МЕЖПАРЛАМЕНТСКАЯ АССАМБЛЕЯ
ГОСУДАРСТВ — УЧАСТНИКОВ
СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

ПАРЛАМЕНТСКАЯ АССАМБЛЕЯ ОРГАНИЗАЦИИ
ДОГОВОРА О КОЛЛЕКТИВНОЙ БЕЗОПАСНОСТИ

Законодательство государств — членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации

Материалы международной
научно-практической конференции

Под редакцией П. П. Рябухина,
В. В. Бондуровского, Г. И. Перекопского

Санкт-Петербург
2014

УДК 327
ББК 67.5
З-19

З-19 **Законодательство государств — членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации**: Материалы международной научно-практической конференции (Санкт-Петербург, 28 ноября 2013 года) / Под ред. П. П. Рябухина, В. В. Бондуровского, Г. И. Перекопского. — СПб.: Секретариат Совета Межпарламентской Ассамблеи государств — участников СНГ. 2014. — 88 с.

ISBN 978-5-86857-054-4

Приветствие участникам и гостям
международной научно-практической конференции
«Законодательство государств — членов Организации
Договора о коллективной безопасности
в сфере обеспечения информационной безопасности:
опыт, проблемы и перспективы гармонизации»

Приветствую участников и гостей международной научно-практической конференции!

Тема вашей конференции актуальна и важна. В современных условиях информационная сфера стала системообразующим фактором жизнедеятельности общества, активно влияющим на состояние политической, экономической, оборонной, социальной и других составляющих безопасности государств — членов Организации Договора о коллективной безопасности.

В основе формирования системы информационной безопасности в интересах каждого из государств — членов ОДКБ и Организации в целом лежит законодательное и нормативно-правовое обеспечение. Принятие государствами — членами ОДКБ обязательств в сфере информационной безопасности в формате ОДКБ и других международных форматах требует ускоренного параллельного развития теории и практики информационной безопасности.

Согласование законодательной политики, скоординированные меры по сближению и унификации национальных законодательств государств — членов ОДКБ в информационной сфере, обеспечение соответствия национальных законодательств международным договорам будут отвечать интересам государств — членов ОДКБ в защите конституционного строя, обеспечении суверенитета, территориальной целостности, политической, экономической и социальной стабильности.

Желаю участникам конференции успехов в работе и профессиональной деятельности!

Председатель Государственной Думы
Федерального Собрания Российской Федерации,
Председатель Парламентской Ассамблеи ОДКБ **С. Е. Нарышкин**

В. О. ШУШИН*

О СОСТОЯНИИ И ПЕРСПЕКТИВАХ СОТРУДНИЧЕСТВА ГОСУДАРСТВ — ЧЛЕНОВ ОДКБ ПО ФОРМИРОВАНИЮ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уважаемые участники конференции!

Хотелось бы высказать слова благодарности руководству Парламентской Ассамблеи ОДКБ и коллегам из Секретариата Парламентской Ассамблеи ОДКБ за организацию нашей конференции.

Обсуждение вопросов законодательного регулирования отношений в сфере информационной безопасности важно именно потому, что от единого понимания правовых подходов к формированию системы информационной безопасности сегодня зависит развитие всей системы обеспечения международной и коллективной безопасности.

Вопросы, связанные с формированием и обеспечением системы коллективной безопасности в информационной сфере, актуальны как никогда. Во всем мире в информационной области происходит ускорение движения к новой фазе развития человечества, к информационному обществу, в котором информация становится одним из ценнейших компонентов национального и международного достояния. Также важно и то, что информационно-телекоммуникационные технологии уже стали одним из важнейших политико-экономических и военных ресурсов.

В данных условиях для достижения общих целей государствам — членам Организации Договора о коллективной безопасности требуются коллективность и скоординированность действий.

Сегодня такой общей стратегической целью в формате ОДКБ является формирование многофункциональной системы коллективной безопасности (основание — Декларация государств — членов Организации Договора о коллективной безопасности о дальнейшем совершенствовании и повышении эффективности

---

* В. О. Шушин, советник управления информационных программ Секретариата Организации Договора о коллективной безопасности, член Научно-экспертного совета Организации Договора о коллективной безопасности.

деятельности организации 2006 г.). При этом есть четкое понимание того, что прилагаемые в указанном направлении коллективные усилия будут неполными, а многие просто могут быть потрачены впустую, если не будет создана система обеспечения информационной безопасности.

В формате ОДКБ существует согласие относительно того, что под информационной безопасностью понимается состояние защищенности личности, общества, государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве.

Под системой информационной безопасности понимается комплекс мер правового, политического, организационного, кадрового, финансового, научно-технического и специального характера, нацеленных на обеспечение информационной безопасности государств — членов ОДКБ. То есть меры правового характера стоят во главе всего комплекса мер.

Учитывая, что формирование надежной системы информационной безопасности ОДКБ — процесс глобальный, длительный и затратный, к реализации комплекса соответствующих мер в этой сфере государства — члены ОДКБ подходят последовательно.

Начало данному процессу положило утверждение Решением Совета коллективной безопасности ОДКБ от 5 сентября 2008 г. Программы совместных действий по формированию системы информационной безопасности государств — членов Организации Договора о коллективной безопасности.

Программа предусматривает следующие основные направления сотрудничества:

— формирование политической, правовой и организационной основ системы информационной безопасности;

— кадровое, научное и финансовое сопровождение;

— разработка мер по обеспечению информационной безопасности объектов, имеющих трансграничное значение;

— укрепление практического взаимодействия заинтересованных министерств и ведомств государств — членов ОДКБ в целях формирования безопасного информационного пространства и противодействия преступности с использованием информационных технологий.

С тем чтобы процесс формирования системы информационной безопасности проходил в правовом поле, в 2010 г. обеспечение информационной безопасности как важное направление со-

трудничества было закреплено в Уставе Организации Договора о коллективной безопасности (Протокол о внесении изменений в Устав Организации Договора о коллективной безопасности от 7 октября 2002 г., подписанный 10 декабря 2010 г.).

В этом же году был принят другой важный документ в формате Организации: Совет коллективной безопасности ОДКБ своим Решением от 10 декабря 2010 г. утвердил Положение о сотрудничестве государств — членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности (далее — Положение).

В соответствии с Положением в формате Организации определены национальные координирующие органы в указанной сфере, и их взаимодействие осуществляется с участием Рабочей группы по вопросам информационной политики и информационной безопасности (далее — Рабочая группа), образованной решением Комитета секретарей советов безопасности ОДКБ.

Здесь важны два аспекта. Первый касается направлений сотрудничества. В самом Положении и в названии Рабочей группы отражены два направления — информационная политика и информационная безопасность.

Второй аспект связан с организацией взаимодействия. Оказалось, что в сфере обеспечения информационной безопасности и тем более построения скоординированной информационной политики в системе исполнительной власти ни у одного государства сегодня нет органа, ответственного за это направление.

В соответствии с Положением в формате ОДКБ определены национальные координирующие органы в сфере обеспечения информационной безопасности, представители которых вошли в Рабочую группу. В большинстве государств — членов ОДКБ, за исключением Республики Казахстан, такими национальными координирующими органами стали национальные органы безопасности (в Республике Казахстан — Аппарат Правительства).

Речь в данном случае идет только о формате ОДКБ. Необходимо учитывать тот факт, что государства — члены Организации Договора о коллективной безопасности являются участниками других международных объединений (например, Содружества Независимых Государств, Шанхайской организации сотрудничества), где также идет процесс регулирования отношений в сфере информационной безопасности. Не хотелось бы, чтобы в связи

с этим возникли какие-либо противоречия, как с точки зрения коллективных интересов, так и с точки зрения национальных приоритетов.

Для того чтобы в формате ОДКБ работа шла последовательно, утверждены два комплексных документа: План первоочередных мероприятий по формированию основ скоординированной информационной политики в интересах государств — членов Организации Договора о коллективной безопасности и План по совершенствованию мер, направленных на укрепление системы информационной безопасности государств — членов ОДКБ. Последний подготовлен во исполнение Перечня мероприятий, направленных на формирование системы обеспечения информационной безопасности в интересах Организации Договора о коллективной безопасности, утвержденного Советом коллективной безопасности ОДКБ в 2011 г. Оба документа предусматривают меры законодательного, организационного и практического характера и рассчитаны на определенную перспективу.

Сегодня в рамках ОДКБ обсуждаются вопросы обеспечения безопасности информационного пространства в зоне действия Договора о коллективной безопасности. Продолжается обсуждение проекта Стратегии коллективной безопасности Организации Договора о коллективной безопасности (далее — Стратегия). Сдерживают достижение консенсуса или хотя бы компромисса разные подходы, заложенные в национальном законодательстве, на которые ссылаются эксперты в ходе согласования.

Коллизия заключается в том, что если действующее законодательство в основном закрепляет существующую ситуацию, то проект Стратегии, иные правовые акты нацелены на будущее.

В проекте Стратегии коллективной безопасности сделана попытка определить угрозы коллективной безопасности по всем направлениям сотрудничества, включая и информационную сферу. В документе речь идет об обеспечении безопасности информационного пространства, где нет государственных границ, единого правового пространства, единых оценок угроз и подходов в обеспечении безопасности.

Мы полагаем, что такими общими угрозами могут считаться:

— расширение использования стремительно развивающихся информационно-телекоммуникационных технологий для нарушения устойчивости функционирования важных объектов инфраструктуры государства и общества, совершения различных

преступлений, подготовки и осуществления социально опасной деятельности;

— распространение, в первую очередь с использованием глобальной информационной инфраструктуры, идеологии политического, национального и религиозного экстремизма, составляющей духовную основу террористической деятельности;

— использование современных информационных технологий для оказания воздействия на личность, общество и государство с целью инспирирования дестабилизирующих ситуаций в ущерб интересам государств — членов ОДКБ;

— избирательное воздействие на информационные и телекоммуникационные системы, сети связи, в первую очередь используемые для управления государством, вооруженными силами, экономической деятельностью, ущерб от которого может быть соизмерим с применением оружия массового поражения;

— превращение информационного пространства в среду для проведения операций и тактических ударов с применением информационных технологий специального характера как в мирное, так и в военное время.

Это в основном то, с чем мы подошли к настоящему моменту. Теперь о будущем.

Система информационной безопасности государств — членов ОДКБ будет формироваться по следующим основным направлениям:

— совершенствование с участием Парламентской Ассамблеи ОДКБ правовой основы сотрудничества в информационной сфере, подготовка предложений по гармонизации национального законодательства в области обеспечения информационной безопасности и совершенствования борьбы с преступлениями в сфере современных информационных технологий. Соответствующие предложения закреплены в Программе деятельности Парламентской Ассамблеи Организации Договора о коллективной безопасности по сближению и гармонизации национального законодательства государств — членов ОДКБ на 2011 – 2015 годы;

— координация позиций по вопросам обеспечения международной информационной безопасности;

— осуществление совместного мониторинга угроз в информационной сфере (здесь большая надежда — на образованную Аналитическую Ассоциацию ОДКБ);

— развитие практического взаимодействия национальных координирующих и уполномоченных органов государств — чле-

нов ОДКБ в сфере обеспечения информационной безопасности в формате ОДКБ, в первую очередь в области защиты объектов важной инфраструктуры и противодействия преступной деятельности в информационной сфере (налицо неурегулированность международных отношений в этих вопросах);

— формирование специальных сил обеспечения коллективной безопасности ОДКБ для противодействия угрозам и проведения операций в информационной сфере как в мирное время, так и при возникновении военных конфликтов любой интенсивности;

— внедрение современных методов защиты информации в органах управления силами и средствами системы коллективной безопасности ОДКБ, в системах защиты объектов, имеющих важнейшее значение для национальной и региональной безопасности;

— координация мероприятий по нейтрализации противоправных воздействий на информационное пространство государств — членов ОДКБ.

В рамках данного направления мы надеемся на скорейшее завершение процесса согласования, подписание и последующую ратификацию Протокола о взаимодействии государств — членов ОДКБ по противодействию преступной деятельности в информационной сфере и согласование других предложений, носящих закрытый характер. Речь идет о координации сотрудничества по киберинцидентам. Также с указанным направлением работы тесно связано предотвращение несанкционированного доступа к информации ограниченного пользования, имеющей значение для целей коллективной безопасности.

Все перечисленное невозможно осуществить без совершенствования сотрудничества в сфере подготовки и переподготовки кадров. Здесь в ОДКБ складывается определенная система, но вопросов еще много.

Система информационной безопасности будет неполноценной без совместных научно-исследовательских, опытно-конструкторских и проектных работ в области информационных технологий, их внедрения и использования в интересах формирования единого информационного пространства государств — членов ОДКБ. Может быть, стоит подумать о создании ассоциации ведущих научно-исследовательских институтов государств — членов ОДКБ, специализирующихся на вопросах информационной безопасности.

К основным направлениям совершенствования скоординированной информационной политики государств — членов ОДКБ относятся:

— укрепление мер доверия друг к другу во всех сферах взаимодействия;

— выработка единых правил сотрудничества в информационной сфере, продвижение их на международный уровень, включая образование совместных структур для укрепления сотрудничества в данной области (в рамках данного направления необходимы скорейшее завершение обсуждения и принятие Перечня базовых принципов государств — членов ОДКБ в области скоординированной информационной политики);

— разработка и системная реализация мер, направленных на формирование положительного образа Организации Договора о коллективной безопасности, широкое, своевременное и скоординированное информирование общественности о целях, задачах и политике ОДКБ, противодействие информационным потокам, формирующим негативное отношение и недостоверное представление о государствах — членах ОДКБ;

— совершенствование информационно-аналитической поддержки по ключевым направлениям деятельности ОДКБ, включая реализацию стратегических приоритетов обеспечения коллективной безопасности Организации;

— разработка и реализация согласованных мер по комплексному и неотложному реагированию на возникающие региональные и глобальные угрозы коллективной безопасности ОДКБ;

— укрепление сотрудничества средств массовой информации государств — членов ОДКБ.

В завершение своего выступления хотел бы отметить следующее. Мы понимаем, что в условиях относительно открытого и не очень регулируемого информационного пространства имеются одни и те же возможности как для создания преимуществ для человечества, так и для незаконных, преступных действий. Именно поэтому необходимы корректное отношение к использованию информационного пространства, ответственность за его использование и эффективное международное сотрудничество. Все составляющие требуют нормативного регулирования. Именно в данной сфере важна синхронизация законодательных мер, иначе будут потери во всех сферах безопасности.

Благодарю за внимание.

В. А. ОЗЕРОВ*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — ВАЖНЕЙШИЙ КОМПОНЕНТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ — ЧЛЕНОВ ОДКБ

Уважаемые участники и гости конференции!

Прежде всего, хотел бы отметить особое значение обсуждаемой сегодня на конференции темы.

Интенсивное развитие информационных и коммуникационных технологий, их широкое применение во всех сферах деятельности человека создали условия для формирования глобальной информационной инфраструктуры, которая предоставляет качественно новые возможности социализации людей, их общения и доступа к накопленным человечеством знаниям.

В этих условиях важно исключить возможность нарушения прав личности, общества и государства в информационной сфере, а также деструктивного и противоправного воздействия на критические элементы национальной информационной структуры.

Деятельность по обеспечению информационной безопасности наших государств вписывается в мировые тенденции борьбы за информационную безопасность и, согласно позиции Совета Федерации, призвана оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве.

Информационная безопасность — это важная составная часть национальной безопасности. Недооценка происходящих в информационной среде процессов чревата принятием неэффективных решений, в том числе и на государственном уровне. Это в свою очередь может привести к росту социальной напряженности и дестабилизации обстановки не только в отдельных странах, но и в целых регионах.

В связи с этим следует отметить, что обсуждаемая нами тема — «Законодательство государств — членов Организации Договора о коллективной безопасности в сфере обеспечения информаци-

* В. А. Озеров, председатель Комитета Совета Федерации Федерального Собрания Российской Федерации по обороне и безопасности.

онной безопасности: опыт, проблемы и перспективы гармонизации» является не только важной, но и крайне актуальной.

Уважаемые коллеги, зона ответственности ОДКБ — это пространство пересечения различных геополитических интересов. В последние годы информационные технологии, призванные выполнять созидательную функцию, направленную на ускорение научно-технического прогресса, к сожалению, стали активно использоваться в межгосударственном противоборстве. Далеко за примерами ходить не нужно, и дело Сноудена тому пример.

