МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Елена Зиновьева*

Развитие информационных и коммуникационных технологий (ИКТ) играет важнейшую роль для экономического и социально-политического развития как каждой страны в отдельности, так и человечества в целом. Однако развитие ИКТ не только создает воможности для роста и равития, но и порождает угрозы международной и национальной безопасности. Межгосударственное противоборство, перешедшее в информационную сферу, чревато конфликтами, крайней формой проявления которых могут стать информационные войны.

В настоящее время открываются новые возможности формирования глобального режима международной информационной безопасности. Автор приходит к выводу, что опыт международного сотрудничества по обеспечению безопасности в иных высокотехнологичных областях, таких как космос, может быть продуктивно использован в отношении глобальной информационной сферы.

Вызовы и угрозы международной информационной безопасности на современном этапе

Развитие информационных и коммуникационных технологий (ИКТ) играет важнейшую роль для экономического и социально-политического развития как каждой страны в отдельности, так и человечества в целом. Однако развитие ИКТ не только создает воможности для роста и равития, но и порождает угрозы международной и национальной безопасности. Межгосударственное противоборство, перешедшее в информационную сферу, чревато конфликтами, крайней формой проявления которых могут стать информационные войны.

В последние годы существенно увеличилось количество деструктивных информационных атак, совершаемых с использованием современных информационно-коммуникационных технологий, причем подобные атаки становятся все сложнее. В ближайшей перспективе объектами их воздействия будут не только информационные ресурсы в сети Интернет, но и критически важные объекты инфраструктуры государств, обеспечивающие функционирование промышленности, транспорта, энергетики и других сфер жизнедеятельности. В докладе Группы правительственных экспертов ООН от 2010 г. указано, что глобальное информационное пространство становится ареной разрушительных действий и что киберугрозы становятся одним из важнейших вызовов 21 века [1]. Резолюции Генеральной Ассамблеи ООН подчеркивают национальную ответственность за обеспечение информационной безопасности на уровне национальных государств [2].

* Зиновьева Елена Сергеевна, кандидат политических наук, доцент кафедры мировых политических процессов МГИМО(У) МИД России

Несмотря на значимость таких угроз, как информационный терроризм и информационная преступность, исследователи полагают, что наибольшую опасность представляет столкновение государств с использованием информационного оружия [3]. Многие страны разрабатывают национальные стратегии по обеспечению безопасности критических информационных инфраструктур, а также ведут работы по созданию как оборонительного, так и наступательного информационного потенциала.

После того, как стало известно о таких супервирусах, как Stuxnet, Flame, Duqu и Gauss, эксперты заявили, что технически сложные и достаточно эффективные системы кибершпионажа широко используются государствами[3]. Военные теоретики высказывают предположение, что информационное пространство становится «пятым полем боя», наряду с землей, морским и воздушным пространством, космосом [4].

Однако есть и более осторожные оценки. Американский политолог, автор концепции «мягкой власти», Д. Най полагает, что информационные технологии, прежде всего, гражданский потенциал в особенности значимы для реализации внешней политики государств. Данный автор выделяет пределяет следующие характеристики информационной сферы, значимые для мировой политики: «низкая стоимость, анонимность, ассиметрия в уязвимости, что позволяет относительно слабым акторам иметь больше возможностей применять жесткую и мягкую силу в киберпространстве, чем в иных традиционных областях мировой политики» [5. P. 1].

Информационное пространство по своей природе транснационально, информационные вызовы и угрозы не ограничиваются пределами отдельных государств. Для обеспечения международной информационной безопасности необходимо сотрудничество, опирающееся на нормы международного права при учете особенностей цифровой среды. Поиск путей предотвращения злонамеренного использования как государствами, так и террористическими и иными преступными организациями ИКТ, способного привести к нарушению международного мира и безопасности, является одним в последние годы из трендов дискуссий политиков, ученых и специалистов в данной области.

