпространстве. Автор подчеркивает, что сегодня в обществе сформировались более четкие представления о конкретных угрозах, которые несет в себе Интернет, участники научного и практического диалога приобрели более обстоятельное понимание природы отношений с использованием различных информационных технологий, ушли в прошлое мифы о беспрецедентной исключительности отношений в так называемом «киберпространстве», о необходимости формирования некой всеобъемлющей системы «киберправа» или, напротив, о неотъемлемо

[1] См.: *Bagnoli V.* The big data relevant market // Concorrenza e mercato: 2016. – Rome, 2016. – P. 82.

присущей природе Интернета глобальной свободе. Результатом формирования нового контекста дискуссии стало широкое признание в целом пригодности существующих правовых режимов регулирования «традиционных» общественных отношений для регулирования отношений в киберпространстве.

Внимание Е.В. Пискуновой направлено на такие информационные преступления, как: 1) экономические киберпреступления – мошенничество и другие преступления экономической направленности, совершаемые с помощью компьютерных технологий. На их примере автор показывает, какие проблемы правового, криминалистического и криминологического характера влекут за собой «компьютеризация» и «информатизация» преступности; 2) преступления против общественной безопасности, нравственности и здоровья населения, совершаемые в Сети. Эта категория преступлений связана с незаконной торговлей оружием, наркотиками, порнографией, а также оказанием других незаконных услуг посредством зашифрованных информационно-телекоммуникационных каналов и сетей; 3) кибертравля и смертельные игры в социальных сетях. Данная категория преступлений объединяет два относительно новых феномена, связанных с прямым и косвенным психологическим насилием над личностью, совершаемым с помощью социальных сетей; 4) киберэкстремизм.

Таким образом, исследования, предпринятые авторами данного сборника, а также обзоры научных источников, в которых представлены точки зрения ученых-юристов разных стран мира по правовым проблемам цифровой информации[1], показывают, что многое еще предстоит понять и сделать в процессах информатизации общественных отношений и применении цифровых технологий во всех сферах жизни, в частности в обосновании и упорядочении научной терминологии в области информатики и телематики. Важную роль в этом призвано сыграть право. Есть также насущная необходимость в дальнейших комплексных исследованиях в рассматриваемой области учеными различных отраслей социальных и технических наук.

Е.В. Алферова

[1] См. также рефераты и обзоры по рассматриваемой тематике в Реферативном журнале «Социальные и гуманитарные науки: Отечественная и зарубежная литература». Сер.: «Государство и право». – Режим доступа: http://elibrary.ru/defaultx.asp и http://inion.ru/ (официальный сайт ИНИОН РАН: см. рубрики: «Новые издания ИНИОН РАН»; «Ресурсы»).

Раздел 1
ВЛИЯНИЕ ПРОЦЕССОВ ИНФОРМАТИЗАЦИИ НА РАЗВИТИЕ ОБЩЕСТВА, ГОСУДАРСТВА И ПРАВА

Д.А. Ловцов

РАЗВИТИЕ ИНФОРМАЦИОННОЙ СФЕРЫ ОБЩЕСТВЕННО-ПРОИЗВОДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ: ДОСТИЖЕНИЯ, УГРОЗЫ БЕЗОПАСНОСТИ И ПРАВОВОЕ РЕГУЛИРОВАНИЕ (Статья)

DOI: 10.31249/pras/2018.01.01

Аннотация. В статье рассмотрены концептуально-теоретические и прикладные аспекты развития инфосферы общественно-производственной деятельности в условиях формирования информационного общества в России. Определены направления обеспечения информационной безопасности личности, общества и государства, обусловленной уровнем защищенности содержательной информации, циркулирующей в глобальных и российских телематических сетях. Обоснованы системологические принципы и условия эффективного двухуровневого (правового и индивидуального) регулирования информационных отношений в инфосфере.

Ключевые слова: информационная сфера; информационные правоотношения; информационная безопасность; информационно-компьютерные технологии; информационная инфраструктура; глобальные телематические сети; правовые эргасистемы; электронное правосудие.

D.A. Lovtsov

Development of information sphere of social and industrial activity: Achievements, security threats and legal regulation (Article)

Abstract. The article deals with the general theoretical and practical aspects of development of information sphere of social and industrial activity, conditioned by forming of information society in Russia. The directions for

supplying the information security of individual, community and state are identified for the urgent level of protection needed to circulate information content efficiently in the global and Russian telematics networks. The systemological principles and terms of the effective two-level (legal and personal) regulation of information relations in infosphere are argued.