Основные угрозы в области информационной безопасности — это использование информационных технологий:

— в качестве информационного оружия в военно-политических целях для осуществления враждебных действий и актов агрессии;

— в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, для пропаганды терроризма, привлечения к террористической деятельности новых сторонников;

— для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

— для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

Поэтому защита национальных информационных ресурсов и оказание взаимной помощи в предотвращении деструктивных информационных воздействий в зоне ответственности ОДКБ становятся жизненно важными для наших стран.

Предлагаю участникам конференции активно высказаться по приоритетным направлениям коллективного противодействия вызовам и угрозам в информационной сфере в целях выработки рекомендаций по единой, скоординированной информационной политике государств — членов ОДКБ.

Нами уже реализуется утвержденная президентами государств — членов ОДКБ Программа совместных действий по формированию системы информационной безопасности госу-

дарств — членов Организации Договора о коллективной безопасности. Она охватывает такие важные направления, как сотрудничество в политической сфере, формирование согласованной нормативно-правовой базы. Ведутся совместные научно-исследовательские работы, осуществляется обмен информацией о достижениях в этой области, практикуется подготовка кадров, проводятся совместные мероприятия, направленные на борьбу с преступлениями в сфере информационных технологий.

ОДКБ тесно сотрудничает с ШОС, ЕврАзЭС и другими организациями в области обеспечения информационной безопасности.

Не случайно площадка ОДКБ регулярно используется для проведения рабочих встреч высших должностных лиц ОДКБ, СНГ, ЕврАзЭС и ШОС, в ходе которых обсуждаются и вопросы углубления взаимодействия по обеспечению информационной безопасности.

С удовлетворением отмечаю, что продолжается сотрудничество в информационной сфере с такими авторитетными международными организациями, как ООН, ОБСЕ, ЕС. Наша задача — максимально эффективно использовать накопленный опыт для выстраивания единой системы защиты информационных ресурсов и коммуникаций государств — членов ОДКБ.

Для нас как законодателей безусловным приоритетом является совершенствование и гармонизация нормативно-правовой базы наших государств.

В рамках ОДКБ удалось создать надежный механизм взаимодействия и взаимного доверия. Положенные в основу нашей деятельности принципы межгосударственных консультаций приносят свои плоды. Они помогают вырабатывать консенсусные решения — без ущерба для каждого участника ОДКБ.

На заседании Совета глав государств Содружества Независимых Государств 25 октября 2013 г. подписано Соглашение о защите секретной информации в рамках Содружества Независимых Государств. Это еще раз свидетельствует о важности вопросов обеспечения информационной безопасности для наших стран.

Уважаемые участники конференции!

Мы перешагнули порог информационной эпохи. И теперь, как никогда ранее, очевидна необходимость формирования единой, коллективной системы информационной безопасности государств — членов ОДКБ.

Стратегическая цель — обеспечение стабильности политического, экономического развития наших государств, условий для военного и идеологического равновесия на региональном и глобальном уровнях.

Надеюсь, что в докладах и выступлениях коллег мы услышим о проблемах и перспективах развития законодательства в этой сфере, о накопленном опыте такой работы в наших странах.

Уверен, что наша конференция придаст новый импульс работе по формированию эффективных подходов к решению проблем информационной безопасности, внесет весомый вклад в обеспечение комплексной безопасности наших стран.

Желаю всем плодотворной и интересной работы!

Спасибо за внимание.

И. Л. БАЧИЛО*

ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВАХ — ЧЛЕНАХ ОДКБ

Все направления деятельности государств — членов Организации Договора о коллективной безопасности в той или иной форме нуждаются в правовом оформлении Парламентской Ассамблеей ОДКБ и соответственно отражаются в национальном законодательстве каждого государства — члена Договора о коллективной безопасности. В связи с этим встает ряд проблем организационно-правового порядка в области гармонизации законодательства членов ОДКБ.

Проблемы информационной безопасности интернет-среды актуальны как никогда. Информационная безопасность является составной частью системы национальной безопасности любого государства, занимая в ней особое место, активно отражается в международных соглашениях. Естественно, что в деятельности государств — членов ОДКБ по обеспечению коллективных решений в области обороны, политики и социального развития должно учитываться состояние правового обеспечения информационной безопасности (далее — ОИБ).

Первые шаги в области правового обеспечения информационной безопасности предусматривались с момента заключения в 1992 г. Договора о коллективной безопасности, но особое внимание данному направлению уделяется с 2008 г. Советом коллективной безопасности, в частности с принятием Программы совместных действий по формированию системы информационной безопасности государств — членов Организации Договора о коллективной безопасности. В 2010 г. принято Положение о сотрудничестве государств — членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности, в 2011 г. Советом коллективной безопасности утверждены Перечень мероприятий, направленных на формирование системы обеспечения информационной безопасности в

* И. Л. Бачило, заведующая сектором информационного права Института государства и права Российской академии наук.

интересах государств — членов Организации Договора о коллективной безопасности, и План первоочередных мероприятий по формированию основ скоординированной информационной политики в интересах государств — членов Организации Договора о коллективной безопасности.

Реализация принятых документов требует адекватного правового обеспечения как на уровне ОДКБ в целом, так и на уровне законодательства каждого члена Организации. И это касается в первую очередь деятельности Парламентской Ассамблеи ОДКБ. В связи с этим необходимо учитывать ряд факторов, которые обусловливают цели, содержание и методы деятельности в области правового обеспечения подготовки и оформления соответствующих решений.

Следует обратить внимание на внешние и внутренние факторы формирования правового реагирования в условиях усложнения ситуации в области информационной безопасности при активном использовании Интернета, а также на факторы, которые касаются самого процесса достижения гармонизации законодательных актов в одном государстве и тем более в системе взаимодействующих суверенных государств.

1. Сложность современного этапа развития информационного общества выражается в том, что в данном процессе формируются многие элементы нового мировоззрения с учетом того, что инфокоммуникационный ресурс погружен в оболочку противоречий индустриального и постиндустриального общества. Ресурсы и средства инфокоммуникаций ориентированы на быстрое, революционное развитие в структуре мировой глобальной экономики на основе конкуренции, борьбы за прибыль и экономическое превосходство. Информационные технологии находятся в опережающей стадии развития по сравнению с готовностью организационно-правовых систем использовать этот ресурс безопасно. И институты властных систем, социального развития большинства государств не успевают ориентироваться на эти условия, ибо находятся на разных уровнях социального, политического, культурного развития, имеют свои национальные ценности и формы их обеспечения. В данных условиях нарастают конфликты, противоречия, растет число киберпреступлений.

Противостояние, конкуренция между государствами во все большей мере приобретают электронную форму. В индустриаль-

ном обществе войны становятся затратными и малопродуктивными, истребляющими популяцию планеты, но не меняющими кардинально процессы объективного характера. Однако не менее разрушительны и новые информационные способы борьбы за сохранение имперских притязаний на разных уровнях взаимодействия людей и их ассоциаций. Таким образом, проблемы информационной безопасности приобретают особую остроту и актуальность.

2. Состояние обеспечения информационной безопасности и ее правовой аспект за последние 15 лет изменились. Переход по многим направлениям отношений к модели «2.0», которая предполагает условия использования «мягкой силы» в отношениях информационного взаимодействия, влияет на расширение информационного поля ОИБ. Это можно проследить на сопоставлении установок Окинавской хартии глобального информационного общества (принята главами государств и правительств «Группы восьми» 22 июня 2000 г.) и Хартии открытых данных, принятой на встрече стран «Группы восьми» 18 июня 2013 г. Приложение к Хартии содержит призыв: «Работая в рамках наших правовых и политических систем, мы выражаем согласие внедрять указанные лучшие практики скорейшим образом и ставим своей целью завершить наши мероприятия самое позднее к 2015 г., в соответствии со сроками, указанными в наших национальных планах действий». В приложении к Хартии также определен ряд направлений в области высокозначимых для совершенствования демократических систем и стимулирования инновационного использования данных, рассматривается возможность обнаружения и доступа к ключевым наборам данных о государственной статистике, государственных картах, государственных выборах и государственном бюджете. В основной части документа формулируется ряд принципов*.

* Можно сказать, что с принятием Хартии открытых данных начался процесс выстраивания порядка в формировании и использовании информационных ресурсов через подготовку национальных планов и их сближение в мировом масштабе. Документ регулирует использование открытых данных по умолчанию. Первый принцип представляет собой публичное заявление о намерениях следовать стратегии или политическому курсу в целях продвижения повестки дня в области открытых данных; второй принцип подразумевает публикацию данных в большом количестве и с высоким

Почему мы обращаем внимание на эти ориентации в использовании открытых данных? Известны новые модели использования «мягкой силы» не только в области реализации традиционных, привычных методов международных отношений: обнаруживаются новые вызовы в сфере обеспечения информационной безопасности*. Это особенно актуально на фоне событий, связанных с публикациями на сайте WikiLeaks и раскрытием масштабов работы Агентства национальной безопасности США ее же специалистом Э. Сноуденом.

Необходимость обеспечения информационной безопасности на национальном уровне и в масштабе межгосударственных объединений обязывает уделять повышенное внимание расширению поля угроз и появлению новых форм киберпреступности. Явно обозначается прямая связь правового обеспечения информационной безопасности в поле глобальной информационной инфраструктуры и национальных сегментов каждого государства в процессе развития сотрудничества по противодействию преступлениям, связанным с использованием инфокоммуникационных систем, прежде всего Интернета.

Для государств — членов Организации Договора о коллективной безопасности это вопросы не только защиты конституционного строя, обеспечения суверенитета, территориальной целостности, политической, экономической и социальной стабильности, но и координирования принципов, мер и форм сближения и гармонизации национального законодательства в области решения задач ОДКБ при сотрудничестве по предотвращению угроз и противодействию преступлениям.

3. Помимо внешних факторов в правовом обеспечении информационной безопасности немалую роль играют факторы, связанные с состоянием правовых систем каждого члена ОДКБ и с со-

---

качеством, что должно помогать людям понимать и использовать их; третий — устанавливает возможность использования открытых данных всеми; четвертый и пятый принципы затрагивают область целей использования открытых данных. Таким образом, признано, что данные являются инструментом повышения результативности действий, эффективности и быстроты реагирования на потребности граждан, стимулирования инноваций в отдельных странах и по всему миру. При этом обеспечивается дальнейшее увеличение спроса на открытые данные.

* *Смирнов А. И., Кохтюлина И. Н.* Глобальная безопасность и «мягкая сила 2.0»: вызовы и возможности для России. М., 2012.

стоянием реального инфокоммуникационного взаимодействия государств в рамках Договора о коллективной безопасности.

В связи с этим следует учитывать как накопившийся опыт информационного доверия к открытым формам информационного взаимодействия, так и выбор методов и средств такого взаимодействия на перспективу с учетом объективных вызовов к формированию единого экономического пространства (что гораздо шире, нежели Таможенный союз).

Наиболее очевидными здесь являются две проблемы:

— различия в национальных системах информационного обеспечения внутренних потребностей в области информатизации и устройства архитектуры национальной информационной инфраструктуры;

— готовность к выстраиванию интегрированных информационных систем с учетом задач, решаемых в рамках таких межгосударственных объединений, как Содружество Независимых Государств, Организация Договора о коллективной безопасности, Евразийское экономическое сообщество и т. п.; выбор методов и форм правового обеспечения в формате работы Межпарламентской Ассамблеи государств — участников СНГ и Парламентской Ассамблеи ОДКБ.

4. Деятельность государств — членов ОДКБ в соответствии с правовой базой Организации реализуется в трех системно связанных направлениях: решение задач в области обороны; в области государственной политики; в области социально-экономического взаимодействия в целях реализации задач национальной и коллективной безопасности.

Каждое из направлений имеет свою специфику информационно-коммуникационного взаимодействия по обеспечению информационной безопасности.

Решение вопросов оборонного значения в наибольшей степени связано с информацией, относимой к государственным секретам, обеспечением информационной безопасности критически важных объектов инфраструктуры, входящей в систему Договора о коллективной безопасности.

Политическое взаимодействие государств — членов Договора обязывает обеспечить согласование действий в части определения субъектов и их методов и форм взаимодействия в рамках ОДКБ с учетом того, что политика становится все более открытой областью информации. Здесь формируются решения, опре-

деляющие и контролирующие глубину и содержание реализации проблем основного предмета Договора.

Третье направление работы ОДКБ связано с обеспечением необходимого взаимодействия в области социально-экономического сотрудничества в целях реализации основных целей Договора о коллективной безопасности. Это важнейшая основа эффективного сотрудничества национальных систем безопасности, которое в наибольшей мере является открытым и доступным для общественного контроля и оценки его результативности.

Представляется, что методология информационного обеспечения и управления состоянием области информационной безопасности должна учитывать различия в методах и формах ОИБ по названным направлениям. В плане формирования и развития информационной базы очевидно значение таких задач, как сближение и унификация законодательства государств — членов ОДКБ, выработка единых терминов в принимаемых нормативных актах как на уровне национального законодательства, так и на уровне обязательных и рекомендательных правовых актов Парламентской Ассамблеи ОДКБ.

Насколько важны эта сторона информационной культуры взаимодействия заинтересованных субъектов и соответствующий уровень ОИБ, можно увидеть на примере сравнительного анализа законодательных актов государств — участников СНГ в сфере связи, который был проведен на очередном заседании Экспертного совета Межпарламентской Ассамблеи СНГ — Регионального содружества в области связи в ноябре 2013 г. Отмечались большие разрывы в датах принятия действующих национальных законов, разная терминология: «связь»/«электросвязь», «о телекоммуникациях»/«об электронных коммуникациях» и т. д. Нет ссылок на какие-либо модельные законы в процессе принятия или обновления национального законодательства.

Модель правового регулирования требует более точного определения предмета и сферы взаимодействия разных субъектов; целей регулирования; принципов и методов правовых решений, что позволит раскрыть инфраструктуру инфокоммуникационного пространства и реализуемых внутрисистемных отношений. Так, профиль работы Экспертного совета МПА СНГ — РСС связан с решением проблем, значение которых невозможно переоценить. Наряду с упорядочением информационных ресурсов

сегодня важнейшее значение имеют вопросы оценки состояния и направлений развития систем связи.

Со времени принятия в Российской Федерации Федерального закона «О связи» (2003 г.) произошли большие изменения в технологиях обеспечения взаимодействия субъектов в обращении информации по сетевым каналам, в отношениях. связанных с обменом информацией между ее потребителями. Они требуют новой правовой основы для регулирования всего комплекса отношений в инфокоммуникационной сфере*. Министерством связи и массовых коммуникаций Российской Федерации разработана Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года, и необходимо отметить, что указанные вопросы получили в документе должное отражение с учетом перспективы развития отрасли.

Эти вопросы касаются не только Российской Федерации. Они важны и для международных объединений — СНГ, ОДКБ, ШОС, ЕврАзЭС и др. Планирование процессов изменения законодательства можно осуществлять с учетом вариантов национальных решений, но их основное содержание диктуется объективными условиями развития процессов информатизации.

Представляется, что при рассмотрении проектов законов, которые согласно планам работы Экспертного совета МПА СНГ — РСС выносятся на его заседания, важно прежде всего обращать внимание на проблемы региональных систем связи и оценивать возможности формирования интегрированных информационных систем. В Положении об Экспертном совете стоит это указать, так как в обсуждаемых проектах законов МПА СНГ данный вопрос не отражен вообще или затрагивается косвенно.

---

* Определение цели правового регулирования на предстоящий период касается стимулирования и ускорения перестройки отрасли связи на IP-технологию пакетной коммутации (из TDM в IP). Стоят вопросы обеспечения управляемости перестройки и создания неразрушающих процессов при соблюдении порядка оказания государственных и негосударственных сетевых сервисов и услуг; строительства виртуальной доверенной среды и организации единой системы оборота юридически значимых электронных документов, гарантированной государством и подконтрольными ему структурами; вопросы форм обеспечения порядка дистанционного заключения и оформления гражданско-правовых сделок по оказанию сетевых сервисов и услуг, порядка их оплаты и реализации; обеспечения сетевых механизмов защиты прав потребителей, интересов государства и общества.

