СТРАТЕГИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И РАЗВИТИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ДЕПАРТАМЕНТА КОНСТИТУЦИОННОГО ЗАКОНОДАТЕЛЬСТВА И ЗАКОНОДАТЕЛЬСТВА О БЕЗОПАСНОСТИ МИНЮСТА РОССИИ
Татьяна Анатольевна Полякова

Одним из основных принципов развития информационного общества в Российской Федерации является обеспечение национальной безопасности в информационной сфере и в этой связи особое значение приобретает утверждение Указом Президента Российской Федерации от 12 мая 2009 года №537 Стратегии национальной безопасности Российской Федерации до 2020 года (далее – Стратегия национальной безопасности).

Стратегия национальной безопасности разработана Советом Безопасности Российской Федерации по поручению Президента России. Ранее действовавшая Концепция национальной безопасности, принятая в 1997 году (в редакции 2000 года), несомненно, сыграла свою положительную роль. Но к настоящему времени произошли серьезные изменения как у нас в стране, так и во всем мире. Стремительно меняется парадигма развития человеческого общества, усиливаются процессы глобализации во всех сферах, осуществляется переход к глобальному информационному обществу, появляются новые вызовы и угрозы военно-политического, криминального, террористического характера – эти тенденции влияют на динамику развития техники и технологий, среди которых нельзя не отметить информационные технологии.

Главное отличие нового документа от Концепции национальной безопасности заключается в подходах к обеспечению национальной безопасности через достижение стратегических национальных приоритетов.

Вместе с целями, угрозами, задачами и предложенными мерами по их реализации образуется стройная система, определяющая состояние национальной безопасности и уровень устойчивого развития государства в краткосрочной (до 2012 года), среднесрочной (до 2015 года) и долгосрочной (до 2020 года) перспективе. В соответствии со Стратегией национальной безопасности должно обеспечиваться устойчивое развитие России, ее становление в качестве конкурентоспособного государства с высокотехнологичной промышленностью, современным оборонным потенциалом и достойным качеством и уровнем жизни народа.

В Стратегии национальной безопасности заложен принцип безопасности через устойчивое развитие, в первую очередь экономики и социальной сферы, предусматривающий социальные, политические и экономические преобразования для создания безопасных условий реализации конституционных прав и свобод российских граждан. Этот принцип также является одним из главных принципов развития глобального информационного общества.

Стратегия национальной безопасности – это документ, имеющий общенациональный характер, который не может быть реализован только усилиями органов государственной власти, нацеленный на повышение качества государственного управления и координацию деятельности органов государственной власти, государственных и общественных организаций по защите национальных интересов России и обеспечению безопасности личности, общества и государства. Следует при этом отметить, что партнерство государства, бизнеса и гражданского общества – это один из основополагающих принципов развития информационного общества.

В Стратегии национальной безопасности отражены ключевые положения Послания Президента Российской Федерации Федеральному Собранию Российской Федерации от 5 ноября 2008 года, в котором определены следующие приоритетные направления в области

внутренней и внешней политики обеспечения национальной безопасности: совершенствование политической системы; оптимизация государственного управления; консолидация усилий и ресурсов федерального центра и регионов на решении задач долгосрочного социально-экономического развития страны; повышение возможностей государства в области национальной обороны и безопасности; развитие производства и новых технологий; создание основы национальной конкурентоспособности; следование идеалам многовековой отечественной культуры и духовности; повышение уровня и качества жизни российских граждан. Указанные направления также отражены в целях, задачах и принципах формирования и развития информационного общества в Российской Федерации.

Стратегия национальной безопасности по своему замыслу, структуре и содержанию взаимоувязана не только с Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, но, как уже отмечалось, и со Стратегией развития информационного общества в Российской Федерации, утвержденной Президентом Российской Федерации 7 февраля 2008 года №Пр-212.

