УДК [342.924:004](575.2)

СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА КЫРГЫЗСКОЙ РЕСПУБЛИКИ В КОНТЕКСТЕ КОНЦЕПЦИИ "БЕЗОПАСНЫЙ КЫРГЫЗСТАН"

Ш.Р. Муслимов

Исследованы проблемы информационной безопасности как одного из факторов безопасности государства, определены меры совершенствования отечественного законодательства для нейтрализации информационных угроз в контексте принятой в КРСУ концепции "Безопасный Кыргызстан".

Ключевые слова: информационная безопасность; защита информации; техническая защита информации; кибертерроризм; киберугрозы.

IMPROVEMENT OF THE INFORMATION LEGISLATION OF THE KYRGYZ REPUBLIC IN THE CONTEXT OF "SAFE KYRGYZSTAN"

Sh.R. Muslimov

Information security is studied as one of the important factors determining the security of the state. It also defines enhancement measures of domestic legislate on to address information security threats in the context of the KRSU concept "Safe Kyrgyzstan".

Key words: : information security; technical security; cyberterrorism; cyber threats.

В системе информационных отношений проблемы безопасности представляют институт не менее многогранный и сложный, чем институт массовых коммуникаций. Информационные технологии открывают область взаимодействия всех субъектов во всех направлениях общественных процессов, как позитивных, так и негативных. Обеспечение информационной безопасности можно сравнить с решением задач здравоохранения или экологической безопасности общества. В отношениях информационной безопасности создается цепочка генетической связи между пониманием и наполнением определенным смыслом таких понятий, как "опасность", "безопасность", "информационная безопасность", "обеспечение информационной безопасности", "правовое обеспечение информационной безопасности". Без понимания связи названных концептов невозможно наполнить необходимым содержанием понятие "правовое обеспечение", раскрывающее состояние законодательства в этой области.

Однозначного определения информационной безопасности пока не сложилось. Отмечаются несколько вариантов определения этого направления в области исследования информационной и коммуникационной деятельности и обеспечения безопасного состояния отношений в информационной сфере. Модельный закон МПА СНГ "О международном информационном обмене" (2002 г.) определяет информационную безопасность как "состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства". Концепция сотрудничества государств-участников Содружества Независимых Государств (СНГ) в сфере обеспечения информационной безопасности, утвержденная Советом глав государств СНГ в 2008 г., трактует информационную безопасность как "состояние защищенности от внешних и внутренних угроз информационной сферы, формируемой, развиваемой и используемой с учетом жизненно важных интересов личности, общества и государства". Большинство понятий в тексте концепции относятся, прежде всего, к задачам защиты информации.

В трактовке, закрепленной в тексте Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности

(Екатеринбург, 2009 г.), "информационная безопасность – состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве". В такой формулировке это базовое понятие охватывает наиболее актуальные угрозы социально-гуманитарного плана, в частности угрозу распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде государства.

В последние 15 лет произошло значительное расширение пространства и методов обеспечения информационной безопасности. Этот процесс хорошо представлен в специальных исследованиях по проблеме глобальной безопасности, учету перехода к ориентации на так называемую "мягкую силу 2.0" и тех вызовов, которые формируют глобальное информационное общество и появление новых источников угроз и преступлений [1]. Переход к "мягкой силе" – по существу к сочетанию жестких и мягких методов воздействия на информационную сферу – связан с пониманием недостаточности методов "защиты" и "охраны" информационных ресурсов и государственной тайны. Фронт информационной безопасности расширен до сферы открытой и доступной информации и ее влияния на все слои и сферы пользователей этим ресурсом.

С учетом таких изменений в Рекомендациях МПА СНГ наряду с охраной и защитой фиксируется принцип обеспечения "безопасности через развитие" [2].

В качестве специального принципа совершенствования законодательства государств-участников СНГ в рекомендациях названа "безопасность через развитие", что предполагает динамичное совершенствование правовых методов обеспечения информационной безопасности по мере развития информационного общества. В качестве одного из показателей информационной безопасности предложено рассматривать динамику социальных индикаторов реализации базовых интересов личности, общества и государства.

