ПРОТИВОСТОЯНИЕ ИНФОРМАЦИОННЫМ УГРОЗАМ В СВЕТЕ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ РОССИИ

Абакумова И.О.,
Сарычев Н.В.

Информационная сфера России характеризуется активным развитием современных средств информационного обмена и различного типа компьютерных систем. Это создает условия для обеспечения информационной поддержки различных сфер национальной политике. Вместе с тем слабое внимание, уделяемое проблемам обеспечения информационной безопасности, что создает объективные условия для незаконного доступа к закрытой информации, ее хищению или разрушению. Особую опасность имеет возможность манипуляций различного рода информацией для негативного воздействия на процесс принятия политических решений, на формирование установок катострофизации и интолерантности, особенно в молодежной среде.

Ключевые слова: *стратегия развития информационного общества, правовое регулирование, информационная безопасность, информационные угрозы, информационная защищенность.*

В настоящее время в Российской Федерации сформировались необходимые условия для перехода к информационному обществу. Это отмечается и в Стратегии развития информационного общества в России, одобренной на заседании Совета Безопасности Российской Федерации 25 июля 2007 г. (далее – Стратегия).

Стратегия является политическим документом и направлена на реализацию положений Окинавской хартии глобального информационного общества[4] и итоговых документов Всемирной встречи на высшем уровне по вопросам информационного общества (Женева, 2003 г., Тунис, 2005 г.). В ней определены цели и принципы развития информационного общества в России, роль государства в данном процессе, предусмотрены основные мероприятия по достижению целей развития информационного общества в России.

Как отметил РФ В.В. Путин во время обсуждения проекта Стратегии, этот документ должен послужить основой подготовки конкретных программ, как в центре, так и на местах. Все используемые информационные технологии, включая электронную коммерцию, электронное правительство, информатизацию науки и образования, здравоохранения и т.д., рассматриваются сегодня как интегрированная, взаимосвязанная совокупность всей информационно-телекоммуникационной сферы и образуют фундамент для перехода к информационному обществу.

При этом особое внимание необходимо уделить вопросам информационной безопасности в самом широком смысле этого слова. Ведь глобализация открывает для нас не только новые возможности, но и создает определенные риски, и мы должны быть готовыми адекватно парировать такие потенциальные угрозы, как, например, кибертерроризм [7].

Наряду с возрастанием роли информации в жизни общества происходит изменение и переосмысление связанных с ней отношений и понятий, что получает отражение в правовом регулировании и, соответственно, в нормотворческой деятельности.

В настоящее время продолжается правовая реформа, активные законотворческие процессы не являются исключением и для информационного законодательства, а особенно такой его подотрасли, как законодательство в области обеспечения информационной безопасности.

Основной целью совершенствования нормативного правового обеспечения информационной безопасности является создание условий для ликвидации, предупреждения и пресечения проявлений угроз безопасности основных объектов национальных интересов в информационной сфере и минимизация последствий проявления этих угроз.

В законодательство Российской Федерации необходимо имплементировать прежде всего правовые нормы, устанавливающие ограничения вредного содержания информации, коммуникационных и информационных услуг в Интернете в соответствии с определенным набором признаков. Имеется положительный зарубежный опыт по законодательному регулированию функционирования системы жалоб

на содержание информации, использования инструментов условного доступа с помощью кодов, шифров и паролей, а также функционирования системы сотрудничества саморегулируемых организаций провайдеров и пользователей с правоохранительными органами. Несомненный интерес представляют предложения о создании международного органа при ООН, координирующего управление в Интернете (так называемой международной паутине) с учетом ее трансграничного характера.

Хотя ст. 10 ФЗ «Об информации, информационных технологиях и защите информации» предусмотрена обязательная идентификация обладателя информации или ее распространителя и запрещено распространение информации, за которую установлена административная и уголовная ответственность, однако правовой механизм реализации этой правовой нормы не разработан.

Очевидно, что информационное законодательство Российской Федерации не охватывает всего сложившегося многообразия отношений, связанных с пресечением деятельности противоправных интернет-сайтов.

