Михаил КУЧЕРЯВЫЙ

ОСНОВНЫЕ НАПРАВЛЕНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ РФ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье рассматриваются основные направления государственной политики РФ, связанные с решением задач по повышению эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и телекоммуникационных технологий.

In the article main directions of the state policy of the Russian Federation, connected with solution of tasks on increasing the efficiency of international cooperation in the field of crime counteraction in the sphere of use of information and telecommunication technologies are considered.

Ключевые слова:

государственная политика, международная информационная безопасность, глобальное информационное пространство, угрозы международной информационной безопасности, информационные и телекоммуникационные технологии, информационная преступность; state policy, international information security, global information space, threats to international information security, information and telecommunication technologies, information crime.

Анализ роли и места Российской Федерации в глобальном информационном пространстве позволяет сделать выводы о наличии объективных предпосылок для активного включения России в мировой общецивилизационный процесс в качестве его ведущего субъекта с целью обеспечения ей благоприятных условий для решения задач собственной модернизации.

В этих условиях принципиальное значение приобретают вопросы реализации государственной политики РФ, связанной с решением задачи по формированию системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях.

Под международной информационной безопасностью автор понимает такое 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[1].

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

Система международной информационной безопасности призвана оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве. Сотрудничество в области формирования системы международной информационной безопасности отвечает национальным интересам РФ и способствует укреплению ее национальной безопасности[2].

КУЧЕРЯВЫЙ Михаил Михайлович – к.полит.н., доцент; руководитель ФСТЭК России по Северо-Западному федеральному округу szfo@fstec.ru

[1] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. // Официальный сайт Совета безопасности РФ; http://www.scrf.gov.ru/documents/6/114.html (дата обращения 31.10.2013).

[2] Там же.

Потенциал глобального информационного пространства активно используется для реализации многих важных функций государственного управления, что, с одной стороны, создает условия для повышения качества жизни граждан, повышения эффективности выполнения функций государственного управления, а с другой – может быть использовано для нарушения устойчивости государственного управления, дезорганизации этого процесса. Большинство критически важных инфраструктурных систем, например, включены в это пространство, что позволяет инициировать техногенные, энергетические и финансовые катастрофы, создать хаос и панику. В то же время система оценок использования и развития глобального информационного пространства в настоящее время отсутствует.

В процессе цивилизационного развития не перестает быть определяющим фактором геополитическая конкуренция. В информационной сфере на ее характере сильно отражаются такие исторически сложившееся обстоятельства, как доминирование США в области информационных и телекоммуникационных технологий. Создав Интернет – глобальную информационно-коммуникационную сеть – и сумев убедить остальной мир в его преимуществах, американская сторона господствует не только в управлении доменными именами. США, как известно, голосовали в ООН против решений о предотвращении гонки вооружений и о 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 американская администрация и в отношении глобального информационного пространства. Администрация США не видит необходимости заключать международный договор об обеспечении безопасности в киберпространстве, идею подготовки которого ранее выдвигала Россия. Об этом прямо заявил представитель американской администрации[1].

Вместе с тем материалы различных проводившихся исследований и имеющиеся публикации свидетельствуют о постоянно растущем числе политически мотивированных атак с применением информационно-телекоммуникационной инфраструктуры[2]. Прошедшие несколько лет продемонстрировали рост информационных угроз, ориентированных на конкретные государства. Такие угрозы могут использоваться для различных целей, начиная с кибершпионажа и заканчивая выведением из строя каких-либо стратегически важных объектов инфраструктуры. «Кибердары» по ядерным объектам Ирана посредством вируса *Stuxnet* вывели из строя центрифуги, а эпидемия компьютерных вирусов, потрясшая планету в последующие годы, отразилась на странах – поставщиках углеводородов[3].

В США разработана и действует система руководящих документов, регламентирующих порядок подготовки и проведения «информационных операций». К основным задачам таких операций относится нарушение функционирования ключевых и критически важных систем потенциального противника посредством использования современных информационных и телекоммуникационных технологий. В мае 2011 г. в США была обнародована Международная стратегия для киберпространства, согласно которой американцы оставляют за собой право использовать все необходимые, в т.ч. и военные, средства для защиты своих национальных интересов в киберпространстве.

В этой связи становится очевидным, что в настоящее время возникла и набирает силу новая военно-политическая угроза всеобщему миру и международной стабильности. Противодействие ей требует, в частности, активизации военной политики в рамках Организации Договора о коллективной безопасности (ОДКБ) – региональной международной организации военно-политического сотрудничества, преследующей цели укрепления

[1] Международная информационная безопасность: проблемы и решения / под общ. ред. С.А. Комова. – М., 2011, кн. 1, с. 85.

[2] Информационная безопасность как составляющая национальной безопасности государства. Материалы международной научно-практической конференции. Минск, 11–13 июля 2013 г. В 3 т. / Институт национальной безопасности Республики Беларусь; гл.ред. С.Н. Князев. – Минск, 2013.

