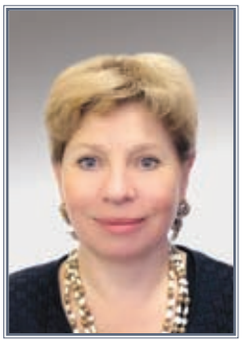
РЕАЛИЗАЦИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В СФЕРЕ ОРГАНИЗАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРОФЕССОР КАФЕДРЫ ИНФОРМАЦИОННОГО ПРАВА, ИНФОРМАТИКИ И МАТЕМАТИКИ РОССИЙСКОЙ АКАДЕМИИ ПРАВОСУДИЯ
ЗАСЛУЖЕННЫЙ ЮРИСТ РОССИЙСКОЙ ФЕДЕРАЦИИ
Татьяна Анатольевна Полякова



В условиях построения информационного общества в Российской Федерации и усиления процессов глобализации в данной сфере особое значение имеет государственная политика в области обеспечения информационной безопасности. В последнее время это особенно очевидно не только в связи с обострением различных международных процессов, но и с динамичностью развития информационных технологий в России.

Глобализация информационной сферы, рост и трансграничность новых вызовов и угроз в информационном пространстве – это реалии современного виртуального мира. В то же время продолжаются дискуссии о правовом положении Интернета и о необходимости закрепления на международном уровне определенных правил поведения в так называемом виртуальном пространстве, о цензуре или необходимости правового урегулирования вопросов, связанных с неправомерным использованием Интернета. Это всего лишь часть вопросов, которые заслуживают самого пристального внимания.

Только за текущий год произошло немало резонансных событий в сфере, связанной с обеспечением международной информационной безопасности. Широкое распространение получили кибератаки, направленные не только на хищения данных, нарушение нормальной работы корпораций и государственных структур, но и нередко имеющие политические мотивы.

Обеспечение международной информационной безопасности становится сегодня одним из приоритетных направлений государственной политики. Ключевым документом, отражающим политику России в этой сфере, являются утвержденные 27 июля 2013 года Президентом Российской Федерации В.В. Путиным «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». Указанный документ, разработанный Советом Безопасности Российской Федерации при участии заинтересованных федеральных органов исполнительной власти, содержит важные инициативы России в сфере международной информационной безопасности и определяет приоритеты не только на текущий момент, но и на последующие годы, что, безусловно, важно для продвижения российских инициатив в этой сфере.

Важно отметить, что в этом политическом документе, имеющем стратегическое значение, обозначены новые подходы к формированию понятия «международная информационная безопасность», которое существенно отличается от тех международных актов (соглашений), в которых оно было закреплено ранее. Международная информационная безопасность определена как «состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры». Кроме того, обозначены цели, задачи, основные направления, а также механизмы реализации государственной политики Российской Федерации в области международной информационной безопасности.

В качестве основных угроз для Российской Федерации в сфере международной информационной безопасности признано использование информационных и коммуникационных технологий как информационного оружия в военно-политических целях, для осуществления враждебных действий и актов агрессии, на-

рушающих территориальную целостность государств и представляющих угрозу международному миру, безопасности и стратегической стабильности; в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников; для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию, а также для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

Общеизвестно, что ряд международных соглашений в этой сфере уже действует – в рамках Шанхайской организации сотрудничества, Организации Договора о коллективной безопасности, БРИКС. Ведется разработка аналогичных соглашений в других форматах. В международном сотрудничестве в данной области важное место занимает реализация ряда инициатив Российской Федерации, а именно: дальнейшее продвижение предложений, связанных с принятием в ООН Конвенции об обеспечении международной информационной безопасности. Концепция указанной конвенции стала результатом многолетней работы российских экспертов и их зарубежных коллег в области международной информационной безопасности (Совета Безопасности Российской Федерации, МИДа России, а также Института проблем информационной безопасности МГУ имени М.В. Ломоносова и ряда федеральных органов исполнительной власти).

Концепция конвенции содержит правила поведения в киберпространстве, развивает предложения, связанные с интернационализацией системы управления Интернетом и установления международного правового режима нераспространения информационного оружия, а также основные угрозы, на борьбу с которыми направлен документ. Среди основных угроз выделяются «использование информационных технологий для враждебных действий и актов агрессии», «подрыв политической, экономической и социальной систем» одного государства другим, «манипулирование потоками в информационном пространстве других государств с целью искажения психологической и духовной среды общества», а также «массированная психологическая обработка населения для дестабилизации общества и государства».