Одной из проблем, стоящих на пути наращивания международного взаимодействия и сотрудничества, а также выработки международно-правовых норм в области информационной безопасности является отсутствие консенсуса относительно терминологии. В настоящее время на международном уровне нет единства мнений относительно терминологии— ведутся дискуссии между государствами, придерживающимися различных толкований понятия «международная информационная безопасность». Россия выступает за широкий подход к определению содержания понятия «международная информационная безопасность», включая в нее как технические аспекты (безопасность информационных сетей и систем), так и обширный круг политико-идеологических аспектов (манипулирование информацией, пропаганда посредством глобальных информационных сетей, информационное воздействие). Страны Запада, прежде всего США, придерживаются узкого подхода, ограничиваясь техническими аспектами, и используют иную терминологию — «кибер-безопасность».

В документах ГА ООН международная информационная безопасность трактуется, прежде всего, исходя из характера угроз. Традиционно выделялась «триада угроз» международной информационной безопасности — использование ИКТ в террористических, преступных и военно-политических целях (под военно-политическими целями понимается использование ИКТ в межгосударственных конфликтах). В частности, подобный подход к определению угроз был закреплен в ряде резолюций ГА ООН, посвященных проблематике информационной безопасности [2].

Россия в 2013 году в документе Основы государственной политики в области международной информационной безопасности на период до 2020 года добавила к триаде угроз опасность вмешательства во внутренние дела суверенного государства посредством ИКТ, нарушение общественной стабильности, разжигание межэтнической, межнациональной розни [6]. По сути, это стало реакцией России на события «арабской весны», когда социальные сети и блоги активно использовались для координации протестного движения.

В международно-правоых документах отстуствуют также международно-признанные определения понятий «информационная война», «информационное оружие». Изучение признаков информационной войны и выработка общепризнанного определения необходи-

мы еще и в силу того, что злонамеренное использование ИКТ для разрешения межгосударственных противоречий силовым способом обладает рядом особенностей, затрудняющих его правовую регламентацию и препятствующих международному сотрудничеству:

- отсутствие «предвоенного» периода и, следовательно, невозможность определения начала «силовых действий» военного характера;

- трансграничность, то есть возможность осуществления, по существу, агрессивных силовых действий на основе злонамеренного использования ИКТ в отношении противника без нарушения границ его территории;

- ИКТ сами по себе не являются оружием, что создает сложности с точки зрения классификации той или иной «атаки», осуществленной с использованием ИКТ, в качестве вооруженного нападения.

Специфика ИКТ не отменяет того факта, что достижение с помощью любой войны, в том числе информационной, целей завоевания или поражения противника противоречит Уставу ООН, принципу суверенного равенства государств.

Несмотря на то, что многие из терминологических вопросов, касающиеся информационного противоборства, до сих пор не разрешены, международные дискуссии о будущих вызовах в сфере информационной безопасности, а также возможных политических, юридических и технических мерах по их преодолению уже начались. Различные подходы к оценке угроз государствами, а также подходы к обеспечению безопасности препятствуют развитию глобального режима международной информационной безопасности. Не существует также согласия относительно того, какую роль должны играть региональные и глобальные международные организации и институты. Однако международное сообщество приходит к пониманию того, что предотвращение конфликта как в информационной сфере, так и спровоцированного информационным противоборством, требует международного сотрудничества.

Проблемы применимости международного права к информационной сфере

В настоящее время использование информационных технологий в военно-политических целях лишь в ограниченной степени попадает в сферу действия норм международного права. Все более актуальной становится адаптация международного права к особенностям информационной сферы. Так, не существует международно-правовых актов, определяющих компьютерные атаки в качестве акта вооруженного нападения. Все установленные международно-правовые принципы, касающиеся таких понятий как «применение силы», «акт агрессии», «вооруженное нападение» предусматривают наличие оружия и его применение, в частности, определенный уровень физического ущерба или захвата территории государства, в отношении которого было произведено нападение. ИКТ сами по себе не являются оружием, они представляют собой преобразование по определенному алгоритму данных, представленных в цифровом виде, что не наблюдаемо с помощью органов чувств человека.

