УДК 341.22
ББК 67.412

Бедрицкий Александр Владимирович*, кандидат политических наук, заместитель начальника отдела евроатлантических исследований РИСИ.

Международные договорённости по киберпространству: возможен ли консенсус?

В последнее время заметно повысился интерес политиков и экспертов к проблематике кибербезопасности. Во многом это связано с тем, что в Соединённых Штатах, сохраняющих за собой технологическое и военное лидерство, на высшем уровне был принят ряд директив и официальных документов, регламентирующих политическую и военную деятельность в киберпространстве. Среди них особо выделяются "Обзор кибернетической политики"[1], "Международная стратегия по киберпространству"[2] и "Стратегия Министерства обороны по действиям в киберпространстве 2011"[3]. Наряду с этим в период президентства Б. Обамы США стали уделять повышенное внимание и международно-договорным аспектам данной проблемы. Активность Вашингтона в вопросах кибервойн и кибербезопасности привела к тому, что международный интерес к этой проблематике резко возрос. Кибербезопасность стала одной из актуальных политических проблем, обсуждаемых в мировых СМИ, на различных международных площадках и в разных форматах.

Однако не США, а именно Россия одной из первых осознала опасности, связанные с милитаризацией информационного пространства[4]

* a.bedritskiy@yandex.ru.

[1] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (Washington, D.C., May 29, 2009) // The White House : website. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[2] International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World / SEAL of the President of the United States. Washington D.C., 2011. May. 26 p.

[3] Department of Defense Strategy for Operating in Cyberspace / Department of Defense United States of America. Washington D.C., 2011. July. 14 p.

[4] Трактовка терминов, разработанных в России и США, наглядно демонстрирует суть противоречий по данному вопросу. *Информационное пространство* – сфера деятельности, связанная с созданием, преобразованием и использованием информации, включая индивидуальное и общественное сознание, информационно-телекоммуникационную инфраструктуру и собственно информацию (Словарь терминов и определений в области информационной безопасности. Изд. 2-е, доп. и перераб. / Военная акад. Генерального Штаба Вооружённых сил Рос. Федерации. Научно-исслед. центр информ. безопасности. М., 2008. С. 40). *Кибернетическое пространство* – условное пространство, образующееся в результате использования электронных и электромагнитных средств хранения, обработки и обмена данными в компьютерных сетях и связанных с ними физических

и противоправной деятельностью в нём. Она была инициатором международного обсуждения вопросов глобальной безопасности в этой сфере, предотвращения её милитаризации и проблем противодействия терроризму в интернет-пространстве.

Ещё в 1998 г. Россия предложила Соединённым Штатам подписать на уровне президентов заявление по вопросам обеспечения информационной безопасности[5]. Проект документа предусматривал совместное определение вызовов и угроз в данной сфере, выработку понятийного аппарата, вынесение вопроса о глобальной информационной безопасности на рассмотрение ООН, включая разоруженческие аспекты проблемы, а также выход на разработку международного многостороннего договора о борьбе с информационным терроризмом и преступностью. Обсуждение проекта заявления не привело к сближению сторон, однако в самом общем виде информационная безопасность была упомянута в "Совместном заявлении об общих вызовах безопасности на рубеже XXI в."[6]

Дальнейшее развитие тема международной информационной безопасности получила в рамках ООН. В декабре 1998 г. Генеральная Ассамблея (ГА) приняла консенсусом (без голосования) подготовленную Россией резолюцию "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности" (документ A/RES/53/70)[7], в которой странам – членам ООН рекомендовалось информировать Генерального секретаря по:

– общей оценке проблем информационной безопасности;

– определению основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов;

– целесообразности разработки международных принципов, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствующих борьбе с информационным терроризмом и преступностью.

В окончательно принятой резолюции, в отличие от представленного Россией проекта, не было прямых ссылок на использование информационных технологий в военных целях, конкретных определений понятий "информационное оружие"[8] и "информационная война", упоминания

инфраструктурах. (The National Military Strategy for Cyberspace Operations (U) // U.S. Department of Defense : website. 2006. December. P. IV. URL: http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf).

[5] *Фёдоров А. В.* Информационная безопасность в мировом политическом процессе / А. В. Фёдоров. М. : МГИМО-Университет, 2006. С. 187.

[6] Стороны признали в нём "важность содействия положительным сторонам и ослабление действий отрицательных сторон происходящей информационно-технологической революции, что является серьёзной задачей в деле обеспечения стратегических интересов наших двух стран в будущем" (см.: Совместное заявление об общих вызовах безопасности на рубеже XXI века (Москва, 2 сентября 1998 года) // Дипломатический вестник МИД России. 1998. Октябрь. № 10.

[7] Обновлённый проект этой резолюции был принят консенсусом в декабре 1999 г., однако принципиальных изменений он не содержал.

[8] Средства и методы, применяемые с целью нанесения ущерба информационным ресурсам, процессам и системам государства, негативного информационного воздействия

о необходимости разработки режима запрещения создания и применения информационного оружия, а также положения о сопоставимости воздействия информационного оружия и ОМУ. Наибольшее противодействие собственно разоруженческим идеям и задачам предотвращения межгосударственного противоборства в информационном пространстве оказали Соединённые Штаты, поэтому в заявлении американской делегации по поводу голосования в Первом комитете ГА ООН (вопросы разоружения и международной безопасности) отмечалась "гибкость, продемонстрированная основным спонсором резолюции в продвижении этой инициативы"[9].

Приняв этот документ, международное сообщество признало сам факт существования проблемы обеспечения информационной безопасности, и эта тема была включена в повестку дня работы ГА ООН.

В 1999 г. Россия представила по этой проблеме развёрнутый документ, многие положения которого были использованы при подготовке "Принципов, касающихся международной информационной безопасности"[10]. В его общих положениях отмечалось, что увеличение военного потенциала отдельных стран за счёт использования новейших информационных технологий ведёт к изменению глобального и регионального балансов сил. По мнению российской стороны, возникает очевидная потребность в международно-правовом регулировании мировых процессов гражданской и военной информатизации, в разработке согласованной международной платформы по проблеме международной информационной безопасности (МИБ). При этом была предложена модель действий международного сообщества, которая предусматривала дальнейшее обсуждение ситуации в указанной сфере и принятие ГА ООН новых, более конкретных резолюций об ограничении угроз как криминального, так и военного характера. Россия предлагала по мере определения общих подходов вести дело к разработке принципов МИБ (режима и кодекса поведения государств), которые для начала можно было бы сформулировать в виде многосторонней декларации, а в перспективе – закрепить в форме международно-правового документа.