Keywords: information sphere; information legal relations; information security; information computing technologies; information infrastructure; global telematics networks; legal ergosystems; electronic justice.

Информационная инфраструктура

Проводимые в России с конца 70-х годов прошлого века теоретико-прикладные исследования проблемы эффективного правового регулирования информационных отношений, возникающих в общественно-производственной деятельности, а также организационно-правового обеспечения информатизации правовых эргасистем в настоящее время характеризуются качественно новыми условиями.

Завершен этап широкомасштабного процесса создания правительственной сетевой инфраструктуры в России «Электронная Россия»[1], в результате которого возникли и поддерживаются осведомляющие интернет-сайты всех органов власти, обеспечивающие практически полную информационную определенность в отношении их государственной деятельности.

В 2006 г. завершено создание первой очереди Государственной автоматизированной системы (ГАС) Российской Федерации «Правосудие»[2], представляющей собой первую отечественную крупномасштабную территориально-распределенную *информационно-правовую систему*, обеспечивающую формирование единого информационного пространства судебной системы России и информационно-аналитическую поддержку судопроизводства на базе принципа сбалансированности информационных потребностей граждан, общества и государства (баланса между потребностью в

[1] В соответствии с Федеральной целевой программой (ФЦП) «Электронная Россия (2002–2010 годы)» см.: Постановление Правительства РФ от 28 января 2002 г. № 65 // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_90180/

[2] В соответствии с ФЦП «Развитие судебной системы России (2002–2006 годы)» см.: Постановление Правительства РФ от 20 ноября 2001 г. № 805 // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34171/

свободном обмене информацией и необходимыми ограничениями на ее распространение).

С 2009 г. в России функционирует Единый портал государственных и муниципальных услуг (ЕПГУ), на котором размещается информация, формы заявок и через который проводятся платежи. В 2015 г. ЕПГУ интегрирован с Единой системой идентификации и аутентификации (ЕСИА). Достигнут существенный прогресс в определении перечня базовых государственных информационных ресурсов и систем (национальных баз данных), используемых в системе государственного управления органами власти и органами местного самоуправления, в том числе при предоставлении государственных или муниципальных услуг. Этот перечень определен постановлением Правительства РФ[1], которое предписывает операторам указанных государственных информационных систем обеспечивать круглосуточный доступ граждан и организаций к определенным сведениям и осуществлять проверку их содержания на предмет полноты и достоверности.

Созданы Единая межведомственная информационно-статистическая система (ЕМИСС), Система межведомственного электронного взаимодействия (СМЭВ) и Система межведомственного электронного документооборота (МЭДО) для межведомственного электронного обмена статистическими данными и документооборота. Идут работы по созданию до 2020 г. так называемого «цифрового правительства»[2] как новой стадии развития «электронного правительства», т.е. нового этапа трансформации государственной социально-экономической системы предоставления услуг на основе использования возможностей режима онлайн и инновационных цифровых технологий, ориентированных на замену многих административных (бюрократических) процедур.

Данные значимые достижения определяют потребность в *комплексном* (системном) проведении дальнейших многоаспектных

---

[1] См.: Постановление Правительства РФ от 24 октября 2011 г. № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)» // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=287914&fld=134&dst=1000000001,0&rnd=0.3500528065182681#015607485358538153

[2] См.: Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_221756/

теоретико-прикладных исследований информационных отношений и правоотношений в условиях интенсивного формирования электронных структур (в первую очередь, электронного правительства, электронного правосудия и др.) *информационного общества*. На основе обобщения результатов исследований, а также полученного практического опыта данных технологических достижений возможна продуктивная и относительно самостоятельная разработка теоретико-прикладных и прикладных аспектов правовой информологии[1] и смежных информационно-правовых наук. В частности, учитывая их природную «двухпрофильность», путем взаимосвязанной разработки эффективных информационно-компьютерных технологий (ИКТ), реализованных на базе средств телематики[2] и вычислительной техники, представляющих собой базовые элементы *информационно-технического обеспечения* (ИТО) любой профессиональной деятельности, включая *юридическую* (только качественное релевантное[3] ИТО может обеспечить повышение рациональности организации и эффективности профессиональной деятельности), и соответствующего *организационно-правового обеспечения* (ОПО) внедрения и использования ИКТ (только качественное релевантное ОПО может обеспечить эффективность внедрения и использования ИКТ).