Практика взаимодействия государств СНГ в области правотворчества и опыт принятия национальных законов в сравнении со временем появления модельного варианта показывают, что модельный закон принимается с отставанием или опережением относительно национального правового акта, видна ориентация на законодательную практику соседних стран. При этом наблюдаются неоднозначное использование отдельных терминов и их самостоятельная трактовка*.

Вместе в тем стоит отметить опыт принятия комплексного закона по проблемам использования информационно-коммуникационных технологий (ИКТ) в Республике Казахстан. С 2007 г. в республике действует закон «Об информатизации», который комплексно охватывает разные стороны процесса использования ресурса ИКТ. Есть немало конкретных оригинальных решений в правовых системах других государств — участников СНГ. И это заслуживает обобщения и учета в дальнейшей работе МПА СНГ и ПА ОДКБ по правовому обеспечению информационной безопасности.

Важное значение имеют критерии оценки состояния законодательства и индикаторы эффективности гармонизации нормативных правовых актов в области обеспечения информационной безопасности в процессе взаимодействия законодательных органов государств — участников СНГ и членов ОДКБ.

5. Особого внимания требуют вопросы интеграционного подхода к использованию потенциала государств — членов ОДКБ при реализации целей Договора о коллективной безопасности и выборе формы принятия и исполнения коллективных правовых решений по предметам ведения ОДКБ. При продуктивном решении указанных вопросов опыт ОДКБ мог бы учитываться в процессе выработки мер в области международной информационной безопасности в условиях обострения проблем использо-

* Широкое применение терминов «обладание», «обладатель» приводит к тому, что ими заменяют обозначение таких субъектов, как органы государственной власти, органы самоуправления, любые организации и граждане. Это не только затрудняет идентификацию участника отношений, но и снижает уровень ответственности субъектов. Происходит это в силу того, что термин «обладание» не подкрепляется правовым статусом обладателя ни как собственника, ни как субъекта права интеллектуальной собственности.

вания вредоносных программ и необходимости реагирования на развитие разных форм киберпреступности.

В сфере правового обеспечения интеграции национального законодательства предстоит усилить внимание к таким направлениям, как создание реестров нормативных правовых актов по проблеме ОДКБ, проведение мониторинга на предмет внесения в них изменений и эффективности применения. Особое значение имеет создание межгосударственных автоматизированных систем и автоматизированных систем управления по учету и ведению реестров национального и модельного законодательства по направлениям деятельности государств — участников Договора о коллективной безопасности. При этом важен и учет актов МПА СНГ по более широкому кругу информационной безопасности в целях снятия дублирования и наибольшей предметной ориентации в рамках каждой из форм сотрудничества.

Было бы оправданным ввести электронную систему учета возникающих информационных конфликтов и угроз, которые являются источником киберпреступлений как в самой инфокоммуникационной сфере, так и в области применения ИТ при совершении преступных деяний против соблюдения прав и обязанностей граждан, взаимодействия субъектов права по вопросам миграции, укрепления социально-экономического сотрудничества, развития институтов государственного управления и т. д. Особого внимания в современных условиях использования интернет-среды как орудия силового воздействия в области международных отношений и обеспечения монопольного влияния наиболее продвинутых в информационных технологиях субъектов заслуживает проблема профессиональной подготовки кадров для отстаивания интересов ОДКБ и формирования национальных институтов обеспечения информационной безопасности. Здесь возможны решения по организации единого центра для государств — членов Договора о коллективной безопасности, что позволило бы расширить опыт проведения совместных мероприятий и укрепить интеграцию в области предотвращения угроз распространения киберпреступлений в информационном пространстве ОДКБ.

О. С. МАКАРОВ*

ОБ ОБОСНОВАНИИ МЕТОДОЛОГИЧЕСКОГО ПОДХОДА К СБЛИЖЕНИЮ И ГАРМОНИЗАЦИИ ЗАКОНОДАТЕЛЬСТВА ГОСУДАРСТВ — ЧЛЕНОВ ОРГАНИЗАЦИИ ДОГОВОРА О КОЛЛЕКТИВНОЙ БЕЗОПАСНОСТИ В СФЕРЕ ЗАЩИТЫ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ

Правовому институту государственных секретов (государственной тайны) на постсоветском пространстве уже два десятилетия. Правовой институт тайны является одним из важнейших институтов, определяющих соотношение интересов личности, общества и государства, частного и публичного права, основания и пределы вмешательства государства в негосударственную сферу. Этим определяется актуальность не только исследования норм, регулирующих вопросы, связанные с определением и защитой государственной тайны, но и в более широкой постановке — исследований институтов тайны в целом.

На четвертом пленарном заседании Парламентской Ассамблеи Организации Договора о коллективной безопасности 27 октября 2010 г. были приняты Рекомендации по сближению законодательства государств — членов ОДКБ по вопросам государственной тайны, разработанные совместно российскими и белорусскими специалистами. Приложением к названным рекомендациям стал Глоссарий основных понятий, используемых в законодательстве о государственной тайне (государственных секретах) государств — членов Организации Договора о коллективной безопасности, включающий 84 группы правовых понятий, в ряде случаев имеющих различающиеся трактовки в национальном законодательстве. В принятом ПА ОДКБ документе отмечено, что разработка рекомендаций по совершенствованию и гармонизации законодательства о защите государственной тайны требует осмысления современного состояния и систематизации понятийного аппарата в этой сфере и в более общем случае — в сфере информационной безопасности. Там же обращено внимание на необходимость разработки проектов нормативных актов

* О. С. Макаров, профессор Института национальной безопасности Республики Беларусь.

с учетом уже содержащихся в ранее принятых законах понятий (терминов) и их определений и с опорой на них.

В целях совершенствования правового регулирования складывающихся общественных отношений в обсуждаемой области, а также унификации законодательства государств — членов ОДКБ по защите государственных секретов представляется целесообразным наладить сотрудничество в вопросах изучения наработанного в независимых государствах опыта и его взаимное заимствование. Тематическая секция «Организационно-правовые основы защиты государственных секретов» прошедшей в июле 2013 г. в Минске международной научно-практической конференции «Информационная безопасность как составляющая национальной безопасности государства» явилась едва ли не первым опытом обмена мнениями между специалистами постсоветских государств в данной сфере. В работе секции приняли участие ученые и специалисты из Республики Беларусь, Республики Казахстан и Российской Федерации*.

Научный подход к правовому регулированию защиты государственных секретов государств — членов ОДКБ позволяет на основе сопоставления различий и тождества национальных механизмов регулирования отношений в данной сфере выстроить логический ряд базовых категорий, определяющих современное состояние и векторы развития защиты государственных секретов государств — членов ОДКБ.

1. Организационно-правовой механизм защиты секретов в том виде, в котором он существует в настоящее время в государствах — членах ОДКБ, является порождением правовой системы защиты охраняемой информации в СССР. Несмотря на изменения, связанные с развитием и особенностями национальных правовых систем, концептуальная платформа данного социально-правового института осталась прежней.

2. Политические и правовые условия в государствах — членах ОДКБ с точки зрения защиты государственных секретов существенно не различаются. Организационно-правовой механизм защиты секретов государств — членов ОДКБ испытывает воздей-

* Информационная безопасность как составляющая национальной безопасности государства: Материалы международной научно-практической конференции: В 3 т. / Под ред. С. Н. Князева и др. Т. 1. Минск, 2013.

ствие одинаковых внешних и внутренних факторов, являющихся порождением современного этапа развития общества.

Первым из таких факторов, очевидно, является коммерциализация информации, связанная с отходом от государственной административно-командной системы и переходом к рыночной экономике. (Под коммерциализацией информации при этом понимается процесс обретения информацией как объектом нематериальным фактически материальной ценности, введения информации в коммерческий оборот, формирования рынка информации и информационных услуг.)

Информатизация общества, повсеместное широкое внедрение информационных технологий привели прежде всего к созданию электронного документооборота. Данный фактор также является базовым. С позиции защиты государственных секретов тенденция перехода на электронный документооборот является определенного рода угрозой, так как режим секретности изначально создавался и длительное время существовал в условиях «бумажного» документооборота. Научно-технический прогресс способствует развитию средств и способов разведки (прежде всего технической) и, как показывает практика, росту ее устремлений. Либеральные тенденции и ускорение социальных процессов приводят к нарастанию внутренних противоречий между секретностью и открытостью общества[*].

3. Казалось бы, в единой среде, в сходных условиях родственные правовые системы должны сохранить свою идентичность. Однако на практике национальные особенности «выходят за рамки погрешности», имеет место тенденция к дифференциации правового регулирования защиты государственных секретов государств — членов ОДКБ. При этом государства не развиваются относительно друг друга, а «старательно копируют правовые решения соседа».

В подтверждение сказанного можно привести наиболее яркие примеры. Так, например, если Республика Беларусь отказывается от понятия «утечка сведений», то в законодательстве Республики Армения оно вводится. Российская Федерация вводит ответственность за добывание государственной тайны без признаков

[*] *Балыбердин А. Л., Вус М. А.* Об актуальности совершенствования системы защиты государственной тайны // Вопросы защиты информации. 2013. № 3 (102). С. 100–106.

измены государству или шпионажа. Практически одновременно Республика Беларусь исключает из категории субъектов преступлений в сфере защиты государственных секретов всех, кроме собственно «секретоносителя». Кыргызская Республика вводит в свое законодательство понятие «военная тайна», в то время как законодатели всех других государств — членов ОДКБ от него отказались. Российская Федерация и Республика Казахстан вводят дополнительный режим защиты информации — «предварительное засекречивание», в то время как Республика Беларусь, например, от него отказывается. Республика Таджикистан вводит механизм, согласно которому при отнесении категорий сведений к государственной тайне для каждой такой категории сведений определяется срок их засекречивания. В большинстве же государств — участников СНГ указанный срок формализован и соотносится со степенями секретности сведений. Можно упомянуть и различия по части основания допуска со статусом уполномоченного органа в системе государственных органов и др.

Оглядываясь на пройденный за два десятилетия путь, нельзя отрицать и целый ряд национальных удач в правовом регулировании защиты государственных секретов. Так, например, весьма демократическим представляется закрепленный в законе о государственной тайне Республики Таджикистан механизм рассекречивания сведений на основании прямого обращения граждан к лицу, засекретившему эти сведения. Представляет интерес позиция законодателей Таджикистана, не ограничивающих выезд «секретоносителей» в пределы государства, с которыми имеются соглашения о взаимной охране государственной тайны. Заслуживает внимания правовое закрепление системы органов защиты государственных секретов Кыргызской Республики.

Как показывает практика, в процессе нормативного регулирования отношений в сфере государственных секретов мы все время оглядываемся на правовые акты союзников, стараемся присмотреться к новым механизмам и юридическим новациям. В то же время анализ эффективности правового регулирования защиты государственных секретов у государств-партнеров нам не доступен, оценки эффективности защиты государственных секретов не известны. Представляется, что такие сведения не должны составлять закрытую информацию, во всяком случае от союзников. Ведь в рамках взаимных договоренностей мы обме-

ниваемся государственными секретами, но фактически получается, что при этом не стремимся помочь друг другу в повышении эффективности механизмов их защиты.

4. В рамках ОДКБ проводятся учения, осуществляется боевое слаживание сил оперативного реагирования, подразделений по чрезвычайным ситуациям. В то же время взаимодействие по проблемам защиты секретов носит чисто утилитарный характер, обеспечивающий в рамках законодательно закрепленных договоренностей передачу конкретных сведений.

Такая тенденция порождает ряд вопросов: достаточен ли темп развития; почему нет взаимного анализа и обмена методиками; может ли система защиты секретов устареть?

Представляется, что традиционный подход, засекречивающий сами механизмы защиты секретов, не конструктивен (во всяком случае, в рамках политического союза).

5. Теоретически, как представляется, существует несколько вариантов развития сложившейся практики. Путь развития национальных правовых механизмов защиты секретов втайне от других партнеров чреват риском устаревания и застоя. Вряд ли разумно слепое копирование, заимствование подходов других стран (блоков), способное увеличить риски потери данных. Выработка единой международной платформы для государств — членов ОДКБ (по примеру НАТО) сегодня вряд ли реалистична. Наиболее приемлемым путем развития и совершенствования национальных правовых механизмов защиты секретов нам представляется обмен между государствами — членами ОДКБ методиками и опытом на основе межгосударственных договоренностей.

Естественно, что последний из указанных путей развития предполагает совместные научные исследования, организацию и проведение научно-практических конференций и семинаров, регулярное повышение квалификации, обучение кадров прогрессивным методикам защиты государственных секретов (в том числе, вероятно, посредством организации и проведения учений, тренировок, деловых игр).

По нашему мнению, формату Организации Договора о коллективной безопасности наиболее соответствует задача создания региональной системы информационной безопасности, включающей защиту государственных секретов государств-членов и обеспечение безопасности такой категории информационных ресурсов, как «межгосударственные секреты».

На базе обоснованного тезиса об отсутствии в настоящий момент среди государств — членов ОДКБ явного лидера в разработке механизма защиты государственных секретов совершенствование данного параметра обеспечения национальной и региональной безопасности необходимо осуществлять не эталонным путем (когда заимствуется правовое решение проблемы одного из государств), а методом анализа, обобщения и распространения положительного опыта каждого из государств-членов. В этой работе координирующая роль должна отводиться структурам управления Организации Договора о коллективной безопасности.

Д. В. ПЕРЕВАЛОВ*

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОТРУДНИЧЕСТВА ГОСУДАРСТВ — ЧЛЕНОВ ОДКБ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Современное общество характеризуется переходом к качественно новому состоянию — информационному обществу, в котором отмечается возрастающее влияние новых информационно-коммуникационных технологий на все сферы общественной жизни, обусловленное стремительным развитием систем передачи данных. Разработка новейших технологий, которые призваны обеспечить потребности личности и общества в информации, влечет за собой поступательное развитие новых средств коммуникации, рост их производства и темпов модификации.

Вместе с тем трансформация общества в условиях информационно-коммуникационной революции формирует новые угрозы информационной безопасности. Актуальной данная проблема является и для государств — членов Организации Договора о коллективной безопасности (далее — ОДКБ, Организация). В частности, экспертами отмечается, что в течение 2013 г. IT-инфраструктура 95% российских организаций как минимум один раз подверглась внешней атаке**. При этом хакерским атакам во многих случаях подвергаются объекты, которые могут быть отнесены к критически важным объектам информационно-коммуникационной инфраструктуры (далее — КВОИ) — IT-инфраструктуры топливно-энергетических, производственных, транспортных, информационно-коммуникационных, коммунальных, финансовых и других систем жизнеобеспечения государства и населения.

В настоящее время сотрудничество государств — членов ОДКБ по вопросам обеспечения безопасности КВОИ требует совершенствования, в первую очередь в вопросах гармонизации

* Д. В. Перевалов, начальник факультета — помощник начальника Института национальной безопасности Республики Беларусь.

** *Воронина Ю.* Прием против взлома // Российская бизнес-газета. 2013. № 923. С. 2.

законодательств в рассматриваемой области. Законодательства стран — членов Организации в сфере обеспечения безопасности КВОИ являются недостаточно унифицированными, слабо учитывают высокий уровень существующих в этой сфере угроз, недостаточно гармонизированы с нормами международного права.

В соответствии с общепризнанными принципами и нормами международного права в качестве приоритетных целесообразно рассматривать следующие направления гармонизации законодательства государств — членов ОДКБ в области обеспечения безопасности КВОИ.

1. Определение понятийно-категориального аппарата, используемого при правовом регулировании обеспечения безопасности КВОИ.

При развитии понятийно-категориального аппарата в рассматриваемой области представляется необходимым принимать во внимание основные формы и характер проявления угроз безопасности КВОИ на территориях государств — членов ОДКБ, особенности создания и функционирования систем обеспечения безопасности объектов. В частности, в Республике Беларусь такая система функционирует в соответствии с Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации». Планируется, что подобная система будет сформирована и в Российской Федерации в соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации», проект которого разработан ФСБ России. Указанные документы содержат термины и их определения, которые не совпадают как по форме, так и по содержанию.

В дальнейшем при разработке конкретных международных и национальных нормативных правовых актов необходимо обеспечить ориентацию всех участников на использование единого понятийно-категориального аппарата.

2. Закрепление основных направлений правового регулирования обеспечения безопасности КВОИ в государствах — членах ОДКБ.

