О ЗАКОНОДАТЕЛЬНЫХ МЕРАХ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРЕДСЕДАТЕЛЬ КОМИТЕТА ГОСУДАРСТВЕННОЙ ДУМЫ
ПО ИНФОРМАЦИОННОЙ ПОЛИТИКЕ,
ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И СВЯЗИ
Леонид Леонидович Левин

Одним из основных приоритетов в работе Комитета Государственной Думы по информационной политике, информационным технологиям и связи (далее – Комитет) является законодательное обеспечение национальной безопасности. В отличие от органов исполнительной власти, задача которых состоит в выявлении и ликвидации конкретных угроз национальной безопасности, Комитет участвует в создании нормативной базы, позволяющей бороться с угрозами национальной безопасности, исключив риски для других сфер общественной жизни (экономики, культуры) и обеспечив соблюдение конституционных прав граждан. Противодействие угрозам в целях сохранения безопасного и устойчивого развития страны неотъемлемо от соблюдения закона. Задача Комитета как раз и заключается в том, чтобы обеспечить государство и общество эффективной законодательной базой, защищающей национальные интересы в информационной сфере.

По экспертным оценкам, 53% взрослого населения Российской Федерации ежедневно выходят в Интернет, а 97% – это доля интернет-пользователей среди 18–24-летних граждан. Неизбежным следствием такого прогресса становится расширение присутствия государства в Интернете. Государство защищает индивидуальные и коллективные права граждан, в том числе осуществляет меры по укреплению безопасности в обычной жизни, и то же самое оно обязано делать в информационно-коммуникационных сетях. Это общемировая тенденция, и в данном смысле наша страна идет в первых рядах. На сегодняшний день мы можем поставить себе в заслугу, что с самого начала был выбран путь законодательного регулирования, а не создания непрозрачных комиссий в составе исполнительной власти, как это сделано в ряде развитых стран.

Политическая обстановка 2014 года в мировой информационной сфере, отражающаяся в первую очередь в сети Интернет, характеризовалась обострением информационного проти-

воборства на фоне введенных против нашей страны ограничительных мер (так называемых санкций ЕС и США). Существенной характеристикой информационного фона было предание гласности фактов хакерских атак, успешная реализация которых ставила под сомнение неуязвимость критических инфраструктурных объектов, к тому же в условиях возможности недружественных актов со стороны отдельных государств в инфосфере. Инерция разоблачений Эдварда Сноудена в сочетании с этими фактами оказывала дополнительное воздействие на депутатов, что привело к появлению десятков законодательных инициатив, основной целью которых было обеспечение национальной безопасности Российской Федерации в инфосфере.

Тщательный отбор и оценка данных инициатив, проведенные Комитетом в тесном сотрудничестве со своим экспертным советом, Общественной палатой Российской Федерации и другими площадками взаимодействия с органами федеральной и региональной исполнительной власти, общественности и бизнеса – то есть тех, кому принятые законы предстояло в дальнейшем выполнять, позволили рекомендовать ряд инициатив к принятию.

В связи со складывающейся ситуацией законопроекты, направленные на обеспечение информационной безопасности Российской Федерации, рассматривались в первоочередном порядке. Можно выделить ряд направлений законодательного обеспечения информационной безопасности, отразившихся впоследствии в принятых Государственной Думой законах.

Первое. Совершенствование механизмов защиты общества от противоправной информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, разжиганию межнациональной и (или) межконфессиональной розни, участию в террористической деятельности, в публичных массовых мероприятиях, проводимых с нарушением установленного порядка, – в отношении той информации, что распространяется в информационно-телекоммуникационных сетях (в том числе в сети Интернет). Положения об их совершенствовании были закреплены в Федеральном законе от 28 декабря 2013 года №398-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» (в части установления порядка ограничения доступа к информации, распространяемой с нарушением закона). Таким образом был поставлен законодательный барьер для использования современных средств коммуникации в целях организации преступных действий, направленных на нарушение работы органов управления страной, было затруднено воздействие на органы власти в обход существующих демократических процедур и создан определенный правовой задел для действий правоохранительных органов по пресечению попыток разрушения государственного строя.