Дальнейшее обсуждение российских инициатив в разных форматах позволило выделить два основных подхода к проблеме информационной безопасности.

США и Европа считали наиболее важным разработать меры информационной безопасности применительно к угрозам террористического и

на оборонные, управленческие, политические, социальные, экономические и другие критически важные системы государства, а также массированной психологической обработки населения с целью дестабилизации общества и государства (см.: Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности : Доклад Генерального секретаря ООН : A/55/140 / Генеральная Ассамблея ООН : Пятьдесят пятая сессия. 2000. 10 июля).

[9] Информационные вызовы национальной и международной безопасности / авт. кол.: И. Ю. Алексеева, И. В. Авчаров, А. В. Бедрицкий и др. / под общ. ред. А. В. Фёдорова, В. Н. Цыгичко. М. : ПИР-Центр, 2001. С. 178.

[10] Принципы, касающиеся международной информационной безопасности, 12 мая 1999 года : [Подлинный текст на рус. яз.] // Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности : Доклад Генерального секретаря ООН : A/55/140 / Генеральная Ассамблея ООН : Пятьдесят пятая сессия. 2000. 10 июля.

криминального характера. При этом перспективу создания информационного оружия и информационную войну как таковую сторонники такого подхода считали скорее теоретической. Соответственно, отпадал и собственно разоруженческий аспект общей проблемы МИБ. Европа сконцентрировалась на разработке конвенции по борьбе с киберпреступностью, а Соединённые Штаты, хотя и уделяли внимание всем аспектам информационного противоборства, практически не стремились к достижению международных договорённостей.

Приверженцы иного курса (в основном представители развивающихся стран) поддерживали идею рассмотрения проблемы международной информационной безопасности в комплексе, считая особенно важным предотвратить саму угрозу развязывания информационной войны. При этом подчёркивалась необходимость безотлагательно приступить к обсуждению и практической разработке международно-правовой основы универсального режима МИБ[11].

Противоречия между сторонниками обеих точек зрения особенно обострились в 2004 г., после того как 8 декабря 2003 г. Генассамблея ООН (традиционно консенсусом) приняла инициированную российской стороной резолюцию[12], переводящую общеполитическое обсуждение вопросов международной информационной безопасности в плоскость поиска практических решений. Эта резолюция должна была запустить механизм работы группы правительственных экспертов ООН, однако из-за обструкционистской позиции США усилия эти оказались безрезультатными. В период правления Дж. Буша-мл. американская делегация дважды голосовала против принятия указанной резолюции, фактически противопоставив позицию США мнению мирового сообщества[13]. В результате работа группы правительственных экспертов оказалась парализованной.

В этой ситуации Россия перенесла центр своей активности на региональный уровень. В октябре 2006 г. состоялось учредительное заседание группы экспертов государств – членов ШОС (председатель А. Крутских), которым было поручено выработать к саммиту в Бишкеке (2007 г.) план действий и определить пути решения проблемы МИБ в рамках компетенции стран-членов. В таком контексте главы государств ШОС договорились о возможных совместных мерах по устранению информационных угроз при соблюдении норм международного права. В ходе Бишкекского саммита был утверждён План совместных действий по обеспечению МИБ, а 16 июня 2009 г. в Екатеринбурге подписано межправительственное Соглашение государств – членов ШОС о сотрудничестве в области обеспечения МИБ. Уникальность этого документа заключалась в том,

---

[11] См.: Информационные вызовы национальной и международной безопасности. С. 186–187.

[12] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности : Резолюция, принятая Генеральной Ассамблеей : A/RES/58/32 / Генеральная Ассамблея ООН : Пятьдесят восьмая сессия : 58/32. 2003. 18 декабря.

[13] *Крутских А. В.* Нужны меры предосторожности, чтобы "киберджин" не стал беспредельничать : интервью с зам. директора департамента новых вызовов и угроз МИД РФ Андреем Крутских / Андрей Крутских ; вела Елена Черненко // Коммерсантъ. ru : интернет-сайт. 2012. 8 февраля. URL: http://www.kommersant.ru/doc/1868399.

что он впервые на международно-правовом уровне зафиксировал наличие конкретных угроз в области информационной безопасности, а также определил основные направления, принципы, формы и механизмы сотрудничества в этой сфере. Как в рамках ШОС, так и в широкой международной практике вступившее в силу Соглашение стало первым договорным актом, охватывающим весь спектр проблем МИБ – от противодействия кибирпреступности и кибертерроризму до вопросов разоружения[14]. Это соглашение ратифицировали четыре участника ШОС (Россия, Китай, Казахстан, Таджикистан), и 2 июня 2011 г. оно вступило в силу.

Таким образом, в условиях, когда на уровне ООН процесс продвижения идеи обеспечения информационной безопасности начал заходить в тупик, страны ШОС заложили основу регионального сотрудничества в этой сфере[15]. Действующее сегодня соглашение стало прецедентом и для стран, не входящих в ШОС. Аналогичный двусторонний документ, в котором чётко зафиксировано совместное понимание угроз, был также подписан Россией и Бразилией[16], которые исходили из того, что основные угрозы международной информационной и коммуникационной безопасности возникают вследствие использования информационных и коммуникационных средств и технологий:

– в международных конфликтах во враждебных целях, включая выведение из строя критически важных инфраструктур;

– для осуществления террористической деятельности и в террористических целях;

– для осуществления преступной деятельности и в преступных целях;

– как фактор доминирования в ущерб интересам и безопасности других государств.

Такие угрозы могут также возникать вследствие стихийных бедствий и технологических аварий, влияющих на безопасное и стабильное функционирование глобальных и национальных информационных и коммуникационных инфраструктур.

На Западе, прежде всего в США и Великобритания, часто говорят о надуманности угрозы информационной войны. Уже не отрицая в целом наличия такой проблемы, оппоненты ссылаются на то, что угроза эта скорее теоретическая. Они напоминают об отсутствии отработанной методики контроля, высказывают опасения о возможном ущербе, который могут нанести меры противодействия свободному обмену информацией и

---

[14] Соглашение стран ШОС о сотрудничестве в области информационной безопасности вступило в силу // ИнфоШОС : интернет-портал. 2011. 16 июня. URL: http://www.infoshos.ru/ru/?idn=8381.