К основным направлениям правового регулирования обеспечения безопасности КВОИ в государствах — членах ОДКБ, носящим приоритетный характер и подлежащим закреплению в

национальном законодательстве стран — членов Организации, следует отнести:

— определение источников угроз, их характера, разработку классификации угроз в рассматриваемой сфере;

— определение деяний, признаваемых правонарушениями в рассматриваемой сфере;

— регламентацию деятельности по выявлению и последующему устранению причин и условий, способствующих формированию и реализации угроз безопасности КВОИ;

— определение мер, направленных на недопущение нанесения ущерба критическим элементам КВОИ;

— осуществление мероприятий по выявлению и пресечению противоправной деятельности, направленной на нарушение или прекращение функционирования КВОИ.

Одним из важнейших аспектов является уточнение закрепляемых в национальном законодательстве стран — членов Организации положений, предусматривающих перечни правонарушений в области обеспечения безопасности КВОИ. Соответствующую разработку и доработку законодательных актов в данной сфере целесообразно осуществлять с учетом отличительных признаков конкретных действий, позволяющих идентифицировать их и выделить из группы сходных по объективной стороне преступлений и правонарушений, которые будут рассматриваться в качестве угроз безопасности КВОИ. Это является необходимым условием повышения эффективности правоприменительной практики, направленной на предупреждение противоправной деятельности в рассматриваемой области.

Требуют разработки и закрепления в специализированных нормативных правовых актах или в отдельных правовых нормах наиболее важные направления деятельности компетентных государственных органов в области обеспечения безопасности КВОИ, такие как:

— создание национальной системы обеспечения безопасности КВОИ;

— формирование и использование сил и средств обеспечения безопасности КВОИ;

— деятельность по идентификации угроз безопасности КВОИ, предупреждению, выявлению и пресечению правонарушений в данной области;

— характер и пределы реализации мер, направленных на пресечение указанных правонарушений;

— распределение объема полномочий и ответственности между компетентными государственными органами, эксплуатирующими КВОИ, осуществляющими контроль за их эксплуатацией, а также определяющими направления правоохранительной деятельности в области обеспечения безопасности КВОИ.

3. Нормативное закрепление основных направлений международного сотрудничества в сфере правового регулирования обеспечения безопасности КВОИ.

В качестве основных направлений международного сотрудничества в сфере правового регулирования обеспечения безопасности КВОИ следует рассматривать:

— проведение согласованной политики по гармонизации национального законодательства в рассматриваемой области;

— совместную работу по предотвращению и устранению причин и условий, способствующих формированию угроз безопасности КВОИ;

— обмен информацией по вопросам предупреждения и пресечения правонарушений в области безопасности КВОИ;

— оказание взаимной правовой, методической, технической и иной помощи;

— координацию деятельности компетентных государственных органов, осуществляющих деятельность по предупреждению и пресечению правонарушений в области обеспечения безопасности КВОИ;

— проведение совместных процессуальных, оперативных и иных мероприятий по документированию и пресечению правонарушений в рассматриваемой области;

— сближение подходов, применяемых при принятии решений о формировании национальных систем обеспечения безопасности КВОИ.

4. Обеспечение введения мер ответственности за подготовку и совершение деяний, которые будут отнесены к правонарушениям в области обеспечения безопасности КВОИ.

За совершение правонарушений в области обеспечения безопасности КВОИ граждане государств — членов ОДКБ, а также иностранные граждане и лица без гражданства в соответствии

с национальным законодательством должны нести уголовную, административную и иную ответственность в зависимости от общественной опасности деяния или наступивших последствий.

В частности, представляется обоснованным введение:

— административной ответственности за нарушение правил безопасности при эксплуатации КВОИ, повреждение или приведение в негодность систем жизнеобеспечения КВОИ;

— уголовной ответственности за указанные правонарушения, если они повлекли за собой гибель людей, животных, возникновение пожара или аварии на КВОИ или иные тяжкие последствия.

Для повышения эффективности деятельности компетентных государственных органов и системы мер, направленных на предупреждение и пресечение правонарушений в области обеспечения безопасности КВОИ, представляется необходимым обеспечить согласование правовых норм в рамках специальных законов, в том числе соответствующих норм уголовного законодательства стран — членов Организации.

К первоочередным целесообразно отнести следующие меры по совершенствованию правового регулирования обеспечения безопасности КВОИ.

1. Определение уровней правового регулирования обеспечения безопасности КВОИ.

В области обеспечения безопасности КВОИ представляется обоснованным рассматривать следующие уровни правового регулирования:

1) межгосударственный уровень;

2) национальный уровень государств — членов ОДКБ.

При этом необходимо учитывать, что при осуществлении правового регулирования рассматриваемой области возникает ряд проблем, основной из которых является сопряжение технических аспектов эксплуатации КВОИ и закономерностей правовой регламентации деятельности компетентных государственных органов по обеспечению их безопасности.

2. Совершенствование обеспечения безопасности КВОИ на межгосударственном уровне.

Представляется, что в рамках ОДКБ целесообразной является разработка рекомендаций по гармонизации законодательства государств — членов ОДКБ в области обеспечения безопасности КВОИ.

Важность разработки подобных рекомендаций обусловлена следующими обстоятельствами:

— необходимостью охраны и защиты национальных интересов безопасности государств — членов ОДКБ в условиях динамичного изменения геополитической и внутригосударственной обстановки и возникновения новых угроз;

— необходимостью обеспечения должной реализации конституционных прав граждан государств — членов ОДКБ и конституционных гарантий по созданию условий для свободного и достойного развития личности;

— необходимостью повышения эффективности деятельности государственных органов государств — членов ОДКБ, связанной с защитой прав и законных интересов граждан в информационной сфере, обеспечением безопасности общества и государства;

— потребностью установления дополнительной правовой регламентации обеспечения безопасности КВОИ как самостоятельного административно-правового режима;

— целесообразностью оптимизации затрат в сфере обеспечения национальной безопасности государств — членов ОДКБ при эксплуатации КВОИ.

3. Совершенствование обеспечения безопасности КВОИ на национальном уровне.

На национальном уровне требуется принятие специальных нормативных правовых актов (законов, указов главы государства, постановлений правительства), непосредственно регламентирующих обеспечение безопасности КВОИ.

Одновременно необходимо создание системы правовых норм в административном, уголовном, трудовом и гражданском законодательствах, определяющих компетенцию и ответственность заинтересованных юридических и физических лиц в данной сфере.

4. Разработка и согласование понятийно-категориального аппарата.

Необходимо добиться обеспечения терминологической ясности и единообразной трактовки законодательными органами государств — членов ОДКБ таких понятий, как:

— информационно-коммуникационная инфраструктура;

— критически важный объект информационно-коммуникационной инфраструктуры;

— угроза безопасности КВОИ;
— критический элемент КВОИ;
— меры безопасности КВОИ.

Определение и закрепление основных направлений сотрудничества государств — членов ОДКБ в области обеспечения безопасности КВОИ позволит обеспечить:

— гармонизацию национальных актов законодательства в сфере обеспечения информационной безопасности в целях формирования и развития единого (общего) информационного пространства государств — членов ОДКБ;

— регулятивную мобильность уполномоченных государственных органов государств — членов ОДКБ в рассматриваемой области;

— выработку механизма установления эквивалентности и взаимного согласования систем обеспечения безопасности КВОИ;

— формирование единой, скоординированной и сопряженной системы правовых, организационных, инженерно-технических, программно-аппаратных и специальных мер обеспечения безопасности КВОИ в государствах — членах ОДКБ.

С. А. ЦВЕТКОВ*

УНИФИКАЦИЯ НАЦИОНАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА ГОСУДАРСТВ — ЧЛЕНОВ ОРГАНИЗАЦИИ ДОГОВОРА О КОЛЛЕКТИВНОЙ БЕЗОПАСНОСТИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ВСТУПЛЕНИЯ ВО ВСЕМИРНУЮ ТОРГОВУЮ ОРГАНИЗАЦИЮ

На современном этапе функционирования государств — членов ОДКБ важное значение имеет унификация национального законодательства в сфере информационной безопасности в соответствии с требованиями Всемирной торговой организации (ВТО).

Базовые принципы ВТО, в соответствии с которыми необходимо унифицировать национальное законодательство, следующие:

— режим наибольшего благоприятствования;

— национальный режим;

— транспарентность.

Для достижения наиболее эффективных результатов в этом направлении необходимо привести законодательство государств — членов ОДКБ в соответствие с конкретными статьями Генерального соглашения по торговле услугами и Соглашения по техническим барьерам в торговле.

Применительно к данной законотворческой деятельности унификация предполагает такое состояние законодательства разных государств, при котором его структура, состав и отдельные положения приводятся к одному и тому же виду. В данном контексте рассматриваются прежде всего национальные законы о стандартизации и о техническом регулировании, так как в значительной степени через эти законы концептуальные основы информационной безопасности трансформируются в конкретные технические условия.

Законодательные основы в области обеспечения информационной безопасности в государствах — членах ОДКБ в условиях

* С. А. Цветков, проректор по научно-исследовательской работе Национального государственного университета физической культуры, спорта и здоровья им. П. Ф. Лесгафта.

вступления в ВТО включают в себя пакет законов — о национальной безопасности, о государственных секретах, об информатизации, об электронном документе и электронной цифровой подписи и др.

Вступление государств — членов ОДКБ в ВТО предполагает возникновение новых факторов в законодательном обеспечении информационной безопасности, которые необходимо учитывать.

Прежде всего, это Генеральное соглашение по торговле услугами. Так, в пункте 4 статьи 6 данного соглашения отмечается: «Для обеспечения того, чтобы меры, относящиеся к квалифицированным требованиям и процедурам, техническим стандартам и требованиям лицензирования, не создавали неоправданных барьеров в торговле услугами, Совет по торговле услугами через соответствующие органы, которые он может создать, разрабатывает любые необходимые правила. Эти правила имеют целью обеспечить, чтобы такие требования, среди прочего... не были более обременительными, чем это необходимо для обеспечения качества услуги...»

Следовательно, это означает, что Совет по торговле ВТО сам определяет, какие правила более обременительны, чем это необходимо для обеспечения качества услуг.

Следует подчеркнуть, что данный подход может иметь определенную долю субъектизма в оценке действия того или иного национального закона в государствах ОДКБ членами Совета по торговле услугами.

Для того чтобы избежать такого вида угроз, необходимо:

1) в государствах — членах ОДКБ организовать подготовку профессиональных специалистов в области разработки законодательных основ по защите информации в условиях открытой экономики;

2) разработать механизмы продвижения подготовленных специалистов в указанной области в ключевые структуры ВТО.

Такой подход позволит минимизировать возможные риски в сфере обеспечения информационной безопасности, связанные со вступлением в ВТО государств — членов ОДКБ.

Т. А. ПОЛЯКОВА*

ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уважаемые коллеги!

Разрешите поприветствовать вас на этом международном форуме, посвященном обсуждению вопросов правового обеспечения информационной безопасности в государствах — членах ОДКБ, имеющегося опыта, проблем и перспектив гармонизации законодательства в данной сфере. Глобализация информационной сферы, трансграничный характер новых вызовов и угроз в информационном пространстве — это реалии современного виртуального мира.

Обеспечение информационной безопасности — задача комплексная, и ее важной составляющей, обусловленной прогрессом в сфере использования информационно-коммуникационных технологий как на международном, так и на национальном уровне, является правовое обеспечение. В связи с этим для формирования системы международной информационной безопасности на основе межгосударственного сотрудничества особую актуальность приобретает изучение национального опыта нормативно-правового регулирования в данной области.

Вопросам укрепления доверия и безопасности в глобальном информационном пространстве уделяется особое внимание как в форматах ООН, ШОС, ОБСЕ, АСЕАН, СНГ, Союзного государства Беларуси и России, ОДКБ, так и на национальном уровне. В современных условиях возникают новые формы вооруженной борьбы в информационном пространстве — информационные войны с использованием информационного оружия, кибертерроризм, киберпреступность, требующие разработки целого комплекса системных правовых мер.

Обеспечение информационной безопасности невозможно без верховенства права — одного из основных принципов глобального информационного общества. И обсуждение вопросов, связанных с формированием адекватных правовых основ обеспечения

* Т. А. Полякова, заместитель директора Департамента конституционного законодательства Министерства юстиции Российской Федерации.

информационной безопасности, представляется особенно актуальным. Это очевидно с учетом динамики развития глобального информационного общества.

В настоящее время в Российской Федерации приоритетные задачи, основные направления, механизмы реализации государственной политики в области обеспечения информационной безопасности, включая вопросы координации (взаимодействия), а также компетенции государственных органов, определены в стратегических, концептуальных и иных правовых документах, утвержденных указами Президента России и отвечающих требованиям стратегического планирования защиты национальных интересов Российской Федерации в информационной сфере.

К ним относятся Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная 12 мая 2009 г., Доктрина информационной безопасности Российской Федерации, утвержденная 9 сентября 2000 г., Стратегия развития информационного общества в Российской Федерации, утвержденная 7 февраля 2008 г., и ряд других.

Особое место занимают Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, подписанные Президентом России В. В.Путиным 24 июля 2013 г. и являющиеся стратегическим документом в данной сфере. Важно отметить, что в этом политическом документе обозначены новые подходы к формированию такого понятия, как «международная информационная безопасность». Международная информационная безопасность определена как «состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры». Под системой международной информационной безопасности в нем понимается «совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства».

В России правовые основы в области обеспечения информационной безопасности заложены в Конституции Российской Федерации, которой в декабре 2013 г. исполняется 20 лет. В Конституции, в частности, закреплены: право на информацию, охра-

на сведений, составляющих государственную тайну (статья 29); недопущение сбора, хранения и распространения информации о частной жизни лица без его согласия (статья 24); право граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 23); компетенция Российской Федерации в решении вопросов о федеральной информации и связи (статья 71); обязанность государства официально публиковать законы и иные нормативные правовые акты (статья 15); ответственность за сокрытие информации о фактах и обстоятельствах, создающих угрозу для жизни и здоровья людей (статья 41) и т. д.

Также конституционно установлены гарантии реализации указанных прав и свобод (признание их неотчуждаемыми, равными и непосредственно действующими) (статьи 17–19). Наряду с государственной защитой гарантируется право каждого на защиту своих прав и свобод всеми способами, не запрещенными законом (статья 45), судебную и международно-правовую защиту прав и свобод (статья 46). Даже такой краткий анализ показывает, что в российском законодательстве имеется значительное количество конституционных правовых норм, связанных с обеспечением информационной безопасности. Это свидетельствует о многогранности и многоаспектности данной сферы правового регулирования.

В целях реализации конституционных правовых норм, а также стратегических правовых документов принято значительное количество законодательных актов как на федеральном уровне (включая федеральные конституционные и федеральные законы), так и на уровне субъектов Российской Федерации.

Основополагающими законодательными актами в сфере информационной безопасности являются федеральные законы «Об информации, информационных технологиях и о защите информации» и «О персональных данных», принятые в 2006 г. и направленные на урегулирование отношений, связанных с обеспечением безопасности в сфере информации и информационных технологий, включая информацию персонального характера. Следует отметить, что сегодня в российском законодательстве закреплены важные для правового регулирования в этой сфере дефиниции, включая такие понятия, как «сайт в сети “Интернет”», «доменное имя», «провайдер хостинга» и др., однако ключевое понятие «Интернет» так и не нашло пока своего правового определения.

В этой области ключевыми являются также законы «О государственной тайне», «О техническом регулировании», «О коммерческой тайне», «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», «О безопасности», «О защите детей от информации, причиняющей вред их здоровью и развитию», «Об электронной подписи» и др.

Правовые нормы, связанные с обеспечением информационной безопасности, также содержатся в Гражданском кодексе Российской Федерации (охрана прав на результаты интеллектуальной деятельности и средства индивидуализации, включая программы для ЭВМ, базы данных, топологии интегральных микросхем и т. д.). В Уголовном кодексе и Кодексе Российской Федерации об административных правонарушениях предусмотрена ответственность за преступления в сфере компьютерной информации (глава 28 УК), за правонарушения в области связи и информации, а также в области защиты информации (статьи 137,138,140,189,283,159.6 и др. УК, глава 13 КоАП).

