РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

как правило, предполагает преследование человека через Интернет или другие электронные коммуникации. Доступ к личной информации в Интернете делает киберпреследования особенно проблематичными.

Быстрый рост и широкое использование электронной обработки данных и электронных деловых операций, осуществляемых через Интернет, наряду с многочисленными случаями международного терроризма, подпитывают необходимость совершенствования методов защиты компьютеров и информации, которую они хранят, обрабатывают и передают. Научные дисциплины компьютерной безопасности и обеспечения информационной безопасности возникли наряду с многочисленными профессиональными организациями – все они разделяют общие цели обеспечения безопасности и надежности информационных систем.

Список использованных источников:

1. Комиссия по предупреждению преступности и уголовному правосудию. Доклад по работе Модели (2 – 4 декабря2009 года) // https://mgimo.ru/files/138094/doklad.pdf.
2. Конвенция о компьютерных преступлениях (Конвенция Совета Европы о киберпреступности, Convention on Cybercrime CETS № 185) (Будапешт, 23 ноября 2001 года)
3. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // http://docs.cntd.ru/document/902140948.
4. Anderson, K. IT Security Professionals Must Evolve for Changing Market, SC Magazine, October 12, 2006.
5. Dhillon, G., Principles of Information Systems Security: text and cases, John Wiley & Sons, 2007.
6. Easttom, C., Computer Security Fundamentals (2nd Edition)Pearson Education, 2011.
7. Lambo, T., ISO/IEC 27001: The future of infosec certification, ISSA Journal, November 2006.
8. Мельников,В.П.Информационная безопасность и защита информации. / В.П.Мельников, С.А.Клейменов, А.М.Петраков // 3-е изд., стер. - М.: Академия, 2008. — 336 с.
9. Черней, Г.А. Безопасность автоматизированных информационных систем. / Г. А. Черней, С. А. Охрименко, Ф. С. Ляху // Ruxanda,1996. - 225 с.
10. Галатенко, В.А. Основы информационной безопасности.
11. Варлатая, С. К. Аппаратно-программные средства и методы защиты информации. / С. К. Варлатая, М.В.Шаханова // Владивосток: Изд-во ДВГТУ, 2007. - 318 с.

УДК 327

МЕЖДУНАРОДНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Атабаев Ахмет Серикбаевич
akhmet.atabayev@mail.ru
Магистрант 2 г.о. специальности
«6М020200 – Международные отношения»
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – к.и.н, и.о. профессора С.К. Алиева

Основная озабоченность государств в сфере обеспечения международной информационной безопасности (МИБ) связана с возможностью применения информационно-коммуникационных технологий в целях не совместимых с задачами обеспечения международной стабильности и безопасности. Важнейшими угрозами здесь

видятся враждебное пользование ИКТ на уровне государств в отношении информационных инфраструктур другого государства (прежде всего, критически важных) в политических, в том числе военных, целях; преступная и террористическая деятельность в киберпространстве.

В XXI векепроисходит трансформация всей военной архитектуры: мы являемся свидетелями «информатизации» вооруженных сил и «интеллектуализации» традиционных вооружений. Информационное оружие становится важным элементом военного потенциала государств. Оно эффективно дополняет традиционные средства ведения вооруженных конфликтов и будет способно в целом ряде случаев полностью заменить их.

Изменяются формы межгосударственных конфликтов: при помощи ИКТ нападения и агрессии могут осуществляться трансгранично, без привлечения армейских подразделений и использования традиционных вооружений и военной техники, руками негосударственных субъектов. Дестабилизация экономики, подрыв суверенитета и основ государственного устройства, нарушение нормального функционирования практически всех инфраструктур государства, в том числе критически важных, могут быть достигнуты за счет применения информационных технологий и средств. В этих условиях эффективное обеспечение национальной и международной безопасности и стабильности невозможно без укрепления международной информационной безопасности, прежде всего за счет снижения угроз враждебного использования ИКТ.

Активная работа по согласованию позиций различных государств относительно объектов обеспечения международной информационной безопасности нашла отражение и в хартии Глобального информационного общества, принятой на встрече лидеров стран «восьмерки» в июле 2000 года в Окинаве (Япония), или Окинавская хартия. В этом документе страны «Группы восьми» определили информационно-телекоммуникационные технологии в качестве основного фактора, формирующего общество XXI века, подтвердили свою готовность содействовать переходу к информационному обществу и признали необходимость решения проблем обеспечения безопасности использования этих технологий. Страны выработали и включили в итоговый документ саммита ключевые направления работы для достижения поставленной цели, в частности, в области укрепления политики и нормативно-правовой базы по борьбе со злоупотреблениями, подрывающими целостность информационных сетей. Стороны согласились с тем, что усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности пространства, осуществлению эффективных мер по борьбе с компьютерной преступностью. Документ предполагает также расширение сотрудничества стран «восьмерки» в рамках Лионской группы по транснациональной организационной преступности. Была поставлена проблема борьбы с попытками несанкционированного доступа и компьютерными вирусами.

