ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ: КОНЦЕПЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ США И ЕЁ МЕЖДУНАРОДНАЯ СОСТАВЛЯЮЩАЯ

Е.В. Батуева

Московский государственный институт международных отношений (университет) МИД России. Россия, 119454, Москва, пр. Вернадского, 76.

Развитие информационно-коммуникационных технологий (ИКТ) и формирование глобального информационного пространства ставят по-новому вопросы обеспечения национальной и международной безопасности. Такие ключевые характеристики информационного пространства, как трансграничность, открытость, доступность, анонимность и сложность установления источника действий в сети обусловили рост акторов в информационном пространстве, а также привлекательность информационной инфраструктуры с точки зрения возможности использования ИКТ в военно-политических, преступных и террористических целях. Противодействие данным видам угроз стало важной составляющей комплекса мер по обеспечению информационной безопасности как на национальном, так и на глобальном уровне. США ведут разработку комплексной стратегии для киберпространства, включающую в себя как максимизацию преимуществ от использования ИКТ во всех стратегически важных областях, так и повышение уровня безопасности информационных систем и сетей страны. При этом на международной арене главной задачей США является обеспечение для себя максимально широких возможностей использования ИКТ для решения военно-политических задач.

США принимают самое активное участие в процессе формирования международной политико-правовой базы в области информационной безопасности и фактически являются единственной страной, представленной во всех региональных организациях, в повестку дня которых включены вопросы киберполитики. Такое широкое международное представительство даёт США возможность активно продвигать собственные инициативы, а также координировать международные усилия в данной области. При этом существует ряд причин, затрудняющих работу международного сообщества по формированию глобального режима информационной безопасности.

Ключевые слова: информационная безопасность, угрозы информационной безопасности, информационно-коммуникационные технологии, киберпреступность, кибертерроризм.

Развитие информационно-коммуникационных технологий (ИКТ) явилось катализатором многочисленных социальных, культурных, экономических и политических процессов как на национальном уровне, так и в глобальном масштабе. На смену индустриальной эпохе пришла постиндустриальная – информационная эпоха, в которой главную роль играют новые технологии и информация. В результате существенную трансформацию прошли как общество, так и государство: возникло общество нового типа – глобальное информационное общество, новый тип экономики – инновационная или информационная экономика, новая система управления государством – электронное правительство.

В связи с активным развитием сетевых технологий произошли существенные изменения в средствах и способах коммуникаций. Возникли «электронные магистрали»[1] глобального информационного обмена, в результате чего снизилось значение таких факторов, как пространство и время, при этом возросла роль многочисленных негосударственных акторов, которые получили возможность осуществлять свою деятельность в глобальном масштабе.

Наряду с позитивными изменениями, которые произошли в мире благодаря новым технологиям, возникли совершенно новые вызовы и угрозы в области безопасности, характерные для информационной эпохи. Широкое использование ИКТ повысило уровень зависимости функционирования государственных, коммерческих и гражданских институтов от стабильной работы информационной инфраструктуры. В свою очередь, на международном уровне глобальные информационные системы и сети стирают традиционные государственные границы, что ведёт к росту взаимозависимости государств в информационном пространстве.

США являются одним из ключевых акторов международных отношений, лидерами в области ИКТ, страной, где зародилась глобальная сеть Интернет. При этом, с одной стороны, технологический прогресс способствовал укреплению США как глобального лидера, а с другой – отсутствие барьера географического расстояния, сетезависимость, рост числа средств и методов осуществления информационных атак резко повысили степень уязвимости страны. Сегодня США занимают второе место в мире по числу пользователей Интернета после Китая [2]. При этом число инцидентов, связанных с компьютерными системами и сетями, в стране постоянно растёт. По данным американского центра реагирования на компьютерные происшествия (US-CERT), с 2006 по 2012 г. рост киберинцидентов составил 782%. За 2012 г. поступило 198 уведомлений об атаках на критическую инфраструктуру, большинство из которых (82) пришлись на сектор энергетики, также атакам подверглись предприятия сектора водоснабжения, химической и ядерной отрасли.