В контексте широкомасштабной правовой реформы, осуществляемой в различных сферах, в частности конституционной, судебной, административной происходит также совершенствование информационного законодательства.

Нельзя не обратить внимания на такой факт, как растущий уровень кибертерроризма, соединенный с неадекватным реагированием законодателя на данные процессы, в частности формирование эффективного информационного законодательства и принятия кодифицированного закона в рассматриваемой сфере. Одной из причин является то, что информационные отношения, по сравнению с другими правовыми отношениями, более динамичны, и этот факт негативно влияет на актуальность принятых (действующих) норм.

Отметим, что в мировой практике наряду с принятием стратегий и законов о национальной безопасности сложилась практика определения информационной безопасности как "кибербезопасности". Это отражает как бы ориентацию на интернет-безопасность, безопасность электронной, сетевой сферы.

Однако вопрос по существу шире. Европейская комиссия ставит вопрос о создании единого Европейского информационного пространства. Создано Европейское агентство по сетевой информационной безопасности (ENISA). За 2011 г. в Европе одиннадцать государств Евросоюза приняли Стратегии кибербезопасности [3]. Стратегия кибербезопасности США, принятая в мае 2011 г., определяет семь направлений ее реализации, в числе которых следующие: экономика, защита национальных сетей (повышение безопасности, надежности, отказоустойчивости); правопорядок – расширение сотрудничества и правовых норм, регулирующих отношения субъектов. Сюда входит военная отрасль: подготовка к современным вызовам безопасности. Рассматривается вопрос об Интернет-правительстве: продвижение эффективных и всеохватывающих правительственных структур. Вопрос международного развития включает построение безопасности, развитие международной компетенции и экономическое процветание.

Доктрина информационной безопасности Российской Федерации, утвержденная в сентябре 2000 г., заложила основу обеспечения баланса интересов общества, государства и человека. В 2009 г. Указом Президента РФ утверждена Стратегия национальной безопасности. Она внесла ряд дополнительных требований к комплексному обеспечению информационной безопасности. Стратегия национальной безопасности, являясь документом концептуальным и практически реализуемым, включает проблему информационной безопасности наряду с другими направлениями обеспечения безопасности страны. Подтверждается значимость информационной безопасности и ее связь со всеми другими направлениями национальной безопасности, возможность и необходимость перевода всех иных направлений безопасности на использование информационных технологий, с одной стороны, и создание необходимых условий для предотвращения нарушений установленного порядка безопасности – с другой. Это касается обороны страны, экономико-производственной сферы, социальной структуры, области культуры и вос-

питания граждан, особенно молодого поколения. Взаимодействие всех направлений национальной безопасности с потенциалом ИКТ и его реальным присутствием во всех областях жизни страны "превращают информационные технологии в мощный катализатор практически всех сфер жизнедеятельности современного общества – экономики, науки, образования, культуры, социально-бытовой сферы". Поскольку информационная безопасность является частью национальной (общегосударственной) безопасности Российской Федерации, следует учитывать, что речь идет не только об обеспечении безопасности в самой информационной сфере и среде, но и об информационной составляющей в каждом из направлений национальной безопасности: политической, экономической, экологической, внутриполитической, международной, пограничной, военной и т. д. Стратегия национальной безопасности лишний раз подтверждает, что информационные ресурсы и технологии составляют стратегический потенциал любого направления деятельности государства, всех его структур и всех институтов гражданского общества.

Одновременно с проблемой безопасности через призму киберпреступности рассматриваются и вопросы свободы в Интернете: поддержка основных свобод и неприкосновенности частной жизни [4].

Интенсивное развитие информационного законодательства Кыргызстана, а также необходимость согласования отечественного информационного законодательства с международным с учетом национальных интересов, вызывает необходимость его реформирования на научной основе, в том числе ввиду возрастающей роли силовых аспектов решения международных конфликтов, в том числе и с помощью террористических и экстремистских методов.

Важное значение в этих условиях приобретает выделение концептуальных основ формирования информационного законодательства, исследования проблемы систематизации информационного законодательства [5].