Причем акцент следует делать на разработке ИТО *юридической деятельности* как первичном по отношению к ОПО ИКТ, которое, в свою очередь, взаимосвязано с *информационным* законодательством и через него – с *информационными правоотношениями в инфосфере*, возникающими, в частности, в результате внедрения и использования ИКТ и являющимися предметом обособленного раздела правовой информологии и, одновременно, относительно новой научно-правовой отрасли – *информационного права*[4].

Тогда обобщенным объектом правовой информологии и ее прикладной области – правовой информатики – можно считать

---

[1] См.: *Ловцов Д.А.* Системология правового регулирования информационных отношений в инфосфере: Монография. – М.: РГУП, 2016.

[2] *Телематика* (от англ. – *telematics*) – термин, используемый вместо термина «ИКТ телекоммуникации» (электронная почта, телекс, телетекс, видеотекс, телетекст, телеконференции и др.).

[3] От англ. *relevancy* – семантическая связанность, соответствие, уместность.

[4] См.: *Ловцов Д.А.* Теория информационного права: Базисные аспекты // Государство и право. – М., 2011. – № 11. – С. 43–51.

информационную сферу[1] (инфосферу) общественно-производственной деятельности – сферу *переработки* (производства, интерпретации, коммуникации[2]) и потребления (осведомление, обучение, принятие решения и др.) юридически значимой (правовой) *содержательной* информации[3], а предметом – процессы переработки правовой информации и процессы создания, внедрения и применения средств компьютерной техники и ИКТ (включая средства телематики, т.е. ИКТ телекоммуникаций). Под информационной сферой понимается сфера активного функционирования взаимодействующих *информационных деятелей* – источников (производителей, авторов, обладателей, операторов) и потребителей (пользователей) информации, использующих различные *информационные среды* (включающие *информационную инфраструктуру*: информацию, коммуникации, информационные системы) и *пространства* для целесообразной переработки и потребления информации.

В частности, распространение юридически значимой (правовой) информации имеет важное государственное значение и поэтому обеспечивается постоянно совершенствующимися информационно-компьютерными средствами и сетевыми технологиями. Например, в профессиональной юридической деятельности широко используются коммерческие настольные компьютерные и сетевые базы данных, называемые справочными правовыми системами (типа «КонсультантПлюс», «Гарант», «Кодекс» и др.). Развивается и государственная информационно-поисковая система и полнотекстовая база данных «Эталон» НЦПИ[4], содержащая более 7 млн правовых документов и материалов. Функционирует Единая система нормативно-справочной информации (ЕС НСИ), содержащая сведения о классификаторах, словарях и справочниках, используемых в государственных и муниципальных информационных системах. В судебной системе начинают всё активнее применяться

---

[1] См.: *Ловцов Д.А.* Системология правового регулирования информационных отношений в инфосфере: Архитектура и состояние // Государство и право. – М., 2012. – № 8. – С. 16–25.

[2] В частности, коммуникация информации в пространстве и во времени (хранение) составляет существо так называемой *информационной работы* в сфере культуры, библиотечного дела, архивов и др.

[3] См.: *Ловцов Д.А.*, *Федичев А.В.* Место и роль правовой информатики в системе информационно-правовых знаний // Правовая информатика. – М., 2017. – № 1. – С. 5–12.

[4] Научный центр правовой информации Министерства юстиции РФ.

ИКТ полиграфологических судебных экспертиз и современные компьютерные полиграфные системы («детекторы лжи»).

Неограниченные возможности развития ИТО юридической деятельности предоставляют глобальные телематические (информационно-компьютерные телекоммуникационные) сети (ГТС) типа Интернет, Релком, Ситек, *Sedab*, *Remart* и др., в частности внедрение рациональных технологий поиска и доступа к информационным ресурсам, размещенным в ГТС, создание сетевых информационных хранилищ и экспертных информационных систем в области права (например, «Эталон-онлайн»); применение геоинформационных[1] технологий эффективной электронной логической обработки многоаспектной правовой информации и др.

