Вестник УрФО № 4(22) / 2016, с. 38–43
УДК 341 : 004.056 + 327 : 004.056 + 004.056

Кузнецов П. У.

ОТДЕЛЬНЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В представленной статье анализируется формирование правового обеспечения международной информационной безопасности. Автор анализирует практический опыт американских экспертов Института Восток-Запад и российских ученых Института проблем информационной безопасности МГУ по разработке терминов в области информационной безопасности международного уровня.

Так же автором исследуются институциональные проблемы применимости традиционного международного права к сфере ИКТ, в частности проблема определения места специальных правовых инструментов в системе традиционных международных правовых средств.

В связи с этим, автор предлагает переосмыслить систему известных для правоведения средств, особенно таких, как: дозволения, запреты, обязывания, ограничения, сдерживания (удержания от совершения злоумышленных действий), связывания, предупреждение, стимулирование и др. Набор названных инструментальных правовых средств должен сбалансировано и гармонично определить контуры правового регулирования общественных отношений по поводу ИКТ на международном уровне.

Ключевые слова: *информация, информационная безопасность, информационно-коммуникационные технологии, информационное общество, информационное право, международная информационная безопасность, киберпространство.*

Kuznetsov P. U.

SOME ASPECTS OF FORMATION OF LEGAL ENSURING INTERNATIONAL INFORMATION SECURITY

In the present article on the basis of the formation of the legal analyzes of international information security. The author analyzes the experience of American experts at the EastWest Institute and the Moscow State Institute of Russian scientists in the field of the development of the terms of the international level of information security issues of information security.

As the author examines the institutional problems of the applicability of international law to the traditional field of ICT, in particular the problem of determining the place of specific legal instruments in the traditional international legal means.

In connection with this, the author proposes to rethink the system known for the Law of funds, especially such as: permission, bans, obliging, limitations, deterrence (deterring malicious acts), binding, prevention, promotion, etc. Set these tools remedies must. balanced and harmonious shape to the legal regulation of social relations on the ICT at the international level.

Keywords: *information, information security, information and communication technologies, information society, information law, the international information security, cyberspace.*

Известно, что защита интересов личности, общества и государства в информационной сфере (информационная безопасность) является одним из важных условий устойчивого развития глобального информационного общества.

Как справедливо подчеркивается в одном из последних докладов международной Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: «открытая, безопасная, стабильная, доступная и мирная ИКТ-среда имеет существенно важное значение для всех, но для ее создания необходимо эффективное сотрудничество между государствами в целях снижения угроз международному миру и безопасности».

Информационно-коммуникационные технологии (ИКТ) открывают широчайшие возможности преобразования экономики и культуры всех стран. Киберпространство является непременным атрибутом нашей повседневной жизни. ИКТ приносят колоссальную пользу движения к прогрессу. Однако они порождают и определенные риски. В последнее время наметились тревожные тенденции, которые создают угрозу реализации прогрессивных целей цифровой цивилизации, а также могут нанести ущерб международному миру и безопасности в целом[2]. Особенно сложная ситуация складывается с информационно-кибернетическим оружием, которое по своей мощи может быть приравнено к оружию массового поражения. По американским данным, 20-30 государств мира способны вести кибернетическую войну.[3]

Основным официальным документом, определяющим государственную политику РФ в области международной информационной безопасности является «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», утв. Президентом РФ 24.07.2013 (№ Пр-1753) [4]. Названный документ определил основной угрозой в области международной информационной безопасности – использование информационных и коммуникационных технологий:

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 жизненно важной (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.

К числу наиболее пагубных нападений с использованием ИКТ относятся нападения на критически важные объекты инфраструктуры и связанные с ними информационные системы государств. Опасность вредоносных нападений с использованием ИКТ на критически важную инфраструктуру является реальной и серьезной.

Существует все более реальная опасность использования ИКТ для террористических целей, в том числе для совершения террористических нападений на объекты ИКТ или связанную с ИКТ инфраструктуру, а не только для вер-

бовки сторонников, финансирования, обучения и подстрекательства, причем, если не принять соответствующих мер, то это может поставить под угрозу международный мир и безопасность.

Многообразие злонамеренных негосударственных субъектов (включая преступные группировки и террористов), их различные мотивы, быстротечность злонамеренных нападений в сфере ИКТ, а также трудности, связанные с определением источника инцидента в сфере ИКТ, увеличивают существующую угрозу. Государства с полным основанием обеспокоены опасностью дестабилизирующих последствий ошибочного понимания намерений другой стороны, потенциалом возникновения конфликта и возможностью нанесения ущерба их экономике.