Представляется, что в федеральном законодательстве должен быть определен правовой механизм признания вредного содержания информации в сети Интернет, установлены обязанности провайдеров по удалению информации экстремистского и террористического толка. Кроме того, не определены основания для прекращения права пользования доменными именами и отмены их регистрации, а также не предусмотрены меры по идентификации пользователей информационно-телекоммуникационных систем и созданию национального электронного пространства доверия, поскольку пока еще должным образом не реализуется Федеральный закон «Об электронной цифровой подписи». Важное значение уделяется вопросам пространства доверия, подтверждения подлинности электронных документов, создания федерального центра по обмену информацией.

В развитии информационного законодательства в России, несомненно, важной является разработка законопроектов по вопросам доступа к информации, особенно к информации о деятельности государственных органов, так называемой публичной информации. Решение этой проблемы необходимо в целях обеспечения прозрачности деятельности органов государственной власти, что является обязательным требованием по международным обязательствам, вытекающим из конвенций ООН и Совета Европы по борьбе с коррупцией. Однако рассмотренный в первом чтении Государственной Думой Федерального Собрания РФ проект Федерального закона «О доступе к информации о деятельности органов государственной власти и местного самоуправления» еще весной 2007 г. до настоящего времени не принят.

Осуществление правосудия сегодня также нуждается в применении информационных технологий, подтверждении подлинности электронных судебных документов, и уже появилось правовое понятие «электронное обеспечение правосудия» [6]. Разработана Государственная автоматизированная система «Правосудие», и ведется работа по подготовке соответствующих процессуальных норм.

Во вступительном слове на заседании Совета Безопасности по вопросу развития информационного общества в России Президент России В.В. Путин отметил, что использование информационных технологий должно служить обязательным критерием эффективности работы ведомств, властей регионов и органов местного самоуправления. Для этого уже сейчас надо выработать объективные оценочные показатели развития и внедрения этих технологий [7].

Следует отметить, что в рамках административной реформы продолжается активная разработка административных регламентов, которые направлены как на повышение эффективности государственного управления, так и в значительной степени на совершенствование оказания гражданам публичных услуг.

Нельзя переоценить и значение для развития информационного законодательства принятой в 2006 г. части четвертой Гражданского кодекса РФ, направленной на защиту интеллектуальной собственности, которая вступила в силу с начала 2008 г.

Учитывая отмеченные современные тенденции в развитии правового регулирования в области обеспечения информационной безопасности, большой массив не всегда согласованных правовых актов, касающихся информационной сферы, и комплексный характер информационного законодательства в целом, а также необходимость имплементации международных правовых норм, представляется целесообразной разработка Основ законодательства Российской Федерации об обеспечении информационной безопасности. Принятие такого правового акта необходимо для развития и совершенствования соответствующего правового регулирования в субъектах РФ. На федеральном уровне также требуется разработка сводного кодифицированного законодательного акта, регулирующего правоотношения в информационной сфере и направленного на совершенствование законодательства в информационной сфере, законодательное закрепление единых основ правового регулирования отношений, возникающих при реализации различными субъектами права на поиск, получение, передачу, производство и распространение информации, осуществление деятельности по

формированию, хранению и использованию информационных ресурсов и систем, необходимых органам государственной власти и местного самоуправления в целях реализации их задач и функций.

Следует различать информационное противоборство (борьбу) в широком (во всех сферах) и узком смысле слова (в какой-либо сфере, например в политической).

Информационное противоборство (борьба) – форма борьбы сторон, представляющая собой использование специальных (политических, экономических, дипломатических, военных и иных) методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах достижения поставленных целей.

Основные сферы ведения информационного противоборства:
- политическая,
- дипломатическая,
- финансово-экономическая,
- военная,
- космическая.

Следует выделить два вида информационного противоборства (борьбы): информационно-техническое и информационно-психологическое.

При информационно-техническом противоборстве главные объекты воздействия и защиты – информационно-технические системы: системы передачи данных (СПД), системы защиты информации (СЗИ) и так далее.

При информационно-психологическом противоборстве главными объектами воздействия и защиты являются:
1. Система принятия политических и экономических решений.
2. Система формирования общественного сознания.
3. Система формирования общественного мнения.
4. Психика политической элиты и населения противостоящих сторон.

Информационное противоборство включает три составные части.

Первая – стратегический анализ, вторая – информационное воздействие, третья – информационное противодействие.

России следует незамедлительно рассмотреть возможность создания специального организационно-управленческого и информационно-аналитического механизма (инструмента), который сможет выполнять организационно-управленческие и информационно-аналитические функции по разработке и проведению информационных операций (оборонительных и наступательных).