К наиболее актуальным научным вопросам, требующим первоочередного обсуждения, представляется целесообразным отнести *обоснование* максимально адекватных концептуально-логических моделей[2] систем правового и индивидуального регулирования (правовых эргасистем) и информационной сферы общественно-производственной деятельности; *определение* базиса лингвистического обеспечения[3] правового регулирования; *разработку* продуктивных концепций[4] проблемно-ориентированного комплексного «*ИКС*»-подхода к исследованию сложных правозначимых явлений как систем, информационной безопасности правовой эргасистемы, *гарантированной* безопасности привилегированной информации в эргасистеме[5], а также *обоснование* состава, структуры и места информационно-правового знания в существующей трех-

---

[1] См.: *Ловцов Д.А., Черных А.М.* Модернизация системы судебной статистики на основе новой геоинформационной технологии // Правовая информатика. – М., 2016. – № 1. – С. 7–14.

[2] См.: *Ловцов Д.А.* Системология правового регулирования информационных отношений: Концептуально-теоретические аспекты // Российское правосудие. – М., 2009. – № 8. – С. 56–61.

[3] *См.*: *Ловцов Д.А.* Лингвистическое обеспечение правового регулирования информационных отношений в инфосфере // Информационное право. – М., 2015. – № 2. – С. 8–13.

[4] См.: *Ловцов Д.А.* Концепция комплексного «ИКС»-подхода к исследованию сложных правозначимых явлений как систем // Философия права. – М., 2009. – № 5. – С. 40–45.

[5] См.: *Ловцов Д.А.* Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. – М., 2017. – № 3. – С. 66–74.

компонентной системе[1] общественных, естественных и технологических наук.

Угрозы информационной безопасности

Вместе с созданием и развитием электронных структур информационного общества в России возникают новые и нетрадиционные угрозы информационной безопасности личности, общества и государства, обусловленные открытостью информационного общества, а также применением иностранными государствами средств так называемого «информационного оружия»[2].

В частности, значительная часть экономики и социальной сферы России (включая управление, банковскую сферу, оптовую и розничную торговлю и др.) полагается в настоящее время на бесперебойное функционирование российских телематических сетей (например, телематических сетей ГАС РФ «Выборы», «Правосудие», «Управление»; АСБР-«Янтарь» Центрального банка РФ и др.), представляющих собой крупномасштабные коммуникационные компоненты ГТС Интернет. Российские телематические сети (РТС) все более широко начинают использоваться при взаимодействии предприятий, учреждений и граждан с органами государственной власти и государственными учреждениями, всё больший масштаб принимает телевещание и распространение других средств массовой информации посредством РТС. В данных условиях даже локальные отказы в РТС могут привести к существенным негативным эффектам.

В связи с этим важное значение приобретает проблема обеспечения *информационной безопасности*[3] пользователей РТС как защищенности их потребностей в качественной (легитимной, достоверной, релевантной, своевременной и др.) информации, необходимой им для нормального выполнения функциональных обязанностей, жизнедеятельности, общения и обучения, а также

---

[1] См.: *Ловцов Д.А.* Информационно-правовое знание: Теоретико-концептуальные аспекты // Научно-техническая информация. Сер. 2. Информ. процессы и системы. – М., 2004. – № 11. – С. 1–6.

[2] См.: *Ловцов Д.А., Сергеев Н.А.* Управление безопасностью эргасистем / Под ред. Д.А. Ловцова. – 2-е изд. – М.: РАУ-Университет, 2001.

[3] См., например: *Ловцов Д.А.* Информационная теория эргасистем: Тезаурус. – М.: Наука, 2005; Теория информационного права: Базисные аспекты: Дискуссия // Государство и право. – М., 2011. – № 11. – С. 43–51.

информационной надежности функционирования РТС. Наиболее уязвимым при этом является использование телекоммуникаций.

Поэтому одним из эффективных путей решения данной проблемы в настоящее время является международно-правовая стандартизация основных *сетеобразующих* протоколов ГТС Интернет.