Второе. Обеспечение защиты прав граждан Российской Федерации и упорядочение распространения информации и обмена данными между пользователями в информационно-телекоммуникационной сети Интернет. Для организаторов распространения информации и обмена данными пользователей в сети Интернет установлена обязанность в течение шести месяцев хранить информацию о приеме, передаче, доставке и обработке голосовой информации, письменного текста, изображений, звуков или любого рода действиях, совершенных пользователями при распространении информации и (или) обмене данными, а также в случаях, установленных федеральными законами, предоставлять указанную информацию уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечивающим безопасность Российской Федерации. Указанные нормы закреплены в Федеральном законе от 5 мая 2014 года №97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей». В данном законе впервые в отечественной практике было введено понятие «организатор распространения информации». Данная мера была выработана в процессе консультаций с правоохранительными органами и общественностью с целью максимально обезопасить обычных граждан, являющихся пользователями информационно-коммуникационной сети Интернет, от случайных ошибок при осуществлении проверок исполнения законодательства.

Третье. Обеспечение защиты персональных данных граждан Российской Федерации, а также уточнение порядка обработки персональных данных в информационно-телекоммуникационных

сетях. В Федеральном законе №152-ФЗ «О персональных данных» установлена обязанность оператора персональных данных обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, расположенных на территории Российской Федерации, а также указывать сведения о месте расположения таких баз данных. Кроме того, определен порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, а также на основании вступившего в законную силу судебного акта установлена возможность ограничивать доступ к указанной информации. Указанные нормы закреплены в Федеральном законе от 21 июля 2014 года №242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях», который вступил в силу с 1 сентября 2014 года. Данный закон довел отечественную нормативную базу до уровня обеспечения защиты персональных данных, существующего в США и Европейском союзе. Исполнение данного закона позволит исключить уничтожение или искажение личных данных граждан Российской Федерации за счет наличия физического доступа к серверам, на которых осуществляется хранение баз данных.

Четвертое. Обеспечение порядка деятельности средств массовой информации с иностранным участием. Установлен запрет на создание либо участие в учреждаемых или действующих в Российской Федерации средствах массовой информации в отношении российского юридического лица с иностранным участием независимо от доли такого участия, и разрешено опосредованное участие в таких средствах массовой информации российским юридическим лицам с иностранным участием, не превышающим 20%. Данные положения закреплены в Федеральном законе от 14 октября 2014 года №305-ФЗ «О внесении изменений в Закон Российской Федерации «О средствах массовой информации». Вступление в силу положений данного Федерального закона предусмотрено с 1 января 2016 года, в полном объеме они будут действовать с 1 января 2017 года. Исполнение данного закона является одним из дополнительных способов обеспечить независимость редакций от влияния иностранных собственников средств массовой информации

Пятое. Обеспечение информационной безопасности сайтов государственных органов и учреждений, муниципальных образований посредством обязательного размещения технических средств на территории Российской Федерации. Соответствующие положения закреплены во вступившем в силу Федеральном законе от 31 декабря 2014 года №531-ФЗ «О внесении изменений в статьи 13 и 14 Федерального закона «Об информации, информационных технологиях и о защите информации» и Кодекс Российской Федерации об административных правонарушениях». Исполнение этого закона должно обеспечить невозможность использования физического доступа к серверам органов государственной и муниципальной власти, а также других учреждений государства и муниципалитетов с целью нарушения их работы или разрушения порядка оказываемых населению государственных и муниципальных услуг.

Острым вопросом национальной безопасности является прекращение зависимости от внешних источников промышленных товаров. Эта задача, затрудняющая влияние внешних сил на отечественную политику и экономику за счет ограничительных мер, определена Президентом России как импортозамещение.

С января 2014 года тема импортозамещения активно обсуждалась в стенах Государственной Думы. В качестве основной задачи рассматривалась выработка конкретных законодательных инициатив, нацеленных на поддержку процесса становления отечественных производств. В первую очередь фокус направлен на программное обеспечение, так как это та сфера, где импортозамещение наиболее логично. Аналогичная деятельность в данный период велась и Министерством связи и массовых коммуникаций Российской Федерации с целью выработки постановления Правительства Российской Федерации, направленного на приоритетность закупок российского софта.