[3] Вус М.А., Шакин Д.Н., Кучерявый М.М. Методологические проблемы обеспечения информационной безопасности критически важных объектов топливно-энергетического комплекса Российской Федерации // Информатизация и связь, 2012, № 7, с. 42–47.

мира, национальной, международной и региональной безопасности и стабильности. Необходимы скоординированные совместные действия государств – членов ОДКБ по формированию действенной системы коллективной безопасности в информационной сфере.

Возрастание угроз военно-политического, террористического и криминального характера, все сильнее проявляющихся в информационной сфере, является существенным препятствием для полномасштабного использования потенциала современных информационных и телекоммуникационных технологий в достижении устойчивого развития мирового сообщества. Наиболее опасной угрозой международному миру и безопасности в информационной сфере является враждебное использование таких технологий, особенности которого следует, в первую очередь, рассматривать сквозь призму военно-политических аспектов этой угрозы.

Политика России и ее союзников исходит из того, что существует область политической активности, в которой могут быть в равной мере заинтересованы все члены международного сообщества. Такой областью является расширение международного сотрудничества и кооперации в сфере информационной безопасности. Главной задачей в данной сфере видится решение актуальных проблем, касающихся кризисного управления и планирования, информационных обменов, расширения связей между государствами, а также между их отдельными министерствами и ведомствами с целью гармонизации национальных законодательств и выработки общих усилий в борьбе с угрозами международной информационной безопасности.

В качестве основных направлений государственной политики РФ, связанной с решением задач по повышению эффективности международного сотрудничества в противодействии преступности в сфере использования информационных и телекоммуникационных технологий, позиционируются продвижение на международной арене инициативы, связанной с необходимостью разработки и принятия под эгидой ООН Конвенции о сотрудничестве в сфере противодействия информационной преступности, и развитие международного сотрудничества в этом направлении.

Одним из важных этапов конструктивного практического сотрудничества государств и международных организаций в области международной информационной безопасности 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. Нужно стремиться к запрещению применения в мирное время технологий информационного воздействия с целью подрыва политической, экономической и социальной систем других государств, психологической обработки населения для дестабилизации общества.

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 же происшедших масштабных и качественных изменений в области инфокоммуникаций прежние правовые нормы зачастую не в состоянии описать новые правоотношения в пространственной матрице цифрового мира.

Специалисты указывают, что для достижения прогресса в решении военных вопросов обеспечения международной информационной безопасности адаптации должны быть подвергнуты как основные принципы международного права, так и принципы отдельных его отраслей (космического, гуманитарного права, международно-правовой ответственности и др.), традиционно применявшиеся только в отношении физической силы. Представляется актуальным, в частности, конкретизировать и закрепить в соот-

ветствующем международном правовом документе содержание роли государства, частного сектора и гражданского общества в рамках решения проблемы обеспечения безопасности при использовании Интернета.

Мировое сообщество постепенно приходит к пониманию того, что эффективно противостоять угрозам в глобальном информационном пространстве необходимо коллективно. Де-факто в мире началось формирование региональных систем информационной безопасности.

Сегодня параллельно происходит формирование двух конкурирующих моделей системы международной информационной безопасности, строящихся на различных основополагающих принципах. В ареал евро-атлантической системы международной информационной безопасности входят США и большинство западных государств. Основу евразийской системы составляют государства – члены Шанхайской организации сотрудничества (ШОС). В эту организацию входят 5 государств – членов ОДКБ.

Евро-атлантическая система международной информационной безопасности нацелена в основном на борьбу с «киберпреступностью». Ее правовой основой являются нормы и принципы Конвенции Совета Европы о киберпреступности (Будапешт, 2001). В центре внимания находятся вопросы безопасности компьютерных систем как инфраструктуры. Под юрисдикцию данной конвенции евроатлантисты пытаются подвести также и так называемый кибертерроризм, отрицая при этом его политическую мотивированность.

Проблемным аспектом названной европейской Конвенции является нарушение отдельными статьями этого документа принципа суверенитета государств и открывающаяся возможность осуществления на практике вмешательства во внутренние дела других государств посредством несанкционированного проведения оперативно-розыскных действий в их национальном киберпространстве. Военно-политические вопросы международной информационной безопасности в евро-атлантической системе отданы на откуп блоку НАТО, который последовательно проводит курс на милитаризацию мирового киберпространства. Еще в 2008 г. в целях обеспечения превосходства в киберпространстве блок НАТО учредил Центр передовых технологий по обеспечению совместной кибероборонь, который размещен в г. Таллинне (Эстония).

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

Основной целью военной политики России и ее союзников в ОДКБ при формировании региональных систем международной информационной безопасности должно стать создание механизмов принятия эффективных коллективных действий, направленных на выявление, предупреждение и пресечение проявления возможностей использования современных информационных технологий для угрозы миру, осуществления актов агрессии или других нарушений мира. Направлениями военного сотрудничества в этой области должно стать выстраивание и последующее совершенствование механизма совместных действий, направленных на противодействие угрозам международной информационной безопасности.