Ряд государств наращивают потенциал в сфере ИКТ для военных целей. Использование ИКТ в будущих конфликтах между государствами становится более вероятным. Разный уровень развития потенциала обеспечения безопасности в сфере ИКТ между государствами может также привести к повышению уязвимости в условиях взаимосвязанного мира.

Существенно важное значение для борьбы с вызовами и угрозами в сфере международной информационной безопасности имеет эффективное сотрудничество между государствами. Обеспечение стабильности и безопасности в информационной сфере может быть достигнуто лишь по линии международного сотрудничества, причем основой такого сотрудничества должны являться нормы международного права и принципы, провозглашенные в Уставе Организации Объединенных Наций.

Одним из важных обстоятельств, препятствующих укреплению международной информационной безопасности, является отсутствие единой позиции по порядку применения норм и принципов международного права к регулированию международных отношений в этой сфере.

Поэтому весьма важным является проблема толкования принципов международного права, установленных Уставом ООН и Декларацией о принципах международного права 1970 г., применительно к ИКТ. Особенно таких принципов как принцип мирного разрешения споров, неприменение силы или угрозы силой, суверенного равенства государств, невмешательства, равноправие и самоопределение народов, добросовестного выполнения обязательств по международному праву и принцип сотрудничества.

Как правильно подчеркивает А.А. Стрельцов, сложность решения проблемы применения международного права безопасности к киберпространству обусловлена следующими основными факторами:

• отсутствие согласия между государствами- членами ООН по многим вопросам правового регулирования;

• процессы злонамеренного использования ИКТ трудно фиксировать. Вследствие этого невозможно без использования специальных технических средств объективно установить ни факты вредоносного использования ИКТ, ни последствия такого использования ИКТ (величина и виды ущерба), ни субъектов, осуществляющих эти деяния. Общепринятые признаки вредоносного использования ИКТ, подлежащие регистрации техническими средствами, международным сообществом не определены. Международная система объективизации событий и идентификации субъектов в киберпространстве отсутствует;

• международными документами средства ИКТ не обладают признаками традиционного оружия. Это существенно затрудняет классификацию применения ИКТ в качестве «вооруженного нападения» или «вооруженных действий», порождающих, соответственно, правоотношения, связанные как с применением права на самооборону, так и с соблюдением норм международного гуманитарного права;

• правоприменение в области международной информационной безопасности осуществляется государствами самостоятельно с использованием национальных или региональных систем технических средств объективизации событий и атрибуции субъектов. В рамках юрисдикции одного государства или группы дружественных государств правоприменение базируется на презумпции добросовестности действий лиц, осуществляющих оперативно следственные мероприятия по фактам злонамеренного использования ИКТ. При взаимодействии государств, не связанных отношениями доверия, презумпция добросовестности невозможна ввиду того, что технологический потенциал многих государств достаточен для того, чтобы фальсифицировать данные о почти любых событиях и субъектах киберпространства;

• в международном праве отсутствуют механизмы закрепления адресного про-

странства применения ИКТ к национальным границам. В настоящее время функции распределения IP-адресов выполняются в основном негосударственными организациями, не являющимися субъектами международных публичных отношений. Это создает дополнительные сложности при определении в киберпространстве границ театров военных действий, нейтральных государств, обозначении объектов и лиц, охраняемых международным публичным правом;

• учитывая, что ни одно государство не имеет международных обязательств в области обеспечения безопасности киберпространства, представляется затруднительным определение границ национального суверенитета и юрисдикции государств. Данный вопрос особенно важен в свете существующей практики государств рассматривать обеспечение безопасности киберпространства в качестве одной из составляющих национальной безопасности.[5]

Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях, являются:

а) создание условий для продвижения на международной арене российской инициативы в необходимости разработки и принятия государствами - членами ООН Конвенции об обеспечении международной информационной безопасности;

б) содействие закреплению российских инициатив в области формирования системы международной информационной безопасности в итоговых документах, изданных по результатам работы Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также содействие выработке под эгидой ООН правил поведения в области обеспечения международной информационной безопасности, отвечающих национальным интересам Российской Федерации;

в) проведение на регулярной основе двусторонних и многосторонних экспертных консультаций, согласование позиций и планов действий с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС, странами - членами Азиатско-тихоокеанского экономического сотрудничества, другими государствами и международными структурами в области международной информационной безопасности;