В докладе Комиссии по кибербезопасности для 44-го президента в 2008 г. прямо подчёркивается, что «неспособность Америки защитить киберпространство является одной из наиболее горящих проблем национальной безопасности, стоящих перед Администрацией» [3, с. 11]. А в 2013 г. впервые, согласно «Оценке глобальных угроз» разведывательного сообщества США, киберугрозы стали главным приоритетом национальной безопасности США, опередив угрозу номер один последней декады – терроризм [4].

Угрозы информационной безопасности США

Несмотря на масштаб «информационного бедствия», на государственном уровне в США не сложилось единого видения угроз кибербезопасности. Анализ показал, что федеральные министерства и ведомства рассматривают информационные угрозы и их источники, исходя из собственной компетенции. Так, Федеральное бюро расследований в своей деятельности исходит их трёх основных групп акторов, представляющих угрозу США в киберпространстве:

– *организованные криминальные группы*, которые в основном угрожают сектору финансовых услуг;

– *государства-спонсоры*, которые заинтересованы в краже данных, включая интеллектуальную собственность и научно-исследовательские разработки предприятий, государственных институтов и подрядчиков министерства обороны;

– *террористические группы*, заинтересованные в использовании сетевых технологий в целях проведения деструктивных действий в отношении критической инфраструктуры страны и тем самым представляющие угрозу национальной безопасности США [5].

Важно отметить, Соединённые Штаты признают, что государства заинтересованы далеко не только в краже интеллектуальной собственности и кибершпионаже, они также создают и используют потенциал, позволяющий перенести традиционные формы государственных конфликтов в киберпространство [6]. Министерство обороны США выделяет четыре ключевые угрозы кибербезопасности:

– *угрозы, исходящие от внешних акторов* (иностранные государства, криминальные группы);

– *угрозы от внутренних акторов* (инсайдеры);

– *угрозы, связанные с уязвимостью сети поставщиков*;

– *угрозы функциональной деятельности министерства* [7].

Министерство внутренней безопасности США относит кибератаки против данных и против физической инфраструктуры к верхне-

[1] Термин ввёл М. Кастельс. Подробнее см. [1].

му эшелону угроз национальной безопасности США [8]. Обобщая ведомственный подход США, можно вывести три ключевые группы информационных угроз: *использование ИКТ государствами в военно-политических целях, киберпреступность и кибертерроризм*, что, в свою очередь, соответствует видению информационных угроз большинства российских и зарубежных исследователей, представителей дипломатических и военных ведомств стран, участвующих в международном диалоге по вопросам обеспечения информационной безопасности.

Информационная безопасность VS, кибербезопасность

Глобальное информационное пространство превратилось в область сложных многоуровневых связей всех акторов мировой политики, в рамках которых зачастую происходит столкновение интересов участников. При этом ИКТ являются технологиями двойного назначения, которые могут быть использованы как в рамках закона, так и в злонамеренных целях, что обуславливает рост числа информационных угроз, трансграничный характер которых требует поиска решений и выработки мер противодействия им не только на национальном, но и на международном уровне. Одной из проблем, обуславливающих сложность развития диалога по вопросам обеспечения международной информационной безопасности (МИБ), является проблема определений. Страны по-разному толкуют и определяют границы информационной безопасности.

В Российской Федерации под информационной безопасностью понимается состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [9]. При этом обеспечение информационной безопасности охватывает как информационно-технологические, так и информационно-психологические аспекты. В США чаще принято использовать термин «кибербезопасность», под которым понимается обеспечение безопасности информации (как в электронном, так и материальной виде), а также систем и сетей, в которых она хранится, обрабатывается и передаётся [10, с. 7]. В понимании США кибербезопасность не включает вопросы информационной и коммуникационной политики как не связанные с национальной безопасностью или защитой инфраструктуры, то есть охватывает исключительно технологические аспекты.

Такая позиция, в частности, объясняется активным использованием Соединёнными Штатами «мягкой силы», направленной на оказание информационного воздействия на конкурирующие государства, политическую, экономическую и социальную сферы жизни общества, в целях обеспечения собственного влияния и доминирования на мировой арене.