В разделе V Стратегии национальной безопасности наряду с организационными, нормативными правовыми основами ее реализации значительная роль отводится мерам информационного характера. В связи с построением информационного общества в Российской Федерации заслуживают особого внимания следующие определенные в указанном документе задачи:

– необходимость информационной и информационно-аналитической поддержки реализации Стратегии национальной безопасности за счет привлечения информационных ресурсов заинтересованных органов государственной власти и государственных научных учреждений с использованием системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия;

– преодоление в среднесрочной перспективе технологического отставания в важнейших областях информатизации, телекоммуникаций и связи, определяющих состояние национальной безопасности;

– разработка и внедрение технологии информационной безопасности в системах государственного и военного управления, системах управления экологически опасными производствами и критически важными объектами;

– обеспечение условий для гармонизации национальной информационной инфраструктуры с глобальными информационными сетями и системами.

Представляется особенно важным также положение, содержащееся в пункте 108 Стратегии национальной безопасности, о том, что угрозы информационной безопасности в ходе реализации указанного стратегического документа предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации, а также повышения уровня защищенности корпоративных и индивидуальных информационных систем. При этом выделено создание единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.

Организационные меры реализации государственной политики Российской Федерации в области национальной безопасности напрямую связаны с целями, задачами и принципами развития информационного общества в части совершенствования системы государственного управления на основе использования информационных и телекоммуникационных технологий.

Фундаментальными положениями Стратегии национальной безопасности являются взаимосвязь и взаимозависимость устойчивого развития государства и обеспечения национальной безопасности. При этом ее важнейшая особенность – это социальная и социально-политическая направленность и обеспечение достойных условий жизни в России, которые признаются такими же приоритетами обеспечения национальной безопасности, как и традиционные направления безопасности – национальная оборона, государственная и общественная безопасность.

Следует отметить, что в указанном документе определены не только стратегические цели обеспечения национальной безопасности в области повышения качества жизни российских граждан, являющиеся целями развития информационного общества в Российской Федерации. Прямо указано, что для противодействия угрозам национальной безопасности в этой области силы обеспечения национальной безопасности во взаимодействии с институтами гражданского общества наряду с другими направлениями обеспечивают доступность информационных технологий, а также информации по различным вопросам социально-политической, экономической и духовной жизни общества.

В связи с этим нельзя не отметить значение принятия давно ожидаемых федеральных законов «О доступе к информации о деятельности органов государственной власти и органов местного самоуправления» (от 9 февраля 2009 года №8-ФЗ) и «О доступе к информации о деятельности судов в Российской Федерации (от 22 декабря 2008 года №262-ФЗ), которые вступают в силу соответственно с 1 января 2010 года и с 1 июня 2010 года.

Следует иметь в виду, что в настоящее время вопросы обеспечения доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти регламентированы постановлением Правительства Российской Федерации от 12 февраля 2003 года №98, которое нуждается в приведении в соответствие с действующим законодательством. В то же время постановлением Правительства Российской Федерации от 18 мая 2009 года №424 в соответствии с частью 6 статьи 15 Федерального закона «Об информации, информационных технологиях и о защите ин-

1

формации» определены особенности подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям и обязанности операторов федеральных государственных информационных систем, созданных или используемых в целях реализации полномочий федеральных органов исполнительной власти и содержащих сведения, указанные в перечне сведений о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательных для размещения в информационно-телекоммуникационной сети Интернет.

В Стратегии национальной безопасности сделаны акценты и на проблемы международной безопасности, связанные с глобализацией, отмечены недостатки международной и региональной архитектуры безопасности, а также отсутствие правовых инструментов и международных механизмов ее обеспечения и угрозы, связанные с развитием информационного общества. К таким проблемам, несомненно, относится и глобализация информационной инфраструктуры, включая вопросы интернационализации управления сетью Интернет.

По вопросу необходимости и возможности правового регулирования отношений в сети Интернет в настоящее время существуют полярные точки зрения, даются различные оценки функционирования в Рунете интернет-сайтов, пропагандирующих терроризм и экстремизм. Делаются выводы о невозможности правового регулирования отношений, связанных с использованием Интернета, учитывая его трансграничность, о проблемах ответственности провайдеров, управления Интернетом и т.д. Однако при этом бесспорно, что глобализация в информационной сфере – угроза не только национальной, но и международной безопасности, порождающая новые угрозы, не совместимые с задачами мировой стабильности и безопасности. Это следует и из Стратегии национальной безопасности.

