КИБЕРБЕЗОПАСНОСТЬ КАК ОСНОВНОЙ ФАКТОР НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ XXI ВЕКА (Часть 1)

Бородакий Юрий Владимирович, *академик РАН, доктор технических наук, профессор*
Добродеев Александр Юрьевич, *кандидат технических наук, старший научный сотрудник*
Бутусов Игорь Викторович

В статье рассматриваются актуальные проблемы обеспечения международной и национальной кибербезопасности и предлагаются подходы к созданию адекватной современным угрозам системы обеспечения кибербезопасности автоматизированных систем органов военного и государственного управления

Ключевые слова: *кибербезопасность, информационная безопасность, инфосфера, киберпространство*

CYBER SECURITY AS A MAIN FACTOR FOR NATIONAL AND INTERNATIONAL SECURITY XXI CENTURY (Part 1)

Yuri Borodakiy, *Member of the RAS, Doctor of Technical Sciences, Professor*
Alexander Dobrodeyev, *Ph.D., Associate Professor*
Igor Butusov

The actual problems of international and national cybersecurity are considered. The approaches to the development of an adequate system of the present threats of cyber security of the military and government automated systems are given.

Keywords: *cybersecurity, information security, infosphere, cyberspace*

1. ВВЕДЕНИЕ

Глобальная информатизация в настоящее время активно управляет существованием и жизнедеятельностью государств мирового сообщества, информационные технологии применяются при решении задач обеспечения национальной, военной, экономической безопасности и др. Вместе с тем, одним из фундаментальных последствий глобальной информатизации государственных и военных структур стало возникновение принципиально новой среды противоборства конкурирующих государств – **киберпространства**, которое не является географическим в общепринятом смысле этого слова, но, тем не менее, в полной мере является международным.

И если сегодня между ведущими в военном и экономическом отношении мировыми государствами сложился в той или иной степени определенный паритет в области применения обычных вооружений и оружия массового поражения, в международном праве зафиксированы основные принципы взаимоотношений этих государств в рамках таких пространств, как наземное, морское, воздушное, космическое, то вопрос о межгосударственном паритете и взаимоотношениях в киберпространстве на настоящее время продолжает оставаться открытым.

В процессе формирования глобального киберпространства происходит конвергенция военных и гражданских компьютерных технологий, в ведущих зарубежных государствах интенсивно разрабатываются новые средства и методы активного воздействия на информационную инфраструктуру потенциальных противников, создаются различные специализированные кибернетические центры и подразделения управления и командования, основной задачей которых является защита государственных и военных информационных

инфраструктур, подготовка и проведение активных деструктивных действий в информационных системах противника. Так, собственные официальные кибервойска уже существуют у США, Китая, Англии, Франции, Германии, Израиля и ряда других государств.

Противоборство в киберпространстве становится принципиально новой сферой противоборства между государствами. Термины и определения с приставкой «кибер…» широко используются как в международных, так и во внутригосударственных дискуссиях и документах, нашли свое отражение в стратегических доктринах отдельных государств и международных организаций, включая НАТО. Стремительно нарастающий в мире интерес к проблематике киберпространства во многом связан с активностью США в вопросах кибервойн и кибербезопасности.

В США, 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 можно выделить «Обзор политики в киберпространстве» (май 2009 г.) [1], «Международная стратегия по киберпространству» (май 2011 г.) [2], «Стратегия Министерства обороны по действиям в киберпространстве 2011» (июль 2011 г.) [3], которую в июле 2011 г. представил, выступая в Университете национальной обороны, заместитель министра обороны Уильям Линн. «В XXI веке биты и байты могут быть такими же опасными, как пули и бомбы»,— заявил он в ходе презентации стратегии. Суть стратегии заключается в том, что киберпространство стало рассматриваться Вашингтоном таким же потенциальным полем боя, как земля, воздух, море и космос. Поэтому США приравнивают акты кибератак к традиционным военным действиям и предусматривают возможность «отвечать на серьезные нападения пропорциональными и справедливыми военными мерами», вплоть до применения ядерного оружия. При этом представители Пентагона отмечают, что разработанная доктрина является лишь первым шагом на пути к освоению киберпространства. В дальнейшем, как отметил заместитель председателя Объединенного комитета начальников штабов США, генерал Джеймс Картрайт, Пентагон должен перейти от политики обороны к политике сдерживания угроз, не забывая при этом и о разработке возможных наступательных мер.