г) продвижение на международной арене российской инициативы в интернационализации управления информационно-телекоммуникационной сетью «Интернет»;

ж) создание условий для заключения между Российской Федерацией и иностранными государствами международных договоров о сотрудничестве в области обеспечения международной информационной безопасности;

и) использование научного, исследовательского и экспертного потенциала ООН, других международных организаций для продвижения российских инициатив в области формирования системы международной информационной безопасности

Одним из важных традиционных международно-правовых средств является укрепление доверия. Меры укрепления доверия способствуют поддержанию международного мира и безопасности. Они могут способствовать расширению межгосударственного сотрудничества, повышению степени транспарентности, предсказуемости и стабильности. В стремлении укрепить доверие, в целях создания мирной ИКТ-среды, государства должны принимать во внимание Руководящие принципы для мер по укреплению доверия, принятые Комиссией по разоружению в 1988 году и утвержденные консенсусом Генеральной Ассамблеей в резолюции 43/78 (H). В целях укрепления доверия и расширения сотрудничества возможно создание системы проведения двусторонних, региональных, субрегиональных и многосторонних консультаций в целях снижения риска ошибочного восприятия, эскалации конфликтов, которые могут быть вызваны инцидентами в сфере ИКТ.

Это может включать добровольное распространение национальных мнений и информации:

• о различных аспектах национальных и транснациональных угроз ИКТ и в сфере использования ИКТ;

• факторах уязвимости и установленных пагубных скрытых функций в продуктах ИКТ;

• передовых методах обеспечения безопасности ИКТ;

• мерах укрепления доверия, разработанных в рамках региональных и многосторонних форумов;

• распространении опыта деятельности национальных организаций, политике и программах, имеющих отношение к безопасности ИКТ;

• национальных законах и стратегиях обеспечения безопасности критически важных объектах инфраструктуры ИКТ.

Государства должны стремиться укреплять трансграничное сотрудничество в устранении транснациональных факторов уязвимости критически важной инфраструктуры ИКТ. Такие меры могут включать создание двусторонних, субрегиональных, региональных и многосторонних основ технических, правовых и дипломатических механизмов укрепления доверия в и предупреждения инцидентов в сфере ИКТ. Ярким примером международного сотрудничества в области информационной безопасности является «Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности», заключенное в г. Екатеринбурге 16.06.2009, которое 2 июня 2011 года вступило в силу.

Странам-членам Шанхайской организации сотрудничества (ШОС) удалось добиться реального прорыва в продвижении идеи формирования международной системы обеспечения международной информационной безопасности (МИБ). Идея и конкретный проект этого соглашения были предложены российской стороной. Соглашение отвечает принципам и задачам деятельности ШОС, предусматривающим координацию действий, оказание взаимной поддержки и налаживание тесного сотрудничества по важнейшим международным и региональным вопросам, к которым, в частности, относится и проблематика обеспечения МИБ.

Уникальность названного документа заключается в том, что он впервые в международно-правовом плане определяет наличие и существо конкретных угроз в области МИБ, а также основные направления, принципы, формы и механизмы сотрудничества сторон в этой сфере. Как в рамках ШОС, так и в международной практике, вступившее в силу Соглашение стало первым договорным актом, направленным на ограничение всего комплекса угроз МИБ, включая их военно-политические, криминальные и террористические аспекты. Вступившее в силу Соглашение отвечает идее и цели создания всеобъемлющей системы обеспечения международной информационной безопасности.

Мировое сообщество по обеспечению информационной безопасности стоит на пороге формирования нового направления в системе правового регулирования – международного права информационной безопасности. В традиционных рамках международного права безопасности и вооруженных конфликтов[6] уже невозможно удерживать новую ИКТ-среду, особенно стихию использования сети Интернет. Поэтому следует говорить не столько о кризисе международного права, сколько о создании его нового формата (международного права 2.0) в контексте безопасности глобального информационного общества**.**

Очевидно, что новые киберобъекты формируют новый класс общественных отношений, возникающих по поводу ИКТ (информационно-коммуникационных технологий) в названной новой киберсферы. Мы переживаем время включения таких объектов отношений в сферу правоотношений, т.е. правовое пространство. Процесс этот сложный, болезненный и достаточно длительный (он длится уже более 25 лет), с момента принятия первых нормативных правовых актов информационной тематики, в т.ч. включения норм права об использовании информационных систем в различные отрасли права.