Сегодня уже невозможно себе представить отсутствие мобильной связи, персональных компьютеров и сети Интернет, которые прочно вошли в повседневную жизнь, но развитие информационных технологий значительно опережает их гуманитарное осмысление, прежде всего в области права.

Информационное общество – это реальность, и отнюдь не виртуальная, которую мировое сообщество осознало и приняло. Это подтверждается как международными актами, так и развитием зарубежного законодательства и информационного законодательства Российской Федерации.

Рассматривая стратегические вопросы национальной безопасности в информационной сфере, необходимо иметь в виду, что важнейшими принципами построения информационного общества, являющимися основным вектором в этой деятельности, не случайно определены такие как укрепление доверия и безопасности, а также верховенство права. В Декларации принципов построения информационного общества (Декларации тысячелетия) отмечается, что информационно-коммуникационные технологии открывают совершенно новые перспективы для достижения более высоких уровней развития. В Российской Федерации имеются необходимые условия для перехода к информационному обществу. В Стратегии национальной безопасности, отличающейся, как уже отмечалось, социальной и социально-политической направленностью, национальная безопасность обеспечивается по формуле «безопасность – через приоритеты устойчивого развития».

Правовое урегулирование информационных отношений при построении информационного общества в России, пронизывающих все сферы жизнедеятельности, требует концептуальных, системных подходов, поскольку резко ускоряющиеся информационно-коммуникативные процессы глобализации эволюционируют в качественно новое состояние – режим реального времени – и создают новые угрозы национальной безопасности.

Одним из необходимых условий построения информационного общества является развитие системы нормативного правового регулирования отношений в области создания и использования информационно-телекоммуникационных технологий. В то же время будет справедливым признать, что именно общественные

2

отношения в информационной сфере, пронизывающей сегодня практически все области жизнедеятельности человека, общества и государства, являются импульсом, влияющим на развитие информационного законодательства. В Стратегии национальной безопасности также отмечается значение мер нормативной правовой поддержки реализации данной Стратегии, а значит и всей информационной сферы. В связи с этим в целях совершенствования правового регулирования должно происходить изменение и переосмысление отношений и понятий, связанных с информационной сферой.

Следует признать, что формирование правовых основ единого информационно-телекоммуникационного пространства России тесно связано с международным и зарубежным опытом и должно осуществляться на основе, как уже отмечалось, принципа системности и сбалансированности правовых норм с учетом общепризнанных принципов и норм международного права.

Эта тенденция в развитии информационного законодательства в России особенно очевидна в связи с необходимостью правового урегулирования целого ряда вопросов, касающихся использования Интернета в противоправных, особенно в террористических и экстремистских целях, что является проблемой международного масштаба. В этой связи следует отметить, что представители Российской Федерации принимают активное участие в деятельности группы экспертов Римской/Лионской «группы восьми» по борьбе с транснациональной организованной преступностью. В частности, в рамках подгруппы по борьбе с преступлениями в сфере высоких технологий разрабатываются проекты, направленные на обеспечение международной информационной безопасности (борьба с анонимностью и использованием сети Интернет в террористических целях, а также борьба с киберпреступностью, взаимодействие с интернет-провайдерами и др.).

В настоящее время актуальным остается вопрос об установлении ограничений 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 (горячих линий) на содержание информации, использованию инструментов условного доступа с помощью кодов, шифров и паролей, а также функционированию системы сотрудничества саморегулируемых организаций провайдеров и пользователей с правоохранительными органами.

В статье 10 Федерального закона от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» предусмотрена обязательная идентификация обладателя информации или ее распространителя, запрещено распространение информации, за которую установлена административная и уголовная ответственность, но не разработан правовой механизм реализации этой правовой нормы. Сегодня анонимность в Интернете – это серьезная неурегулированная проблема, создающая определенные условия для совершения противоправных действий и представляющая угрозу безопасности.