Важным шагом на пути формирования информационного законодательства стало Постановление Правительства Кыргызской Республики (КР) "О проекте Концепции информационной безопасности Кыргызской Республики" от 11 июля 2008 г. № 372.

Этот документ является основой следующего: 1) выработки предложений по совершенствованию законодательства в сфере обеспечения информационной безопасности Кыргызской Республики; 2) дальнейшего формирования и совершенствования нормативной правовой базы и разработки целевых программ обеспечения информационной безопасности Кыргызской Республики; 3) развития и совершенствования правового, методического, научно-технического и организационного обеспечения работ, относящихся к этой сфере [6].

Правовой фундамент для утверждения нормативно-правовых актов, регулирующих информационные отношения, и зарождение информационного законодательства был заложен принятием Закона КР "Об информатизации". По нашему мнению, в национальном информационном законодательстве системообразующим фактором его должен стать Кодекс, который будет развивать определенные в Конституции КР положения информационных отношений, в том числе относительно информационной безопасности. Он должен объединить и развивать нормы и принципы общественных отношений, которые определены в Конституции КР; учитывать ратифицированные нормативные акты (соглашения, конвенции) международного права; легализовать позитивные обычаи в сфере информационных отношений и нормы общественной морали, которые сегодня выступают в роли стандартов, за которыми определяется цивилизованность не только отдельной страны, но и мирового содружества в целом.

Таким образом, на концептуальном уровне принимаются определенные меры по повышению эффективности реализации государственной информационной политики, которая определенным образом коррелирует с государственной антитеррористической политикой. Кроме этого, принимаются нормативно-правовые акты по различным направлениям информационной тематики и вносятся изменения и дополнения в уже действующие документы. В то же время работы по совершенствованию законодательства в сфере информационной безопасности в целом носят фрагментарный характер, в то время как недостатки действующего информационного законодательства КР в контексте формирования эффективной антитеррористической политики требуют системного решения. Именно поэтому уместна позиция большинства исследователей вышеупомянутой проблематики, которые обращают внимание на необходимость его систематизации [7, 8].

Непосредственно формирование информационного законодательства в Кыргызстане обусловливает необходимость его совершенствования через теоретические разработки систематизационных основ. При выборе конкретной формы систематизации следует учитывать не только сложный и специфический характер информационных отношений и становления информационного права как самостоятельной отрасли права, но и тот факт, что информационное право пока не является систематизированной отраслью. Требуют учета и пробле-

мы борьбы с терроризмом, выступающим одной из угроз международному миру и безопасности.

Важное значение для эффективной систематизационной деятельности информационного законодательства приобретает выработка ее на основе унифицированных принципов. Так, по мнению современных ученых, в основе систематизации норм информационного права должны быть проработаны юридической наукой и проверенные практикой основные принципы: объединение традиций и новаций правоведения; инкорпорация норм действующего информационного законодательства в новую систему через агрегацию институтов права; формирование межотраслевых институтов права на основе связей с отраслевыми институтами [9, с. 27].

В противоположность фрагментарному решению проблем правового регулирования правовых отношений в информационной сфере наиболее адекватным способом повышения эффективности отечественного информационного законодательства считается проведение широкомасштабной, постепенной его систематизации через призму трех основных форм: инкорпорации, консолидации и кодификации. На научном уровне методологические основы решения данного вопроса сформированы в рамках развития школы информационного права (И.Л. Бачило, А.А. Антопольский, Г.В. Белов, А.К. Жаров, В.Н. Монахов, С.В. Петровский, С.И. Семилетов, В.А. Копылов и др.), приверженцы которой системно исследуют данные проблемы, предлагая разнообразные контексты и матрицы для решения актуальных вопросов в различных сферах жизнедеятельности, в том числе и в сфере противодействия экстремизму и терроризму.