[15] *Прокофьев К. В.* Информационная безопасность: основные проблемы международно-правового сотрудничества / К. В. Прокофьев // Адвокатская практика. 2008. № 5. С. 33–36.

[16] О подписании Соглашения между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности: Распоряжение Правительства РФ от 13.05.2010 № 721-р : Текст документа по состоянию на июль 2011 года : Проект // BestPravo: Информ.-правовой портал : интернет-сайт. URL: http://www.bestpravo.ru/rossijskoje/xi-zakony/w9k.htm.

конкуренции на рынке информтехнологий[17]. Тем не менее перспектива монополизации информационной сферы и военное использование информационно-телекоммуникационных средств являются предметом озабоченности не только России и стран ШОС.

Эти вопросы нашли своё отражение в докладе Генеральному секретарю ООН по вопросам информационной безопасности, представленном на 65-й сессии ГА в июле 2010 г. Документ подготовила группа правительственных экспертов 15-и стран (включая Индию). 12 сентября 2011 г. на 66-й сессии ГА постпреды РФ, Китая, Таджикистана и Узбекистана при ООН предложили совместный проект "Правил поведения в области обеспечения международной информационной безопасности"[18], а 22 сентября 2011 г. на закрытой встрече глав спецслужб и силовых ведомств 52 стран в Екатеринбурге Россия ознакомила участников с разработанным Советом безопасности и МИД проектом Конвенции об обеспечении информационной безопасности ООН[19]. Эти два документа взаимосвязаны и создают предпосылки для дальнейшего комплексного обсуждения проблемы МИБ на международном уровне. Проект Конвенции опирается на подготовленные при непосредственном участии России и принятые ранее резолюции ГА ООН – "Роль науки и техники в контексте международной безопасности и разоружения" от 20 ноября 2000 г. (A/RES/55/29) и "Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур" от 21 декабря 2009 г. (A/RES/64/211). Таким образом, проект сохраняет преемственность с принятыми ранее документами ООН.

Авторы проекта Конвенции об обеспечении информационной безопасности ООН придерживаются комплексного взгляда на информацию и информационную войну, которая определяется как межгосударственное противоборство в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам; для подрыва политической, экономической и социальной систем; массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.

Такой подход отражает направления информационного противоборства, которые проявляются в реальной политике ряда стран. Однако он

---

[17] *Крутских А. В.* Война и мир: международные аспекты информационной безопасности / А. В. Крутских // Научные и методологические проблемы информационной безопасности : сб. ст. / под ред. В. П. Шерстюка. М. : МЦНМО, 2004. С. 91.

[18] Правила поведения в области обеспечения международной информационной безопасности : Приложение к письму постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединённых Наций от 12 сентября 2011 г. на имя Генерального секретаря : A/66/359 : [Подлинный текст на английском, китайском и русском языках] / Генеральная Ассамблея ООН : Шестьдесят шестая сессия. 2011. 14 сентября.

[19] Конвенция об обеспечении международной информационной безопасности ООН (концепция), 21–22 сентября 2011 г. // EXPO IT Security : интернет-проект. URL: http://expo-itsecurity.ru/upload/iblock/a2f/Convention.pdf.

подвергается резкой критике, прежде всего со стороны США – страны, открыто стремящейся к "глобальному контролю над киберпространством"[20].

Негативное отношение США к инициативам России и ШОС объяснялось ещё и тем, что указанные проекты были предложены как раз накануне Лондонского форума по киберпространству, прошедшего в ноябре 2011 г.[21] Созвать эту представительную международную конференцию предложил в феврале 2011 г. на Мюнхенской конференции по безопасности глава британского МИД У. Хейг. Предполагалось, что на ней будет обсуждаться прежде всего британская модель безопасности в киберпространстве, фактически повторяющая американскую. По мнению У. Хейга, основные угрозы в киберпространстве включают в себя ставшие уже традиционными криминальные и террористические действия в информационных сетях, а также "использование передовых технологий репрессивными правительствами в целях нарушения прав своих граждан, ограничения конфиденциальности информации и свободы слова, блокирования информации, доступ к которой многие из нас считают само собой разумеющимся". В качестве примера влияния информационной открытости на "демократизацию общества" британский министр привёл события "арабской весны". Эта открытость, как он считает, "помогла обычным гражданам выстоять против деспотических режимов, привлекая внимание остального мира к их жестокости". Была упомянута также и угроза "кибервойн", понимаемых как "враждебная атака" на другое государство посредством повреждения инфраструктуры или похищения секретной информации[22]. При этом единственным признанным на Западе примером "кибервойны" по-прежнему считается серия кибератак на сайты правительства Эстонии в мае 2007 г., последовавших в ответ на решение эстонских властей о переносе памятника советским воинам. У. Хейг рассчитывал, что конференция будет способствовать принятию согласованного международного решения по киберпространству с привлечением основных участников (включая Россию). Однако даже простое сопоставление перечней угроз в российской и британской моделях даёт чёткое представление об их принципиальном различии.

Российскую модель информационной безопасности представил на Лондонской конференции министр связи и массовых коммуникаций РФ И. Щёголев, посвятивший своё выступление фактически представлению упоминавшихся выше проектов Конвенции и Кодекса поведения государств в информационном пространстве. Он заявил, что принципиальным моментом в концепции Конвенции является полное сохранение государственных суверенитетов и границ национального регулирования в виртуальном пространстве. Что же касается обеспечения прав и безопасности субъектов информационного взаимодействия – как национального, так и трансграничного, то оно возможно только на основе совместного

[20] The National Military Strategy for Cyberspace Operations (U). P. IX.

[21] London Conference on Cyberspace (1–2 November 2011) // Foreign and Commonwealth Office : website. URL: http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/.

[22] "Угрозы являются реальными" – глава британского МИДа о кибербезопасности // Коммерсантъ.ru : интернет-сайт. 2011. 21 октября. URL: http://kommersant.ru/doc/1799757.

комплексного решения правовых, организационных и технологических вопросов, для чего необходимо принять международный свод правил (кодекс) поведения в глобальном информационном пространстве и универсальную конвенцию под эгидой ООН[23].