Нельзя не признать, что информационное законодательство развивается не такими быстрыми темпами, как этого требует время. Так, до настоящего времени еще не приняты федеральные законы о внесении изменений в законодательные акты в связи с принятием еще в 2006 году так называемого «трехглавого закона» «Об информации, информационных технологиях и о защите информации» и Федерального закона «О персональных данных». Эта сложная, но необходимая работа по приведению законодательства в соответствие с указанными федеральными законами нуждается в активизации. Особенно это касается создания законодательных правовых механизмов, необходимых для реализации Федерального закона «О персональных данных» и имплементации положений международных актов (Конвенции о защите физических лиц при автоматизированной обработке персональных данных), соответствующий проект закона был принят Государственной Думой в первом чтении еще в ноябре 2005 года.

Кроме того, не определены основания для прекращения права пользования доменными именами и отмены их регистрации, не установлены обязанности провайдеров по удалению информации экстремистского и террористического толка, а также не предусмотрены меры

3

4

по идентификации пользователей информационно-телекоммуникационных систем и созданию «национального электронного пространства доверия». Пока еще должным образом не реализуется Федеральный закон «Об электронной цифровой подписи».

Нуждается в более широком применении информационных технологий и судебная система в Российской Федерации. Внедряется Государственная автоматизированная система Российской Федерации «Правосудие». Все это приводит к необходимости разработки соответствующих процессуальных норм, в частности для подтверждения подлинности электронных судебных документов.

В информационном обществе использование информационных технологий должно служить обязательным критерием эффективности работы ведомств, властей регионов и органов местного самоуправления. Для этого необходимы объективные оценочные показатели их развития и внедрения.

Следует отметить, что в рамках административной реформы, проводимой в России, продолжается активный процесс разработки административных регламентов, которые направлены как на повышение эффективности государственного управления, так и в значительной степени на оказание гражданам публичных услуг.

В целях обеспечения информационной открытости деятельности органов исполнительной власти и органов местного самоуправления, повышения качества и доступности предоставляемых ими государственных и муниципальных услуг постановлением Правительства Российской Федерации от 15 июня 2009 года №478 одобрена Концепция единой системы информационно-справочной поддержки граждан и организаций по вопросам взаимодействия с органами исполнительной власти и органами местного самоуправления с использованием информационно-телекоммуникационной сети Интернет и утверждены Правила размещения сведений о государственных и муниципальных услугах (функциях) в федеральных государственных информационных системах «Сводный реестр государственных и муниципальных услуг (функций)» и «Единый портал государственных и муниципальных услуг (функций)».

Задача формирования нормативной правовой базы в информационной сфере определена как одна из приоритетных при построении глобального информационного общества и должна обеспечивать каждому доступ к информации, идеям и знаниям, вносить в эти области свой вклад при построении открытого информационного общества.

Информационные войны, информационный терроризм и киберпреступность стали, к сожалению, реальностью нашего времени. Сегодня международное сообщество осознало, в том числе благодаря российским инициативам, угрозу национальной и глобальной информационной безопасности и готово к практическим шагам по ее нейтрализации. Во многих странах предпринимаются порой весьма жесткие меры в этой сфере, но они оказываются малоэффективными, прежде всего вследствие трансграничного характера новых угроз и анонимности нарушителей. Никто не может чувствовать себя надежно защищенным, в одиночку сражаясь с информационными угрозами.

Система информационной безопасности в Российской Федерации должна обеспечивать сохранение государственной и других видов тайн, защищать информационные ресурсы и информационно-телекоммуникационную инфраструктуру от воздействия информационного оружия, угроз информационного терроризма и использования информационных технологий в преступных целях.

Построение информационного общества связано с необходимостью научных исследований фундаментальных положений права исходя из эволюционирования функций государства не только по обеспечению национальной безопасности, но и выделения функции государства по обеспечению информационной безопасности в качестве самостоятельной.

Необходимость системного методологического подхода к исследованию указанных вопросов связана с тем, что информационная безопасность играет все более значимую роль в общей системе обеспечения национальной безопасности Российской Федерации и это целиком отображает задачи Стратегии национальной безопасности. Так, при определении сфер, на которых долж-

5

ны быть сосредоточены усилия и ресурсы сил и средств обеспечения национальной безопасности, информационная сфера занимает не последнее место (пункт 7 Стратегии национальной безопасности), а в значительной степени пересекается практически со всеми другими.