Американская повестка дня для международного сообщества по вопросам кибербезопасности

На международной арене США ведут диалог по вопросам информационной безопасности начиная с 1992 г. Внешнеполитическую линию США по данному направлению можно условно разделить на два ключевых периода – «Клинтон–Буш» и «Обама». В период администраций Билла Клинтона и Дж. Буша-мл. США уделяли большое внимание повышению уровня безопасности критической инфраструктуры и продвижению культуры информационной безопасности. При этом в качестве ключевых угроз международной информационной безопасности США выделяли исключительно криминальное использование ИКТ, а после событий 2001 г. список угроз пополнился кибертерроризмом.

Площадками для изучения вопросов противодействия угрозам информационной преступности и кибертерроризма стали ОБСЕ, «Большая восьмёрка», второй и третий комитеты ООН. На их полях США выступали с инициативами по созданию эффективных международных механизмов обмена информацией и сотрудничества при проведении расследований нарушений, связанных с использованием Интернета, усовершенствованию законодательной базы государств в области компьютерных правонарушений и её гармонизации. Одним из ключевых для США направлений по выработке международного законодательства стала работа над конвенцией Совета Европы о киберпреступности, подписанная странами-членами в Будапеште в 2001 г. и содержащая руководящие принципы для национальных законодательных систем и межгосударственного сотрудничества в сфере деятельности правоохранительных органов.

Будапештская конвенция является базовым документом, лежащим в основе западных подходов к вопросам киберпреступности и первой попыткой международно-правовой классификации уголовных преступлений в информационной сфере. Однако применение ряда её положений (в частности, пункта “b” статьи 32 о трансграничном доступе к компьютерным данным[2]) может нанести ущерб суверенитету и национальной безопасности государств-участников. Фактически эти положения санкционируют иностранные правоохранительные органы без уведомления проводить расследования на территории государств-участников конвенции. Существенным недостатком конвенции является и то, что она уже не соответствует времени. Документ не содержит норм, криминализирующих кибертерроризм и формы его проявления,

[2] Согласно данному пункту Конвенции, Сторона может получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным.

а также не учитывает возможность осуществления кибератак в целях шпионажа или в военно-политических целях, что подчёркивает его определённую однобокость.

Несмотря на это, США продолжают продвигать конвенцию в качестве основополагающей базы по борьбе с киберпреступностью, отрицая какую-либо необходимость в новом международном документе. Параллельно с американскими инициативами российская сторона с 1998 г. выступает за комплексное рассмотрение угроз информационной безопасности, включая использование ИКТ в военно-политических, криминальных и террористических целях. Данный подход нашёл своё воплощение в Резолюции Первого комитета ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», которая с каждым годом получает всё большую поддержку (в 2013 г. достигнуто рекордное число соавторов российской резолюции – более 40 стран).

Стоит отметить, что вплоть до 2009 г. США пытались всячески размыть военно-политическую компоненту. Изначально США предлагали перенести рассмотрение вопросов информационной безопасности во Второй (по экономическим и финансовым вопросам) и Шестой (по правовым вопросам) комитеты ООН. В 2001 г. Соединённые Штаты и их союзники фактически заблокировали работу первой Группы правительственных экспертов по международной информационной безопасности (ГПЭ по МИБ), которая не смогла прийти к единому видению вопросов информационной безопасности и выработать общий документ. Далее, с 2005 по 2008 г. США голосовали против российского проекта резолюции по МИБ. При этом на национальном уровне в период с 1998 по 2008 г. США активно создавали механизмы защиты критической инфраструктуры, информационных систем и сетей, а также вели разработку стратегии по ведению информационных войн и информационных операций в целях обеспечения глобального информационного превосходства. Таким образом, политика сдерживания диалога по военно-политической составляющей была призвана выиграть время для формирования национальной комплексной стратегии для киберпространства.

С началом президентства Барака Обамы «перезагрузка» коснулась переговоров по вопросам МИБ. Ещё на этапе предвыборной гонки Б. Обама выделял в качестве основных угроз национальной безопасности использование ядерного и биологического оружия, а также кибератаки [11]. Победив на выборах, он взял курс на пересмотр внешней политики США в области обеспечения информационной безопасности. Так, была поставлена задача активизировать международный диалог по вопросам «киберповестки дня» и обеспечить в нём лидирующую позицию США. При этом Центром стратегических и международных исследований рекомендовалось уделить особое внимание отношениям с такими потенциальными оппонентами, как Россия и Китай [3].