Естественно, что такой подход встретил резкое сопротивление со стороны США. Накануне конференции заместитель госсекретаря США М. Познер заявил о неприемлемости предложений, "превращающих Интернет из пространства, управляемого множеством людей и заинтересованных сторон, в подконтрольную центральным правительствам систему"[24]. Любопытно, что при этом в самих США на официальном уровне Интернет рассматривается как важнейший канал влияния на другие страны[25]. Поэтому не удивительно, что эксперт Центра стратегических и международных исследований в Вашингтоне Д. Льюис обвинил Россию и Китай в "размытии" тематики конференции и заявил о неприемлемости их предложений[26].

Тем не менее Россия и заинтересованные страны продолжают работать над проектом Конвенции. 6–7 марта 2012 г. в Нью-Дели был проведён российско-индийский семинар, посвящённый его обсуждению, в ходе которого эксперты пришли к заключению, что разработка международного правового документа по вопросам формирования системы международной информационной безопасности и принятие его на уровне ООН является своевременным и актуальным шагом[27]. 13—15 марта 2012 г. в Пекине состоялось очередное заседание группы экспертов государств – членов ШОС по МИБ. В ходе этого заседания обсуждались уже вопросы практического взаимодействия в рамках Соглашения между правительствами государств – членов ШОС в области обеспечения международной информационной безопасности, а также сотрудничества по продвижению в мировом сообществе общих правил поведения в области обеспечения МИБ[28]. Согласованный проект документа был представлен на 6-м ежегодном международном форуме "Партнёрство государства, бизнеса и

---

[23] Выступление Игоря Щёголева на конференции по вопросам киберпространства (The London Conference on Cyberspace), Лондон, 1 ноября // Минкомсвязь России : интернет-сайт. 2011. 10 ноября. URL: http://minsvyaz.ru/ru/speak/index.php?id_4=42975.

[24] Советник госсекретаря по инновациям А. Росс, выступая перед студентами МГИМО, тоже заявил, что США категорически против того, чтобы "какие-либо люди мешали простым пользователям свободно общаться друг с другом" даже во имя защиты национальной безопасности (см.: *Черненко Е.* Россия зашла на интернет-форум со своими правилами / Елена Черненко // Коммерсантъ.ru : интернет-сайт. 2011. 1 ноября. № 205 (4746). URL: http://www.kommersant.ru/doc/1807713/print).

[25] U.S. National Strategy for Public Diplomacy and Strategic Communication : Released June 2007 / Strategic Communication and Public Diplomacy ; Policy Coordinating Committee (PCC). 2007. June.

[26] *Черненко Е.* Указ. соч.

[27] Российско-индийский научный семинар "Концепция Конвенции об обеспечении международной информационной безопасности" (6–7 марта 2012 г., Нью-Дели) // Институт проблем международной безопасности : интернет-сайт. 2012. 28 марта. URL: http://www.iisi.msu.ru/news/news54/.

[28] Заседание Группы экспертов государств – членов ШОС по международной информационной безопасности (13–15 марта 2012 г., Пекин) // Институт проблем международной безопасности : интернет-сайт. 2012. 28 марта. URL: http://www.iisi.msu.ru/news/news55/.

гражданского общества по обеспечению информационной безопасности", который проходил в Гармиш-Партенкирхене (Германия) 26–27 апреля 2012 г. Однако, несмотря на то, что А. Крутских, назначенный на должность спецкоординатора по вопросам политического использования информационно-коммуникационных технологий, избегал в своём выступлении прямого обсуждения вопросов межгосударственного противоборства в киберпространстве, западные эксперты так и не изменили негативного отношения к российским инициативам. В частности, К. Раушер из Института Восток – Запад заявил, что контроль за интернет-пространством будет противоречить первой поправке к американской конституции[29].

Таким образом, на сегодняшний день для России и США – двух стран, способных выдвинуть собственные модели информационной безопасности, которые находят сторонников в мире, единственным общим моментом в понимании киберугроз остаётся использование киберпространства в преступных целях.

Собственно, именно киберпреступность была одной из немногих информационных угроз, которую Запад был готов охотно обсуждать с Россией. Более того, и ЕС, и США неоднократно призывали Москву ратифицировать соответствующую конвенцию Совета Европы[30]. (Тот факт, что наша страна так и не присоединилась к ней, является одним из главных аргументов в критике российских инициатив, в том числе и со стороны части российского экспертного сообщества[31].)

Однако было бы глубоко ошибочным утверждать, что Россия не уделяет должного внимания вопросам противодействия преступности в киберпространстве. Более того, многие её инициативы получают политическую и практическую поддержку на Западе. Так, в ноябре 2006 г.

---

[29] Идея РФ о борьбе с киберпреступниками напугала Запад: русские хотят задушить свободный Интернет // NEWSru.com : информ. интернет-сайт. 2012. 26 апреля. URL: http://www.newsru.com/world/26apr2012/itsafety.html.

[30] Конвенция СЕ по киберпреступности, получившая название Будапештской, была принята Комитетом министров в ноябре 2001 г. Она охватывает большинство вопросов, включая незаконный доступ к компьютерным системам, перехват данных, воздействие на данные, воздействие на работу системы, противозаконное использование устройств, подлог и мошенничество с использованием компьютерных технологий, правонарушения, связанные с детской порнографией, авторскими и смежными правами. В ней не рассматриваются вопросы межгосударственного противоборства в киберпространстве. Наша страна отказалась подписать этот документ из-за формулировка п. "B" ст. 32 о трансграничном доступе к компьютерным системам, которая напрямую угрожает суверенитету России: "Сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, имеющего законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему" (см.: Convention on Cybercrime (Budapest, 23.XI.2001) // Council of Europe : website. URL: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm).

[31] *Демидов О. В.* Международное регулирование информационной безопасности в свете российских национальных интересов : проект докл. / О. В. Демидов // Научные записки ПИР-Центра : сб. [в рамках проекта "Международная информационная безопасность и глобальное управление интернетом"]. 2011. 7 декабря. С. 32–33. URL: http://www.pircenter.org/kosdata/page_doc/p2713_1.pdf. Аргументация автора фактически копирует основные положения американских программных документов, рассматриваемых ниже.

в Санкт-Петербурге в ходе Глобального форума по партнёрству государства и бизнеса в противодействии терроризму Россия, председательствовавшая в "большой восьмёрке", выступила с рядом долгосрочных инициатив по борьбе с киберпреступностью, которые были высоко оценены зарубежными партнёрами, получили всестороннюю поддержку и перешли в практическую плоскость.