В своих стратегических документах Пентагон признал киберпространство новым полем возможных боевых действий, НАТО приравнивает кибератаки на страну – члена альянса к вооруженному нападению. Специалисты в области информационных технологий наиболее развитых государств мира (США, страны – члены блока НАТО, Япония, Китай и др.) единодушно отмечают тот факт, что «государство, контролирующее киберпространство, будет контролировать войну и мир» [4].

Кибербезопасность – стратегическая проблема государственной важности, затрагивающая все слои общества. Государственная политика кибербезопасности (National Cyber Security Strategy – NCSS) служит средством усиления безопасности и надежности информационных систем государства. Вслед за США, стратегии кибербезопасности приняты в Канаде, Японии, Индии, Австралии, Новой Зеландии, Колумбии и некоторых других государствах. В ряду стран-членов Евросоюза стратегии кибербезопасности приняли: Швеция (2008 г.), Эстония (2008 г.), Финляндия (2008 г.), Словакия (2008 г.): Чехия (2011 г.), Франция (2011 г.), Германия (2011 г.), Литва (2011 г.), Люксембург (2011 г.), Голландия (2011 г.), Великобритания (2011 г.). Список стран наглядно показывает, что проблема кибербезопасности признается важной во всем мире.

С 2008 г. НАТО проводит ежегодные киберучения с отработкой взаимодействия международных сил альянса в области информационной безопасности. Так, в апреле 2013г. на учениях под названием «Locked Shields-2013» отрабатывались мероприятия отражения кибератак компьютерных сетей. Организатор учений – центр изучения передового опыта НАТО в области кибербезопасности, совместно с министерствами обороны Эстонии и Финляндии. В мероприятии приняли участие около 250 специалистов из 9 стран: Эстонии, Финляндии, Литвы, Германии, Польши, Нидерландов, Италии, Словакии и Испании.

В рамках повышения уровня подготовки кадров АНБ США проводит ежегодные учения «Cyber Defense Exercise» в формате конкурса среди обучающихся в гражданских колледжах и военных академиях страны. Основные цели учения – вызвать у американских военнослужащих интерес к сфере информационных технологий и повысить уровень их знаний.

Европейское агентство по сетевой и информационной безопасности (European Network and Information Security Agency, ENISA) в октябре 2012 года провело киберучения «European Cyber Exercise» с целью определения готовности организаций государственного и частного секторов к отражению кибератак. В учениях приняли уча-

стие более 300 специалистов по компьютерной безопасности из банков, интернет-провайдеров и государственных учреждений 25 государств. Это уже вторые учения в киберпространстве, проведенные под эгидой ЕС с ноября 2010 г.

Наряду с этим в период президентства Барака 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.

В опубликованном еще в 2009 г. ежегодном «Отчете о виртуальной преступности», крупнейшей в мире компанией McAfee, занимающейся технологиями безопасности, однозначно утверждается, что «международная гонка кибервооружений стала реальностью», количество политически мотивированных кибератак в мире выросло, ***а ряд стран обладают кибероружием или занимаются его разработкой***. По оценкам экспертов США в области информационной безопасности, в настоящее время таких государств более тридцати.

Глава Кибернетического командования США генерал Кит Александер, выступая на конференции центра НАТО по кибероборонe, проходившей в Таллине в июне 2013 г., впервые признал, что инциденты в киберпространстве «могут привести к масштабному вооруженному конфликту между государствами». Хамадун Туре, генеральный секретарь Международного союза электросвязи ООН, утверждает, что «следующая мировая война, если она состоится, будет проходить в киберпространстве».

В современных условиях совершенно справедливо утверждение о том, что войны XXI веке будут кибернетическими по своей основной сути. Следовательно, для любого государства безопасность в киберпространстве (кибербезопасность) становиться острой и специфической проблемой в обеспечении своей национальной безопасности и защиты своих интересов.

2. ОСНОВНЫЕ ТЕРМИНЫ, ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Термин «кибербезопасность» ворвался в нашу жизнь, с одной стороны, давно, с момента создания компьютера и компьютерных систем, с другой стороны, очень мощно и значимо на сегодняшний день потому, что общество стало заложником бурной, масштабной и значимой информатизации жизни и зависимости от неё повседневной жизнедеятельности, экологии и здоровья и, в широком смысле, – существования.