Смена политического руководства Соединённых Штатов и изменения стратегического характера, произошедшие в киберполитике страны, непосредственно повлияли на ход дискуссии в рамках Первого комитета ООН. По итогам работы второй ГПЭ по МИБ 2009–2010 гг. был подготовлен доклад, который содержит комплексное видение угроз (использование ИКТ в преступной и террористической деятельности, а также в качестве инструментов ведения войны, разведки и в политических целях) и их источников (преступные элементы, террористы и государства, а также физические лица, группы и организации, которые выполняют посреднические функции в осуществлении подрывной сетевой деятельности от имени других). Кроме того, эксперты отметили необходимость дальнейшей выработки международных норм и совместных механизмов, а также общей терминологии, до сих пор являющейся камнем преткновения в международном диалоге [12].

Третья ГПЭ ООН по МИБ 2012–2013 гг. совершила важный шаг вперёд, приняв компромиссный документ, в котором учтены как формулировки США об общей применимости действующих норм международного права (в частности, Устава ООН) к поведению государств в информационном пространстве, так и российской стороны, которая заложила положение о возможности разработки необходимых новых норм, правил и принципов ответственного поведения государств [13]. Следующая, четвёртая ГПЭ продолжит работу по заданным направлениям в 2014 г.

Несмотря на позитивные подвижки в позиции США в рамках ГПЭ по МИБ, они не готовы присоединиться к двум другим российским инициативам по вопросам обеспечения МИБ, которые, в отличие от необязательных решений Группы экспертов, представляют собой проекты международных политико-правовых документов. В 2011 г. российская сторона вместе с партнёрами по ШОС – Китаем, Казахстаном и Узбекистаном – вышли с предложением принять в рамках ООН «Правила поведения в области обеспечения международной информационной безопасности», что способствовало бы формированию основы для международных норм и правил, регулирующих действия государств в информационном пространстве.

В проекте одиннадцать правил охватывают основные аспекты обеспечения информационной безопасности. В частности, они обязывают государства:

– не использовать ИКТ для осуществления враждебных действий, актов агрессии, создания угроз международному миру и безопасности или распространения информационного оружия;

– сотрудничать в борьбе с преступной или террористической деятельностью с использованием ИКТ;

– обеспечивать безопасность на всех этапах поставок продукции и предоставления услуг в сфере ИКТ [14].

Важно отметить, что данная инициатива была выдвинута сразу после принятия Соединёнными Штатами «Международной стратегии для киберпространства» 2011 г., в которой США оставляют за собой право ответных действий на кибератаки с использованием всех доступных средств, включая военные. США выступили с заявлением о нерелевантности положений «Правил поведения государств», подчеркнув, что в документе предлагается заменить существующие нормы международного права, регулирующие вопросы применения силы и отношения между государствами во время вооружённых конфликтов, новыми, не в полной мере определёнными правилами и концепциями [15].

Очевидно, подход США к предложенным правилам поведения можно также экстраполировать на концепцию конвенции ООН «Об обеспечении международной информационной безопасности», представленную Россией в сентябре 2011 г. в ходе Второй Международной встречи высоких представителей в г. Екатеринбурге. Положения концепции конвенции направлены, в частности, на предотвращение возможной гонки информационного вооружения и милитаризации информационного пространства в целом, а также на недопущение господства какого-либо государства в информационном пространстве, что не соответствует интересам США и идёт в противовес проводимой США политике в области кибербезопасности.

Борьба за лидерство в переговорном процессе по МИБ

Занимая жёсткую позицию в отношении российских проектов, США одновременно понимают, что простым выступлением «против» они не смогут добиться существенных выгод для себя, так как число сторонников российских инициатив постоянно растёт. В этой связи США попытались укрепить свои позиции в формате НАТО, а также активизировали двусторонние отношения с Москвой и Пекином по вопросам кибербезопасности. НАТО для США является удобной платформой для продвижения наработок в области ведения информационных операций и кибервойны, а также для укрепления внутренних мер по обеспечению безопасности критической инфраструктуры. О киберугрозах в НАТО говорят с 2002 г., когда в документах Пражского саммита была подчёркнута важность повышения обороноспособности для противостояния кибератакам. Серьёзным толчком к развитию данной темы стали кибератаки на Эстонию в 2007 г., в результате чего в 2008 г. впервые была принята «Политика НАТО в области кибероборонны».