В предложенном Россией в Санкт-Петербурге документе основными угрозами кибербезопасности были признаны: использование возможностей Интернета для пропаганды идей терроризма и радикализма, получения доступа (террористическими группами) к чувствительной информации, прямая угроза функционированию критически важных инфраструктур, управление которыми осуществляется по спутниковым и интернет-каналам[32].

На тот момент о необходимости и готовности искать пути противодействия угрозам в информационной сфере прямо заявили некоторые российские и зарубежные компании: "Аэрофлот", "Газпром", "ЛУКойл", "Норильский никель", АЛРОСА, IBS Group., General Electric, SAP, Siemens, Citigroup, Motorola, Microsoft, Telenor, Ericsson и др. Были выдвинуты и конкретные предложения. В частности, Finmeccanica (Италия) создала частный консультативный совет по внедрению защищённых систем связи в энергетических компаниях. WISeKey (Швейцария) и IBS (Россия) представили защищённые системы связи между правительством и бизнесом. Ericsson (Швеция) согласилась сотрудничать с государственными структурами для предоставления им приоритетной возможности пользования линиями мобильной связи в чрезвычайных ситуациях.

При этом Россия исходит из того, что в настоящее время назрела необходимость разработки нового универсального документа, который заменил бы устаревшую и во многом ущербную Конвенцию о киберпреступности Совета Европы 2001 г. (Будапештскую конвенцию) и не содержал бы одиозных и дискриминационных положений. Позиция России заключается в том, что разработка такой конвенции должна вестись под эгидой ООН. Это позволит, с одной стороны, максимально учесть озабоченности всех стран мира, а с другой – придать документу действительно глобальный масштаб, без которого борьба с киберпреступностью не может быть достаточно эффективной.

В мае 2010 г. благодаря российской инициативе Комиссия ООН по предупреждению преступности и уголовному правосудию приняла решение создать открытую межправительственную группу экспертов для всеобъемлющего изучения проблем киберпреступности[33].

Таким образом, российские инициативы в настоящее время охватывают весь спектр угроз в информационной сфере. Однако, чтобы понять суть проблемы, необходимо проанализировать американские внешнеполитические инициативы последнего времени, напрямую касающиеся военного использования киберпространства.

---

[32] G8 Initiative For Public-Private Partnerships To Counter Terrorism. Private Sector Action Beyond 2006 : EWI's Discussion paper. 2006. November. P. 7.

[33] *Markoff J.* The New York Times. Step Taken to End Impasse Over Cybersecurity Talks / John Markoff // The New York Times : website. 2010. July 16. URL: http://www.nytimes.com/2010/07/17/world/17cyber.html.

Несмотря на то, что Соединённые Штаты на протяжении длительного времени избегают обсуждать разоруженческий аспект МИБ, идея выработки соглашения по контролю над вооружениями в информационной сфере впервые обсуждалась более 15 лет назад именно американцами – специалистами Стэнфордского университета[34]. Тогда она не нашла поддержки в официальном Вашингтоне, а при республиканской администрации США вообще не проявляли сколько-нибудь заметного интереса к переговорам по информационной безопасности в любом формате.

Ситуация изменилась лишь с приходом к власти Б. Обамы, что нашло отражение в программных документах, формирующих политику Вашингтона. Обсуждая характер возможного соглашения, США исходят из трёх главных соображений[35].

1. Военное использование киберпространства целесообразно и будет иметь важное значение. Соединённые Штаты не намерены связывать себя какими-либо ограничениями на развёртывание, испытания и использование военных возможностей в этой сфере в целом. В дальнейшем в интересах защиты критически важных инфраструктур характеристики конкретных кибернетических угроз будут детализироваться и по ним могут быть подписаны международные соглашения. Однако вопрос о том, насколько такие соглашения будут ограничивать наступательный потенциал США и, соответственно, будет ли целесообразным международное обсуждение этих вопросов, должен решаться в ходе всесторонних исследований и моделирования[36].

2. Соединённые Штаты будут настаивать на том, чтобы эти соглашения не исключали возможности осуществлять возмездие (сдерживание) в случае проведения против них кибернетических атак другими странами. Они также будут последовательно выступать за право предупреждать кибернетические атаки, поскольку считают такие действия активной защитой своих инфраструктур.

3. Поскольку в случае проведения кибератаки достаточно трудно выявить страну-агрессора, Соединённые Штаты, возможно, будут заинтересованы в подписании многостороннего соглашения, определяющего пропорциональность ответа на кибератаку, исходя из её масштаба, продолжительности и потенциальной угрозы для гражданских объектов. Это, естественно, потребует выработки в той или иной мере режима верификации.

Впервые о необходимости наладить международное сотрудничество в деле обеспечения кибербезопасности говорилось в "Обзоре кибернетической политики". Там, в частности, утверждалось, что Соединённые Штаты не в состоянии обеспечить свою кибербезопасность только собственными силами, поэтому необходимо сформировать соответствующую американским интересам международную коалицию стран, разделяю-

---

[34] *Soo Hoo K. J., Greenberg L., Elliott D.* Strategic Information Warfare – A New Arena for Arms Control? : Working paper / Kevin J. Soo Hoo, Lawrence Greenberg, David Elliott. 1996. October.

[35] *Elliott D.* Weighing the Case For a Convention to Limit Cyberwarfare / David Elliott // Arms Control Association : website. 2009. November. URL: http://www.armscontrol.org/act/2009_11/Elliott.

[36] *Hamre J.* Cyberwar! : Interview / John Hamre // PBS Frontline. 2003. February 18.

щих американские подходы, которые смогут выработать технические и правовые нормы, *учитывающие вопросы национальной юрисдикции, национального суверенитета, а также право использования силы*[37]. В интересах снижения кибернетической угрозы Соединённые Штаты совместно с союзниками намерены разрабатывать нормы и принципы поведения в кибернетическом пространстве, укреплять совместную правовую базу противодействия киберпреступности, а также выработать механизмы сдерживания потенциальных агрессоров от проведения кибернетических атак.