В этих условиях необходима адаптация норм права, чтобы компьютеры и программные коды можно было классифицировать как системы вооружения. Термин «информационное оружие» используется в ряде международных документов, принятых в рамках ШОС и СНГ [7]. Например, согласно ст. 1 Соглашения между Правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16.07.2009 главной угрозой международной информационной безопасности является «разработка и применение информационного оружия, подготовка и ведение информационной войны», ее признаками являются «... воздействие на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться пред лицом агрессора и не может воспользоваться законным правом самозащиты, нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах, деструктивное воздействие на критически важные структуры» [7]. Подобный подход может быть использован международным сообществом в качестве основы для выработки общепризнанного определения информационного оружия.

Анонимность ИКТ и, как следствие, сложность идентификации агрессора могут привести к приписыванию факта при-

менения силы государству, чьи информационные системы были использованы для осуществления атаки без уведомления. Как представляется, использование территории третьего государства без его ведома с целью осуществления информационной атаки влечет за собой его вовлечение в конфликт, но не перенесение на него ответственности за агрессию. Необходима выработка соответсвующих международно-правовых норм и мер доверия, что предполагает интенсификацию международного взаимодействия государств и перевод его на новый, более высокий уровень сотрудничества в области информационной безопасности.

Проникновение ИКТ во все сферы жизни общества и государства ставит задачу поиска оптимального баланса между безопасностью и свободой, правом на доступ к информации и ответственностью государств за действия в глобальном информационном пространстве. Согласно Докладу Группы правительственных экспертов ООН по международной информационной безопасности государственные усилия по обеспечению информационной безопасности должны идти рука об руку с защитой прав человека и фундаментальных свобод [1: P. 2]. Кибер-шпионаж, покушение государства на частную жизнь пользователей интернета (о чем стало известно в результате разоблачений Э. Сноудена) представляют собой реальную угрозу информационной безопасности

Информационные технологии - «движущаяся мишень», они настолько динамичны, что правовые нормы не всегда «успевают» адекватно отразить новую информационную реальность. Тем не менее, это не отменяет регламентацию межгосударственных отношений нормами международного публичного права. В то же время многие из его положений были разработаны применительно к традиционным войнам и требуют доработки, если не по духу, то по форме. Недостаточность международно-правовой базы затрудняет развитие и углубление международного сотрудничества.

Вместе с тем, несмотря на специфические характеристики ИКТ, вытекающие из Устава ООН общепризнанные принципы международного права jus cogens и соответствующие нормы международного права, а именно невмешательство во внутренние дела государств и неприменение силы и угрозы силой остаются незыблемыми как в традиционном, физическом, так и в новом, цифровом пространстве.

Российский подход к обеспечению международной информационной безопасности

С 1998 г. Россия инициативно выступает за развитие международного сотрудничества в области обеспечения информационной безопасности как на региональном, так и на глобальном уровне, а также за адаптацию международного права к особенностям информационной сферы.

Россией были достигнуты договоренности о сотрудничестве по международной информационной безопасности со странами ШОС, Белоруссией, Кубой. В 2013 году был заключен ряд важных договоренностей с США, направленных на формирование мер укрепления доверия в глобальном информационном пространстве. По инициативе России проблематика международной информационной безопасности рассматривалась на высоком политическом уровне и многосторонней основе, в рамках ОБСЕ, ШОС, ОДКБ, Международного союза электросвязи (МСЭ), в ходе Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), в рамках СНГ и Регионального содружества в области связи (РСС). Работа также ведется «на полях» таких форумов, как «Группа восьми», «Группа двадцати», БРИКС. В официальных документах названных международных форумов и организаций были закреплены положения о наличии угроз для международной информационной безопасности и о необходимости международного сотрудничества в данной области.

Россия исходит из потребности выработки определенных правил поведения государств в информационном пространстве. Это предполагает заключение международных договоренностей, на основании которых государства отказались бы от использования, передачи и применения средств информационного воздействия, то есть осуществления любых возможных агрессивных действий в информационном пространстве. Кроме того, обеспечение международной информационной безопасности предполагает противодействие международной информационной преступности и терроризму.

Россия активно участвует в международных переговорах по обеспечению информационной безопасности, что является практическим воплощением официальной позиции нашей страны, изложенной как в Стратегии развития информационного общества Российской Федерации, так и в Кон-

цепции внешней политики Российской Федерации, в соответствии с которыми перед российской дипломатией ставится задача обеспечить эффективное вхождение страны в глобальное информационное общество [18].