Необходимо отметить, что в концепции в целях обеспечения международной информационной безопасности предлагается обязать государства руководствоваться принципом неделимости безопасности, запрета укрепления своей безопасности в ущерб безопасности других, попыток добиться господства в информационном пространстве над другими государствами.

Ряд ее положений направлен на защиту государства от кибернападения и от помощи извне местной оппозиции в организации twitter-революции; обязывает государства воздерживаться от разработки и принятия планов, способных спровоцировать возрастание угроз в информационном пространстве; содержит запрет на использование информационно-коммуникационных технологий для вмешательства во внутренние дела другого государства и предписывает воздерживаться от клеветнических утверждений, оскорбительной или враждебной пропаганды для осуществления интервенции или вмешательства во внутренние дела других государств. Также предлагается закрепить принцип невмешательства в информационное пространство и право каждого государства устанавливать суверенные нормы и управлять своим информационным пространством в соответствии с национальными законами. Кроме того, предусмотрены обязанность государств защищать свободу слова в Интернете и запрет на ограничение доступа граждан к информационному пространству, однако при этом указывается, что право на введение указанных ограничений может быть использовано в целях защиты национальной и общественной безопасности.

Для реализации основных положений Стратегии национальной безопасности Российской Федерации до 2020 года, в соответствии с которой одним из путей предотвращения угроз является совершенствование безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации, были разработаны «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», определившие не только факторы, принципы, влияющие на формирование государственной политики в данной сфере, но и задачи государственного регулирования, включая совершенствование нормативно-правовой базы, а также промышленной и научно-технической политики в области обеспечения безопасности автоматизированных систем управления критически важных объектов; развитие фундаментальной и прикладной науки, технологий и средств обеспечения безопасности, совершенствование образования, подготовки и повышения квалификации кадров в данной области, повышение общего уровня культуры информационной безопасности граждан.

На решение организационно-правовых проблем кибербезопасности также направлен Указ Президента Российской Федерации от 15 января 2013 года №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», в соответствии с которым на ФСБ России возложены полномочия по созданию государственной системы обнаружения, предупреждения, а также ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации – информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представи-

тельствах и консульских учреждениях Российской Федерации за рубежом.

В то же время развивается российское законодательство в области информационных технологий.

В соответствии с Указом Президента Российской Федерации от 7 мая 2012 года №601 «Об основных направлениях совершенствования системы государственного управления» Правительству Российской Федерации было поручено обеспечить достижение к 2018 году не менее 70% доли граждан, использующих механизм получения государственных и муниципальных услуг в электронной форме, сформировать систему раскрытия информации о разрабатываемых проектах нормативных правовых актов, результатах их общественного обсуждения в сети Интернет, обеспечить доступ в сети Интернет к открытым данным, содержащимся в информационных системах органов государственной власти Российской Федерации, создание условий для публичного представления предложений граждан с использованием специализированного ресурса в сети Интернет.

Необходимо отметить, что во исполнение Указа Президента Российской Федерации от 4 марта 2013 года №183 «О рассмотрении общественных инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса «Российская общественная инициатива» создан и функционирует соответствующий интернет-ресурс.

Широкий отклик получило принятие Федерального закона от 2 июля 2013 года №187-ФЗ «О внесении изменений в законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях», так называемого «антипиратского закона», определяющего порядок ограничения доступа к информационным ресурсам, посредством которых осуществляется распространение аудиовизуальных произведений и фонограмм с нарушением интеллектуальных прав правообладателей. Несмотря на то что он вступил в действие с 1 августа 2013 года, уже достаточно активно высказываются предложения по его совершенствованию.

Также важно отметить внесение изменений в федеральные законы от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 9 февраля 2009 года №8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», направленных на дальнейшую реализацию политики по обеспечению открытости информации о деятельности государственных органов и органов местного самоуправления.

Предусматривается предоставление такой информации государственными органами и органами местного самоуправления неограниченному кругу лиц посредством ее размещения в сети Интернет в форме открытых данных. Такой формат размещения допускает автоматизированную обработку указанной информации без предварительных изменений человеком для ее повторного использования.

Кроме того, в целях принятия органами исполнительной власти мер, направленных на ускоренное развитие российской отрасли информационных технологий в 2013–2018 годах, упрощения взаимодействия государства и бизнеса, повышения прозрачности распоряжениями Правительства Российской Федерации от 11 июня 2013 года №953-р (в редакции от 17 августа 2013 года) и от 20 июля 2013 года №1268-р утверждены планы мероприятий («дорожные карты») «Повышение качества регуляторной среды для бизнеса» и «Развитие отрасли информационных технологий» соответственно, в которых нашли отражение актуальные организационно-правовые вопросы, связанные с обеспечением информационной безопасности.