В современных условиях вопросы кибербезопасности выходят с уровня защиты информации на отдельном объекте вычислительной техники на уровень создания единой системы кибербезопасности государства, как составной части системы информационной и национальной безопасности, отвечающей за защиту не только информации в узком смысле этого слова, но и всего киберпространства.

Вместе с тем, для корректного формирования и решения проблем обеспечения кибербезопасности в системах государственного и военного управления необходимо, по мнению авторов, в первую очередь, уточнить понятийный аппарат в данной области, роль и место проблем кибербезопасности в ряду проблем национальной, военной, информационной безопасности и технологической независимости.

Сегодня не существует однозначно признанного международным сообществом определения киберпространства, при этом используется большое количество ведомственных (частных) определений, которые вытекают из целей и задач организаций, их использующих. Используемые определения в большой степени зависят от того, с какой точки зрения рассматривается киберпространство – с точки зрения обеспечения защиты информационно–коммуникационной инфраструктуры государства, либо с точки зрения ведения активных боевых действий в киберпространстве.

Между тем, отсутствие в международном праве консенсуса в отношении того, что понимать под терминами «киберпространство», «кибервойна», «кибератака», «кибертерроризм», «киберкатастрофа», «кибербезопасность» и т.п. является негативным фактором при построении отношений между государствами.

«Википедия», свободная энциклопедия, распространяемая в сети Интернет, определяет киберпространство, как «метафорическую абстракцию, используемую в философии и в компьютерной технологии, которая является (виртуальной) реальностью, представляет ноосферу, второй мир как «внутри» компьютеров, так и «внутри» компьютерных сетей».

Общегосударственное определение киберпространства впервые прозвучало в докладе исследовательской службы конгресса США

в 2001 г., где киберпространство определено как «всеохватывающее множество связей между людьми, созданное на основе компьютеров и телекоммуникаций вне зависимости от физической географии» [5].

В Министерстве обороны США, начиная с 2001 г., в различных уставных документах происходила трансформация формулировки «киберпространство». Так, в Едином уставе комитета начальников штабов вооруженных сил (КНШ ВС) США Joint Pub. 3-13 2006 г. (Информационные операции) киберпространство определено как «сфера (область), в которой применяются различные радиоэлектронные средства (связи, радиолокации, разведки, навигации, автоматизации, управления и наведения), использующие электромагнитный спектр частот для приема, передачи, обработки, хранения, видоизменения (трансформации) и обмена информации и связанная с ними информационная инфраструктура ВС США» [6].

Эволюция взглядов и подходов американского военного руководства к формулированию понятийного аппарата в сфере борьбы в киберпространстве подтверждает факт пересмотра основных положений военного искусства с учетом изменившегося характера военно-стратегической обстановки и глубокого проникновения информационных и компьютерных технологий в сферу деятельности вооруженных сил. При этом ведется активная проработка на экспертном уровне теории ведения боевых действий в киберпространстве, успех которых будет зависеть: от заблаговременно созданного технологического задела; освоения соответствующих способов и форм кибернетического противоборства.

Формируется «система кибервооружения» (организационно- функциональное объединение системы киберсредств, инфраструктуры и кадрового ресурса) с целью проводить операции в киберпространстве и оказывать влияние на мировые процессы через эту сферу.

Опубликованный в 2012 г. стандарт в области кибербезопасности ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности» определяет ***киберпространство***, как «комплекс среды и, как следствие в результате взаимодействия людей, программного обеспечения и услуг в Интернете с помощью технологии устройств и сетей, подключенных к ней, которых не существует в любой физической форме», а ***кибербезопасность*** – это безопасность в киберпространстве. Стандарт определяет связи термина cybersecurity (кибербезопасность) с сетевой безопасностью, прикладной безопасностью, Интернет-безопасностью и безопасностью критичных информационных инфраструктур с точки зрения западных специалистов. В стандарте приводится рисунок, который визуализирует связь различных терминов (рис.1). С точки зрения международных экспертов все эти термины объединяет понятие information security (информационная безопасность).