Однако ряд препятствий тормозил продвижение инициатив: в законодательстве не было понятия «российский производитель программного обеспечения», а без него невозможно сформулировать требования к закупщикам: становится непонятно, кого следует поддерживать. Кроме того, в области интеллектуальных технологий плохо работали законы №44-ФЗ и 223-ФЗ о закуп-

ках для государственных и муниципальных нужд. Ежегодно государственными и муниципальными органами заключаются десятки тысяч контрактов, на закупки иностранного программного обеспечения тратятся миллиарды долларов.

Принимая во внимание остроту проблемы и недопустимость дальнейшего затягивания процесса избавления государственных и муниципальных органов и учреждений от зависимости от иностранных поставщиков, Комитет активно участвовал в разработке законопроекта, предложенного Институтом развития Интернета («Единый реестр российских программ для ЭВМ или баз данных»), который впоследствии был внесен в Государственную Думу рядом депутатов. Решая внести этот законопроект, Комитет также руководствовался тем, что программное обеспечение – наиболее перспективная тема для импортозамещения. В других технологических сегментах сферы ведения Комитета (вещательная аппаратура, связь, полиграфия) речь в лучшем случае может идти о локализации иностранных решений или об упрощении импорта из стран БРИКС. В сфере интеллектуальных технологий (особенно программного обеспечения) мы имеем готовые конкурентоспособные компании, в том числе мирового уровня. В сложной внешнеполитической и экономической ситуации целесообразно использовать самые сильные стороны отечественной экономики.

Сложившаяся к 2014 году ситуация на отечественном рынке софта была крайне несправедлива. Как и для любого высокотехнологичного бизнеса, проблема спроса для программного обеспечения – ключевая. Компании – разработчики программ из западных стран опираются на свои отечественные рынки. В то же время российские государственные закупщики в условиях политического давления и прямых санкций продолжали кормить западных производителей. Ситуация сохранялась, несмотря на прямые указания президента о безотлагательных мерах по импортозамещению. Отключение крымских пользователей устранило последние иллюзии, хотя в целом заинтересованная часть общественности утратила их уже после опубликованных разоблачений Эдварда Сноудена.

С учетом госкомпаний до 70% рынка программного обеспечения приходится на государственные и муниципальные организации. По различным сегментам рынка корпоративного программного обеспечения доля, принадлежавшая в 2014 году иностранным поставщикам, составляла от 50 до 97%. Граничные цифры – это 50% у западных поставщиков на рынке сервисов обмена информацией (включая почту) и 97% на рынке офисных программ. В то же время отечественные решения в программном обеспечении позволяли удовлетворить две трети спроса в пределах Российской Федерации. Однако российский софт занимал меньше трети рынка.

25 марта 2015 года состоялось расширенное заседание Комитета с целью обсудить законодательные возможности поддержки научно-технической революции, о необходимости которой говорил президент и которая в нынешних условиях невозможна без вывода в Интернет всей экономики страны. Фактически речь идет о создании новой экономики на базе электронных сетей обмена данными. На заседании присутствовали представители всех субъектов интереса в отрасли: бизнес, отраслевые ассоциации, регуляторы и потребители. Бизнес поддержал предложение Института развития Интернета оформить в виде законопроекта давно обсуждавшуюся в отрасли идею создания реестра отечественных программ и обязательности мотивированного объяснения закупки иностранного программного обеспечения госорганами. Надо сказать, что у нас сложилась своеобразная культура госзакупок западных программ. Эта культура не только представляет собой комфортный стереотип поведения закупщика, но и к тому же явно имеет коррупционную составляющую. Например, весной 2015 года, когда стала очевидной неизбежность принятия государственных мер по регулированию закупок импортных программных продуктов, начались лихорадочные закупки иностранного программного обеспечения, включая программы, по которым есть конкурентные отечественные решения (антивирусы).

Так как проблема не терпела отлагательств, отрасль сочла закон наиболее перспективным способом реализации данной идеи. Невыполнение закона – это подрыв авторитета государства (в том числе подписывающего закон президента).

Суть вышеупомянутого законопроекта подразумевала принятие двух мер: во-первых, создается реестр отечественных программ; во-вторых, закупщику вменяется в обязанность мотивированно объяснять причины приобретения иностранных программ при наличии отечественных аналогов.