К ним относятся вопросы использования электронных документов и унификации форматов обмена данными при взаимодействии органов государственной власти и предпринимателей, вопросы использования электронных документов в суде, а также развития исследований в области информационных технологий, экспорта информационно-коммуникационной продукции, совершенствования институциональных условий ведения бизнеса в области информационных технологий, включая совершенствование законодательства для обеспечения развития облачных вычислений и др. Важность проблемы обеспечения информационной безопасности при использовании облачных вычислений обусловлена в первую очередь отсутствием каких-либо стандартов безопасности облачных сред и инструментов измерения уровня рисков и угроз.

Особого внимания также заслуживает утвержденная постановлением Правительства Российской Федерации от 27 декабря 2012 года №1406 Федеральная целевая программа «Развитие судебной системы России на 2013–2020 годы», предусматривающая широкое применение информационно-коммуникационных технологий в судебной системе, в частности использование облачных вычислений.

В связи с тем что использование облачной среды для реализации функций государственного управления, развития судебной системы и некоторых других проектов сегодня определено как приоритетная задача, среди наиболее масштабных государственных проектов в этой области следует отметить Национальную облачную платформу, создающуюся в рамках государственной программы «Информационное общество (2011–2020 годы)», которая представляет собой комплекс интегрированных информационных систем, предназначенный для предоставления органам исполнительной власти различного уровня, органам местного самоуправления, коммерческим организациям и физическим лицам услуг по модели облачных вычислений. Сервисы Национальной облачной платформы направлены на решение глобальных задач в области информатизации, касающихся основных социальных сфер, таких как здравоохранение, образование, жилищно-коммунальное хозяйство и безопасность, так как их применение может позволить автоматизировать большинство процессов, снизив тем самым затраты на содержание собственной инфраструктуры. Вместе с тем особую остроту приобретают вопросы обеспечения информационной безопасности при ее использовании.

В целях развития информационных технологий в системе арбитражных судов предполагается реализация таких мероприятий как:

- Создание облачной вычислительной архитектуры, которая позволит максимально эффективно, надежно и безопасно использовать технологии и специализированное облачное программное обеспечение для автоматизации судебного и общего делопроизводства, что в дальнейшем существенно сократит затраты на развертывание, поддержку и модернизацию программного обеспечения. Важно отметить, что в рамках этого мероприятия планируется разработка единой облачной системы автоматизации судопроизводства и электронного документооборота, создание главного центра обработки данных Высшего Арбитражного Суда Российской Федерации на базе арбитражных судов Московского региона, а также создание 10 центров обработки данных в федеральных арбитражных судах округов. Решение этих задач позволит реализовать возможность удаленного доступа как со стороны судов, так и со стороны участников судебных процессов из любой точки страны и мира, с любого устройства, в том числе мобильного.
- Расширение возможностей использования мобильных устройств в качестве доступа к информационным ресурсам, программным комплексам и базам данных арбитражных судов Российской Федерации посредством использования облачных технологий для судей и работников аппарата судов (мобильное правосудие).

Однако следует признать, что основным сдерживающим фактором при использовании облачных технологий в деятельности органов государственной власти и органов местного самоуправления, а также более широкого распространения облачных технологий в целом является недостаточное нормативное урегулирование вопросов, связанных с использованием облачных технологий.

В настоящее время отсутствуют нормативно-правовые акты, устанавливающие основные правила использования облачных технологий, законодательно не урегулированы вопросы обеспечения безопасности и конфиденциальности информации, передаваемой поставщику облачных услуг, не закреплены нормы, определяющие административную и гражданско-правовую ответственность поставщика облачных услуг, а также ответственность руководителей и работников организаций, оказывающих облачные услуги. Необходимость правового решения данной проблемы связана и с разработкой Минкомсвязи России единой сети передачи данных для органов государственной власти (так называемого «государственного облака»), создаваемой в целях повышения качества телекоммуникационных и вычислительных услуг, предоставляемых органами власти, а также формирования условий, стимулирующих ликвидацию «цифрового неравенства».