Анализ документов и выступлений официальных лиц позволяет сделать вывод, что Россия выступает за демилитаризацию информационного пространства, т.к. гонка вооружений в информационной сфере способна расшатать сложившиеся договоренности о разоружении и международной безопасности. Согласно Основам государственной политики в области международной информационной безопасности на период до 2020 года Россия ставит целью государственной политики в области международной информационной безопасности содействие установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности; достижению этой цели, среди прочего, будет способствовать создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности [6]. В Концепции внешней политики Российской Федерации указано, что Россия будет добиваться выработки под эгидой ООН правил поведения в области обеспечения международной информационной безопасности [8].

Россия поддерживает возможность закрепления в системе международного права правила предотвращения вооруженных конфликтов с использованием ИКТ. Часть таких правил нашла отражение в концепции Конвенции об обеспечении МИБ, представленной Российской Федерацией 21-22 сентября 2011 года в Екатеринбурге на Международной встрече высоких представителей, ответственных за вопросы безопасности [9] и в инициативе стран ШОС «Правила поведения в области обеспечения международной информационной безопасности» [10], распространенной в 2011 г. в ходе 66-й сессии Генассамблеи ООН в качестве официального документа.

Однако различие в интересах государств, а также отсутствие международно правовой базы препятствует развитию сотрудничества между государствами. Как предсталяется, первым шагом на пути к формированию глобального режима информационной безопасности может стать выработка мер доверия, которые позволят изменить восприятие возможных угроз, таким образом изменив межгосударственные отношения и поведения государств в исследуемой области.

Перспективы международного сотрудничества по обеспечению информационной безопасности

Проблема международной информационной безопасности вышла на международную повестку дня в 1990-е гг. и с тех пор не утрачивает актуальности. Международные переговоры по проблемам информационной безопасности ведутся на двусторонней основе, а также в рамках глобальных и региональных международных организаций, таких как ООН, ОБСЕ, НАТО, ОДКБ, ШОС и др. Инициатором формирования глобального правового режима, не допускающего использования информационных технологий в целях, несовместимых с международной стабильностью, стала Россия.

Следует отметить значительное число международных инициатив по информационной безопасности в последние годы. Необходимость отражения киберугроз также была обозначена в Стратегической концепции НАТО 2010 г.[11] В июне 2011 г. вступило в силу Соглашение между Правительствами государств – членов ШОС в области обеспечения международной информационной безопасности [7].

Деятельность международных организаций не ограничивается созданием площадок для дискуссий и принятием международно-правовых актов, также создаются специализированные центры, принимаются и реализуются программы действий. В 2009 г. был создан Центр оценки и мониторинга киберугроз НАТО в Эстонии. В рамках ОДКБ реализуется утвержденная президентами Программа совместных действий по формированию системы информационной безопасности. Программа охватывает такие направления, как сотрудничество в политической сфере, совместные научные и исследовательские разработки и обмен информацией о достижениях в этой области, подготовка кадров, унификация законодательной и нормативно-правовой базы, совместное обеспечение безопасности

жизненно важных объектов, проведение совместных мероприятий, направленных на борьбу с преступлениями в сфере информационных технологий [12]. Более того, с 2009 г. в рамках ОДКБ проводятся специализированные учения под названием «ПРОКСИ» («Противодействие криминалу в сфере информации»), направленные на отработку опыта совместного противодействия информационной преступности.

Принципы ответственности государств, такие как территориальность, сотрудничество, обмен данными, самооборона могут рассматриваться как отправная точка для международного сотрудничества по обеспечению международной информационной безопасности. Наращивание информационных потенциалов государствами создает угрозу их использования, что актуализирует вопрос о демилитаризации информационного пространства и принятии соответствующих международно-правовых обязательств. Особое значение приобретает выработка мер доверия, необходимых для предотвращения эскалации международных конфликтов в информационной-сфере.