Совместное международное совершенствование (модификация) сетеобразующих протоколов (*регламентов* и соответствующих процедур) сети Интернет осуществляется с момента их создания, и в первую очередь следующих двух базовых протоколов:

– *глобальной динамической маршрутизации BGP* (англ. *Border Gateway Protocol* – протокол пограничного шлюза) – выбора наилучшего (предпочтительного) маршрута передачи информации для каждого места назначения (автономной системы и терминала) и передачи его другим маршрутизаторам, использующим *BGP*;

– *разрешения доменных имен DNS* (англ. *Domain Name System* – система доменных имен) – трансляции символьных доменных имен в *IP*-адреса узлов сети Интернет.

Разработано множество относительно эффективных (безопасных, надежных, достоверных, устойчивых) вариантов сетеобразующих протоколов, принятых интернет-сообществом в форме *RFC* (*Requests for Comments* – «требования к обсуждению»), играющих роль международных технико-правовых стандартов.

В частности, разработан и принят стандартизирующей международной организацией (СМО) *IETF* (*Internet Engineering Task Force* – Инженерный совет Интернета) стандарт (*RFC*) защищенного протокола разрешения доменных имен *DNSSec* (*DNS Security*), предлагающий весьма надежную криптографическую защиту протокола *DNS* и сохраняющий полную обратную совместимость с ним, т.е. обеспечивающий возможность в защищенном от искажений виде выполнять трансляцию символьных доменных имен в *IP*-адреса узлов сети Интернет. При этом основными вспомогательными протоколами являются:

– *RRSIG* – протокол хранения и передачи подписей служебной информации протокола *DNS;*

– *DNSKEY* – протокол хранения и передачи открытых ключей;

– *NSEC* – протокол защиты отрицательных ответов.

Существуют принятые СМО *IETF* международные стандарты модифицированного протокола глобальной маршрутизации *BGP*:

– *SIDR-RPKI* (*Resource PKI*) – предусматривает построение системы «проверки источника» (*origin validation*) информации о блоках сетевых адресов, опирающейся на существующую систему

региональных интернет-регистратур[1], основан на использовании электронной цифровой подписи (обеспечивая невозможность подделки информации по пути ее следования к потребителю) и требует использования расширения инфраструктуры публичных ключей *PKI (Public Key Infrastructure* – инфраструктура открытых ключей) для аутентификации;

– *RCP* (*Route Control Platform* – платформа управления маршрутами) – предусматривает концептуальное разделение принятия решений о маршрутизации и реализации собственно транзита трафика между двумя различными элементами: платформой управления маршрутами и собственно маршрутизатором.

Вместе с тем проблема информационной безопасности российских телематических сетей и их пользователей остается актуальной, что обусловлено как несовершенством традиционных и предлагаемых СМО модифицированных сетеобразующих протоколов, так и возможностью несанкционированного доступа к циркулирующей привилегированной информации с использованием «популярных» с конца 90-х годов *нетрадиционных информационных каналов* («скрытых», «сублимографических» и др.)[2]. Например, в результате несанкционированного воздействия на протокол *BGP* возможно изменение маршрутов передачи привилегированной информации с выходом из контролируемой зоны для ее сбора и содержательного анализа (криптоанализа), что может остаться незамеченным для взаимодействующих абонентов используемого сегмента ГТС. При несанкционированном воздействии на протокол *DNS* и искажении таблиц *IP*-адресов (необходимых для трансляции символьных доменных имен) ряда серверов возможна задержка и даже потеря передаваемых сообщений, а также их замена и инфильтрация нелегитимных данных.

---

[1] В выделенном регионе регистрирует домены, выдает *IP*-адреса, выделяет адреса автономных систем и др.

[2] В России не так давно разработан ряд соответствующих технико-правовых норм для защиты от НИК. (См., например: ГОСТ Р 53113.1–2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1: Общие положения / Исполн. *Д.Б. Кабелев, А.А. Грушо, А.В. Гусев, Д.А. Ловцов* и др. – М.: Стандартинформ, 2008; ГОСТ Р 53113.2–2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2: Рекомендации по организации защиты информации, ИТ и АС от атак с использованием скрытых каналов / Исполн. *Д.Б. Кабелев, А.А. Грушо, А.В. Гусев, Д.А. Ловцов* и др. – М.: Стандартинформ, 2009).