В целях реализации законодательных норм принят большой массив подзаконных правовых актов, включая указы и распоряжения Президента России. Например, Указ № 31с от 15 января 2013 г. «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», постановления и распоряжения Правительства Российской Федерации, а также нормативные правовые акты федеральных органов исполнительной власти (ФСБ России, Минкомсвязи России, ФСТЭК России, МВД России).

Обеспечению информационной безопасности граждан, а также самой информационной инфраструктуры посвящена подпрограмма «Безопасность в информационном обществе», включенная в государственную программу «Информационное общество (2011–2020 годы)» от 20 октября 2010 г.

Основными задачами в этой подпрограмме являются:

— обеспечение контроля и надзора, разрешительной и регистрационной деятельности в сфере связи, информационных технологий и массовых коммуникаций;

— обеспечение безопасности функционирования информационных и телекоммуникационных систем;

— развитие технологий защиты информации, обеспечивающих неприкосновенность частной жизни, личной и семейной тайны, безопасность информации ограниченного доступа;

— противодействие распространению идеологии терроризма, экстремизма, пропаганды насилия.

Следует отметить, что в 2013 г. распоряжениями Правительства от 20 июля и 1 ноября утверждены план мероприятий («дорожная карта») «Развитие отрасли информационных технологий» и Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года для формирования единого системного подхода государства к развитию отрасли информационных технологий, включая виды деятельности, связанные с обеспечением информационной безопасности.

Для реализации основных положений Стратегии национальной безопасности Российской Федерации, связанных с предотвращением угроз безопасности функционирования информационных и коммуникационных систем критически важных объектов повышенной опасности, разработаны Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. В них определены принципы формирования государственной политики в области обеспечения безопасности автоматизированных систем управления критически важных объектов, а также задачи государственного регулирования в данной сфере, включая совершенствование нормативно-правовой базы.

На решение организационно-правовых проблем обеспечения кибербезопасности также направлен Указ Президента Российской Федерации от 15 января 2013 г., которым предусмотрено создание государственной системы обнаружения, предупреждения, а также ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации — информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях за рубежом.

В 2013 г. также внесены изменения в федеральные законы «Об информации, информационных технологиях и о защите инфор-

мации» и «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», направленные на дальнейшую реализацию политики по обеспечению открытости информации о деятельности государственных органов и органов местного самоуправления. Предусматривается предоставление такой информации государственными органами и органами местного самоуправления неограниченному кругу лиц посредством ее размещения в Интернете в форме открытых данных.

Кроме того, в целях принятия органами исполнительной власти мер, направленных на ускоренное развитие российской отрасли информационных технологий в 2013–2018 годах, упрощение взаимодействия государства и бизнес-сообщества, повышение прозрачности, распоряжениями Правительства Российской Федерации от 11 июня 2013 г. № 953-р (в редакции от 17 августа 2013 г.) и от 20 июля 2013 г. № 1268-р утверждены так называемые дорожные карты «Повышение качества регуляторной среды для бизнеса» и «Развитие отрасли информационных технологий», в которых отражены организационно-правовые вопросы, связанные с обеспечением информационной безопасности (использование электронных документов и унификация форматов обмена данными при взаимодействии государственных органов и предпринимателей, а также в суде, развитие исследований в области информационных технологий, экспорта информационно-коммуникационной продукции, совершенствование институциональных условий ведения бизнеса в области информационных технологий, включая совершенствование законодательства для обеспечения развития облачных вычислений, и др.).

Следует отметить важность проблемы обеспечения информационной безопасности при использовании облачных вычислений и утверждения необходимых стандартов безопасности облачных сред и инструментов измерения уровня рисков и угроз. Наиболее масштабным государственным проектом в этой области является Национальная облачная платформа, создающаяся в рамках государственной программы «Информационное общество (2011–2020 годы)».

Однако пока не урегулированы основные правила использования облачных технологий, касающиеся обеспечения безопасности и конфиденциальности информации. Правовое решение данной проблемы связано и с разработкой Единой сети передачи

данных для органов государственной власти, создаваемой в целях повышения качества телекоммуникационных и вычислительных услуг, предоставляемых органами власти, а также формирования условий, стимулирующих ликвидацию «цифрового неравенства».

Не менее актуальной является проблема обеспечения безопасности персональных данных, используемых в информационных системах. Важно отметить, что 15 мая 2013 г. в Совет Европы Россией передана ратификационная грамота, подтверждающая завершение почти семилетней процедуры ратификации одного из наиболее актуальных международных правовых актов в области защиты персональных данных — Конвенции о защите физических лиц при автоматизированной обработке персональных данных. Это важный шаг в направлении обеспечения безопасности человека в киберпространстве и общеевропейском правовом пространстве.

Последним этапом, связанным с ратификацией данной Конвенции, стало принятие в мае 2013 г. Федерального закона, в соответствии с которым внесены изменения в 14 законодательных актов, направленные на обеспечение соблюдения конфиденциальности и защиты персональных данных в различных сферах, а также на уточнение случаев получения согласия субъекта персональных данных на их обработку.

В настоящее время в Совете Федерации Федерального Собрания Российской Федерации осуществляется разработка проекта стратегии кибербезопасности, направленной на формирование цифрового суверенитета России, создание механизмов мониторинга киберугроз, формирование пространства информационной безопасности, осуществление взаимодействия государства, бизнес-сообщества и гражданского общества в сфере кибербезопасности, совершенствование нормативно-правовой базы, поддержку отечественных производителей программного обеспечения, подготовку квалифицированных кадров и т. д.

Таким образом, национальное законодательство в указанной сфере в России активно развивается. Вместе с тем остается широкий спектр правовых проблем, связанных с обеспечением информационной безопасности личности, общества и государства, кибербезопасности, неприкосновенности частной жизни, защиты права на доступ к информации, защиты информационных систем, ресурсов и сетей, расширением применения информационных технологий в государственном управлении и при оказании

государственных услуг и т. д. Кроме того, на различных уровнях продолжаются дискуссии о правовом статусе Интернета и о необходимости закрепления на международном уровне определенных правил поведения в так называемом виртуальном пространстве, о цензуре или необходимости правового урегулирования вопросов, связанных с неправомерным использованием Интернета. Это всего лишь часть вопросов, которые заслуживают самого пристального внимания и в рамках ОДКБ, поскольку только в 2013 г. произошло немало резонансных событий в сфере, связанной с обеспечением международной информационной безопасности. Распространение получили кибератаки, направленные на хищение данных, нарушение нормальной работы корпораций и государственных структур, а также имеющие политические мотивы.

Основной угрозой в сфере международной информационной безопасности признано применение информационных и коммуникационных технологий:

— в качестве информационного оружия в военно-политических целях, для осуществления враждебных действий и актов агрессии, нарушающих территориальную целостность государств, угрожающих международному миру, безопасности и стратегической стабильности;

— в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

— для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию, а также для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

Общеизвестно, что ряд международных соглашений в данной сфере уже действует. В рамках ШОС, ОДКБ, БРИКС и других международных организаций ведется разработка новых соглаше-

ний. В международном сотрудничестве важное место занимает дальнейшее продвижение предложений, связанных с принятием Конвенции об обеспечении международной информационной безопасности, концепция которой стала результатом многолетней работы российских экспертов в области международной информационной безопасности во взаимодействии с зарубежными коллегами. Она содержит правила поведения в киберпространстве, развивает предложения, связанные с интернационализацией управления Интернетом, установлением международного правового режима нераспространения информационного оружия и т. д. Среди основных угроз определены использование информационных технологий для враждебных действий и актов агрессии, подрыв политической, экономической и социальной систем одного государства другим, манипулирование потоками в информационном пространстве других государств с целью искажения психологической и духовной среды общества, а также массированная психологическая обработка населения для дестабилизации общества и государства.

Предлагается установить обязанность государств руководствоваться принципом неделимости безопасности. Установлен запрет на укрепление своей безопасности в ущерб безопасности других, на попытки добиться господства в информационном пространстве, а также использовать информационно-коммуникационные технологии для вмешательства во внутренние дела других государств, на клеветнические утверждения, оскорбительную или враждебную пропаганду в целях осуществления интервенции или вмешательства во внутренние дела других государств и т. д.

Также предлагается закрепить принцип невмешательства в информационное пространство друг друга и право каждого государства устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством. Кроме того, предусмотрены обязанность государств защищать свободу слова в Интернете и запрет на ограничение доступа граждан к информационному пространству в целях защиты национальной и общественной безопасности.

Необходимо отметить, что значительное место в развитии сферы информационной безопасности занимают научные исследования и подготовка квалифицированных кадров. К основным

направлениям научных исследований в области обеспечения информационной безопасности в России относятся гуманитарные и научно-технические. При этом выделено более 100 приоритетных направлений научных исследований в данной сфере.

В целях обороны и обеспечения безопасности государства создан Фонд перспективных исследований, в рамках деятельности которого будут осуществляться исследования по проблематике информационной безопасности, в частности разработка методов и средств обхода антивирусных систем, средств сетевой защиты, средств защиты операционных систем. В области информационных технологий заявлены такие темы, как методы и средства борьбы с дезинформацией в Интернете; подтверждение подлинности и целостности сканированных документов без применения электронной подписи; новые механизмы и способы работы с оборудованием, не имеющим стандартных программных и аппаратных интерфейсов.

Очевидно, что для формирования и реализации национальной политики государств — членов ОДКБ в сфере обеспечения информационной безопасности особое значение имеет развитие фундаментальных научных исследований в области информационно-коммуникационных технологий и систем, стратегических компьютерных технологий и программ, поскольку необходимо системное правовое регулирование на основе тщательного анализа и развития международных правовых норм, использования зарубежного опыта и взаимодействия на пути продвижения инициатив в области международной информационной безопасности.

Сегодня требуются универсальные международные правовые механизмы для легитимного, взвешенного решения вопроса интернационализации управления Интернетом, для взаимодействия при расследовании преступлений в сфере использования информационных и коммуникационных технологий на основе продвижения и принятия под эгидой ООН Конвенции о сотрудничестве в сфере противодействия информационной преступности.

Необходимы создание правовых условий, развитие правового регулирования, а не адаптация гуманитарного права, в целях обеспечения снижения риска использования информационно-коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств.

М. А. ПЛИСЮК*

О СОГЛАСОВАННОЙ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВ — ЧЛЕНОВ ОРГАНИЗАЦИИ ДОГОВОРА О КОЛЛЕКТИВНОЙ БЕЗОПАСНОСТИ

Уважаемые коллеги!

Разрешите поблагодарить за возможность выступить на столь важном мероприятии.

Тематика конференции, а именно проблематика информационной безопасности, представляется весьма актуальной и востребованной в современных условиях.

В Институте ОДКБ данная тема рассматривается как одна из приоритетных и ей уделяется повышенное внимание.

Как представляется, для обеспечения информационной безопасности в рамках ОДКБ необходимо следующее:

— добиться доминирования в информационном пространстве Организации духовно-нравственных ценностей;

— блокировать распространение в мировом информационном пространстве негативных материалов о государствах ОДКБ, целенаправленно искажающих их традиции и историю.

Главами государств — членов Организации Договора о коллективной безопасности на заседаниях Совета коллективной безопасности ОДКБ неоднократно подчеркивалась необходимость принятия дополнительных мер по развитию совместного информационно-аналитического потенциала в целях построения эффективной системы коллективной безопасности, пропаганды деятельности ОДКБ. 11 марта 2013 г. Секретариат ОДКБ провел международный семинар-совещание с руководителями информационно-аналитических структур государств — членов ОДКБ. На нем было принято решение о создании Аналитической Ассоциации ОДКБ, которая предназначена для разработки плана мероприятий и стратегии скоординированной информационной политики в интересах государств — членов Организации, информационно-аналитической поддержки решений глав государств —

* М. А. Плисюк, исполнительный директор автономной некоммерческой организации «Институт ОДКБ», член Научно-экспертного совета Организации Договора о коллективной безопасности.

членов ОДКБ, налаживания деловых контактов, обмена информацией, проведения экспертного и ситуационного анализа и для обеспечения более тесного взаимодействия Сторон.

Ассоциация также будет участвовать в разработке базовых принципов скоординированной информационной политики, в числе которых: позитивное освещение международной активности государств — членов ОДКБ, прежде всего в части реализации согласованных подходов, отстаивания позиций, одобренных уставными органами Организации, противодействия попыткам блокирования коллективных инициатив союзников в международных организациях; противодействие реализации замыслов третьих стран, стремящихся к использованию информационного пространства ОДКБ в целях искажения итогов Второй мировой и Великой Отечественной войн, политического давления и вмешательства во внутренние дела под предлогом оказания содействия развитию демократических процессов или под иными надуманными предлогами; противодействие пропаганде идеологии терроризма и экстремизма, расовой и религиозной нетерпимости, оскорбляющей национальные и духовно-нравственные ценности народов, проживающих на территории государств — членов ОДКБ. Данные базовые принципы скоординированной информационной политики на пространстве ОДКБ, направленной на развитие диалога культур и цивилизаций, будут представлены главам государств — членов Организации Договора о коллективной безопасности для утверждения на заседании Совета коллективной безопасности ОДКБ.

В связи с этим хотелось бы подчеркнуть, что Институт ОДКБ активно подключился к деятельности Аналитической Ассоциации и принимает участие в большинстве проводимых под эгидой данной структуры мероприятий.

Мы убеждены, что в рамках ОДКБ должны существовать подразделения информационного реагирования — стратегическая информационная разведка ОДКБ, действующая в глобальном информационном пространстве, выстраивающая систему прогнозов в интересах Организации. Главная задача такой структуры — обеспечение готовности к эффективным действиям в условиях возможного кризиса посредством тщательной предварительной подготовки и планирования.

Дальнейшее развитие ОДКБ требует скорейшего создания эффективной системы информационного противодействия, так как

информационная война против России и других стран ОДКБ не прекращается.

ОДКБ следует продолжить выработку адекватных мер реагирования в целях нейтрализации существующих угроз в гуманитарной сфере. Государствам — членам ОДКБ необходимо уделять повышенное внимание таким направлениям, как:

— выработка международно-правовых механизмов защиты информационного пространства ОДКБ от распространения идеологии терроризма, негативного информационного воздействия на население стран ОДКБ в блогосфере и социальных сетях;

— формирование основ межгосударственной системы противодействия идеологии терроризма, акциям информационно-психологического давления в блогосфере и социальных сетях, попыткам осуществления акций информационно-психологического терроризма, направленных против населения стран ОДКБ;

— совершенствование национального законодательства государств — членов ОДКБ, направленного на повышение социальной ответственности СМИ, противодействие деструктивной деятельности СМИ;

— формирование государственных регулирующих структур в религиозной сфере, нацеленных на информационное противодействие радикализации и рекрутированию молодежи в террористические организации. Привлечение к процессу информационно-идеологического противодействия служителей традиционного исламского культа, деятелей культуры и сферы образования;

— использование общественных, культурных и иных гуманитарных ресурсов государств — членов ОДКБ для противодействия идеологии терроризма и экстремизма, обеспечения населения стран ОДКБ достоверной и объективной информацией, исключающей предвзятость и целенаправленное искажение фактов;

— распространение полной и точной информации о внешнеполитических инициативах и действиях, о процессах и планах внутреннего социально-экономического развития, достижениях культуры и науки государств — членов ОДКБ;

— развитие собственных эффективных средств влияния ОДКБ на общественное мнение в Евразии, оказание необходимой государственной поддержки в данной сфере.

Важнейшим направлением в деятельности ОДКБ является гуманитарное сотрудничество и использование технологий так

называемой мягкой силы в целях содействия созданию в Евразии безопасной среды, способствующей развитию национальных культур, межнациональных и межрегиональных культурных связей, возрождению и сохранению культурно-нравственных ценностей, укреплению духовного единства народов Евразии.

ОДКБ — надежный гарант безопасности Евразии. Динамика развития Организации дает основание с оптимизмом говорить о ее будущем. Необходимо развивать ОДКБ как организацию, гарантирующую стабильность и безопасность в Евразии, устраняя некоторые недостатки в ее деятельности.

Благодарю за внимание.