Не менее актуальной является проблема обеспечения безопасности персональных данных, используемых в различных информационных системах. Представляется важным отметить, что 15 мая 2013 года передана на хранение Генеральному секретарю Совета Европы (СЕ) Т. Ягланду грамота о ратификации Российской Федерацией Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки данных личного характера. Таким образом, в России завершена почти 7-летняя процедура, связанная с ратификацией одного из актуальнейших международных правовых актов в области защиты прав человека в процессе использования современных информационно-коммуникационных технологий. Сделан значительный шаг на пути к полноформатному участию Российской Федерации в усилиях государств – членов Совета Европы по укреплению безопасности человека в киберпространстве и общеевропейском правовом пространстве.

Последним этапом, связанным с ратификацией указанной конвенции, стало подписание Президентом Российской Федерации 7 мая 2013 года Федерального закона №99-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» и Федерального закона «О персональных данных». Данным Федеральным законом внесены изменения в 14 законодательных актов, среди которых Трудовой кодекс, Гражданский процессуальный кодекс, федеральные законы о прокуратуре, об актах гражданского состояния, о негосударственных пенсионных фондах, о государственной социальной помощи, о государственном банке данных, о детях, оставшихся без попечения родителей, о связи, о лотереях и др. Изменения направлены на соблюдение конфиденциальности и обеспечение защиты персональных данных в регулируемых этими актами сферах, а также уточнение случаев получения согласия субъекта персональных данных на их обработку либо случаев, когда такого согласия не требуется.

Одновременно продолжается процесс модернизации указанной конвенции и очень важно, что Российская Федерация полноправно участвует в этой работе. Развивается законодательство в области защиты персональных данных в Российской Федерации, издаются подзаконные акты Правительства Российской Федерации и федеральных органов исполнительной власти складывается судебная практика.

В настоящее время в Совете Федерации Федерального Собрания Российской Федерации осуществляется разработка проекта стратегии кибербезопасности Российской Федерации, направленного на формирование цифрового суверенитета России и представленного временной комиссией Совета Федерации по развитию информационного общества в феврале 2013 года. Данный проект направлен на создание механизмов мониторинга киберугроз и выработки ответов на них, формирование культуры информационной безопасности, реализацию партнерства государства, бизнеса и гражданского общества в сфере кибербезопасности, совершенствование нормативно-правовой базы, поддержку отечествен-

ных производителей программного обеспечения, подготовку квалифицированных кадров и т.д.

Необходимо отметить, что значительное место в развитии сферы информационной безопасности занимает научное исследование указанных вопросов и подготовка квалифицированных кадров.

В Основных направлениях научных исследований в области обеспечения информационной безопасности Российской Федерации, утвержденных 7 марта 2008 года, определены гуманитарные, научно-технические проблемы, а также проблемы кадрового обеспечения информационной безопасности Российской Федерации, при этом выделено 113 приоритетных проблем научных исследований в области обеспечения информационной безопасности Российской Федерации.

В соответствии с доктриной информационной безопасности Российской Федерации одним из приоритетных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации также является совершенствование системы подготовки кадров в области обеспечения информационной безопасности.

Федеральным законом от 16 октября 2012 года №174-ФЗ «О Фонде перспективных исследований» в целях содействия осуществлению научных исследований и разработок в интересах обороны страны и безопасности государства создан Фонд перспективных исследований, которым в соответствии с информацией, размещенной на официальном сайте Минобороны России, будут осуществляться исследования по проблематике информационной безопасности, в частности разработка методов и средств обхода антивирусных систем, средств сетевой защиты и защиты операционных систем. Также в блоке информационных технологий заявлены такие темы, как методы и средства борьбы с дезинформацией в Интернете; подтверждение подлинности и целостности сканированных документов без применения электронной подписи; новые механизмы и способы работы с оборудованием, не имеющим стандартных программных и аппаратных интерфейсов либо имеющим неизвестные интерфейсы.

Очевидно, что для формирования системных подходов к реализации государственной политики в сфере обеспечения информационной безопасности в Российской Федерации особое значение имеет развитие научных исследований в данной сфере. В связи с этим важно отметить, что в Программу фундаментальных научных исследований в Российской Федерации на долгосрочный период (2013–2020 годы), утвержденную распоряжением Правительства Российской Федерации от 27 декабря 2012 года №2538-р, включены фундаментальные исследования в области информационно-коммуникационных технологий и систем, стратегических компьютерных технологий и программ.

СТАТЬЯ ПОДГОТОВЛЕНА ПРИ УЧАСТИИ
НАУЧНОГО СОТРУДНИКА ИНСТИТУТА ГОСУДАРСТВЕННОГО
И МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ НИУ ВШЭ
А.И. Химченко