Представляется, что при построении информационного общества особого внимания заслуживают вопросы выработки государственной политики в области обеспечения информационной безопасности, создания государственной системы правовой информации, правовых механизмов государственного учета и регистрации информационных систем и ресурсов, необходимых для системы навигации на основе мониторинга государственных (федеральных и региональных), а также муниципальных и иных информационных систем и ресурсов, их учета и интеграции, обеспечения решения задач по предоставлению государственных информационных услуг в рамках систем межведомственного взаимодействия органов государственной власти.

Широкий спектр проблем информационной безопасности личности, общества и государства, развития культуры кибербезопасности, обеспечения неприкосновенности частной жизни и реализации прав на доступ к информации, защиты информационных систем, ресурсов и сетей, расширения применения информационных технологий в государственном управлении и при оказании государственных услуг, а также целый ряд других проблем информационной безопасности нуждаются в системном правовом регулировании на основе тщательного анализа международных правовых норм, с использованием зарубежного опыта, российской правоприменительной практики.

Транснациональность угроз информационной безопасности и уровень ущерба при их реализации заставляют сегодня как никогда признавать проблему обеспечения информационной безопасности как глобальную, требующую усилий всего мирового сообщества. Заслуживает особого внимания предложение о создании международного органа при ООН, координирующего управление в Интернете.

Учитывая роль ООН в современном мире как беспрецедентную, можно сделать вывод, что сегодня нет других таких универсальных площадок, как ООН, для согласования интересов участников глобального информационного общества и решения вопросов, связанных с обеспечением международной информационной безопасности, включая интернационализацию управления Интернетом. ООН накопила богатый опыт, выработала систему международного права. Ни одна страна в одиночку не способна решить международные проблемы информационной безопасности, поэтому так важно создание и развитие системы международной информационной безопасности на основе международного информационного права.

Анализ стратегических программ, разработанных в экономически развитых странах, показывает, что их основная цель – достижение лидирующих позиций в экономике и социальном развитии. Все используемые информационные технологии, включая электронную коммерцию, электронное правительство, информатизацию науки и образования, здравоохранения и т.д., рассматриваются как интегрированная, взаимосвязанная совокупность всей информационно-телекоммуникационной сферы – фундамент для перехода к информационному обществу.

Решение всех этих проблем в правовом государстве тесно связано с созданием в Российской Федерации современной, эффективной системы правосудия, которая будет адекватно решать стоящие перед ней задачи на основе применения современных информационных технологий, обеспечивая доступность правосудия, самостоятельность судов и независимость судей, повышение авторитета судебной власти, поддержание требуемого баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации. Это является важной составляющей построения в России информационного общества. Для этого необходимо внедрение электронного документооборота, определение понятия электронного документа, механизма подтверждения его подлинности, использование в качестве письменных доказательств в суде и т.д.

Очевидно, что в условиях террористической угрозы государственная политика в информационной сфере смещается в сторону обеспечения информационной

безопасности. Для установления организационно-правовых особенностей обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры различных видов собственности и установления форм и методов государственного регулирования ее обеспечения необходимо не только принятие федерального закона, касающегося особенностей обеспечения информационной безопасности указанных объектов, но и усиление ответственности за несоблюдение требований по информационной безопасности.

Среди первоочередных мер по совершенствованию нормативного правового обеспечения информационной безопасности необходима разработка концепции правовых основ информационного общества Российской Федерации, включая вопросы партнерства государства, бизнеса и гражданского общества. Назрела необходимость скорейшего принятия федеральных законов об информации ограниченного доступа (информации конфиденциального характера), об информационном взаимодействии органов государственной власти, законодательном закреплении роли Совета Безопасности Российской Федерации по выработке государственной политики в области обеспечения национальной безопасности, включая и информационную сферу.

В целях реализации Стратегии национальной безопасности необходимо законодательно установить государственную регистрацию и учет государственных информационных систем и ресурсов.