М. А. ВУС, М. М. КУЧЕРЯВЫЙ*

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВОЕННО-ПОЛИТИЧЕСКИЕ, МЕЖДУНАРОДНО-ПРАВОВЫЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ

Информационная революция в технической сфере и экспансия информации как основного ресурса производства привели к глобализации хозяйственной жизни и способствовали выходу на мировую арену большого числа новых, разнообразных по своему составу акторов. Социальная значимость данных процессов определяется включением доступности информационных услуг и информационных технологий в число параметров, характеризующих качество жизни современного человека, реализацию его основных прав и свобод. В связи с этим возрастает значение глобального информационного пространства (ГИП).

Сущность, содержание и возможные формы использования современных информационно-коммуникационных технологий (ИКТ) во враждебных и преступных целях, возникающие в связи с этим угрозы позволяют говорить о принципиально новой геостратегической, геоинформационной и геополитической ситуации, характеризующейся возникновением новых вызовов и рисков в сфере национальной и международной безопасности, представляющих серьезную опасность для граждан, общества, государства и международного сообщества в целом.

Объективным следствием разрыва между бурно развивающимся информационным обществом и мерами по регулированию вновь возникающих общественных отношений стала растущая информационная преступность. Информация, информационные ресурсы и технологии стали предметом и целью преступных посягательств, средой, в которой совершаются противоправные деяния, а также средством или орудием преступлений.

---

* М. А. Вус, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, М. М. Кучерявый, руководитель Управления Федеральной службы по техническому и экспортному контролю России по Северо-Западному федеральному округу.

Информационная преступность имеет сегодня транснациональные масштабы. Глобальность информационного пространства поставила проблему обеспечения международной информационной безопасности (МИБ)*. Потенциал ГИП активно используется для реализации многих важных функций государственного управления. Это, с одной стороны, создает условия для повышения качества жизни граждан, эффективности выполнения функций государственного управления, а с другой — может быть использовано для нарушения устойчивости и дезорганизации государственной системы. Большинство систем, критически важных для поддержания и развития инфраструктуры, включены в это пространство, что позволяет инициировать техногенные, энергетические и финансовые катастрофы, создавать хаос и панику. В то же время система оценок использования и развития ГИП в настоящее время отсутствует.

В процессе цивилизационного развития геополитическая конкуренция всегда являлась одним из определяющих факторов. В информационной сфере на ее характере отражается такое исторически сложившееся обстоятельство, как доминирование США в области ИКТ и Интернета. Создав Интернет и сумев убедить остальной мир в его преимуществах, американская сторона стала лидером не только в управлении доменными именами.

США голосовали в ООН против решений о предотвращении гонки вооружений и мерах установления доверия в космической деятельности, заявляя при этом, что никакой гонки вооружений в космосе нет. Такой же позиции, ориентированной на сохранение условий, обеспечивающих безнаказанность проведения глобальных информационных операций, придерживается администрация США и в отношении ГИП.

Вместе с тем материалы различных проводившихся исследований и имеющиеся публикации (в частности, ежегодные отчеты McAfee.Inc) свидетельствуют о постоянно растущем количестве политически мотивированных атак с применением информационно-телекоммуникационной инфраструктуры. Прошедшие не-

* Под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором исключена возможность нарушения прав личности, общества и государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

сколько лет продемонстрировали рост информационных угроз, направленных на конкретные государства. Такие угрозы могут использоваться для различных целей, начиная от кибершпионажа и заканчивая выведением из строя каких-либо стратегически важных объектов инфраструктуры. Например, «кибердары» по ядерным объектам Ирана посредством вируса Stuxnet в 2010 г. вывели из строя центрифуги, а эпидемия компьютерных вирусов, потрясшая планету в последующие годы, затронула страны — поставщики углеводородов.

В США разработана и действует система руководящих документов, регламентирующих порядок подготовки и проведения так называемых информационных операций. К основным задачам таких операций, как правило, относится нарушение функционирования ключевых и критически важных систем потенциального противника посредством использования современных ИКТ. Еще в 2009 г. было учреждено Кибернетическое командование США, имеющее статус рода войск. В мае 2011 г. США была обнародована Международная стратегия по действиям в киберпространстве, согласно которой американцы оставляют за собой право использовать все необходимые, в том числе и военные, средства для защиты своих национальных интересов в киберпространстве*.

В связи с этим становится очевидно, что в настоящее время возникла и набирает силу новая военно-политическая угроза всеобщему миру и международной стабильности. Противодействие ей требует, в частности, активизации военно-политического сотрудничества в рамках Организации Договора о коллективной безопасности (ОДКБ) — региональной международной организации, созданной в целях обеспечения национальной, международной и региональной безопасности и стабильности. Необходимы скоординированные совместные действия государств — членов ОДКБ по формированию эффективной системы коллективной безопасности в информационной сфере.

Угрозы военно-политического, террористического и криминального характера, проявляющиеся в информационной сфере, препятствуют полномасштабному использованию потенциала

* Американская администрация не видит необходимости заключать международный договор об обеспечении безопасности в киберпространстве, идею подготовки которого ранее выдвигала Россия. Об этом прямо заявил представитель американской администрации.

современных информационных и телекоммуникационных технологий для достижения целей устойчивого развития. Наиболее опасной угрозой международному миру и безопасности в информационной сфере является враждебное использование данных технологий. Особое значение имеет военно-политический аспект этой угрозы.

Позиция России и ее партнеров по ОДКБ состоит в том, что существует область политической активности, в которой могут быть в равной мере заинтересованы все члены международного сообщества. Такой областью является расширение международного сотрудничества в сфере информационной безопасности. Главная задача в данной сфере состоит в решении актуальных проблем, касающихся кризисного управления и планирования, информационного обмена, расширения связей между государствами, а также между их отдельными министерствами и ведомствами с целью гармонизации национальных законодательств и выработки общих подходов в борьбе с угрозами международной информационной безопасности.

Распоряжением Президента В. В. Путина в 2013 г. утверждены Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. В соответствии с данным документом цель государственной политики России «заключается в содействии установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности».

Пункт 8 Основ государственной политики Российской Федерации в области международной информационной безопасности гласит:

«Основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии...;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры...;

в) для вмешательства во внутренние дела суверенных государств...;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ».

В качестве основных направлений государственной политики Российской Федерации, связанной с решением задач по повышению эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий, определены продвижение на международной арене российской инициативы, касающейся необходимости разработки и принятия под эгидой Организации Объединенных Наций конвенции о сотрудничестве в сфере противодействия информационной преступности, и развитие международного взаимодействия в данном направлении.

Одним из важных этапов конструктивного практического сотрудничества государств и международных организаций в области МИБ должна стать выработка совместных мер по развитию норм международного права в области ограничения распространения и применения информационного оружия. Необходимо стремиться к установлению международно-правовых барьеров на пути бесконтрольного распространения и применения информационного оружия. Следует добиваться запрещения целенаправленного информационного воздействия на критически важные объекты (государственные структуры), которое способно привести к катастрофическим разрушениям и жертвам среди населения. Необходимо стремиться к запрещению применения в мирное время технологий информационного воздействия с целью подрыва политической, экономической и социальной систем других государств.

В современном международном праве существует ряд понятий, характеризующих воздействие одного государства на другое как агрессию, применение силы или угрозы силой и вмешательство во внутренние дела. Эти понятия могут быть применимы к действиям как вооруженных сил, так и террористических групп и банд, поддерживаемых государством, и т. п. Однако современная трактовка этих понятий обусловлена исторической практикой развязывания и ведения военных действий традиционными средствами вооруженной борьбы. В силу произошедших масштабных и качественных изменений в области информацион-

ных коммуникаций прежние правовые нормы часто не в состоянии описать новые правоотношения в цифровом пространстве.

Специалисты указывают, что для достижения прогресса в решении вопросов, связанных с обеспечением МИБ, пересмотру должны быть подвергнуты основные принципы как международного права в целом, так и отдельных его отраслей (космического, гуманитарного права, международно-правовой ответственности и др.). Представляется актуальным, в частности, конкретизировать и закрепить в соответствующем международном правовом документе роль государственных институтов и гражданского общества в решении проблемы обеспечения безопасности использования Интернета.

Мировое сообщество постепенно приходит к пониманию того, что эффективно противостоять угрозам в ГИП можно только коллективными усилиями. Де-факто в мире началось формирование региональных систем информационной безопасности*.

Сегодня параллельно происходит формирование двух конкурирующих моделей системы МИБ, строящихся на различных основополагающих принципах. В евро-атлантическую систему МИБ входят США и большинство западных государств. Основу евразийской системы составляют государства — члены Шанхайской организации сотрудничества (ШОС). В эту организацию входят пять государств — членов ОДКБ.

Евро-атлантическая система МИБ нацелена в основном на борьбу с киберпреступностью. Ее правовой основой являются нормы и принципы Конвенции Совета Европы о преступности в киберпространстве (Будапешт, 2001 г.). Основное внимание уделяется вопросам безопасности компьютерных систем как инфраструктуры. Предпринимаются попытки подвести под юрисдикцию данной Конвенции и так называемый кибертерроризм, с отрицанием при этом политической мотивированности**.

---

* Под системой международной информационной безопасности понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства.

** Теракты 11 сентября 2001 г. фактически стерли грань между криминальной и военно-политической угрозой международной безопасности.

Основной проблемой является нарушение в отдельных статьях этого документа принципа суверенитета, открывающаяся возможность осуществления на практике вмешательства во внутренние дела других государств посредством несанкционированного проведения оперативно-разыскных действий в их национальном киберпространстве. Военно-политические вопросы МИБ в евроатлантической системе входят в сферу ответственности блока НАТО, последовательно проводящего курс на милитаризацию мирового киберпространства. Еще в 2008 г. в целях обеспечения превосходства в киберпространстве блок НАТО учредил Центр передовых технологий и повышения квалификации в области совместной кибероборонь, который размещен в Таллине (Эстония).

Евразийская система МИБ строится на основе уважения общепризнанных принципов международного права и системного подхода к решению проблемы противодействия криминальным, террористическим и военно-политическим угрозам, которые могут возникать как в гражданской, так и в военной сфере. Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, вступившее в силу в 2011 г., создает прочную основу для налаживания военного сотрудничества в области МИБ.

Основной целью военной политики ОДКБ в ходе формирования региональных систем МИБ должно стать создание механизма осуществления эффективных коллективных действий, направленных на выявление, предупреждение и пресечение возможностей использования современных информационных технологий для осуществления актов агрессии. Основным направлением военного сотрудничества в этой области должно стать выстраивание и последующее совершенствование механизма совместных действий, направленных на противодействие угрозам МИБ. Оно в свою очередь включает такие аспекты военного сотрудничества, как:

— разработка механизма и методологии мониторинга информационного пространства;

— выработка и реализация мер совместного реагирования на угрозы в области МИБ;

— создание механизмов координации обеспечения информационной безопасности в зоне ответственности ОДКБ.

Вопросы совершенствования военного и военно-технического сотрудничества актуальны для всех государств — членов ОДКБ. В целях укрепления сотрудничества необходим эффективный информационно-консультативный обмен. Нормативно-правовой механизм координации должен быть основан на совместной разработке и принятии политико-правовых документов по важнейшим вопросам обеспечения информационной безопасности. Вполне очевидно, что такая работа требует расширения контактов и укрепления связей между органами военного управления, военно-научными и военно-учебными заведениями в вопросах обеспечения информационной безопасности, а также совместной научно-исследовательской деятельности по разработке и применению средств противодействия угрозам МИБ.

С прагматических позиций целесообразными представляются, в частности, формирование и проведение единой технической политики в области разработки средств обеспечения информационной безопасности, построение единой системы сертификации средств ее обеспечения и технологий их создания на пространстве ОДКБ, базирующейся на обязательных требованиях. Такие требования могли бы быть оформлены в виде технических регламентов в области МИБ и установлены отдельным договором или иным международным правовым актом государств — членов ОДКБ.

Современные достижения в области телекоммуникаций и информатизации, а также во многом нерешенные вопросы регулирования возникающих общественных отношений в информационно-телекоммуникационной сфере привели к появлению новых рисков и угроз. В настоящее время на российском и зарубежном телекоммуникационных рынках осуществляются масштабные проекты по модернизации оборудования и самих сетей на базе пакетных технологий. Сети IP при этом становятся важнейшим объектом с точки зрения возникновения реальных угроз информационной безопасности. В подавляющем большинстве этих сетей сегодня используются стандартные, чаще всего уязвимые протоколы, а средства безопасности применяются на прикладном уровне.

Следует подчеркнуть, что телекоммуникационная инфраструктура (ТИ) по отношению к международной информационной безопасности выступает как средство реализации угроз в сфере МИБ и как объект их реализации. В последние годы проблема

обеспечения МИБ при трансграничном обмене информацией с использованием сетей на базе IP существенно обострилась и требует межгосударственной координации. Вместе с тем политическая поддержка решения вопросов, связанных с возможностью использования ТИ как средства и объекта реализации угроз международной информационной безопасности, находится в ведении Первого комитета ООН, а техническая поддержка информационной безопасности ТИ — в ведении Международного союза электросвязи.

Доступность и широкое использование современных информационных и коммуникационных технологий (ИКТ) является фактором, существенно расширяющим возможности для развития информационной преступности, информационного терроризма, осуществления информационных операций деструктивной направленности. С точки зрения безопасности деструктивную роль играет существующая сегодня практика анонимности в электронных коммуникациях. Это нарушает принцип информационного равенства. Возникает ситуация, при которой законопослушный гражданин сообщает о себе достоверную информацию, а преступники пользуются возможностью уйти от регистрации. Абсолютного права на анонимность быть не должно. По сути, справедлив тезис о том, что абсолютная анонимность приводит к абсолютному криминалу, резкому росту возможности возникновения информационных войн. Анонимность — фактор, поощряющий преступника, существенно затрудняющий любое расследование, розыск, нередко делающий невозможным привлечение к ответственности злоумышленника.

Распространение угроз в информационной сфере, масштабы преступных деяний с использованием информационно-телекоммуникационных ресурсов — весомый аргумент в пользу создания защищенной транспортной сети и внедрения государством технологий обязательной идентификации пользователей. Однако практическое решение задачи ограничения анонимности при трансграничном информационном обмене как механизма обеспечения международной информационной безопасности является достаточно сложным в техническом, организационном, политическом и международном юридическом аспектах.

Мировое сообщество постепенно приходит к пониманию того, что эффективно противостоять угрозам в глобальном информационном пространстве можно только общими усилиями.

В представленной на 65-й сессии Генеральной Ассамблеи ООН в 2010 г. записке Генерального секретаря было отражено коллективное мнение экспертов по международной информационной безопасности из 15 государств о потенциальных угрозах и рисках, рекомендациях по их уменьшению, а также о возможных совместных мерах в данной области.

В 2011 г. в Екатеринбурге на Международной встрече высоких представителей, курирующих вопросы безопасности, была представлена концепция Конвенции об обеспечении международной информационной безопасности.

Политическим импульсом для интеграции усилий мирового сообщества по решению проблем обеспечения международной информационной безопасности может стать принятая 27 мая 2011 г. Довильская декларация «Группы восьми»: «Неизменная приверженность свободе и демократии». В тексте этого документа говорится: «Мы абсолютно убеждены, что необходимо стремиться одновременно к достижению свободы и безопасности, соблюдению транспарентности и конфиденциальности в той же неразрывной связи, как между соблюдением прав человека и исполнением им своих обязанностей. Защита этих базовых механизмов и принципов и предоставление соответствующих гарантий должны осуществляться как в Интернете, так и в любой другой сфере нашей жизни».

В 2013 г. по договоренности президентов России и США создана двусторонняя рабочая группа по вопросам угроз в сфере использования информационно-коммуникационных технологий в рамках Российско-Американской Президентской комиссии. По официальным сообщениям, эта группа должна будет встречаться на регулярной основе и проводить «оценку возникающих угроз, разрабатывать, предлагать и координировать конкретные совместные меры по реагированию на такие угрозы, а также по укреплению доверия».

А. И. СМИРНОВ*

СТРАТАГЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВЗГЛЯД ИЗ РОССИИ

Начало XXI в. — один из самых драматичных периодов в истории человечества.

Современная ситуация характеризуется геополитической нестабильностью. К числу наиболее острых проблем относятся межцивилизационное противостояние, международный терроризм, угроза рецессии, рецидивы холодной войны, обострение локальных и региональных конфликтов, природные, социальные и техногенные катастрофы.