Эксперты выделяют следующие частные направления военного сотрудничества:

1) разработка механизма и методологии мониторинга информационного пространства;

2) выработка и реализация мер совместного реагирования на угрозы в области международной информационной безопасности;

3) создание механизмов координации обеспечения информационной безопасности в зоне ответственности Организации[1].

Вопросы совершенствования военного и военно-технического сотрудничества актуальны и для всех государств

[1] Международная информационная безопасность: проблемы и решения / под общ. ред. С.А. Комова. – М., 2011, кн. 1, с. 113.

– членов ОДКБ. В целях укрепления сотрудничества необходим эффективный информационно-консультативный обмен между сторонами. 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 по вопросам обеспечения информационной безопасности, а также совместной научно-исследовательской деятельности по разработке и применению средств противодействия угрозам международной информационной безопасности.

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

Современные достижения в области телекоммуникационных и информационных технологий, а также 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 протоколы, имеющие уязвимые стороны, а средства безопасности используются на прикладном уровне.

По мнению автора, информационная инфраструктура по отношению к международной информационной безопасности выступает в двух ролях: как средство реализации угроз в сфере международной информационной безопасности и как объект их реализации.

В последние годы существенно обострилась и требует межгосударственной координации проблема обеспечения международной информационной безопасности при трансграничном обмене информацией с использованием информационных сетей. При этом проблема политической поддержки вопросов использования информационных сетей как средства и объекта реализации угроз в контексте международной информационной безопасности находится в ведении ООН, а проблематика технической поддержки информационной безопасности информационных сетей – в ведении Международного союза электросвязи[1].

Доступность и широкое использование современных информационных и коммуникационных технологий является фактором, существенно расширяющим возможности развития информационной преступности, информационного терроризма, осуществления информационных операций деструктивной направленности. С позиций безопасности деструктивную роль играет существующая сегодня практика анонимности в электронных коммуникациях. Это нарушает принцип информационного равенства, при котором 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, зачастую делающий невозможным привлечение злоумышленника к ответственности.

Растущий уровень угроз информационным ресурсам и масштабы преступности с их использованием – весомый повод в пользу создания защищенной сети и внедрения государством технологий обязательной идентификации пользовате-

[1] Там же, с. 232.

лей. Однако на практике решение задачи ограничения анонимности при трансграничном информационном обмене как механизма обеспечения международной информационной безопасности является достаточно сложным в техническом и организационном плане и крайне непростым в политическом и международном юридическом аспекте.

Мировое сообщество постепенно приходит к пониманию того, что эффективно противостоять угрозам в глобальном информационном пространстве необходимо коллективно. В представленной на 65-й сессии Генеральной Ассамблеи ООН в 2010 г. записке Генерального секретаря ООН было отражено коллективное мнение экспертов по международной информационной безопасности из 15 государств о потенциальных угрозах, рисках и уязвимостях, даны рекомендации по их уменьшению, а также приведены возможные совместные меры в данной области.

В 2011 г. в г. Екатеринбурге на международной встрече высоких представителей, ответственных за вопросы безопасности, Россия представила концепцию Конвенции об обеспечении международной информационной безопасности[1].

Политическим импульсом интеграции усилий мирового сообщества по решению проблем обеспечения международной информационной безопасности может стать принятая 27 мая 2011 г. главами государств – членов «Группы восьми» Довильская декларация: «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 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»[2].

В текущем году по договоренности президентов РФ и США в рамках российско-американской президентской комиссии создана двусторонняя рабочая группа по вопросам угроз в сфере использования информационных и коммуникационных технологий. 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»[3].

В данной связи автор отмечает, что геостратегическая ситуация вокруг РФ складывается сегодня под влиянием кардинальных изменений, происходящих в системе формирующегося нового облика России и нового облика мирового устройства в глобальном информационном пространстве. Геостратегическое положение России предъявляет жесткое требование: быть в постоянной готовности к отражению внешних угроз, в т.ч. и угроз в информационной сфере, со стороны иностранных государств и их коалиций. Речь идет о тех государствах, геополитические интересы которых находятся в противоречии с национальными интересами России и дружественных ей стран или могут войти в такое противоречие.

В данной связи представляется очевидным вывод автора о том, что основными направлениями государственной политики РФ должна быть предусмотрена система мер, направленная на решение задач по созданию условий, способствующих снижению риска возможного использования инновационных информационных и коммуникационных технологий в целях осуществления враждебных действий по дискредитации информационного суверенитета государств и их союзов.

[1] Там же, с. 101–106.

[2] Там же, с. 114–133.

[3] Совместное заявление заместителя секретаря Совета безопасности Российской Федерации Н.В. Климашина и координатора Белого дома по кибербезопасности Г. Шмидта // Официальный сайт Совета безопасности РФ; http://www.scrf.gov.ru, /documents/19/663.html (дата обращения 01.11.2013).