В «Стратегической концепции НАТО для обороны и безопасности» 2010 г. отмечается, что альянс предпримет все необходимые меры, включая на национальном уровне государств-членов, для предотвращения, обнаружения и защиты от кибератак, а также восстановления после них. В этих целях предусмотрено координирование национальных усилий в области кибербезопасности, включение киберзащиты в оборонительные планы, обеспечение централизованной киберзащиты всех военных и гражданских структур НАТО [16]. О важности вопросов кибербезопасности для альянса говорит и тот факт, что в обновлённой версии «Политики НАТО в области кибероборонны» 2011 г. действие ст. 5 распространяется на киберугрозы. Подчёркивается, что НАТО будет оказывать широкую поддержку союзникам и партнёрам в целях предотвращения и противодействия кибератакам, а также помощь странам, подвергнувшимся атакам в восстановлении критически важных информационных систем[3] [17].

Распространение ст. 5 Вашингтонского договора на кибератаки оставляет открытым вопрос, какого именно масштаба атаки могут повлечь активацию механизмов коллективной обороны. И хотя Ст. 5 была задействована лишь однажды (после террористических атак на США в сентябре 2001 г.), данная инициатива закладывает опасный потенциал и может спровоцировать эскалацию конфликта в случае некорректной оценки киберугрозы и источника кибератаки. В целом за последние годы альянс существенно продвинулся в вопросах кибербезопасности во многом благодаря американским инициативам. Стоит отметить, что формат сотрудничества Россия–НАТО, несмотря на предложения российской стороны, не предусматривает обсуждения вопросов кибербезопасности.

С точки зрения двустороннего диалога наибольший интерес для США представляют Россия и Китай – страны, обладающие конкурентоспособным киберпотенциалом, который может представлять угрозу кибербезопасности США, а также являющиеся ключевыми игроками в переговорном процессе по обеспечению МИБ, чья позиция по целому ряду вопросов идёт вразрез с подходом Соединённых Штатов. Так, в отношениях с Россией наметился положительный сдвиг. Успехи, достигнутые в рамках ООН, были подкреплены реальными договорённостями о сотрудничестве. 17 июня 2013 г. по итогам встречи на полях саммита «Группы восьми» президенты Российской Федерации и Соединённых Штатов Америки выступили с совместным заявлением о новой области сотрудничества в укреплении доверия.

Впервые за всю историю многосторонних и двусторонних отношений были достигнуты три ключевые договорённости, формирующие

[3] Сам документ является закрытым. Информация о нём содержится в ряде официальных релизов на сайте НАТО. См. [17].

комплексную систему мер доверия между Россией и США в киберпространстве. Принятые документы предполагают организацию каналов прямой связи между:

– группами оперативного реагирования на компьютерные инциденты в целях создания механизма обмена информацией для обеспечения более эффективной защиты критически важных информационных систем;

– центрами по уменьшению ядерной опасности для содействия обмену срочными сообщениями, которые могут снизить риск недопонимания, эскалации и конфликта;

– должностными лицами высокого уровня по вопросам урегулирования потенциально опасных ситуаций, вызываемых событиями, которые могут создавать угрозы безопасности в сфере использования ИКТ и самим ИКТ.

Кроме того, было принято решение о создании в рамках российско-американской Президентской комиссии двусторонней рабочей группы по вопросам угроз в сфере использования ИКТ и самим ИКТ в контексте международной безопасности, которая будет встречаться на регулярной основе для дальнейшей координации и развития сотрудничества в данной сфере [18]. Достигнутые договорённости закладывают солидный фундамент для развития двустороннего сотрудничества по вопросам кибербезопасности. Как представляется, данная российско-американская формула сотрудничества может в дальнейшем служить в качестве модели двустороннего и многостороннего взаимодействия по противодействию угрозам в киберпространстве с другими странами.