Именно через призму такого подхода следует рассматривать положение "Обзора", согласно которому различия в национальных законодательствах (по вопросам расследования и наказания за киберпреступления, ограничения в доступе к информации, авторского права, защиты информационно-телекоммуникационных систем и реагирования на кибератаки) сами по себе порождают серьёзные вызовы безопасности. А это значит, что для создания защищённой и надёжной цифровой инфраструктуры международные нормы крайне необходимы.

Этот тезис был развит в документе "Международная стратегия по киберпространству", принятом в мае 2011 г.[38] Авторы стратегии исходят из того, что в глобальном масштабе необходимо обеспечить реализацию трёх принципов: свободы поиска, получения и распространения информации и идей ("фундаментальные свободы"); охраны права частной собственности в информационных сетях; свободы обмена информационными потоками.

В связи с этим международные нормы поведения в киберпространстве, согласно американской трактовке, должны:

– отстаивать соблюдение "фундаментальных свобод" (все государства должны уважать права людей выражать свои взгляды и объединяться в группы);

– уважать частную собственность (национальные законодательства должны признавать права интеллектуальной собственности, включая патентное право, коммерческую тайну и *копирайт*);

– уважать частную жизнь (личность должна быть защищена от незаконного вторжения государства в свою частную жизнь в информационных сетях);

– защищать от преступности (государства должны выявлять и преследовать киберпреступников, ликвидировать правовые и технические возможности для преступной деятельности, на постоянной основе сотрудничать с международными следственными органами);

– признавать право на самооборону (в соответствии с Уставом ООН государства должны иметь право на самооборону в случае, если агрессия исходит из киберпространства)[39].

Задача американской дипломатии – добиваться признания этих норм на всех возможных уровнях: в формате двусторонних и многосторонних

---

[37] См.: Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (Washington, D.C., May 29, 2009).

[38] International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World / SEAL of the President of the United States. Washington D.C., 2011. May. P. 5.

[39] Ibid. P. 10.

переговоров, через международные и транснациональные организации (*multi-stakeholder organizations*) и деловое сотрудничество.

В случае враждебных действий со стороны террористов, криминальных структур, а также государств и подконтрольных им криминально-террористических организаций, угрожающих нарушить вышеизложенные принципы, США оставляют за собой право на сдерживание или оборону.

Вопросы международного сотрудничества рассматриваются и в "Стратегии Министерства обороны США по действиям в кибрепространстве"[40]. Согласно этому документу Пентагон должен поддерживать тесные связи с американскими союзниками по линии оборонных ведомств для защиты общих интересов в киберпространстве и разработки мер сдерживания потенциальных агрессоров. Такое сотрудничество призвано не только повысить уровень взаимодействия в рамках уже сложившихся альянсов, но и способствовать распространению американской модели кибербезопасности в мире.

Соединённые Штаты рассчитывают в ближайшем будущем разработать технические стандарты и правовые нормы, касающиеся юрисдикции и ответственности отдельных стран в киберпространстве; провести ревизию правовых аспектов применения силы и предложить свои разработки в качестве модели. В США считают, что заключение соответствующих соглашений, принятие стандартов и процессуальных регламентов даже в рамках одной международной организации окажет глобальный эффект, и прочие страны, в том числе и не разделяющие американских подходов, не смогут их игнорировать[41]. Таким образом, основную задачу администрация демократов видит в принятии коалиционной стратегии обеспечения кибербезопасности в рамках НАТО.

Надо сказать, что американцы предприняли значительные усилия для того, чтобы распространить принципы коллективной безопасности НАТО и на информационно-телекоммуникационную сферу. И здесь необходимо отметить необычайно деятельную роль заместителя министра обороны США В. Линна, который весь сентябрь 2010 г. на различных европейских площадках последовательно настаивал на включении вопросов кибербезопасности в новую стратегическую концепцию альянса. Он, в частности, заявлял, что кибернетическое пространство стран НАТО должно быть защищено точно так же, как их территории защищены ядерным щитом и объединённой системой ПВО/ПРО. Для этого, по его мнению, отлично подходит концепция единой системы предупреждения о нападении времён "холодной войны"[42]. Это высказывание полностью отражает позицию госсекретаря США Х. Клинтон, ещё в феврале 2010 г. заявлявшую, что кибератаки, в результате которых под угрозой оказываются системы энергоснабжения или военные системы управления, необходимо расценивать как атаки военные. Исходя из этого, по мнению высокопоставленных американских чиновников, в соответствии со ст. 5 Устава

[40] Department of Defense Strategy for Operating in Cyberspace / Department of Defense United States of America. Washington D.C., 2011. July. P. 9–10.

[41] Ibid. P. 20.

[42] *Benitez J.* US urges NATO to build "cyber shield" / Jorge Benitez // Atlantic Council : website. 2010. September 16. URL: http://www.acus.org/natosource/us-urges-nato-build-cyber-shield.

НАТО член альянса, подвергшийся нападению, вправе рассчитывать на помощь в рамках системы коллективной безопасности[43].

Изначально американские идеи "активной кибероборонs" не нашли широкой поддержки среди европейских союзников по НАТО, и многие эксперты сомневались в том, что консенсус по этому вопросу будет найден[44]. Тем не менее в ст. 19 новой Стратегической концепции альянса (принята в 2010 г. на саммите в Лиссабоне), определяющей основные вызовы и угрозы, говорится о необходимости создания потенциала для выявления, предотвращения и защиты от кибернетических атак. Для этого требуется задействовать механизмы объединённого планирования, координировать национальные программы защиты киберпространства, включая совместную работу систем предупреждения и реагирования на кибератаки, а также создать единую систему информационной безопасности для всех структур НАТО[45].

По итогам Лиссабонского саммита было принято совместное заявление лидеров ЕС и США, в котором не только подчёркивалась важность решения проблемы кибербезопасности, но и объявлялось о создании рабочей группы ЕС – США по кибербезопасности и киберпреступности, которой было поручено заняться рядом конкретных приоритетных разработок[46].