Для защиты критических и информационных инфраструктур было решено привлекать представителей промышленности и других негосударственных организаций посредников. Действительно, правительства в одиночку не способны обеспечить безопасность киберпространства, в связи с чем особую важность приобретают усилия каждого пользователя киберпространства по содействию обеспечению безопасности в том участке пространства, которым он владеет или пользуется, и это не только промышленные предприятия, но и организации всех секторов экономики, университеты, местные органы власти, а также частные пользователи Интернета.

Таким образом, страны «Группы восьми» пошли на закрепление в итоговом документе лишь вопросов целостности информационных сетей и пресечения преступлений в компьютерной сфере, игнорируя тем самым военно-политическую составляющую проблемы МИБ. Фактически проблема военного применения ИКТ на уровне государств не была отражена в документе, а ведь именно военный аспект использования информационных средств и технологий является первостепенным по своей значимости и наиболее опасным с

точки зрения потенциальных последствий применения информационного оружия.

Проблематика МИБ продвигалась также по линии Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) (первый этап — 10-12 декабря 2003 года, Женева, второй — 16—18 ноября 2005 года, Тунис). Важную роль в объединении мирового сообщества вокруг темы МИБ сыграла прошедшая в г. Марракеш (Марокко) с 23 сентября по 18 октября 2002 года 16-я Полномочная конференция (ПК) Международного союза электросвязи. Решением ПК был принят «Вклад Международного союза электросвязи в Декларацию принципов и План действий ВВУИО». В этом документе отражено опасение стран—членов МСЭ относительно того, что ИКТ могут оказывать негативное воздействие на безопасность государств как в гражданской, так и в военной области, а также признана необходимость предотвращения использования информационных ресурсов или технологий для преступных или террористических целей.

Конференция предложила мировому сообществу рассмотреть существующие и потенциальные угрозы безопасности информационных и коммуникационных сетей. Было решено внести вклад в реализацию усилий ООН, направленных на оценку состояния информационной безопасности, а также рассмотрение вопроса о разработке, в долгосрочной перспективе, международной конвенции по безопасности в среде информационных сетей и сетей связи. Нашедшие отражение во вкладе МСЭ формулировки по МИБ в дальнейшем легли в основу соответствующих положений итоговых документов региональных конференций по подготовке к ВВУИО — Общеевропейской (Бухарест, 7-9 ноября 2002 года) и Азиатско-Тихоокеанской (Токио, 13-15 января 2003 года).

Включение столь важных формулировок по МИБ в декларации подготовительных встреч к ВВУИО имело принципиальное значение. Оно заложило основу для последующего закрепления проблематики МИБ в повестке дня самого саммита, что, в свою очередь, явилось важным шагом в направлении общего правового регулирования проблематики МИБ.

Формулировки по МИБ вошли в оба итоговых документа первого (женевского) этапа ВВУИО.

В Декларации принципов (раздел «Укрепление доверия и безопасности при использовании ИКТ») указывается на то, что упрочение основы для доверия, включая информационную безопасность и безопасность сетей, является предпосылкой становления информационного общества. В Декларации также зафиксировано, что государства, принявшие ее, признавая принципы универсального и недискриминационного доступа к ИКТ для всех стран, поддерживают деятельность ООН, направленную на предотвращение возможности использования ИКТ в целях, которые несовместимы с задачами обеспечения международной стабильности и безопасности и способны оказать отрицательное воздействие на целостность государственных инфраструктур, нанося ущерб их безопасности. Они также исходят из того, что следует предотвращать использование информационных ресурсов и технологий в преступных и террористических целях.

В Плане действий отмечается, что доверие и безопасность относятся к главным опорам информационного общества. В качестве важнейших направлений конкретных мер по укреплению доверия и безопасности при использовании ИКТ в документе выделены в том числе следующие:

- содействие сотрудничеству между государствами в рамках ООН и со всеми заинтересованными сторонами в рамках соответствующих форумов в целях анализа существующих и потенциальных угроз в области ИКТ, а также решения других вопросов информационной безопасности и безопасности сетей;
- изучение законодательства, которое дает возможность эффективно расследовать и подвергать преследованию ненадлежащее использование ИКТ;
- содействие эффективным мерам взаимопомощи в этой сфере, а также профилактике компьютерных инцидентов;
- поощрение активного участия заинтересованных стран в проводимой ООН деятельности по укреплению доверия и надежности при использовании ИКТ.