Первоначально законопроект мог показаться излишне подробным в сравнении с принятой практикой. Например, он содержал критерий определения программного обеспечения как отечественного (по принадлежности исключительных прав), что было обусловлено отсутствием определения национальной принадлежности программ в отечественном законодательстве (его не было даже в Таможенном кодексе Таможенного союза: таможенное оформление применимо к носителям, а к программному обеспечению – нет). Отсутствие такого критерия рассматривалось как один из тормозов для принятия мер поддержки отечественных производителей программного обеспечения.

Подготавливая данный законопроект к рассмотрению Государственной Думой, Комитет понимал, что в других развитых странах (на Западе и в КНР) данные вопросы часто решаются на уровне подзаконных актов и даже неформальных рычагов, но у нашей страны может быть своя специфика. Например, наше избирательное законодательство тоже намного более детальное, чем западное. И у наших партнеров по БРИКС существуют прямые законодательные ограничения на закупки иностранного софта для госорганов.

Рассматриваемый закон позволит сдвинуть ситуацию с мертвой точки, четко определить круг отечественных производителей, поддержка которых должна быть приоритетом всех заинтересованных федеральных и региональных органов власти, а также однозначно определит ответственность Правительства России за дальнейшие шаги (по существующему законодательству, реализация данного закона невозможна без специального постановления правительства).

Говоря о дальнейших шагах, можно сразу обратить внимание на то, что данный закон является крайне мягкой мерой. Фактически он направлен на стимулирование общественного контроля (со стороны отечественного бизнеса) и повышение эффективности маркетинговых инструментов российских разработчиков программного обеспечения (через накопление мотивировок). В дальнейшем возможно ужесточение закона за счет введения санкций вследствие формальных или недобросовестных мотивировок, хотя привлечение к ответственности возможно и сейчас за мошенничество, халатность или коррупцию, а также прямое предоставление преимущества зарубежным производителям при госзакупках. Но об этом можно говорить только по мере накопления опыта. Отечественное производство программного обеспечения – это «нежный драгоценный цветок», который выращивался много лет, и здесь мы не можем рисковать. Так, например, как это было, когда пытались пересадить чиновников на «Волги». В отличие от автопрома, отечественный софт крайне конкурентоспособен, и нам не хотелось бы подрывать его репутацию неуклюжими мерами защиты. Вместе с тем никто не ограничивает возможностей правительства (согласно закону №44-ФЗ) вводить дозированные и секторальные ограничительные меры в сегментах рынка, где отечественное программное обеспечение полностью конкурентоспособно (антивирусы, бизнес-приложения).

Рекомендуя данный закон к принятию, Комитет отдавал себе отчет, что налоговые и кредитные стимулы в виде законодательных инициатив займут слишком много времени, а целевое субсидирование в текущей экономической ситуации маловероятно. Поэтому целесообразно двигаться по пути дальнейшего стимулирования справедливой конкуренции.

Таким образом, 2014 год стал переломным в законодательной деятельности в отношении информационной безопасности Российской Федерации. Внимание общества было перефокусировано на тему защиты отечественных информационно-коммуникационных сетей. Созданная как «единое окно» взаимодействия общественности (в первую очередь деловой) с государством некоммерческая организация Институт развития Интернета начала прямое сотрудничество с парламентом, в итоге был принят ряд законов, непосредственно направленных на защиту отечественного информационного пространства.

Дальнейшее совершенствование законодательной базы (кроме развития идей, закрепленных в уже принятых законах) необходимо осуществлять как за счет законодательного обеспечения безопасности составляющих Федерации – регионов и муниципалитетов, так и за счет развития международных систем безопасности с целью обеспечения суверенитета России в целом.

Развитие технических средств, коммерциализация значительных массивов технологий двойного назначения и вредоносного программного обеспечения четко ставят вопрос о создании систем противодействия иностранным техническим разведкам и технической защиты информа-

ции на уровне не только субъектов Федерации, но и отдельных муниципалитетов. Такие системы должны быть способны – во взаимодействии с федеральными органами – противостоять агрессивным действиям как отдельных государств или их блоков, так и негосударственных формирований.