На полях ОБСЕ в декабре 2013 г. Постоянный совет ОБСЕ одобрил прорывной по своей сути документ «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью снижения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий». Разработка данного документа стала возможна благодаря уже достигнутым между ключевыми игроками США и РФ договорённостям по вопросам укрепления мер доверия в киберпространстве. Это важный первый шаг международного сообщества в сторону повышения транспарентности, предсказуемости и стабильности в киберпространстве. Дальнейшая работа над перечнем мер будет продолжена.

Согласно официальной позиции США, именно Китай представляет наибольшую угрозу не только информационной безопасности Соединённых Штатов, но и экономической, и в целом национальной безопасности [19]. При этом Китай является важнейшим для США экономическим партнёром – 40% всего технологического импорта США обеспечивается Китаем. Несмотря на низкий уровень доверия между странами, которые на регулярной основе подвергаются кибератакам со стороны друг друга, для США принципиально важно найти точки соприкосновения с Китаем и двигаться к выработке совместных договоренностей в области кибербезопасности. В июле 2013 г. состоялась первая встреча двусторонней группы по кибербезопасности, работа которой будет направлена на разработку мер укрепления доверия и правил поведения государств в киберпространстве. Особое внимание будет уделено вопросам кибершпионажа и краже интеллектуальной собственности. Первые совместные шаги в данном направлении страны уже сделали в рамках ГПЭ ООН по МИБ 2012–2013 гг.

Принимая во внимание роль Китая в Азиатско-Тихоокеанском регионе, США заинтересованы в том, чтобы сбалансировать киберпотенциал КНР. В этой связи они развивают и модифицируют договорённости о коллективной обороне с учётом вопросов кибербезопасности с Австралией, Японией и Южной Кореей. Также США активно продвигают идею выработки мер по укреплению доверия в рамках такого представительного форума, как Региональный форум Ассоциации государств Юго-Восточной Азии (АРФ). Кроме того, в задачи США входит активная работа с такими интернет-державами, как Бразилия, Южная Африка и Индия (страны БРИКС), которые во многом поддерживают подход России и Китая к обеспечению информационной безопасности.

В целом США проводят серьёзную дипломатическую работу со всеми ключевыми игроками в киберпространстве, с тем чтобы заручиться их поддержкой при продвижении собственных инициатив. Однако, как представляется, будущий глобальный порядок в такой крайне чувствительной сфере, как киберпространство, во многом будет определяться развитием отношений США с Россией и Китаем.

Краткие итоги

Несмотря на то что на международном уровне по-прежнему сохраняются принципиальные разногласия по вопросам правового регулирования сферы кибербезопасности, наметившийся сдвиг в позиции нынешнего руководства Соединённых Штатов и включение в многосторонний переговорный процесс по всему комплексу вопросов МИБ является положительным сигналом. США отошли от политики блокирования инициатив оппонентов. Новым курсом стала выработка переговорной линии и повестки дня с крупными игроками в сфере информационной безопасности.

Сегодня можно говорить о том, что США не ставят перед собой задачу выработать международный правовой режим безопасности в киберпространстве, так как заинтересованы максимально долго сохранять свободу действий и использовать информационное пространство в военно-политических целях, тем самым обеспечивая своё глобальное лидерство. Тем не менее тот факт, что даже самые технологически развитые страны, такие, как США, признали

невозможность обеспечения информационной безопасности в одностороннем порядке, свидетельствует о том, что международное сообщество будет продолжать двигаться по пути выработки глобального режима обеспечения международной информационной безопасности.