Качественно новым этапом в мобилизации союзников в плане не только продвижения идеи обеспечения МИБ на международной арене, но и организации практического сотрудничества по ее реализации в рамках обширного Евразийского региона стало заседание 15 июня 2006 года Совета Шанхайской Организации Сотрудничества (ШОС). На нем главы государств—членов ШОС приняли специальное заявление по международной информационной безопасности. В своем заявлении руководители Республики Казахстан, Китайской Народной Республики, Киргизской Республики, Российской Федерации, Республики Таджикистан и Республики Узбекистан выразили озабоченность тем, чтов настоящее время появляется реальная опасность использования ИКТ в целях, способных нанести серьезный ущерб безопасности человека, общества и государства в нарушение основополагающих принципов равноправия и взаимного уважения, невмешательства во внутренние дела суверенных государств, мирного урегулирования конфликтов, не-применения силы, соблюдения прав человека. Подчеркивалось, что угрозы использования ИКТ в преступных, террористических и военно-политических целях, не совместимых с обеспечением международной безопасности, могут реализовываться как в гражданской, так и в военной сфере и привести к тяжелым политическим и социально-экономическим последствиям в отдельных странах, регионах и в мире в целом, к дестабилизации общественной жизни государств.

25-27 октября 2006 года во исполнение решения, содержащегося в Заявлении глав государств—членов Шанхайской организации сотрудничества по международной информационной безопасности от 15 июня 2006 года, состоялось учредительное заседание Группы экспертов государств — членов ШОС по МИБ. В заседании приняли участие эксперты всех государств—членов ШОС. В ходе заседания была официально образована Группа и согласованы институциональные основы ее работы, а председателем консенсусом был избран эксперт Российской Федерации как государства, инициировавшего рассмотрение в ШОС проблематики МИБ.

Выработанный Группой план действий государств—членов ШОС по обеспечению международной информационной безопасности был одобрен Решением Совета министров иностранных дел государств-членов 9 июля 2007 года и утвержден Решением Совета глав государств—членов ШОС, который состоялся 16 августа 2007 года. Планом предусматривается сотрудничество государств-членов в таких вопросах, как:

- выработка единого понятийного аппарата применительно к сфере МИБ;
- осуществление анализа угроз в области МИБ и выработка предложений по мерам противодействия им;
- выработка предложений по созданию практических механизмов мониторинга угроз в области МИБ и координации действий по обеспечению МИБ в пространстве ШОС;
- изучение и сопоставление национальных законодательств в сфере обеспечения информационной безопасности;
- исследование вопроса о международно-правовом регулировании и состоянии международно-правовой базы сферы МИБ;
- координация позиций стран—членов ШОС по МИБ в рамках международных организаций и форумов;
- разработка и осуществление мер доверия между государствами- членами ШОС в сфере обеспечения информационной безопасности; изучении возможных путей оказания взаимной **помощи** в области предотвращения деструктивных информационныхвоздействий и чрезвычайных ситуаций в сфере информационной безопасности, координации оперативного реагирования на них и ликвидации их последствий;
- изучение целесообразности разработки и заключения межправительственного соглашения о сотрудничестве в рамках ШОС в области обеспечения МИБ.

С этой целью и в духе создания режима коллективной информационной безопасности участники могли бы взять на себя обязательства отказаться от:

- разработки, создания и использования средств воздействия и нанесения ущерба информационным ресурсам и системам другого государства;
- несанкционированного вмешательства в информационно-телекоммуникационные системы и информационные ресурсы, а также их неправомерного использования;
- действий, ведущих к доминированию и контролю в информационном пространстве;
- противодействия доступу к новейшим информационным технологиям, создания условий технологической зависимости в сфере информатизации в ущерб другим государствам;
- поощрения действий международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных правонарушителей, представляющих угрозу информационным ресурсам и критически важным структурам государств;
- разработки и принятия планов, доктрин, предусматривающих возможность ведения информационных войн и способных спровоцировать гонку вооружений, а также вызвать напряженность в отношениях между государствами и собственно возникновение информационных войн;
- использования информационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационной сфере;
- трансграничного распространения информации, противоречащей принципам и нормам международного права, а также внутреннему законодательству конкретных стран;

манипулирования информационными потоками, дезинформации и сокрытия информации с целью искажения психологической и духовной среды общества, эрозии традиционных культурных, нравственных, этических и эстетических ценностей;

- информационной экспансии, приобретения контроля над национальными информационно-телекоммуникационными инфраструктурами другого государства, включая условия их функционирования в международном информационном пространстве.

Согласно договору государства и другие субъекты международного права должны будут нести международную ответственность за деятельность в информационном пространстве, осуществляемую ими, под их юрисдикцией или в рамках международных организаций, членами которых они являются, и за соответствие любой такой деятельности положениям договора.

Список использованных источников:

1. Научные и методологические проблемы информационной безопасности: Сб. ст. / Под ред. В. П. Шерстюка. М.: МНЦМО, 2004.
2. Council of Europe: Convention on Cybercrime. [Электронный ресурс]. — Режим доступа: http://conventions.coe.int/treaty/en/projects/FinalCybercrime.htm
3. G8 Summit: Okinawa Charter on Global Information Society. Okinawa. 2000. July 23. [Электронныйресурс]. — Режимдоступа: http://europa.eu.int/comm/ extemal_relations/g8/intro/global/info_society.htm.
4. International Expert Conference on Computer Network Attacks and Applicability of International Humanitarian Law (17-19 November 2004, Stockholm, Sweden) / Ed. by K. Bystrom. Publisher: Swedish National Defence College. Stockholm.