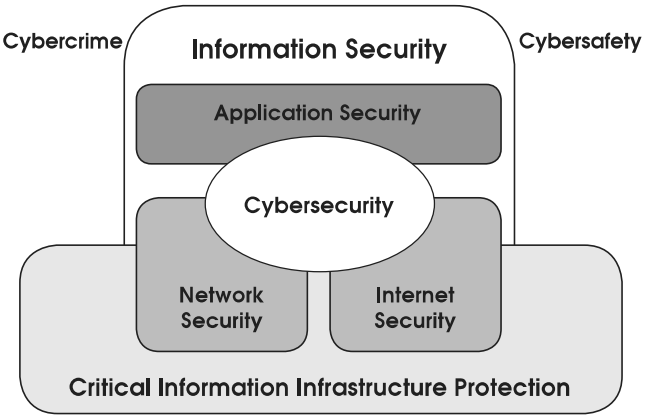

Рис.1. *Связь термина «кибербезопасность» с сетевой безопасностью, прикладной безопасностью и Интернет-безопасностью.*

В рекомендации Международного Союза Электросвязи X.1205 МСЭ-Т «кибербезопасность» определена как набор средств, стратегий, принципов обеспечения безопасности, мер по обеспечению безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, практического опыта, страхования и технологий, которые могут быть использованы для защиты киберпространства, ресурсов организации и пользователя.

В свою очередь авторами предложены некоторые, уточненные по сути, основные определения, на которые они опираются при изложении материала в данной статье.

Киберпространство - глобальная область информационной среды, включающая в свой состав взаимозависимую совокупность информационно-технической инфраструктуры, в том числе информационные и телекоммуникационные сети и компьютерные системы, предназначенные для хранения, обработки, модификации и обмена данными.

Кибербезопасность (философское определение) – это свойство или состояние системы сохранять надежность и функциональную устойчивость в условиях современного информационного противоборства.

Кибербезопасность (определение по технической сущности) – информационная безопасность компьютерных информационно-управляющих систем, обеспечивающая их высокую надежность и функциональную устойчивость в условиях современного информационного противоборства. *Или, иначе, кибербезопасность – это информационная безопасность в компьютерной инфосфере в условиях современного информационного противоборства.*

3. НОРМАТИВНО-ПРАВОВЫЕ ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ И УСИЛИЯ РОССИИ ПО ОБЕСПЕЧЕНИЮ НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ КИБЕРБЕЗОАСНОСТИ

Киберпространство России является составной частью общемирового киберпространства. Угрозы кибербезопасности для российского общества во многом аналогичны угрозам, имеющим место в других странах, а многие из них являются прямым следствием неправомерных действий зарубежных киберпреступников (или спецслужб).

Россия, как одно из ведущих государств мира, является первоочередным объектом для негативных кибервоздействий в стремлении других стран на мировое лидерство. В настоящее время существует потенциальная угроза нарушения функционирования критически важных информационных систем основных объектов жизнеобеспечения государства, ВС РФ, МВД, ФСБ, ФСО, МЧС России при массированном воздействии компьютерных атак на их уязвимости. При этом прежние базовые информационные защищенные компьютерные технологии и традиционные средства защиты информации недостаточны и уже не обеспечивают необходимого уровня защищенности и функциональной устойчивости.

Складывающаяся в современном мировом киберпространстве обстановка вокруг России требует принятия адекватных мер противодействия, чтобы потенциальные противники (или конкуренты) не могли завоевывать и удерживать информационное превосходство над РФ как в мирное, так и в военное время. Надо незамедлительно выработать основные принципы и стратегию, обеспечивающие нейтрализацию киберагресии (кибервоздействий) и информационных операций, которые могут проводится в отношении России потенциальным противником, создавать и развивать силы и средства обеспечения кибербезопасности критически важной инфраструктуры государства.

Определенные шаги в этом направлении уже сделаны. В сентябре 2000 г. Президентом Российской Федерации В.Путиным утверждена Доктрина информационной безопасности Российской Федерации, подписаны Указ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» и «Основы государственной политики РФ в области международной информационной безопасности РФ на период до 2020 года», проходит рассмотрение проект Федерального закона РФ «О безопасности критической информационной инфраструктуры РФ».

Совет Федерации планирует доработать до конца года законопроект стратегии кибербезопасности РФ для последующего внесения на рассмотрение в Совет Безопасности. «Концепция стратегии кибербезопасности РФ» разрабатывается в Совете Федерации под руководством члена Комитета Совета Федерации по науке, образованию, культуре и информационной политике, председателя временной Комиссии Совета Федерации по развитию информационного общества Р.Гаттарова с весны текущего года. В проекте стратегии указывалось, что она «ориентируется на разумную и относительную самостоятельность и ресурсную независимость РФ в инфраструктурном, технологическом аспектах в киберпространстве и прежде всего в Интернете».