Список литературы

1. Castells M. The Rise of Network Society. The Information Age: Economy, Society and Culture, 1996, Vol. 1. Wiley, 2000. 594 p.
2. Internet World Stats. Usage and Population Statistics. Режим доступа: http://www.internetworldstats.com/top20.htm (дата обращения: 10.12.2013).
3. Securing Cyberspace for the 44th Presidency. Center for Strategic and International Studies. Washington D.C., December 2008. Режим доступа: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (дата обращения: 12.12. 2013).
4. Clapper J.R. Worldwide Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence, March 12, 2013, p. 1. Режим доступа: http://www.intelligence.senate.gov/130312/clapper.pdf (дата обращения: 14.12.2013).
5. The Cyber Threat. On the Front Lines with Shawn Henry. Federal Bureau of Investigation, March 27, 2012. Режим доступа: http://www.fbi.gov/news/stories/2012/march/shawn-henry_032712 (дата обращения: 16.12.2013).
6. Доклад Генерального секретаря. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Документ ГА ООН A/66/152, 15.07.2011, с. 19-20. Режим доступа: http://www.un.org/Docs/journal/asp/ws.asp?m=A/66/152 (дата обращения: 10.12.2013).
7. Department of Defense Strategy for Operating in Cyberspace. Washington D.C.: U.S. Department of Defense, July 2011, p. 3.
8. The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation. Department of Homeland Security, December 2011. Режим доступа: http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf (дата обращения: 16.12.2013).
9. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. // Российская газета. 28.09.2000. № 187.
10. Joint Terminology for Cyberspace Operations. Washington. D.C.: Department of Defense. Режим доступа: http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf (дата обращения: 16.12.2013).
11. Johnson, Glen. Obama warns against "fighting the last war". USA Today, July 16, 2008. Режим доступа: http://www.usatoday.com/news/politics/2008-07-16-2873054939_x.htm (дата обращения: 16.12.2013).
12. Записка Генерельного секретаря ООН. Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Документ A/65/201, 30.07.2010. Режим доступа: http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=R (дата обращения: 17.12.2013).
13. Записка Генерального секретаря ООН. Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Документ A/68/98, 24.06.2013, Раздел III. Режим доступа: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=http://www.un.org/disarmament/sgreports/68/&Lang=R (дата обращения:17.12.2013).
14. Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 г. на имя Генерального секретаря ООН. Документ A/66/359. Режим доступа: http://www.un.org/Docs/journal/asp/ws.asp?m=A/66/359 (дата обращения: 17.12.2013).
15. Statement by the Delegation of the United States of America, to the Other Disarmament Issues and International Security Segment of Thematic Debate, in the First Committee of the Sixty-seven Session of the United Nations General Assembly. New York, November 1, 2012. Точка доступа: http://geneva.usmission.gov/2012/11/23/us-first-committee/ (дата обращения: 17.12.2013).
16. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation. Lisbon, November 19, 2010. Режим доступа: http://www.nato.int/cps/en/SID-14EF0623-198FC77E/natolive/official_texts_68580.htm (дата обращения: 18.12.2013).
17. New threats: the cyber-dimention. NATO Review Magazine. Точка доступа: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm (дата обращения 18.12.2013).
18. Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия. 17.06.2013. Точка доступа: http://news.kremlin.ru/ref_notes/1479 (дата обращения: 18.12.2013).

19. The National Military Strategy of the United States of America "Redefining America's Military Leadership". Washington D.C.: Department of Defense, February 8, 2011, p.3; Mandiant Intelligence Center Report. APT1: Exposing One of China's Cyber Espionage Units. Режим доступа: http://intelreport.mandiant.com (дата обращения: 20.12.2013).

Об авторе

Батуева Елена Владимировна – аспирант кафедры мировых политических процессов МГИМО(У) МИД России. E-mail: Ebatueva@gmail.com

VIRTUAL REALITY: U.S. INFORMATION SECURITY THREATS CONCEPT AND ITS INTERNATIONAL DIMENSION

E.V. Batueva

Moscow State Institute of International Relations (University), 76 Prospect Vernadskogo, Moscow, 119454, Russia

Abstract: *The development of ICT and the formation of the global information space changed the agenda of national and international security. Such key characteristics of cyberspace as openness, accessibility, anonymity, and identification complexity determined the rise of actors in cyber space and increased the level of cyber threats. Based on the analyses of the U.S. agencies' approach, the author defines three major groups of threats: use of ICT by states, criminals and terrorists. This concept is shared by the majority of the countries involved in the international dialogue on information security issues and is fundamental for providing cyber security policy on both national and international levels.*

The United States is developing a complex strategy for cyber space that includes maximization of ICT's advantages in all strategically important fields as well as improvement of national information systems and networks security.

On the international level the main task for the American diplomacy is to guarantee the U.S. information dominance. The United States is the only country that takes part practically in all international and regional fora dealing with cyber security issues. However process of the development of a global cyber security regime is not going to be fast due to countries' different approaches to key definitions and lack of joint understanding of cyber security issues as well as due to the position of the countries, among all the United States, that are not interested in any new obligatory international norms and principles. Such American policy aims at saving the possibility of using cyberspace capacity in reaching political and military goals, thus keeping the global leadership.