Меры доверия традиционно используются для улучшения отношений между государствами. Они направлены на формирование атмосферы доверия, изменения восприятия угроз, исходящих от взаимодействующих государств, и трансформации межгосударственных отношения и поведения государств с целью предупреждения и урегулирования конфликтов, управления кризисными ситуациями. В информационном пространстве уже были предприняты попытки по формированию мер доверия, однако на двусторонней, а не многосторонней основе. Наиболее известной попыткой стало создание «горячей линии» между Россией и США в сфере информационной безопасности [13]. В настоящее время обсуждается возможность формирования мер доверия на глобальном и региональном уровнях, в том числе в рамках ОБСЕ, которые могут включать в себя создание центров обмена информацией о информационных угрозах или же проведение семинаров, разъясняющих программы развития информационного пространства, принятых в участвующих государствах.

Возможно также применение мер повышения прозрачности в целях повышения межгосударственного доверия, относительно того, что другие государства под видом обороны не готовятся к нападению в информационной сфере. Так, на базе ОБСЕ уже проводилась серия семинаров по военным доктринам государств-участников, можно расширить подобный опыт на информационную сферу. Подобные меры прозрачности предполагают обмеры информации о стратегиях действия в информационном пространстве / киберпространстве, а также информациях о действиях, направленных на обеспечение кибероборонны. Перспективным также видится создание точек обмена информацией и обмен лучшими практиками.

Еще одним возможным напрвлением международного сотрдничества может стать заключение «превентивного» международного договора. Превентивные договоры запрещают целые классы вооружений, что может послужить моделью для международного сотрудничества в информационной сфере. Страны НАТО выступили с предложением выработать договорный механизм контроля вооружений в информационной сфере, т.е. «конвенцию о кибероружии» с целью обеспечить безопасность киберпространства и не допустить распространения кибероружия [14]. Кроме того, в качестве модели можно использовать регулятивные договоренности по контролю над вооружениями, аналогичные СНВ 1, которые ограничивают определенный тип вооружений. Подобные договоренности могут покрывать весь «жизненный цикл» вооружений, начиная с НИОКР, затем хранение и примерение, а впоследствии демонтаж. Подобные договоренности также ограничивают приобретение или передачу информации о вооружении, в том числе на этапе исследований. Однако, принимая во внимание двойственный характер информационного оружия, маловероятно, что подобные договоренности будут целесообразны, так как практически невозможно доказать, что НИОКР направлен на создание информационных вооружений, а не информационного потенциала для использования в гражданских целях.

Еще один возможный подход к международному сотрудничеству – нормативный. Подобный подход позволяет накладывать ограничения на упреждающее применение информационного оружия. Опыт таких международных соглашений, как Конвенция о запрещении военного или любого иного враждебного использования средств воздействия на природную среду, которая запрещает упреждающее военное использование целого ряда технологий, может

быть использован в отношении информационного оружия. Ряд государств декларировали приверженности принципам отказа от использования военных технологий и в других сферах, однако от подобных заявлений легко отказаться впоследствии, и они не гарантируют, что иные потенциальные агрессоры не готовятся к атакам подобного рода. Как отмечает Д. Льюис, в информационном пространстве приверженность принципу не использовать кибер-оружение в целях первого удара, потребует также отказаться от кибер-шпионажа, так как технологии атаки и кибершпионажа тесно связаны между собой. Это может быть серьезным препятствием к реализации подобных договоренностей, так как большинство государств так или иначе использует кибершпионаж [15: С. 58].

Еще одной мерой может быть полное запрещение. Такие конвенции, как Конвенция о запрещении химического оружия или Конвенция о запрещении биологического оружия запрещают владение, хранение и передачу целого класса вооружений. Применение подобного подхода к информационному оружию затруднено в силу того, что отсутствует терминологическое единство в данной области, в частности, не существует консенсусных определений таких понятий, как информационное оружие / кибероружие, а также, принимая во внимание тот факт, что многие из технологий информационного воздействия являются технологиями двойного назначения.

Ключевая цель, на достижение которой направлена разработка и применение норм, правил и регулирующих институтов, таких как международные правила поведения и принципы поведения государств, - это поддержание мирного, безопасного, стабильного и предсказуемого глобального информационного пространства.