Совместные действия по реализации принятых решений не заставили себя ждать. Уже в январе 2011 г. заместитель главы Пентагона В. Линн вновь посетил Брюссель для предметного обсуждения вопросов кибербезопасности с руководством НАТО и ЕС[47]. На встрече он заявил, что киберугрозы переросли уровень простого электронного шпионажа: они не просто нарушают работоспособность отдельных сайтов, но направлены в первую очередь против жизненно важных инфраструктур. Именно такое представление об угрозах должно быть положено в основу разрабатываемой стратегии кибербезопасности НАТО[48], которая будет фундаментом для подготовки национальных стандартов в европейских странах. При этом в ходе Мюнхенской конференции по безопасности, прошедшей в начале февраля 2011 г., Соединённые Штаты предложили принять общие для всех государств правила поведения в киберпространстве, основанные на том, что негосударственные игроки являются в этом

---

[43] *Benitez J.* NATO's Cyber Threat / Jorge Benitez // Atlantic Council : website. 2010. July 3. URL: http://www.acus.org/natosource/natos-cyber-threat.

[44] *Benitez J.* US call for NATO cyber-strike capacity causes division / Jorge Benitez // Atlantic Council : website. 2010. October 5. URL: http://www.acus.org/natosource/us-call-nato-cyber-strike-capacity-causes-division.

[45] Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon. Lisbon, 2010. November 19. P. 4.

[46] Совместное заявление лидеров Соединённых Штатов и Европейского союза (21 ноября 2010 г., Лиссабон) // Окна в NATO : интернет-сайт. 2010. 20 ноября. URL: http://nato.w-europe.org/show.php?art=2590&rubr=27.

[47] *Benitez J.* Dept. SecDef meeting with NATO and EU to improve cyber security / Jorge Benitez // Atlantic Council : website. 2011. January 24. URL: https://www.acus.org/natosource/dept-secdef-meeting-nato-and-eu-improve-cyber-security.

[48] *Benitez J.* NATO networks vulnerable to cyber threat: US / Jorge Benitez// Atlantic Council : website. 2011. January 28. URL: http://www.acus.org/natosource/nato-networks-vulnerable-cyber-threat-us.

пространстве отнюдь не главными. По мнению американской стороны, несмотря на то, что идеи войны и мира слишком просты для нынешней эпохи взаимозависимости, всё же требуется учитывать и возможность ведения конфликтов, "отличных от войны"[49]. Причиной "сложности" кибернетического пространства западные эксперты считают тесное переплетение в нём интересов (военных, экономических, социальных, дипломатических) различных государств, а потому попытки инициировать межгосударственные конфликты в этом пространстве вполне могут привести к хаосу, причём вероятность такого развития событий будет возрастать по мере роста информатизации[50]. Исходя из такого понимания кибербезопасности, было предложено отнести это пространство к категории "общих" наряду с космическим, воздушным и морским, которые считаются "всеобщим достоянием" и защищать которые призван Североатлантический альянс[51].

Согласно проекту концепции кибернетической обороны НАТО эффективная защита киберпространства должна включать три взаимосвязанных направления: широкое международное сотрудничество, разработку коалиционной политики и повышение оборонного потенциала для действий в киберпространстве[52].

Следует согласиться с российским экспертом А. Фененко[53], утверждающим, что включение кибернетического пространства в категорию "общих пространств" отражает фундаментальный сдвиг в идеологии международной безопасности, которая сегодня перерастает "территориальные" рамки геополитики XIX в. Если в начале 90-х гг. прошлого века представители западной либеральной политической философии (О. Тоффлер, Ф. Фукуяма) считали, что освоение "новых пространств" послужит фактором, объединяющим государства либо даже размывающим их природу, то современные тенденции демонстрируют обратное.

Взаимодействие в рамках "общих пространств" предполагает сегодня не столько межгосударственное сотрудничество в их освоении, сколько соперничество за принципы их раздела, а увеличение их числа порождает новые формы межгосударственных или даже транснациональных конфликтов, возрождая теории "жёсткой силы" и геополитического соперничества[54]. Отсюда и неизбежный всплеск интереса современной общественно-политической мысли к геополитическим разработкам позапрошлого столетия.

---

[49] *Watts S.* Cyber war Geneva Conventions call / Susan Watts // BBC News : website. 2011. February 3. URL: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/programmes/newsnight/9386445.stm.

[50] *Hunker J.* Cyber War and Cyber Power: Issues for NATO Doctrine : Research Paper / Jeffrey Hunker ; Research Division ; NATO Defense College, Rome. 2010. November. № 62. P. 3.

[51] *Barrett M., Bedford D. et al.* Assured Access to the Global Common. USA, Norfolk, Virginia / Major General Mark Barrett, Dick Bedford, Elizabeth Skinner, Eva Vergles // MNE 7. Access to the Global Commons : website. 2011. April 3. URL: http://mne.oslo.mil.no:8080/Multinatio/MNE7/NATOACTAcc/file/ACT%20Access%20to%20the%20Global%20Commons_Final%20report.pdf.

[52] Ibid. P. 4–42.

[53] *Фененко А.* Международное соперничество за освоение общих пространств / А. Фененко // Международные процессы. 2010. Январь – апрель. Т. 8, № 1 (22). С. 14–30.

[54] Там же.

Внешнеполитическая деятельность США, направленная на распространение американских взглядов на кибербезопасность среди своих союзников, служит фоном для активизации двусторонних российско-американских консультаций и переговоров. До выработки единых для западных стран подходов к проблеме кибербезопасности Соединённые Штаты старались всячески избегать обсуждения этой темы с Россией. Например, в рамках российско-американских переговоров о сокращении стратегических наступательных вооружений в июле 2009 г. российская сторона ставила вопрос и о подписании соглашения, запрещающего военные действия в кибернетическом пространстве. Однако американская делегация отвергла саму возможность подобной договорённости и традиционно порекомендовала России как можно скорее присоединиться к Конвенции Совета Европы о киберпреступности[55].

Во второй половине 2010 г. ситуация в корне изменилась. В докладе, подготовленном так называемой "Группой Мудрецов" во главе с М. Олбрайт[56], содержались рекомендации перейти к "конструктивному диалогу" с Россией, которая рассматривается как потенциальный партнёр в отношении Ирана, а также как государство, от которого во многом зависит успех операции НАТО в Афганистане. Этот диалог распространяется сегодня и на сферу кибербезопасности. Хотелось бы подчеркнуть, что один из наиболее активных пропагандистов идей МИБ на международной арене А. Крутских (в то время – заместитель директора департамента МИД России по новым вызовам и угрозам) ещё в 2004 г. отмечал высокую вероятность того, что под воздействием объективных обстоятельств в области мировой информатизации тема информационной безопасности станет одной из важнейших в наших переговорах с США по вопросам стратегической стабильности и будущего наших взаимоотношений[57]. Именно это и происходит в настоящее время. Однако такой разворот в сторону России был обусловлен прежде всего тем, что основные параметры новой стратегической концепции НАТО к тому времени были уже выработаны и члены альянса смогли прийти к общему пониманию угроз в киберпространстве, наметить дальнейшие пути совместных действий на международной арене.