Назрела необходимость создания в России системы информационного противоборства, частью которой должна стать внешнеполитическая пропаганда России. Для того, чтобы выигрывать информационные войны, необходимо создать специальные организационно-управленческие и аналитические структуры для противодействия информационной агрессии против нашей страны.

Так, после начала грузинской агрессии 8 августа 2008 года президент России Д.А. Медведев, прервав отпуск, принимает решение: военной силой прекратить геноцид осетинского народа и принудить грузинское руководство к миру. Для Саакашвили и его заокеанских покровителей действия России стали полной неожиданностью. Ожидали дипломатических заявлений, а в ответ на агрессию против Южной Осетии и убийство российских миротворцев регулярные российские воинские части с тяжелой боевой техникой: танками, гаубицами, системами залпового огня, авиацией – перешли Рокский перевал. Российские войска вошли не только в Южную Осетию, народ которой в августе 2008 года подвергся огню на уничтожение со стороны грузинских вояк, действовавших поистине с жестокостью фашистов, но и в Абхазию, чтобы предотвратить возможность повторения югоосетинской трагедии.

После наказания агрессора в соответствии с нормами международного права, непрерывно наращивается информационное давление на нашу страну, которая защитила осетинский народ от уничтожения. По сути, в августе 2008 года против России была развернута грязная информационная война. Активное участие в ней принимали, прежде всего, американские и британские СМИ. В материалах CNN, Би-би-си и ряда других СМИ доминировали антироссийские материалы. В США, Великобритании и некоторых других странах усилились попытки негативного формирования образа России.

Агрессивная антироссийская пропаганда пытается навязать мировому сообществу отрицательные информационные клише о России. К сожалению, «пятидневная августовская война» на Кавказе показала нашу несостоятельность в отстаивании своих целей и интересов в мировом информационном пространстве.

Поэтому России в ближайшее время нужно сформулировать и дать адекватный информационный ответ, в первую очередь на европейском и постсоветском пространстве. Прошедшее после «пятидневной августовской войны» на Кавказе время показало, что пока российская политическая элита пытается сделать соответствующие выводы после информационной агрессии США, Великобритании и ряда других стран против России. Прошло несколько публичных мероприятий с участием ведущих

российских экспертов, на которых анализировался ход информационной войны против России (17 сентября 2008 года – организованный Общественной палатой «круглый стол» «Информационная агрессия против России: методы противостояния», 2 октября 2008 года – организованная партией «Справедливая Россия» Международная конференция «Информационные войны в современном мире»).

Главная проблема, которая была очевидной в ходе дискуссий, – это явная недооценка роли информационного противоборства современной российской политической элитой в условиях усиления глобальной экономической и геополитической конкуренции в мире.

После принуждения Грузии и ее заокеанских покровителей к миру геополитическая и геоэкономическая роль России в мире во многом будет определяться тем, сможет ли она создать эффективную систему информационного противоборства. Время требует одновременного создания мощных информационно-аналитических и информационно-пропагандистских структур, предназначенных для реализации информационных моделей урегулирования конфликтов [5].

России необходимо восстановить свой потенциал механизма внешнеполитической пропаганды, который был основательно разрушен в 90-е годы. В этой сфере, как и в сфере ядерных вооружений, к сожалению, произошло одностороннее информационное разоружение. К концу 90-х годов прошлого века, например, на всем африканском континенте не осталось ни одного российского корреспондентского пункта, ни одного представительства отечественных информационных агентств. Сегодня эту «информационную нишу», которую мы покинули после распада СССР, активно заполняет Китай.

Впрочем, отрадно, что провал 90-х годов был осознан российским руководством. С приходом к власти президента В.В. Путина началось постепенное уверенное восстановление утраченных позиций. Ключевым шагом в этом направлении является создание в 2006 году спутникового телеканала Russia Today. Напомним, что ведущий западный новостной канал CNN был создан в 1980 году. В СССР выделялись огромные деньги на строительство и развитие ракетно-ядерных сил. Однако денег на создание советского спутникового телеканала не нашлось.