****

В настоящее время открываются новые возможности формирования глобального режима международной информационной безопасности. Долгое время США удерживали лидерство в области развития информационных технологий, сознательно ограничивая возможности формирования глобального правового режима информационной безопасности. Однако изменение характера угроз информационной безопасности привело к тому, что наиболее развитая в информационном плане держава оказалась крайне уязвимой.

Российские исследователи проводят параллели между международно-правовым регулированием в области освоения космического пространства и развития информационного общества [16], [17]. В обоих случаях развитие новых технологий формирует взаимозависимость и порождает вызовы и угрозы гражданского и военного характера. Разработка правовой базы, регулирующей поведение государств в космическом пространстве в целях обеспечения международной безопасности, шла поэтапно, параллельно разрабатывались и общие принципы поведения и проблемы ограничения отдельных действий государств в данной сфере (напр., запрещение ядерных испытаний в космосе). Для регулирования чувствительных, спорных направлений деятельности, которые сложно было вписать в рамки строго обязательных международно-правовых документов, были найдены приемлемые формы деклараций и принципов. Как представляется, опыт международного сотрудничества по обеспечению безопасности в иных высокотехнологичных областях, таких как космос, может быть продуктивно использован в отношении глобальной информационной сферы.

Статья подготовлена в рамках работ по гранту РГНФ 14-57-00005 «Международное сотрудничество по обеспечению информационной безопасности».

Литература:

1. General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/65/201, 30 July 2010.

2. Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/63/37. 02.12.2008.

3. Neuneck G. Civilian and military cyberthreats: shifting identities an attribution. // The Cyber Index. International Security Trends and Realities. UNIDIR, 2013.P. 115 // http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

4. Lewis J., Timlin K. Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization, UNIDIR, 2011.

5. Nye J. CyberPower, Belfer Center for Science and International Affairs, 2010 // http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf

6. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утвержден 01.08.2013 / Совет Безопасности РФ // http://www.scrf.gov.ru/documents/6/114.html

7. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009 г.

8. Концепция внешней политики Российской Федерации. Утверждена 12.02.2013 // http://www.mid.ru.

9. Конвенция об обеспечении международной информационной безопасности (концепция). Утверждена 22.09.2011 // http://mid.ru.

10. Правила поведения в области обеспечения международной информационной безопасности: письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 г. на имя Генерального секретаря. A/66/359 // http://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf

11. Active Engagement, Modern Defense. Strategic Concept for the Defense and Security of the Members of NATO. Lisbon, 2010 // http://www.nato.int.

12. Кожевников А.В. О коллективных мерах государств-членов ОДКБ в сфере обеспечения информационной безопасности. // Международный терроризм в информационную эпоху: реалии кибертерроризма и кибероружия, терроризм и средства массовой информации. Сборник материалов международной конференции. М., 2010 // http://catu.su.

13. Черненко Е.В. РФ и США сближаются в киберпространстве // Коммерсант. 15.05.2013 // http://www.kommersant.ru/doc/2188303

14. Arimatsu L. A treaty for governing cyber-weapons: Potential benefits and practical limitations // Cyber Conflict (CYCON). 2012. 4th International Conference on. IEEE, 2012.

15. Lewis J. Confidence-building and international agreement in cybersecurity // Disarmament Forum. no. 4. 2011.

16. Крутских А.В. К политико правовым основаниям международной информационной безопасности // Международные процессы. 2007. № 13 // www.intertrends.ru/thirteen/003.htm.

17. Федоров А.В. Информационная безопасность в мировом политическом процессе. М., МГИМО, 2006.

18. Енгибарян Р.В. Дипломатическая служба. // Право и управление. XXI век. 2011. № 1. С. 87-88.

INTERNATIONAL COOPERATION FOR INFORMATION SECURITY

The development of information and communication technology (ICT) plays a crucial role in the economic and socio-political development of each country and humanity in general. However, the development of ICT not only creates an opportunity for growth and development, but also generates threats to international and national security. Interstate confrontation, which has entered the information sphere, is fraught with conflicts, an extreme form of which can be information wars.

At present, new opportunities for a global regime of international information security are opening up. The author concludes that the experience of international cooperation to ensure security in other high-tech fields such as space can be efficiently used for the global information sphere.