В соответствии с рекомендациями М. Олбрайт в 2010 г. начались консультации между США и Россией на экспертном уровне. Несколько российских чиновников посетили Пентагон, Госдепартамент и Министерство внутренней безопасности США, где предметом обсуждения стали непосредственно вопросы кибербезопасности. А уже в начале июня 2010 г. глава кибернетического командования МО США и директор Агентства национальной безопасности К. Александер выступил в Центре стратегических и международных исследований в Вашингтоне с предложением

---

[55] *Markoff J., Kramer A. E.* U.S. and Russia Differ on a Treaty for Cyberspace / John Markoff, Andrew E. Kramer // The New York Times. 2009. June 28.

[56] NATO 2020: Assured Security; Dynamic Engagement / [Madeleine K. Albright, Jeroen van der Veer et al.] ; NATO Public Diplomacy Division // North Atlantic Treaty Organization : website. Brussels, 2010. May 17. URL: http://www.nato.int/strategic-concept/expertsreport.pdf.

[57] *Крутских А. В.* Война и мир: международные аспекты информационной безопасности. С. 91.

начать совместно с Россией работу над принципиально новым договором, ограничивающим проведение атак в киберпространстве[58]. Он особо подчеркнул, что более ранние предложения Москвы по этому вопросу могут стать отправной точкой для начала дискуссии, но американские эксперты должны, тщательно изучив российские предложения, выдвинуть встречные идеи, отражающие американские взгляды на проблему.

В рамках международного экспертного сотрудничества Институт Восток – Запад и Институт проблем информационной безопасности МГУ разработали общий понятийный аппарат в сфере информационной безопасности. В результате были согласованы 20 базовых терминов возможной двусторонней договорённости[59], которые можно сгруппировать в три крупных кластера: *поле действий* (киберпространство, кибернетическая инфраструктура, киберсервисы, критически важное киберпространство, критически важная кибернетическая инфраструктура, критически важные киберсервисы), *виды угроз* (киберпреступление, кибертерроризм, киберконфликт, кибервойна, кибербезопасность), *способы действий* (боевые действия в киберпространстве, кибератака, киберконтратака, оборона и противодействие в киберпространстве, кибервойна, оборонительные возможности в киберпространстве, наступательные возможности в киберпространстве, использование преимуществ в киберпространстве, средства киберсдерживания). Даже простое перечисление терминов, по которым российские и американские эксперты смогли достичь согласия, явно указывает на справедливость официальной позиции российской стороны, настаивающей на необходимости рассматривать проблемы международной информационной безопасности в разоруженческом аспекте. В то же время предметная область оказалась несколько суженной: в первоначальных российских инициативах говорилось об информации в целом (включая психику и сознание человека), а в предложении совместной российско-американской группы – только о киберпространстве (т.е. о сфере использования информационной техники).

Наряду с этим группа провела исследование, непосредственно затрагивающее вопросы межгосударственного противоборства в киберпространстве, а именно – применимость к нему положений Гаагских и Женевских конвенций[60]. Поскольку эти положения затрагивают прежде всего вопросы соблюдения международного гуманитарного права в условиях войны, то возможность применять их к киберпространству напрямую зависит от способности сторон провести всесторонний анализ кибервойны и кибероружия, параметры которых до сих пор недостаточно определены, а также провести аналогии с вооружениями, использование

[58] *Gorman S.* U.S. Back Talks on Cyber Warfare / Siobhan Gorman // The Wall Street Journal. 2011. June 4.

[59] *Rauscher K. F. Yaschenko V.* The Russia-U.S. Bilateral on Cybersecurity. Critical Terminology Foundations / Karl Frederick Rauscher, Valery Yaschenko ; EastWest Inst. ; Information Security Inst. of Moscow State Univ. 2011. April. Iss. 1. P. 18–41; *Rauscher K. F., Korotkov A.* Russia-U.S. Bilateral on critical infrastructure protection. Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace / Karl Rauscher, Andrey Korotkov ; The EastWest Inst. 2011. Iss. 1.

[60] *Rauscher K. F., Korotkov A.* Op. cit.

которых запрещено дополнительными протоколами 1977 г. к Женевской конвенции о защите гражданского населения во время войны.

Совместная работа российских и американских экспертов даёт надежду на то, что разработка общих подходов к проблематике международной информационной безопасности в целом и к ведению конфликтов в киберпространстве в частности возможна. Их деятельность создаёт фундамент для будущих двусторонних договорённостей, хотя рассчитывать на быстрое достижение консенсуса по всему спектру рассматриваемых вопросов, думается, не следует.

* *
*

Из проведённого анализа переговорного процесса легко сделать вывод, что существует значительное расхождение в подходах к обеспечению кибербезопасности, обсуждаемых в двустороннем российско-американском формате, и в том, как эта проблема интерпретируется в официальных документах США и НАТО. Учитывая, что в вопросах внешней политики и при ведении переговоров Соединённые Штаты всегда чётко придерживаются собственных документов, касающихся национальной безопасности, вполне возможно, что американцы не будут принимать во внимание имеющиеся экспертные наработки. Во всяком случае, российские инициативы о принятии конвенции по МИБ и правил поведения в информационном пространстве сталкиваются в ООН с противодействием США.

Несмотря на активизацию переговоров по вопросам информационной безопасности, трудно ожидать, что стороны в ближайшее время придут к консенсусу. Гораздо более вероятно, что Соединённые Штаты будут пытаться всячески продвигать свою модель кибернетической безопасности, а в случае отсутствия прогресса на переговорах возложат всю ответственность за происходящее на Россию, как это уже было в отношении европейской конвенции о киберпреступности. Под видом готовности обсуждать проблемы информационной безопасности и начать переговорный процесс по ограничению вооружений в информационной сфере Соединённые Штаты продвигают собственную модель информационной безопасности, стараясь закрепить за собой лидирующие позиции в мире.

Ключевые слова: *международная информационная безопасность – киберпространство – Россия – США – дипломатия.*

Keywords: *international information security – cyberspace – Russia – USA – diplomacy.*