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» государственные информационные системы создаются на основании федеральных законов, законов субъектов Российской Федерации, а также на основании правовых актов государственных органов. В то же время действующее сегодня Временное положение о государственном учете и регистрации баз и банков данных, утвержденное постановлением Правительства Российской Федерации от 28 февраля 1996 года №226 «О государственном учете и регистрации баз и банков данных», устанавливает правила учета и регистрации баз и банков данных с использованием при их создании средств федерального бюджета, то есть в соответствии с ранее действовавшим федеральным законом. В связи с чем имеются значительные различия как в понятийном аппарате, так и в концептуальных основах правовой регламентации учета и регистрации государственных информационных систем и ресурсов.

Необходимость обеспечения информационной безопасности государственных информационных систем и ресурсов требует внесения соответствующих дополнений в Федеральный закон «Об информации, информационных технологиях и о защите информации», связанных с их государственной регистрацией, а также введением оценки их соответствия требованиям о защите информации. При этом следует учитывать, что в соответствии со статьей 5 Федерального закона «О техническом регулировании» оценка соответствия государственной информационной системы представляет собой прямое или косвенное определение соблюдения указанных требований, предъявляемых к объекту, которым является и государственная информационная система.

Таким образом, в качестве приоритетных задач правового обеспечения информационной безопасности, вытекающих из Стратегии национальной безопасности, следует также отметить необходимость:

– правового урегулирования вопросов, связанных с созданием и использованием сайтов сети Интернет, включая определение правового статуса доменного имени, интернет-издания, интернет-провайдера, а также реализацию конституционного запрета на пропаганду и агитацию, направленную на возбуждение социальной, расовой, национальной и религиозной вражды, экстремизма, в том числе терроризма, осуществляемую с использованием возможностей сети Интернет;

– развития законодательства об информации ограниченного доступа, в том числе определения принципов соотношения видов тайн и формирования соответствующих правовых режимов конфиденциальности, законодательного урегулирования режима служебной тайны;

– выработки механизмов реализации законодательства об обеспечении доступности информации о деятельности органов государственной власти и органов местного самоуправления, вопросов формирования открытых государственных информационных ресурсов в целях создания условий для разъяснения основных направлений государственной политики, обоснования принимаемых решений, поддержания информационного взаимодействия общества и государства, предоставления гражданам своевременной и объективной публичной информации;

– принятия нормативных правовых актов, обеспечивающих реализацию концепции электронного правительства, в том числе касающихся предоставления государственных услуг с использованием информационно-коммуникационных технологий, развития электронного документооборота и электронной коммерции на основе использования общедоступных информационно-телекоммуникационных сетей;

– совершенствования законодательства в части усиления защиты прав пользователей и субъектов, представляющих услуги связи и информационные услуги, создания эффективных механизмов контроля за соблюдением законодательства Российской Федерации в сфере информационных технологий и связи, включая и законодательство о персональных данных;

– правового закрепления механизмов реализации государственной поддержки отечественных производителей информационных и коммуникационных технологий;

– усиления ответственности за несоблюдение требований защиты критически важных объектов в части закрепления механизма отнесения объектов информационной инфраструктуры к крити-

чески важным и обеспечения их информационной безопасности, включая разработку и принятие требований к техническим и программным средствам, используемым в информационной инфраструктуре этих объектов;
– совершенствования законодательства о национальной безопасности и государственной тайне;
– создания национальной системы правовой информации;
– гармонизации и имплементации положений международных правовых актов в федеральное законодательство, связанных с реализацией положений о защите персональных данных, доступе к информации о деятельности органов государственной власти и местного самоуправления и обеспечении их транспарентности, направленных на борьбу с коррупцией и киберпреступностью, использованием электронных сообщений в международных договорах в области связи и защиты информации;
– продвижения международных инициатив и разработки международных правовых актов, направленных на создание международной системы информационной безопасности, включая интернационализацию управления Интернетом, обеспечение юридически значимого электронного документооборота.

Стратегия национальной безопасности исходит из принципа рациональной достаточности и эффективности, что особенно актуально в условиях мирового кризиса. Отмеченные проблемы правового обеспечения развития информационного общества несомненно связаны с задачами по обеспечению национальной безопасности, но пока не нашли еще оптимального решения и требуют современных подходов. В информационной сфере постоянно происходят значительные изменения, требующие неослабевающего внимания к этим вопросам, не только определения новых приоритетов и задач в информационной сфере, но и их практической реализации.