Elena Zinovieva,
Candidate of Science (Political Sciences)),Associate Professor, Department of political processes, MGIMO (University) under the MFA of Russia

Ключевые слова:
международное сотрудничество, информационная безопасность, меры доверия

Keywords:
international cooperation, information security, confidence-building measures

References:

1. General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/65/201, 30 July 2010.

2. Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/63/37. 02.12.2008.

3. Neuneck G. Civilian and military cyberthreats: shifting identities an attribution. // The Cyber Index. International Security Trends and Realities. UNIDIR, 2013.P. 115 // http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

4. Lewis J., Timlin K. Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization, UNIDIR, 2011.

5. Nye J. CyberPower, Belfer Center for Science and International Affairs, 2010. P. 1. URL: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf

6. Osnovy gosudarstvennoj politiki Rossijskoj Federacii v oblasti mezhdunarodnoj informacionnoj bezopasnosti na period do 2020 goda. [Basics of the state policy of Russian Federation in the field of international information security]. 01.08.2013. / Security Council of Russian Federation // http://www.scrf.gov.ru/documents/6/114.html

7. Soglashenie mezhdu pravitel'stvami gosudarstv – chlenov Shanhajskoj organizacii sotrudnichestva o sotrudnichestve v oblasti obespechenija mezhdunarodnoj informacionnoj bezopasnosti. [Treaty of the SCO member states on the cooperation in the field of international information security]. 2009.

8. Koncepcija vneshnej politiki Rossijskoj Federacii [Concept of the foreign policy of Russian Federation]. 12.02.2013 // http://www.mid.ru.

9. Konvencija ob obespechenii mezhdunarodnoj informacionnoj bezopasnosti (koncepcija). [Convention on the international information security (concept)] 22.09.2011 // http://mid.ru.

10. Pravila povedenija v oblasti obespechenija mezhdunarodnoj informacionnoj bezopasnosti: pis'mo postojannyh predstavitelej Kitaja, Rossijskoj Federacii, Tadzhikistana i Uzbekistana pri Organizacii Ob'edinennyh Nacij ot 12 sentjabrja 2011 g. na imja General'nogo sekretarja. [Rules of behavior in the field of international information security: letter of permanent representatives of China, Russia, Tajikistan and Uzbekistan at the UN to the UN Secretary General 12.09.2011] A/66/359 // http://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf

11. Active Engagement, Modern Defense. Strategic Concept for the Defense and Security of the Members of NATO. Lisbon, 2010 // http://www.nato.int.

12. Kozhevnikov A.V. O kollektivnyh merah gosudarstv-chlenov ODKB v sfere obespechenija informacionnoj bezopasnosti. [On the collective measures on the OCST member-states in the field of information security] // Mezhdunarodnyj terrorizm v informacionnuju jepohu: realii kiberterrorizma i kiberoruzhija, terrorizm i sredstva massovoj informacii. Sbornik materialov mezhdunarodnoj konferencii. M., 2010 // http://catu.su.

13. Chernenko E.V. RF i SShA sblizhajutsja v kiberprostranstve. [Russia and USA cooperate in the cyber sphere] // Komersant, 15.05.2013 // http://www.kommersant.ru/doc/2188303

14. Arimatsu L. A treaty for governing cyber-weapons: Potential benefits and practical limitations // Cyber Conflict (CYCON), 2012 4th International Conference on. IEEE, 2012.

15. Lewis J. Confidence-building and international agreement in cybersecurity // Disarmament Forum. no. 4. 2011.

16. Krutskih A.V. K politiko pravovym osnovanijam mezhdunarodnoj informacionnoj bezopasnosti [Towards legal and political foundations of the information security] // Mezhdunarodnye process [International trends]. 2007. № 13 // www.intertrends.ru/thirteen/003.htm

17. Fedorov A.V. Informacionnaja bezopasnost' v mirovom politicheskom processe. [Information security in the global political process]. M.: MGIMO, 2006.

18. Engibarjan R.V. Diplomaticheskaja sluzhba. [Diplomatic service]// Pravo i upravlenie. XXI vek. 2011. № 1. S. 87-88.