Как известно, для того, чтобы включить любой технологически сложный объект жизни в правовую сферу, требуется с помощью средств логики и лингвистики подвергнуть их комплексному исследованию с позиций разных научных специальностей.

В первую очередь необходимо когнитивно обработать термины, обозначающие границы технически сложных объектов (выявить и понять их технологические признаки, имеющие правовое значение).

Во-вторых, необходимо все существенные понятийные признаки и черты с помощью юридической техники преобразовать в правовые свойства и значения, т.е. технически сложные слова и словообразования привести в удобную для правоведов форму.

В-третьих, на основе правовых признаков и значений названных сложных терминов необходимо сформулировать определение (дефиницию), т.е. подготовить такие термины для включения их в состав модели правового поведения, т.е. в норму права.

Долгое время в науке отсутствовал набор признаваемых основных терминов и их зна-

чений, предназначенных для использования в нормативных документах международного уровня по вопросам информационной безопасности.

В 2011 году совместными усилиями американских экспертов Института Восток-Запад и российских ученых Института проблем информационной безопасности МГУ был достигнут консенсус по терминологии в трех ключевых областях кибербезопасности. Была создана концептуальная основа для обеспечения процесса создания определений для общего международного словаря как необходимого этапа выработки «Правил дорожного движения». Речь идет о двустороннем проекте Россия-США по выработке основ критически важной терминологии в области кибербезопасности. [7] Названным проектом разработаны первые двадцать терминов в области информационной безопасности международного уровня. Авторы этого проекта считают, что они создали основу, опираясь на которую можно работать дальше – как в двустороннем формате между нашими странами, так и в многостороннемс аспекте.

Думается это действительно так, хотя внимательный анализ названного проекта позволяет сделать вывод о том, что каждый из названных терминов и их определений необходимо подвергнуть правовому осмыслению, поскольку предлагаемые их значения могут «пробуксовывать» в ходе их применения в правоприменительной практике.

Не менее важным аспектом являются институциональные проблемы применимости традиционного международного права к сфере ИКТ. Речь идет об определении места специальных правовых инструментов в системе традиционных международных правовых средств.

Здесь необходимо переосмыслить систему известных для правоведения средств, особенно таких, как: дозволения, запреты, обвязывания, ограничения, сдерживания (удержания от совершения злоумышленных действий), связывания, предупреждение, стимулирование и др. Набор названных инструментальных правовых средств являются правовыми конструкциями первого уровня, которые с помощью сочетания жестких и мягких режимами должны сбалансировано и гармонично определить контуры правового регулирования общественных отношений по поводу ИКТ на международном уровне.

Примечания

1. Семидесятая сессия Генеральной Ассамблеи ООН открылась 15 сентября 2015 года в 15.00 в Центральных учреждениях ООН в Нью-Йорке // Генеральная Ассамблея ООН. URL: http://www.un.org/ru/ga/70 (дата обращения: 08.09.2016).

2. Бирюков А. В. Современные международные научно-технологические отношения: монография. М., 2014. С. 100 – 104.

3. Бирюков А. В. Указ.соч. С.100.

4. Совет безопасности Российской Федерации // Совет безопасности Российской Федерации. Официальный сайт. URL:http://www.scrf.gov.ru/ (дата обращения: 08.09.2016).

5. Стрельцов А. А. Проблемы адаптации международного права к информационным конфликтам // Труды Седьмого международного научного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» и Седьмая научная конференция Международного исследовательского консорциума информационной безопасности 22-25 апреля 2013 года г.Гармиш-Партенкирхен, Германия». М. 2013. С. 124-128.

6. Международное право. Учебник для вузов. Отв. редакторы – проф. Г.В.Игнатенко и проф. О.И.Тиунов. М., 1999. С. 431 – 464.

7. Двусторонний проект: Основы критически важной терминологии // Института проблем информационной безопасности МГУ. Официальный сайт. URL:http://www.iisi.msu.ru/articles/article36/ (дата обращения: 08.09.2016).

Кузнецов Петр Уварович, заведующий кафедрой информационного права Уральского государственного юридического университета, доктор юридических наук, профессор. Россия, 620066, г. Екатеринбург, ул. Комсомольская. E-mail: petr_kuznecov@mail.ru

Kuznetsov Petr Uvarovich, Head of Information Law department Ural State Law University, Doctor of Jurisprudence, Professor. Russia, 620066, Ekaterinburg, Komsomolskaya street, 21. E-mail: petr_kuznecov@mail.ru