В 2013 году организованы работы по созданию Национального центра управления обороной государства (НЦУОГ), предназначенного для решения задач контроля и управления всеми силами и средствами, действующими в интересах обороны страны как в военное, так и в мирное время, в том числе и системой кибербезопасности России. В этом же году принято решение и организованы работы по созданию в Минобороны России киберкомандования для защиты общенациональных интересов в киберпространстве. Как ожидается, базовый состав российского киберкомандования будет сформирован к концу 2014 года.

В соответствии с Федеральным законом Российской Федерации от 16 октября 2012 года № 174-ФЗ в России создан Фонд перспективных исследований в целях содействия осуществлению научных исследований и разработок в интересах обороны страны и безопасности государства, связанных с высокой степенью риска достижения качественно новых результатов в военно-технической, технологической и социально-экономической сферах, в том числе и в сфере кибербезопасности государства.

На международном уровне Россия была инициатором международного обсуждения вопросов глобальной безопасности в этой сфере, прежде всего в ООН, а также на других региональных и двусторонних площадках [7].

Именно России принадлежит инициатива в официальной постановке перед международным сообществом и ООН проблем обеспечения международной информационной безопасности (МИБ). Россия еще в середине 1998 г. предложила США подписать на уровне президентов совместное заявление, посвященное исключительно проблематике МИБ. 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. Однако информационная безопасность была упомянута только в самом общем виде в подписанном в Москве Президентами России и США 2 сентября 1998 г. «Совместном заявлении об общих вызовах безопасности на рубеже XXI века» [8].

В сентябре 1998 г. Генеральному секретарю ООН К. Аннану был представлен российский вариант проекта резолюции Генассамблеи ООН, «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в котором акцентировалась необходимость учитывать «серьезную опасность использования достижений в информационной сфере в целях, не совместимых с задачами поддержания мировой стабильности и безопасности, соблюдением принципов неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека».

В декабре 1998 г. Генасамблея ООН приняла подготовленную Россией резолюцию, однако она не содержала ссылок на использование информационных технологий в военных целях, конкретного определения «информационное оружие» и необходимости разработки режима запрещения его создания и применения. 8 декабря 2003 г. Генассамблея ООН приняла инициированную российской стороной резолюцию [9], которая предполагала работу группы правительственных экспертов ООН в области международной информационной безопасности, однако усилиями США эта работа оказалась сорванной.

В этих условиях Россия основные усилия в области обеспечения МИБ перенесла на региональный уровень. Так, в октябре 2006 г. состоялось учредительное заседание группы экспертов государств – членов ШОС, которым было поручено выработать план действий и определить пути решения проблемы МИБ в рамках компетенции стран-членов организации. В ходе саммита в Бишкеке в 2007 г. 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. Впервые на международно-правовом уровне были зафиксированы конкретные угрозы в области информационной безопасности и определены основные направления и формы сотрудничества в этой сфере. Соглашение было ратифицировано Россией, Китаем, Казахстаном и Таджикистаном и 2 июня 2011 г. вступило в силу.

Перспектива монополизации информационной сферы и военное использование информационно-телекоммуникационных средств являются предметом озабоченности не только России.

В докладе Генеральному секретарю ООН по вопросам информационной безопасности, подготовленном группой правительственных экспертов 15-и государств и представленном на 65-й сессии Генассамблеи в июле 2010 г. эти вопросы нашли свое отражение. В сентябре 2011 г. на 66-й сессии Генассамблеи Россией, Китаем, Таджикистаном и Узбекистаном был предложен совместный проект «Правил поведения в области обеспечения международной информационной безопасности» [10], 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 [11]. 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 Генассамблеи 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).

Проект Конвенции определяет информационную войну как «межгосударственное противоборство в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и дру-

гим 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 подвергся резкой критике со стороны США, которые открыто стремятся к «глобальному контролю над киберпространством».

Тем не менее, Россия и заинтересованные страны продолжают работать над проектом Конвенции. В марте 2012 г. в Нью-Дели был проведён российско-индийский семинар, посвящённый его обсуждению.

В ноябре 2006 г. в Санкт-Петербурге в ходе Глобального форума по партнёрству государства и бизнеса в противодействии терроризму Россия выступила с рядом долгосрочных инициатив по борьбе с киберпреступностью, которые получили всестороннюю поддержку участников форума. 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. Таким образом, российские инициативы в настоящее время охватывают практически весь спектр угроз в информационной сфере.