Все это делает возможным отдельно взятым государствам управлять работоспособностью сети Интернет в других государствах того же региона. Поскольку угроза попыток влияния на региональную интернет-регистратуру со стороны властей страны, в которой она расположена, представляется вполне реальной, так как соответствующая организация является, как правило, юридическим лицом, подчиняющимся законам страны пребывания, в том числе и ее силовым органам и спецслужбам, и отказ, в частности, от выполнения требования спецслужб об изъятии какой-либо записи из базы данных (что приведет к прекращению маршрутизации для соответствующего блока сетевых адресов) представляется маловероятным.

Более того, существует риск «политических» деструктивных атак как на *DNSSec*, так и на *SIDR*. Причем, если в *первом* случае атака возможна только как прямое недружественное действие по отношению к соответствующему государству или владельцу зоны *DNS*, а значит, последствия и резонанс такой атаки будут максимальны, то во *втором* случае местом проведения атаки является база данных региональной интернет-регистратуры[1], а объектом может быть отдельный блок сетевых адресов, содержащий конкретные сетевые ресурсы в конкретной стране, т.е. такая атака может направляться на конкретный ресурс, организацию и др. и не позиционироваться как недружественный акт на международном уровне. Однако и в первом случае для атак такого рода все возможности имеются, поскольку управление корневой (*root*) зоной *DNS* осуществляет американская организация *ICANN* (*Internet Corporation for Assigned Names and Numbers* – Международная корпорация по присвоению имен и номеров), а техническое сопровождение работ по созданию и наполнению зоны осуществляет американская организация *Verisign, Inc*[2].

Вообще говоря, все атаки, типичные для *SIDR,* имеют смысл и для *DNSSec*, в частности уничтожение валидной записи искажением одного бита при ее передаче (электронная цифровая подпись будет неверна), имитация отказа держателя зоны от использования

[1] При европейской региональной интернет-регистратуре *RIPE* (*Reseaux IP Europeens* – Европейские *IP*-сети) создана наиболее развитая база информации об актуальных связях автономных систем между собой.

[2] Компания, поддерживающая разнообразные сетевые структуры, включая 2 из 13 существующих корневых серверов *DNS*, и др. (г. Рестон, штат Вирджиния).

DNSSec («downgrade attack»), атаки на «центр» инфраструктуры и на каналы, по которым он распространяет информацию, и др.

Кроме того, применение криптографических средств в данных сетеобразующих протоколах вносит в них множество новых возможных «уязвимостей», связанных со стойкостью используемых криптографических алгоритмов, с используемыми процедурами генерации, распределения, хранения и смены ключей; процедурами выпуска и отзыва сертификатов электронной цифровой подписи и др. В этой связи необходимо заметить, что если в протоколе *DNSSec* предусмотрена возможность выбора и использования различных криптографических алгоритмов, то проект *SIDR* предусматривает использование только одного криптографического алгоритма, и даже необходимость (в случае его компрометации) наличия механизма его смены (*algorithm rollover*) не осознавалась до недавнего времени разработчиками этого проекта.

Наиболее тревожным представляется тот факт, что последовательное внедрение валидации информации с помощью криптографических средств приведет к выделению в сети определенных «центров», которые будут выполнять роль и функции «центров доверия». Такие «центры» станут, очевидно, привлекательной целью для различного рода атак, как технологических, так и организационно-политических. Также важным представляется то, что надежность сетеобразующих протоколов после их модернизации становится зависимой от надежности используемых в них криптографических алгоритмов, а также уверенности в их высоком качестве и отсутствии недекларированных возможностей.

Наконец, процесс внедрения разрабатываемых модернизаций займет, скорее всего, значительный период времени (возможно, несколько лет), и все это время глобальные сети будут должны обеспечивать функционирование протоколов одновременно и в «модернизированном», и в «немодернизированном» режимах, что открывает различные возможности для проведения *«downgrade attacks»*, а также сохраняет возможности для различных форм киберпреступности (включая крэкинг, спаминг, фишинг, кибersквотинг[1] и др.).

---

[1] *Крэкинг* (от англ. *craking* – взлом) – компьютерный взлом систем защиты информации (в частности, системы защиты программного обеспечения).