Key words: information security, information security threats, cyber security threats, ICT, cyber crime, cyber terrorism.

References

1. Castells M. The Rise of Network Society. The Information Age: Economy, Society and Culture, 1996, Vol. 1. Wiley, 2000. 594 p.
2. Internet World Stats. Usage and Population Statistics. Available at: http://www.internetworldstats.com/top20.htm (accessed: December 10, 2013)
3. Securing Cyberspace for the 44th Presidency. Center for Strategic and International Studies. Washington D.C., December 2008. Available at: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (accessed: December 12, 2013)
4. Clapper J.R. Worldwide Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence, March 12, 2013, p. 1. Available at: http://www.intelligence.senate.gov/130312/clapper.pdf (accessed: December 14, 2013)
5. The Cyber Threat. On the Front Lines with Shawn Henry. Federal Bureau of Investigation, March 27, 2012. Available at: http://www.fbi.gov/news/stories/2012/march/shawn-henry_032712 (accessed: December 16, 2013)
6. Report of the Secretary-General. Developments in the field of information and telecommunications in the context of international security. Document UNGA A/66/152, 15 July 2011, p. 16. Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/66/152 (accessed: December 10, 2013)

7. Department of Defense Strategy for Operating in Cyberspace. Washington D.C.: U.S. Department of Defense, July 2011, p. 3.
8. The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation. Department of Homeland Security, December 2011. Available at: http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf (accessed: December 17, 2013)
9. Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii ot 9 sentiabria 2000 g. [Information Security Doctrine of the Russian Federation from September 9, 2000] Rossiiskaia gazeta [Russian newspaper], 28 sentiabria 2000 g., № 187. (in Russian)
10. Joint Terminology for Cyberspace Operations. Washington. D.C.: Department of Defense. Available at: http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf (accessed: December 16, 2013)
11. Johnson, Glen. Obama warns against "fighting the last war". USA Today, July 16, 2008. Available at: http://www.usatoday.com/news/politics/2008-07-16-2873054939_x.htm (accessed: December 16, 2013)
12. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Document A/65/201, 30 July 2010. Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201 (accessed: December 17, 2013)
13. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Document A/68/98, 24 June 2013, Section III. Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 (accessed: December 17, 2013)
14. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. Document A/66/359. Available at: http://www.un.org/Docs/journal/asp/ws.asp?m=A/66/359 (accessed: December 17, 2013)
15. Statement by the Delegation of the United States of America, to the Other Disarmament Issues and International Security Segment of Thematic Debate, in the First Committee of the Sixty-seven Session of the United Nations General Assembly. New York, November 1, 2012. Available at: http://geneva.usmission.gov/2012/11/23/us-first-committee/ (accessed: December 17, 2013)
16. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation. Lisbon, November 19, 2010. Available at: http://www.nato.int/cps/en/SID-14EF0623-198FC77E/natolive/official_texts_68580.htm (accessed: December 18, 2013)
17. New threats: the cyber-dimention. NATO Review Magazine. Available at: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm (accessed: December 18, 2013)
18. Sovmestnoe zaiavlenie prezidentov Rossiiskoi Federatsii i Soedinennykh Shtatov Ameriki o novoi oblasti sotrudnichestva v ukreplenii doveriia [Joint statement of the Presidents of the Russian Federation and the United States of America on the new sphere of cooperation in confidence building]. 17.06.2013. Available at: http://news.kremlin.ru/ref_notes/1479 (accessed: December 18, 2013) (In Russian)
19. The National Military Strategy of the United States of America "Redefining America's Military Leadership". Washington D.C.: Department of Defense, February 8, 2011, p.3; Mandiant Intelligence Center Report. APT1: Exposing One of China's Cyber Espionage Units. Available at: http://intelreport.mandiant.com (accessed: December 20, 2013)

About the author

Batueva Elena Vladimirovna – graduate student of chair of world political processes of MGIMO(U) MFA of Russia.
E-mail: ebatueva@gmail.com