В Стратегии национальной безопасности Российской Федерации до 2020 года отмечено: «Возросла уязвимость всех членов международного сообщества перед лицом новых вызовов и угроз».

Появились и угрозы информационной безопасности.

За прошедшие полвека в мире произошла беспрецедентная информационная революция, принципиально изменившая геополитическую ситуацию и приведшая к возникновению новых вызовов и угроз международной безопасности.

Ведущие государства разработали и реализовали концептуальные и доктринальные стратагемы использования потенциала информационно-коммуникационных технологий (ИКТ) в геополитической конкуренции.

На заседании Совета безопасности 5 июля 2013 г., посвященном вопросам совершенствования военной организации Российской Федерации на период до 2020 года, было отмечено: «Идет милитаризация космоса и киберпространства. Широко используются механизмы специальных операций и инструменты так называемой мягкой силы. Всю совокупность этих факторов мы обязаны учитывать в своей практической работе... В современных военных конфликтах растет значение информационных технологий. Так называемые информационные атаки уже применяются для решения задач военно-политического ха-

* А. И. Смирнов, президент Национального института исследований глобальной безопасности.

рактера. Причем, по оценкам специалистов, их так называемая поражающая сила может быть выше даже, чем от обычных видов оружия».

В новой редакции Концепции внешней политики Российской Федерации, утвержденной 12 февраля 2013 г., впервые введено понятие «мягкая сила» — «комплексный инструментарий решения внешнеполитических задач с опорой на возможности гражданского общества, информационно-коммуникационные, гуманитарные и другие альтернативные классической дипломатии методы и технологии».

В Концепции также обращено внимание на риски, связанные с деструктивным и противоправным использованием «мягкой силы» в целях оказания политического давления на государства, вмешательства в их внутренние дела, манипулирования общественным мнением и сознанием, и обозначены меры, направленные на обеспечение национальной и международной информационной безопасности, предотвращение угроз политической, экономической и общественной безопасности Российской Федерации, возникающих в информационном пространстве, борьбу с терроризмом и иными криминальными угрозами в сфере применения информационно-коммуникационных технологий, противодействие их использованию в военно-политических целях, противоречащих международному праву, включая действия, направленные на вмешательство во внутренние дела государств, а также представляющие угрозу международному миру, безопасности и стабильности.

Учитывая особую важность этой проблемы, Россия будет добиваться выработки под эгидой ООН единых правил в сфере обеспечения международной информационной безопасности.

Стратагемы непрямых действий и контролируемой нестабильности («управляемого хаоса») являются наиболее эффективными средствами ведения геополитической борьбы на международной арене, которые используются в целях ослабления реальных и потенциальных противников с помощью новейших информационно-коммуникационных технологий.

В самом начале XXI в. влияние интернет-среды было существенно ниже влияния печатных СМИ и телевидения. Однако такие события, как «арабская весна», беспорядки 2011 г. в

Великобритании, акция «Захвати Уолл-стрит» в США и др., продемонстрировали потенциал веб-сервисов нового поколения как инструмента влияния на события в мире.

В Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, утвержденных Президентом Российской Федерации 24 июля 2013 г., к числу основных приоритетов отнесено участие России в формировании механизмов международного сотрудничества в области противодействия угрозам использования ИКТ в террористических и экстремистских целях, в том числе для вмешательства во внутренние дела суверенных государств.

В целом Основы закрепляют стремление Российской Федерации к масштабному сотрудничеству в деле укрепления мер доверия в сфере применения ИКТ и повышения эффективности переговорного процесса в области формирования системы международной информационной безопасности.

К основным угрозам в области международной информационной безопасности отнесено использование ИКТ:

«а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ».

По данным ЦРУ, 120 стран разрабатывают информационное оружие — оружие шестого поколения для сетецентрических войн (СЦВ). Для сравнения: оружие массового уничтожения создают 30 стран. Уже ведутся и латентные, и явные информационные войны, в том числе с использованием боевых кибервирусов.

Основными задачами в таких войнах являются:

— дезорганизация функционирования информационных систем критически важных военных, административных, промышленных объектов противника;

— информационно-психологическое воздействие на военно-политическое руководство, войска и население (паника, недоверие к руководству, страх и т. д.).

В США создана система ведения информационных войн технической и психологической направленности.

Объединенный центр передового опыта по кибероборону НАТО разработал первое в мире руководство о применении положений действующего международного права к кибервойнам.

Разработано 95 правил, в соответствии с которыми ответить на атаку государство может, либо привлекая агрессора к ответственности, либо «пропорциональными контрмерами»; если считать атаку вооруженным нападением, правомерна самооборона, в том числе с использованием традиционного оружия; кибератаки по силе воздействия следует приравнять к применению химического, биологического и радиологического оружия; вооруженным нападением не могут быть признаны кибершпионаж, киберкражи и атаки на сайты (кроме ущерба в государственном масштабе); государство-агрессор должно нести ответственность, даже если оно атакует при помощи посредников из других стран.

12 сентября 2011 г. постоянные представители России, Китая, Таджикистана и Узбекистана при ООН направили совместное письмо в адрес Генерального секретаря ООН с просьбой распространить проект резолюции «Правила поведения в области обеспечения международной информационной безопасности» в качестве официального документа 66-й сессии Генеральной Ассамблеи ООН.

Наряду с Правилами — «мягким» вариантом — разработана юридически обязывающая концепция обеспечения международной информационной безопасности для обсуждения в ООН.

В ходе встреч и консультаций Великобритания и США выступали против нее, так как, по их мнению, это приведет к появлению цензуры и ужесточению государственного контроля над Интернетом.

Россия разработала универсальную конвенцию о сотрудничестве в сфере противодействия информационной преступности, идея которой отражена, в частности, в декларации 12-го Конгресса ООН по предупреждению преступности и уголовному правосудию (Сальвадор, Бразилия, апрель 2010 г.).

При разработке конвенции учитывались, в частности, положения: Конвенции ООН против коррупции, Конвенции ООН против транснациональной организованной преступности, Конвенции Совета Европы о преступности в киберпространстве, а также ряда глобальных антитеррористических конвенций.

17 июня 2013 г. в ходе саммита «Большой восьмерки» в Лох-Эрн (Северная Ирландия) президенты Российской Федерации и США приняли заявление, в котором выразили понимание наличия угроз военно-политического, криминального и террористического характера в сфере использования ИКТ, а также объявили о заключении договоренностей, направленных на укрепление доверия между Россией и США на трех уровнях:

— между представителями системы национальной безопасности;

— между силовыми ведомствами по линии национальных центров по уменьшению ядерной опасности для уведомлений об атаках на объекты критической информационной инфраструктуры;

— между экспертными группами в целях предотвращения компьютерных инцидентов и мониторинга вредоносной активности в сетях.

2–4 июля 2013 г. во Владивостоке проводилась 4-я Международная встреча высоких представителей, курирующих вопросы безопасности. В мероприятии приняли участие делегации

60 стран (представители советов безопасности, аппаратов президентов и глав правительств, министерств и ведомств, участвующих в выработке политики в области национальной безопасности, а также руководство ООН).

По инициативе КНР было продолжено обсуждение вопросов обеспечения международной информационной безопасности. Участники отметили, что совместная деятельность постепенно закладывает основы сотрудничества, однако для практического взаимодействия предстоит выработать единые критерии под эгидой ООН.

Была также подчеркнута необходимость формирования нового международного механизма безопасного развития и использования конвергентных технологий как альтернативного ответа на новые вызовы и угрозы глобального характера.

6 ноября 2013 г. в ходе заседания Первого комитета на 68-й сессии Генеральной Ассамблеи ООН консенсусом принята резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

В 2013 г. достигнуто рекордное число соавторов резолюции — более 40 стран.

Резолюция подтверждает, что ООН как единственная универсальная организация, ответственная за поддержание международного мира и безопасности, должна и дальше играть ключевую роль в обсуждении вопросов международной информационной безопасности.

Наряду с военно-политическими, криминальными и террористическими угрозами в данной сфере особую обеспокоенность вызывают попытки установления контроля над глобальным информационным пространством через ИКТ.

В преамбуле резолюции содержится тезис о важности уважения прав и свобод человека в сфере использования ИКТ при условии невмешательства во внутренние дела государства и уважения национального суверенитета.

Резолюция идет в русле доклада группы правительственных экспертов ООН по МИБ 2013 г., сфокусированного на необходимости предотвращения конфликтов в информационном пространстве в противовес подходам, предполагающим их легитимизацию. Новая ГПЭ по МИБ в 2014 г. увеличена с 15 до 20 человек

Расширен ее исследовательский мандат по изучению использования ИКТ в ходе конфликтов и международного права.

26 ноября 2013 г. Комитет ООН по социальным и гуманитарным вопросам и вопросам культуры (Третий комитет) принял резолюцию, подготовленную Германией и Бразилией, о недопустимости электронного шпионажа («Право на неприкосновенность личной жизни в цифровой век»).

В силу того что резолюции ООН носят рекомендательный характер, необходимо разрабатывать и принимать юридически обязывающие документы ООН по проблематике международной информационной безопасности. Для этого следует использовать экспертный потенциал России в сфере обеспечения международной информационной безопасности.

Р. М. ЮСУПОВ, В. М. ШИШКИН*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КИБЕРБЕЗОПАСНОСТЬ: СЕМАНТИЧЕСКИЙ КОНФЛИКТ ИЛИ РАЗУМНОЕ СОСУЩЕСТВОВАНИЕ

Следует признать, что после того, как в 2000 г. был утвержден основной концептуальный документ, призванный определять стратегию государства в области обеспечения информационной безопасности (ИБ), — Доктрина информационной безопасности Российской Федерации (далее — Доктрина ИБ), прошло значительное для информационно-коммуникационных технологий (ИКТ) при существующих темпах их развития время. За прошедшие годы существенно расширились или возникли новые сферы применения ИКТ. Не будет преувеличением утверждать, что мы живем в информационном обществе, поскольку в настоящее время ИКТ используются практически во всех сферах жизнедеятельности на индивидуальном, общественном, производственном и государственном уровнях. Более того, на всех уровнях возникла критическая зависимость от них, что, естественно, внесло изменения в проблематику, связанную с информационной безопасностью.

К сожалению, концептуально невнятно сформулированный проект Стратегии кибербезопасности стал информационным поводом для многочисленных и порою странных сообщений в СМИ. Можно только приветствовать разработку документов, актуализирующих Доктрину, особенно ее публичные аспекты. Однако отличительной особенностью готовящегося документа стала фактически тотальная замена понятийного аппарата, принятого в аналогичных по назначению действующих государственных регламентах, а одним из аргументов для данной инициативы — принятие в последние годы в ряде западных стран различных стратегий кибербезопасности.

* Р. М. Юсупов, директор Санкт-Петербургского института информатики и автоматизации Российской академии наук, В. М. Шишкин, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук.

Сфера информационной безопасности в последние годы стала ареной активного словотворчества, не всегда оправданного, поскольку введение новых терминов и понятий совсем не обязательно приводит к уточнению сущности представляемых объектов и явлений. Происходит это на фоне настойчивого внедрения калькированной англоязычной терминологии, основанной на иной лингвистической и понятийной традиции. Таким образом, существует опасность неадекватного словоупотребления, навязывания ложных смыслов в столь ответственной сфере деятельности. Мы исходим из того, что оправданием для введения новых терминов или их интерпретаций является обозначение принципиально новых явлений или объектов, и нет оснований полагать, что понятийная основа информационной безопасности должна выходить за пределы достаточно богатой отечественной научно-технической традиции.

Развитие предметной области, которая в отечественной практике получила собирательное наименование информационной безопасности, имеет не слишком долгую историю. Однако за короткое время произошли столь масштабные и беспрецедентные изменения, что узкоспециальные вопросы защиты информации — предмет интереса преимущественно государственных органов и ограниченного количества технических специалистов — превратились даже не в междисциплинарные, а в глобальные проблемы информационной безопасности. Они стали обращать на себя внимание широкого круга специалистов гуманитарной сферы. Активно разрабатывался юридический аспект данной проблемы, сформировавшийся в целое направление юридической науки — информационное право. Даже технические аспекты нередко актуализировались в правовой сфере (например, до сих пор не получившая удовлетворительного разрешения проблема безопасности персональных данных).

В то же время информационные системы все в большей степени функционируют на основе взаимодействия человека и машины, но уже не в традиционном смысле, предполагающем участие в процессе функционирования профессионального оператора. Человек из средства поддержки процесса во многих случаях становится целью функционирования, и проявления человеческого фактора становятся поэтому все более разнообразными. Операторами выступают как рядовые потребители информационных услуг, так и квалифицированные злоумышленники.

Поэтому закономерно, что Доктрина в значительной мере посвящена гуманитарным аспектам. Очевидно, что мы имеем дело с частным проявлением более общего, фундаментального и закономерного для современной цивилизации противоречия между человеком и созданной им техносферой. Однако, в отличие от техносферных рисков, угрожающих физическому здоровью, угрозы, имеющие информационную природу, часто воздействуют на сущность человеческой личности — духовную и психологическую сферы, что обостряет указанное противоречие.

При этом технические и технологические аспекты обеспечения информационной безопасности, как всякая инженерная деятельность, традиционно ориентированы прежде всего на защиту информационных активов, процессов, коммуникаций. Именно данное направление, стимулируемое экономическими факторами, стало активно развиваться. Поэтому, интеграционный период начала 2000-х гг. сменился дифференциацией: безопасность собственно ИКТ, или, иными словами, кибербезопасность, становясь предметно многообразной, обособляется от множества нетехнологических проблем.

Приблизительно в это же время США, первыми среди западных стран и за несколько лет до них, принимают The National Strategy to Secure Cyberspace, подписанную Президентом Дж. Бушем-младшим в феврале 2003 г., в которой среди прочего довольно четко и однозначно (для англоязычного контекста) определяются понятие cyberspace: "...an interdependent network of information technology infrastructures called cyberspace", назначение данного документа: "The National Strategy to Secure Cyberspace provides a framework for protecting this infrastructure that is essential to our economy, security, and way of life", и многократно без дополнительных определений используются такие, видимо, общеупотребительные термины, как cybersecurity, cybersystem и т. п. Примечательно, что при этом в электронном словаре Министерства обороны США содержится термин «информационная безопасность», но термин «кибербезопасность» отсутствует. Неопределенность понятий заставляет задаться вопросом: о чем, в сущности, идет речь? Термины, органичные для английского текста, цитируются в оригинале, поскольку в калькированном виде они не будут являться переводом на русский язык, а в переводе с использованием давно привычных русских терминов потеряют точность и специфику первоисточника.

Следует отметить, что Российская Федерация, приняв за три года до этого Доктрину информационной безопасности, стала первым государством, где на самом высоком уровне был утвержден столь масштабный интегрирующий документ, определяющий политику обеспечения информационной безопасности во всех ее аспектах. А на международном уровне именно по инициативе России еще в 1993 г. при участии СПИИРАН был разработан и подготовлен для рассмотрения в ООН проект Конвенции о запрещении военного или любого иного враждебного использования методов и средств воздействия на инфосферу (Convention on the prohibition on military or any other hostile use of methods and means influencing the infosphere).

В середине 2000-х гг., возможно под влиянием названной The National Strategy, кибертерминология стала целенаправленно внедряться в некоторые научные тексты. Основной причиной послужила указанная выше потребность дифференцировать технические аспекты в широком контексте информационной безопасности. Так, например, в 2006 г. вышел сборник трудов Института системного анализа РАН под названием «Проблемы кибербезопасности информационного общества» и на следующий год в продолжение тенденции — сборник, включающий раздел «Управление киберрисками и кибербезопасностью». Авторам рекомендовалось при описании технологических аспектов использовать вместо прилагательного «информационные» приставку «кибер-». Соответственно, возникли такие понятия, как «киберсистемы», «кибертехнологии», «киберпроцессы», «киберобъекты», «киберкомпоненты», «киберриски» и т. п. В начальных школах России вскоре появится новый предмет под названием «киберобразование». Об этом сообщает «Русская служба новостей» со ссылкой на заявление главы группы разработчиков Стратегии кибербезопасности.