Спаминг (от англ. *spamming, spam* – колбасные обрезки: от ***spice ham*** – пряная ветчина) – назойливая сомнительная корреспонденция и сообщения рекламного, информационного и др. характера, отправляемые по телематической

В связи с наличием принципиально неустранимых уязвимостей современных сетеобразующих протоколов снижение вероятности отказов сети Интернет на территории России можно обеспечить только комплексом организационно-правовых и технологических мероприятий, направленных либо на снижение допустимости реализации уязвимостей за счет ограничений, накладываемых на информацию, циркулирующую в сетеобразующем протоколе, либо на уменьшение негативного эффекта при ее реализации (уменьшение времени обнаружения причин уязвимости, локализация области распространения неверной информации, уменьшение времени восстановления сетевой связности и др.).

В такой комплекс мероприятий, как показали проведенные исследования[1], должны, в частности, входить:

– разработка регламентов для основных операторов национального сегмента сети Интернет по конфигурированию протокола глобальной маршрутизации *BGP*, учитывающих мировую

сети в адрес большого количества абонентов-пользователей без получения предварительного их согласия, что перегружает сеть и может создать серьезные помехи оперативному информационному взаимодействию абонентов.

Фишинг (от англ. *fishing* – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным абонентов-пользователей (логинам, паролям), используя массовые рассылки электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, *например:* от имени банков (Сити банк, Альфа-банк), сервисов *(Rambler*, *Mail.ru)* или внутри социальных сетей (*Facebook*, ВКонтакте, *Одноклассники.ru*). В письме, как правило, содержится прямая ссылка на веб-сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на ней свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к закрытым архивам, банковским счетам (аккаунтам), персональным данным и др.

Киберсквотинг (от англ. *cybersquatting*) – приобретение доменных имен, созвучных названиям известных организаций, учреждений, предприятий, компаний или просто с привлекательными названиями, с целью их дальнейшей перепродажи или размещения рекламы.

[1] См.: *Ловцов Д.А., Кабелев Д.Б.* Ситуационное управление защищенным обменом привилегированной информацией в АСУ специального назначения // Труды 30-й Всеросс. науч.-техн. конф. «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (30 июня – 1 июля 2011 г.): В 5 т. / РАН, РАО. – Серпухов: Серп. воен. ин-т, 2011. – Т. 4. – С. 166–169.

практику и имеющих целью уменьшить вероятность реализации уязвимостей данного протокола;

– разработка регламентов для операторов национального сегмента сети Интернет, обеспечивающих использование операторами локальных баз данных и локальной системы корневых серверов;

– разработка регламентов[1] по использованию в системах защиты сетеобразующих протоколов сети Интернет и обеспечивающих служб сертифицированных криптографических средств защиты информации, опирающихся на отечественные криптографические алгоритмы;

– разработка регламентов по внесению информации о критически важных ресурсах сети Интернет в сетеобразующие протоколы и мерах по обеспечению ее неискаженного состояния для операторов сети Интернет, предоставляющих соединение с сетью Интернет для подобных ресурсов;

– создание распределенной системы мониторинга и предупреждения о фактах распространении недостоверной информации по сетеобразующим протоколам;

– создание распределенной системы мониторинга актуальной сетевой информации о критически важных ресурсах сети Интернет, а также о ресурсах, поддержание непрерывной работоспособности которых считается важным с экономической, политической или социальной точек зрения;

– создание локальной системы корневых серверов протокола *DNS*, синхронизированной по содержанию с глобальными корневыми серверами, но находящейся под национальным контролем и управлением;

– внедрение средств обеспечения целостности и непротиворечивости информации в базах данных регистратур *DNS*, защиты этих баз данных от возможных атак, а также средств и методик контроля целостности информации в этих базах;

---

[1] См., например: *RFC* 5830. *GOST* 28147–89. *Encryption, decryption and message authentication code* (*MAC*) *algorithms / Executors: D. Kabelev, I. Ustinov, I. Emelianova, V. Dolmatov.* – 2010. – *March; RFC* 5831. *GOST* R 34.11–94. *Hash function algorithm / Executors: D. Kabelev, I. Ustinov, V. Dolmatov, S. Vyshensky*. – 2010. – *March; RFC* 5832. *GOST* R 34.10–2001. *Digital signature algorithm / Executors: D. Kabelev, I. Ustinov, V. Dolmatov, S. Vyshensky.* – 2010. – *March; RFC* 5933. *GOST* R 34.10–2001. *Use of GOST signature algorithms in DNSKEY and RRSIG resource records for DNSSEC / Executors: D. Kabelev, I. Ustinov, V. Dolmatov, A. Chuprina.* – 2010. – *July*.