В настоящее время ни один из федеральных законов, в том числе и федеральные законы от 6 октября 1999 года №184-ФЗ «Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации» и от 6 октября 2003 года №131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», не предусматривает прямого механизма финансирования работ по защите информации субъектами Федерации и муниципалитетами. Отсутствие такого механизма (конкретных бюджетных статей) является одним из факторов, сдерживающих выполнение требований уже давно действующего законодательства в сфере информационной безопасности, в том числе и положений Указа Президента Российской Федерации от 17 марта 2008 года №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Законодательное закрепление на федеральном уровне финансирования мероприятий по обеспечению информационной безопасности путем внесения в бюджетную классификацию соответствующих статей расхода может стать (за счет упрощения отчетности) фактором повышения эффективности обеспечения защиты информации.

В целях реализации данной идеи Комитету следует обсудить с заинтересованными федеральными органами исполнительной власти, а также с наиболее квалифицированными представителями органов местного самоуправления, ка́к конкретно определять статью расходов в предполагаемых поправках к вышеназванному закону №131-ФЗ. Необходимо определить принципы финансового обеспечения осуществления органами государственной власти субъекта Российской Федерации и органами местного самоуправления полномочий по предметам ведения Российской Федерации и по предметам совместного ведения Российской Федерации и субъектов Российской Федерации, которые будут использованы при финансировании шагов по противодействию иностранным техническим разведкам и по защите информации в системе региональной государственной гражданской службы и муниципальной службы. Также в этой сфере целесообразно выявить возможные противоречия и не подпадающие под действие законодательства моменты, связанные с отнесением сведений к служебной тайне, их защитой и снятием ограничений на доступ к указанным сведениям в целях обеспечения прав, свобод и законных интересов граждан и организаций, осуществлением установленных законодательством Российской Федерации полномочий федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

На направлении международного сотрудничества по обеспечению безопасности Российской Федерации наиболее актуальной задачей в сфере ведения Комитета является совершенствование правовых механизмов информационной безопасности и информационного взаимодействия в рамках Евразийского экономического союза. Один из главных компонентов здесь – создание и развитие интегрированной информационной системы и трансграничного пространства доверия в рамках этого объединения. Такая задача обусловлена необходимостью реализовывать положения статьи 23 Договора о Евразийском экономическом союзе «Информационное взаимодействие в рамках Союза» и приложения 3 к Договору о Евразийском экономическом союзе «Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза».

Необходимость законодательной работы на международном уровне вытекает из тенденций развития нашей страны и ее места в мировом сообществе. В ближайшие два года в Интернет будет вовлечено абсолютно всё активное население России. С другой стороны, неизбежное развитие технологии «Интернет вещей» (Internet of Things) сделает всю экономику экономикой трансграничных сетей. Поэтому законодательной власти предстоит внести свою долю в обеспечение устойчивости и независимости функционирования информационно-коммуникационных сетей от волюнтаристских воздействий со стороны отдельных политиков в мировом сообществе. Наши партнеры по БРИКС на всех мероприятиях, не исключая и прошедших в мае 2015 года переговоров на высшем уровне, пос-

тоянно высказывали озабоченность фактическим диктатом одной страны в Интернете. Диктат этот выражается не только в наличии у этой страны рычагов политического контроля, но и в монополизации отдельных ключевых сегментов производства программного обеспечения и инфраструктуры. Создание альтернативы сложившейся системе требует взаимного открытия экономик стран БРИКС и разработки взаимоприемлемых стандартов. Первичным условием для движения в этом направлении будет создание отечественной операционной системы на основе программного обеспечения с открытым кодом. Всё это требует последовательного диалога, продвижения пробных, экспериментальных проектов и предсказуемого и прозрачного изменения нормативной базы. Хотя открытый код не является средством обезопасить себя от наличия программных закладок, особенно когда программы разрабатываются в большом количестве юрисдикций и с участием специалистов различной организационной принадлежности (чего невозможно избежать в современных условиях), создание национальной операционной системы (даже в режиме перспективной разработки) станет серьезным шагом к обеспечению доверия к отечественной схеме управления информационно-коммуникационными сетями на национальном и международном уровне.

В ближайшее время российской законодательной власти в целом и Комитету Государственной Думы по информационной политике, информационным технологиям и связи в частности предстоит существенное расширение сотрудничества с региональными и муниципальными органами власти, органами законодательной власти ближайших партнеров Российской Федерации в мировом сообществе. В условиях постоянно растущей трансграничности и ускорения обмена содержанием в информационно-коммуникационных сетях это делать необходимо.