Кафедра защиты информации МИФИ в 2012 г. переименована в кафедру кибербезопасности. В программе подготовки термины «кибербезопасность» и «информационная безопасность» перемежаются между собой и могут быть без заметной потери смысла заменены друг другом. В списке компетенций указана «способность осуществлять подбор, изучение и обобщение... нормативных и методических материалов по вопросам обеспечения кибербезопасности», которых, однако, пока не существует в Российской Федерации.

Можно иронизировать по поводу этой словесной «кибератаки», но вместе с тем необходимо попытаться понять гносеологические причины ее неприятия. Следует напомнить, что корневой префикс cyber- в англоязычном, а точнее — американском контексте, откуда происходят соответствующие термины, и кибер- в русском имеют пересекающиеся, но не совпадающие смыслы. Источником является созданное Н. Винером научно-техническое направление — кибернетика, история дальнейшего развития которого в нашей стране и за рубежом была не вполне одинакова.

В СССР кибернетика стала активно развиваться как особая отрасль науки по инициативе академика А. И. Берга в конце 50-х гг. XX в. прежде всего как направление теоретической мысли, затем — в разнообразных технических приложениях, а вскоре ее методы стали успешно применяться и в других отраслях науки (возникли, например, экономическая кибернетика, медицинская кибернетика и т. д.). При этом создание и успешное в то время развитие отечественных средств вычислительной техники, а позднее и вычислительных сетей началось значительно раньше и происходило независимо от кибернетических концепций.

В дальнейшем, уже в условиях массового распространения вычислительной техники и использования информационных технологий, в том числе сетевых, возникло новое научное направление под названием информатика. Соотношение кибернетики и информатики, интеграционные тенденции в данной области — отдельная интересная и дискуссионная тема. Трудно сказать, куда приведет этот процесс. Пока они представляют собой пересекающиеся, но все же относительно самостоятельные отрасли со своей методологией и традициями. Прилагательные «кибернетический» и «информационный» семантически жестко не связаны и тем более не воспринимаются как синонимы.

Совершенно иная ситуация сложилась в США. Кибернетизация научно-технического сознания и компьютеризация происходили одновременно, и поскольку информация является одним из ключевых понятий кибернетики (cybernetics), а компьютер как устройство обработки информации стал основным техническим средством воплощения кибернетических воззрений, их неотъемлемой частью, все, что связано с использованием компьютерных технологий, ассоциировалось с кибернетическими системами. Кроме того, в силу морфологических особенностей английского

языка короткое, удобное слово «cyber» легко и органично вошло в различные словоформы и в широкий обиход.

Термин «информатика» (informatics) в этой языковой среде не вполне понятен, требует пространных пояснений и не эквивалентен по смыслу привычному «computer science». Следует отметить еще один любопытный факт. На рубеже веков, когда в рунете появились первые фразеологические онлайн-переводчики текстов, один из них при переводе на английский уже привычного и распространенного тогда понятия «информационная безопасность» давал неорганичное для английского языка словосочетание «information safety», а при обратном переводе кальки с русского — «information security» — неожиданное и специфическое понятие, используемое в финансовой сфере деятельности.

Удивляет современная не публицистическая, а научная или наукообразная апологетика внедрения кибертерминологии. Создается впечатление, что некоторые авторы рациональными средствами пытаются решить иррациональную задачу с априори заданным результатом. При этом не возникает конструктивных предложений, зато появляются поводы для неконструктивных дискуссий. Трудно, например, согласиться с мнением, что понятие «информационная безопасность» недостаточно широко, и с предложением в более общем его понимании использовать термин «кибербезопасность». Это противоречит не только более или менее разумным мотивам его использования, но и англоязычным первоисточникам. Один из авторов считает, что «информационное пространство является частью кибернетического», а «синонимичным кибернетическому пространству является... виртуальное пространство». Эти утверждения можно не комментировать, достаточно сравнить с приведенным выше четким конструктивным определением из оригинала — The National Strategy to Secure Cyberspace. И совсем непонятным с точки зрения логики является то, что автор, признавая неоднозначность термина «кибербезопасность» (в том числе cybersecurity в англоязычных источниках), возможность толкования его в узком, широком и других смыслах, предлагает использовать это неоднозначное понятие вместо многозначного, но определенного — «информационная безопасность», внося тем самым еще большую неопределенность и неоднозначность в понятийный аппарат.

В сборнике статей авторитетных авторов, среди которых Посол по особым поручениям МИДа России А. В. Крутских (статья

«О проблеме обеспечения международной информационной безопасности»), имеется раздел «Проблемы информационной безопасности», в который входят статьи заместителя директора Института проблем информационной безопасности МГУ А. А. Стрельцова «Основные направления совершенствования правового обеспечения информационной безопасности Российской Федерации» и ректора МГУ В. А. Садовничего «Как защитить человека от инфогенных рисков?». Авторы, за исключением ректора МГУ, обходятся без кибертерминов, но и у них они используются в большей степени для улучшения стиля, с тем чтобы исключить частые повторения одних и тех же слов, и контекстуально воспринимаются как синонимы традиционных понятий.

Что касается проекта Стратегии кибербезопасности Российской Федерации, то, по мнению активно пишущего на темы информационной безопасности интернет-писателя и блоггера А. Лукацкого, «то, что получилось, выглядит вполне достойно... и очень похоже на аналогичные стратегии иных государств». Видимо, последнее обстоятельство является достаточным показателем качества документа. Так может быть, дело именно в западном выборе инициаторов проекта Стратегии? Но как их инициатива будет согласовываться, хотя бы формально, например, с планами Межпарламентской Ассамблеи СНГ разработать к 2014 г. проект Стратегии обеспечения информационной безопасности для государств — участников СНГ? И как соотнести «кибератаки» из проекта Стратегии и «компьютерные атаки», о которых говорится в Указе Президента Российской Федерации от 15 января 2013 г. № 31с?

Что касается Европы, то одной из первых национальную стратегию в данной сфере приняла Эстония. Несколько позже, в 2009 г., Cyber Security Strategy of the United Kingdom появилась в Великобритании. Основной объем европейских стратегий пришелся на 2011 г. Наиболее значимые и самостоятельные из них — Cyber-Sicherheitsstrategie für Deutschland в Германии и Défense et sécurité des systèmes d'information. Stratégie de la France во Франции. Обращает на себя внимание то, что Франция, демонстрируя традиционное стремление к культурной независимости, предлагает отличное от остальных документов название — «Защита и безопасность информационных систем», исключающее какую-либо неясность касательно содержания и конструктивности намерений. Кроме того, в том же 2011 г. в развитие первых версий стратегий в США и Великобритании вышли дополняющие и

развивающие их International Strategy for Cyberspace "Prosperity, Security, and Openness in a Networked World" и "The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world", а также "Cybersecurity Strategy of the European Union".

Европейские документы различны по глубине и детализации, но вместе с тем необходимо признать, что они производят благоприятное впечатление благодаря целостности содержания, конкретности и ясному пониманию целей и задач по защите национальных интересов. В этом смысле они действительно могут быть примером для подражания. Важно, что, благодаря своей внятности, акценту на технологических аспектах сетевого взаимодействия, они не оставляют места для бессмысленных дискуссий и являются прямым руководством к действию.

В то время как мы обсуждаем Стратегию кибербезопасности, почти незаметно проходят процессы, на которые никоим образом не повлияет ее принятие или непринятие. Данные процессы входят в прямое противоречие с устаревшей, как полагают некоторые, Доктриной информационной безопасности, явно угрожая национальным интересам России в информационной сфере. Согласно неофициальной, но правдоподобной информации иностранные собственники активно скупают крупные интернет-порталы в разных городах России, в результате чего аудитория проамериканских сайтов станет сравнима с аудиторией федеральных каналов (более 12 млн человек в месяц). Напомним, что объем информации, целенаправленно передаваемой от одной страны к другой, является мерой информационной агрессивности. При этом неважно, какой характер имеет передаваемая информация.

Как показывают обсуждения, формальные терминологические дискуссии неконструктивны. Актуальными являются не дефиниции понятий — в целом они, насколько возможно, давно определены, а осмысление новой и перспективной реальности, выработка адекватных ей практических мер обеспечения безопасности. Значимыми являются в первую очередь новые и многочисленные проблемы, связанные с обеспечением безопасности сетевого информационного взаимодействия, функционированием автоматизированных систем управления критически важными объектами и процессами.

Несомненно, назрела необходимость развития и актуализации системы документов, понятийного аппарата, отражающих новые

реалии и определяющих политику государства в сфере информационной безопасности, общественные интересы в данной области. Однако при этом речь должна идти о системном подходе и преемственности без стремления к излишней альтернативности.

Более важной представляется разработка не декларативных стратегических документов, а программ конкретных действий, направленных на противодействие наиболее актуальным угрозам. Необходимо разрабатывать программы сетевого взаимодействия, с указанием сроков, источников выполнения и финансирования, предполагающих ответственность за результаты. Необходимо развитие нового направления обеспечения информационной безопасности, включающего выявление угроз, организацию сбора информации, ее хранение и обеспечение доступа к ней. В данной области имеет место отставание и, как следствие, зависимость от внешних ресурсов. Кроме того, нужны программы научно-методологического обеспечения решения проблем информационной безопасности.

Однако по большинству актуальных вопросов информационной безопасности — технологических, организационных, законотворческих — независимо от наличия каких-либо доктринальных документов и терминологических дискуссий усилиями государственной власти, научного и технического сообщества работа так или иначе ведется и будет вестись, хотя бы в силу профессиональных потребностей и обязанностей. Совершенно беззащитными в современных условиях оказались рядовые граждане — участники информационного взаимодействия, пользователи услуг в сфере ИТК. Поэтому на первый план должна быть выдвинута задача ликвидации безграмотности в области информационной безопасности во всех ее аспектах, включая и защиту от киберопасности.

Никто не может запретить употребление любых терминов, в том числе профессиональных англицизмов или журналистских клише, но в сфере государственной политики произвол недопустим. Использование чужого понятийного аппарата, каким бы универсальным и интернациональным он ни казался, замена не столько терминов, сколько смыслов, по сути, есть акт разоружения в информационном противоборстве. Можно отказаться от своих научных традиций, но тогда придется отказаться от независимости, не только научно-технической, но и со временем политической.

ДЕКЛАРАЦИЯ

международной научно-практической конференции «Законодательство государств — членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации»

Участники международной научно-практической конференции констатируют, что в условиях глобализации информационного пространства информация и информационные технологии играют важнейшую роль в формировании экономического и политического могущества государств, обеспечении их суверенитета и независимости и их роль будет только возрастать. В связи с этим нарастает борьба за достижение информационного превосходства, и ее наиболее острой формой становится информационная война, к практике которой, уже не стесняясь, прибегают некоторые страны, первыми переступившие порог информационной эпохи. Во многих государствах создаются специальные командования, подразделения в национальных органах безопасности и обеспечения правопорядка, ориентированные на защиту информационного пространства.

Современные телекоммуникационные технологии, создаваемые для развития общения между отдельными людьми и народами, призванные служить локомотивом инновационного развития, гарантом экономической стабильности и конкурентоспособности, одновременно используются деструктивными силами для негативного воздействия на информационно-психологическую среду государств, распространения идеологии экстремизма и терроризма, дискредитации демократических ценностей и совершения иных преступлений.

Информационная сфера, не имеющая границ, с присущими только ей внутренними законами и правилами поведения является чувствительным фактором жизнедеятельности общества, недооценка которого может привести к политическим и экономическим кризисам и, как следствие, к социальной напряженности, протестным проявлениям и дестабилизации обстановки.

Поэтому вопросы обеспечения международной информационной безопасности являются сегодня актуальными. От эффективности их решения зависит вся система национальной и

коллективной безопасности. В этой ситуации все государства — члены Организации Договора о коллективной безопасности (ОДКБ) стали соавторами и поддержали резолюцию Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», предпринимают активные действия по развитию международного сотрудничества в этой сфере и законодательного обеспечения собственной информационной безопасности.

В основе формирования системы информационной безопасности в интересах каждого из государств — членов ОДКБ и Организации в целом лежит законодательное и нормативно-правовое обеспечение. Первыми важными шагами стало утверждение в 2008 году Советом коллективной безопасности ОДКБ (СКБ ОДКБ) Программы совместных действий по формированию системы информационной безопасности государств — членов Организации Договора о коллективной безопасности и в 2010 году Положения о сотрудничестве государств — членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности. Достижение практических целей сотрудничества в этой сфере должны обеспечить рассчитанные на длительную перспективу Перечень мероприятий, направленных на формирование системы обеспечения информационной безопасности в интересах государств — членов Организации Договора о коллективной безопасности, и План первоочередных мероприятий по формированию основ скоординированной информационной политики в интересах государств — членов Организации Договора о коллективной безопасности, принятые СКБ ОДКБ в 2011 году.

Принятие государствами — членами ОДКБ обязательств в сфере информационной безопасности в формате ОДКБ и других международных форматах требует ускоренного параллельного развития теории и практики информационной безопасности, основой которых должно стать формирование национальной законодательной базы, призванной обеспечить правовую основу практического сотрудничества в области информационной безопасности.

Согласование законодательной политики, скоординированные меры по сближению и унификации национального законодательства государств — членов ОДКБ в информационной сфере, обеспечение соответствия национального законодательства меж-

дународным договорам будут отвечать интересам государств — членов ОДКБ в защите конституционного строя, обеспечении суверенитета, территориальной целостности, политической, экономической и социальной стабильности.

В первую очередь это касается создания механизмов обеспечения устойчивого функционирования и безопасности использования глобальной информационной инфраструктуры и ее национальных сегментов, развития и совершенствования сотрудничества по противодействию преступлениям в сфере информационных технологий.

Бурные процессы развития социальных сетей и их все более заметная роль в обеспечении национальных интересов при проведении информационной политики, в первую очередь в молодежной среде, требуют ускоренной правовой регламентации их использования.

Оставаясь верными принципам и нормам международного права, положениям международных договоров и соглашений, подписанных главами государств — членов ОДКБ в целях укрепления сотрудничества и совершенствования взаимодействия по формированию безопасного информационного пространства государств — членов ОДКБ, участники международной научно-практической конференции считают необходимым содействовать:

— ускорению процесса гармонизации и возможной унификации национального законодательства, направленного на формирование системы коллективной безопасности государств — членов ОДКБ;

— формированию модели обеспечения информационной безопасности, позволяющей учесть новый вид потенциальных угроз, возникающих в условиях открытой экономики;

— разработке, принятию законов и нормативных правовых актов, направленных на обеспечение информационной безопасности, сосредоточив усилия в области информационной безопасности в первую очередь на разработке соответствующих рекомендаций и модельных законов, направленных на защиту критически важной информационной инфраструктуры;

— осуществлению мер скоординированной информационной политики, направленных на выработку общего понимания проблем, целей, средств и способов защиты государств — членов ОДКБ от неблагоприятного информационного воздействия,

активизации усилий по согласованию базовых принципов государств — членов ОДКБ в области скоординированной информационной политики и закреплению их в законодательных актах на национальном уровне;

— осуществлению согласованной политики государств — членов ОДКБ в подготовке и повышении квалификации кадров, работающих в сфере информационной безопасности;

— развитию связей парламентов государств — членов ОДКБ с профильными научными и исследовательскими организациями, средствами массовой информации, молодежными и общественными организациями в интересах укрепления системы коллективной безопасности государств — членов ОДКБ.

СОДЕРЖАНИЕ

Научное издание

Законодательство государств — членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации

Материалы международной
научно-практической конференции

Под редакцией П. П. Рябухина,
В. В. Бондуровского, Г. И. Перекопского

Редакторы *Н. В. Куликова, Д. Н. Ставицкая*

Изготовление оригинал-макета *Т. И. Ягудина*

Подписано в печать 07.04.2014. Формат 60x84 1/16. Бумага офсетная. Гарнитура Ньютон. Печать офсетная. Усл. печ. л. 5,13. Уч.-изд. л. 4,72. Тираж 250.
Заказ 0919-о-14.

Адрес Секретариата Совета МПА СНГ: 191015, С.-Петербург, ул. Шпалерная, д. 47.
Телефоны редакции: (812) 326-69-24, 326-68-01.
web-страница: www.iacis.ru; e-mail: SYV@iacis.ru

Отпечатано с оригинал-макета в типографии «Капли дождя»: 190005, С.-Петербург, Измайловский пр., д. 16/30, лит. Б. Тел./факс: (812) 325-08-48.