Также следует обратить внимание и на деятельность таких украинских ученых, как И. Аристова, К. Беляков, В. Гурковский, В. Цимбалюк, Н. Швец и другие. В рамках исследований названных авторов различными способами доводится идея необходимости кодификации информационного законодательства и выделения в будущем кодифицированном акте следующих разделов: правовой режим информационных ресурсов; правовое регулирование СМИ; охрана прав на содержание компьютерных программ; усовершенствование защиты прав интеллектуальной собственности, в том числе авторского права при размещении и использовании произведений в сети Интернет; охрана баз данных; дистанционное обучение; телемедицина; предоставление органами государственной власти и органами местного самоуправления юридическим и физическим лицам информационных услуг с использованием сети Интернет; правовое регулирование защиты конфиденциальной информации и др.

Одновременно исследования нормативно-правовой базы в сочетании с анализом научной мысли позволяют сделать вывод, что деятельность по кодификации информационного законодательства в недостаточной степени включает в себя направление правового регулирования технической защиты информации, что является особенно важным в контексте формирования обновленной стратегии противодействия терроризму и экстремизму.

В связи с этим было бы уместно в ходе проведения работ по кодификации отечественного информационного законодательства большее внимание уделить нормативно-правовому регулированию следующих вопросов: 1) противодействие техническим разведкам; 2) защита информации в информационно-телекоммуникационных системах; 3) конструирование интернет-отношений с последующей выработкой механизмов их государственного регулирования; 4) формирование действенных механизмов защиты персональных данных техническими средствами; 5) защита речевой информации и данных в линиях и средах; 6) организация взаимодействия и координация развития системы технической защиты информации с сохранением государственного контроля за данной сферой [10].

В частности, мы считаем, что указанные направления деятельности требуют урегулирования в соответствующих разделах будущего кодификационного акта Кыргызстана вследствие прогнозируемого увеличения количества совершаемых кибератак, а также в связи с ускоренным развитием киберугроз и отчасти отсутствием действенной защиты государственных информационных ресурсов.

Литература

1. *Смирнов А.И.* Глобальная безопасность и “мягкая сила 2.0.”: вызовы и возможности для России / А.И. Смирнов, И.Н. Кохтюлина. М., 2012. С. 98–103.
2. *Бачило И.Л.* О совершенствовании и гармонизации национальных законодательств государств-участников СНГ в сфере обеспечения информационной безопасности / И.Л. Бачило, В.В. Бондуровский, М.А. Вус // Информационное право. 2013. № 1. С. 24–27.
3. National Cyber Security Strategies / European Union Agency for Network and Information Security (ENISA). 2012. URL: http://www.enisa.europa.eu/ activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper. На русск. яз.: Государственные стратегии кибербезопасности // Интернет-пор-

тал SecurityLab.ru. 2012, 4 сент. URL: http://www.securitylab.ru/analytics/429498.php
4. Библиодосье “О разработке стратегии национальной кибербезопасности Российской Федерации: состояние, предпосылки, механизмы и перспективы”. М., 2013. С. 28. URL: http://sartraccc.ru/Pub_inter/ kiber_bezop.pdf
5. Концепция Информационного кодекса Российской Федерации / под ред. И.Л. Бачило. М.: Канон+, 2014.
6. Постановление Правительства КР “О проекте Концепции информационной безопасности КР” от 11 июля 2008 г. № 372 // ИПС “Токтом”. Бишкек, 2009.
7. Концепция развития информационного законодательства в Российской Федерации / Ин-т гос-ва и права РАН. Сект. прав человека // Гос-во и право. 2005. № 7. С. 47–61.
8. *Макаров О.С.* К вопросу о принципах обеспечения информационной безопасности / О.С. Макаров // Вопр. правоведения. 2013. № 3. С. 192–200.
9. Основы информационного права Украины: учеб. пособие / В.С. Цимбалюк, В.Д. Гавловский, В.В. Гриценко и др.; под ред. М.Я. Швеца, Г.А. Калюжного, П.В. Мельника. М., 2004.
10. *Муслимов Ш.Р.* Некоторые правовые проблемы киберпространства в информационном обществе / Ш.Р. Муслимов // Теоретич. и практ. аспекты развития совр. науки: материалы II международной НПК. Бишкек, 2013. С. 261–264.