На данный момент единственным многосторонним международным документом, играющим существенную роль в координации усилий мирового сообщества по вопросам кибербезопасности, является Европейская Конвенция по киберпреступлениям, принятая Советом Европы 23 ноября 2001 г. в Будапеште. Конвенция содержит классификацию компьютерных преступлений, а также рекомендации органам законодательной и исполнительной власти государств по борьбе с этими преступлениями. В данный момент под конвенцией подписались ряд стран Евросоюза (39 стран из 47), а также США, Канада, Япония и ЮАР.

Тот факт, что наша страна так и не присоединилась к ней, является одним из главных аргументов в критике российских инициатив в области кибербезопасности, в том числе и со стороны части российского экспертного сообщества.

Продолжение следует.Во второй части статьи будут рассмотрены основные научно-технические проблемы и современные тенденции обеспечения кибербезопасности автоматизированных систем органов военного и государственного управлении, информационно-управляющих систем общего и специального назначения.

Литература

1. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. - Washington D.C.: The White House, 2009.
2. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. - Washington D.C.: The White House, 2011.
3. Department of Defense Strategy for Operating in Cyberspace. - Washington D.C.: U.S. Department of Defense, 2011.
4. Бантин Д.Э. К вопросу о формировании киберпространственного командования ВВС США. - Вашингтон, 2007.
5. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны - реальная угроза национальной безопасности. – М.: Изд-во КРАСАНД, 2011.
6. Information Operations. Joint Publication 3-13. - Washington D.C.: Joint Chiefs of Staff, 2006.
7. Бедрицкий А.В. Международные договорённости по киберпространству: возможен ли консенсус?.// Проблемы национальной стратегии, № 4 (13), 2012.
8. Совместное заявление об общих вызовах безопасности на рубеже XXI века (Москва, 2 сентября 1998 г.) // Дипломатический вестник МИД России, № 10, 1998.
9. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция Генеральной Ассамблеи ООН A/RES/58/32 - Генеральная Ассамблея ООН: 58-я сессия, № 58/32, 2003.
10. 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 ООН A/66/359 - Генеральная Ассамблея ООН: 66-я сессия, 2011.

11. Конвенция ООН об обеспечении международной информационной безопасности (концепция). 2011. http://www.scrf.gov.ru/documents/6/112.html.

References

1. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. - Washington D.C.: The White House, 2009.
2. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. - Washington D.C.: The White House, 2011.
3. Department of Defense Strategy for Operating in Cyberspace. - Washington D.C.: U.S. Department of Defense, 2011.
4. Bantin D.E. K voprosu o formirovanii kiberprostranstvennogo komandovaniya VVS SShA. - Vashington, 2007.
5. Parshin S.A., Gorbachev Yu.E., Kozhanov Yu.A. Kibervojny - realnaya ugroza nacional noj bezopasnosti. – M.: Izd-vo KRASAND, 2011.
6. Information Operations. Joint Publication 3-13. - Washington D.C.: Joint Chiefs of Staff, 2006.
7. Bedrickij A.V. Mezhdunarodnye dogovoryonnosti po kiberprostranstvu: vozmozhen li konsensus?.// Problemy nacionalnoj strategii, № 4 (13), 2012.
8. Sovmestnoe zayavlenie ob obshhix vyzovax bezopasnosti na rubezhe XXI veka (Moskva, 2 sentyabrya 1998 g.) // Diplomaticheskij vestnik MID Rossii, № 10, 1998.
9. Dostizheniya v sfere informatizacii i telekommunikacij v kontekste mezhdunarodnoj bezopasnosti. Rezolyuciya General noj Assamblei OON A/RES/58/32 - General naya Assambleya OON: 58-ya sessiya, № 58/32, 2003.
10. Pravila povedeniya v oblasti obespecheniya mezhdunarodnoj informacionnoj bezopasnosti. Prilozhenie k pismu postoyannyh predstavitelej Kitaya, Rossijskoj Federacii, Tadzhikistana i Uzbekistana pri Organizacii Ob"edinyonnyh Nacij ot 12 sentyabrya 2011 g. na imya Generalnogo sekretarya OON A/66/359 - Generalnaya Assambleya OON: 66-ya sessiya, 2011.
11. Konvenciya OON ob obespechenii mezhdunarodnoj informacionnoj bezopasnosti (koncepciya). 2011. http://www.scrf.gov.ru/documents/6/112.html.