Советская политическая элита недооценивала фактор информации. А CNN наращивал свое влияние. Как сказал один американский генерал в 1991 году, во время операции «Буря в пустыне», пока CNN не скажет, что мы выиграли войну, мы ее не выиграли. И это соответствует действительности. Многие сюжеты «победных» действий американских войск были сняты совсем не на поле сражений, а в штате Невада силами специалистов Голливуда, который великолепно умеет имитировать ведение боевых действий. Вспомним хотя бы известный случай с освобождением рядовой Джессики Линч уже во время второй иракской войны в 2003 году. Этот эпизод являлся пропагандистской акцией Пентагона и репетировался заранее, что еще раз демонстрирует всю мощь информационного оружия.

Таким образом, 26 лет отделяют нас от CNN, за годы нашей «информационной спячки» нашли свои ниши Би-би-си и Foxnews, глобальными каналами стали Al Jazzira и Euronews.

Информационная сфера России характеризуется активным развитием современных средств информационного обмена и различного типа компьютерных систем. Это создает условия для обеспечения информационной поддержки деятельности аппарата управления на всех уровнях и во всех ветвях власти.

Вместе с тем слабое внимание, уделяемое проблемам обеспечения информационной безопасности, создает объективные условия для незаконного доступа к закрытой информации, ее хищения или разрушения. Особую опасность имеет возможность манипуляций различного рода информацией для негативного воздействия на процесс принятия политических решений [2].

В перечне видов угроз информационной безопасности, обозначенных в Доктрине, стоит обратить особое внимание на:

- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- манипулирование информацией (дезинформация, сокрытие или искажение информации) [1].

Основными целями защиты от информационно-психологических угроз для России являются:

1. Защита от разрушительных информационно-психологических воздействий среды общества, психики населения, социальных групп граждан.

2. Противодействие попыткам манипулирования процессами восприятия информации населением со стороны враждебных России политических сил, проводимых е целью ослабления обороноспособности государства.

3. Отстаивание национальных интересов, целей и ценностей России в информационном пространстве (глобальном, национальном, региональном, субрегиональном, стран СНГ).

4. Постоянное отслеживание отношений российское общества к важнейшим проблемам национальной безопасности (диагностика общественного мнения, психологического состояния нации).

Ведущие страны мира в настоящее время располагают мощным потенциалом информационного противоборства (прежде всего, США, Китай, Израиль, Франция, Великобритания, Германия), который может обеспечить им достижение политических и экономических целей, тем более что отсутствуют международные юридические нормы ведения информационной борьбы.

Для защиты от негативных воздействий социальных объектов в ходе глобальной геополитической информационной борьбы, необходимо создание системы информационно-психологического обеспечения как составной части национальной безопасности России. Данная система должна обеспечить защиту психики политической элиты и населения России от негативного информационно-психологического воздействия (т.е. защите сознания россиян от негативных информационных потоков геополитических противников России). Ее основная задача – обеспечение психологической безопасности политической элиты и населения России.

В Доктрине информационной безопасности Российской Федерации определены следующие основные источники внутренних угроз информационной безопасности.

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно – финансовой сферы, промышленности, сельского
- хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

- нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;
- недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;
- распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;
- деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Из внутренних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

- информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;
- недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

– информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;
– распространение за рубежом дезинформации о внешней политике Российской Федерации;
– нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;
– попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях [1].

На основе национальных интересов РФ в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов РФ в информационной сфере.

Первая составляющая национальных интересов РФ в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов РФ в информационной сфере включает в себя информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов РФ в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Четвертая составляющая национальных интересов РФ в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России [3].

ЛИТЕРАТУРА

1. Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09.09.2000 г. № Пр-1895 // Российская газета. 2000. № 187.
2. Кирьянов А.Ю. Сущность информационного аспекта национальной безопасности Российской Федерации // Международное публичное и частное право. – 2005. № 3. – С. 42.
3. Ковалева Н.Н. Информационное право России: учебное пособие. – М.: Издательско-торговая корпорация «Дашков и К», 2007. – С. 234.
4. Окинавская хартия глобального информационного общества от 22 июля 2000 г. // Дипломатический вестник. 2000. № 8. С. 5156.
5. Панарин И. Информационные войны реальный фактор геополитики. Системы информационного противоборства // URL: http://www.centrasia.ru/newsA.php?st=1224016740
6. Постановление Правительства РФ от 21 сентября 2006 г. № 583 «О Федеральной целевой программе «Развитие судебной системы России на 20072011 годы» // Собрание законодательства РФ. 2006. № 41. Ст. 4248.
7. Стратегия развития информационного общества в России // Информационное право. 2007. № 3(10). С. 35.