ИНТЕРНЕТ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В АРАБСКОМ МИРЕ

Е.С. ПЕЛЕВИНА
Аспирантка
Северо-западный институт управления РАНХиГС (Санкт-Петербург)

Ключевые слова: Арабский Восток, информационные технологии, Интернет, информационные войны, кибертерроризм

В наше время появляются или готовы появиться новые формы терроризма: ядерный, биологический, химический, экологический, психологический и компьютерный (кибернетический) (КБТ)[1]. Последний, учитывая массовую информатизацию общества, несет одну из самых серьезных угроз человечеству, включая, разумеется, и арабские государства.

Новейшие информационные технологии, феномен Интернета вывели мир на качественно новый уровень, когда борьба государств за сферы влияния переходит и в виртуальную плоскость. С распространением процессов глобализации в конце 1990-х гг. арабские страны на собственном опыте столкнулись с положительными и отрицательными сторонами ее информационного аспекта.

КИБЕРНЕТИЧЕСКИЕ УГРОЗЫ В СОВРЕМЕННОМ МИРЕ

В течение длительного времени благополучие общества в подавляющем большинстве стран и его экономическая стабильность основывались и основываются на работе сетей передачи информации и вычислительных сервисов. Однако на нормальное функционирование ключевых информационных и коммуникационных систем влияет много негативных факторов[2], что делает одной из базовых задач государств обеспечение кибернетической безопасности как на локальном, страновом, так и на международном уровнях.

По данным отчета по кибербезопасности компании *Symantec*, киберпреступления по всему миру за 2015 г. нанесли ущерб в $158 млрд. По оценке компании, всего жертвами киберпреступлений за прошедший год стали 594 млн человек. Преступления обошлись, в среднем, в $358 на человека. При этом на устранение последствий кибератак, в среднем, уходил 21 час[3].

Общепринятое определение компьютерного терроризма таково: это сознательное и целенаправленное применение ресурсов информационных систем для реализации террористических действий в киберпространстве (КБП), а также для достижения других целей в интересах террористических группировок.

Термин КБТ тесно связан с другим важным понятием - кибернетические атаки (КБА). Современные угрозы информационной безопасности (кибербезопасности[4]) характеризуются высокой гибкостью, а КБА уже давно стали эффективным средством для достижения широкого спектра целей, разнообразие которых ограничено только воображением и фантазией применяющей их стороны.

По данным известной «Лаборатории Касперского»[5], наиболее опасные киберугрозы в мире - специально созданное кибероружие и манипуляции

ИСТОРИЯ РАЗВИТИЯ КИБЕРТЕРРОРИЗМА И ПРИМЕРЫ КИБЕРУГРОЗ[6]

- 1960 г. - появление первых транзисторных вычислительных систем и, как следствие, возникновение первых примитивных киберпреступлений, состоявшихся преимущественно в 1970-х гг.;
- начало 1980-х гг. - переход от физических повреждений к противоправному использованию компьютерных систем и манипулированию электронными данными;

- 1982 г. - сотрудниками компании *Xerox* Дж.Шоком и И.Хуппа впервые введен термин компьютерный «червь»;

- 1983 г. - первый арест «виртуальных преступников», группы хакеров «Банда 414» (Милуоки, США), которая взломала 60 компьютеров;

- 1987 г. - зарегистрировано первое семейство компьютерных вирусов «Иерусалим»;

- 1988 г. - создан первый мультиплатформенный червь, способный перемещаться в сети Интернет; эпидемия в результате действия «червя Морриса»: повреждено 4 тыс. интернет-серверов, общий вред - более $98 млн;

- 1989 г. - появление первого антивирусного программного обеспечения *McAfee*;

- 1990 г. - первый в истории суд над «автором» компьютерного вируса американским студентом Р.Моррисом, приговоренным к 3 годам лишения свободы условно и штрафу в $10 тыс.;

- 1992 г. - создано первое полиморфное семейство вирусов *Mutation Engine*;

- 1993 г. - в Лондоне злоумышленники, совершив кибератаку, предъявили ряду брокерских контор, банков и крупных фирм требование о выплате 10-12 млн ф.ст. отступных;

- 1994 г. - организация «Фронт освобождения Интернета», открыв кибервойну компаниям *National Broadcasting Corporation* и *General Electric*, с помощью КБА вывела из строя их внутренние сети;

- 1995 г. - группа хакеров «*Strano Network*» реализовала мощную КБА на компьютеры правительства Франции;

- 1996 г. - террористическая организация «Тигры освобождения Тамил-Илама» провели КБА против дипломатических представительств Шри-Ланки;

- 1997 г. - в результате действий неустановленного хакера прервалась передача медицинских данных между наземной станцией НАСА и космическим кораблем «Атлантис»; ФБР США расследовало 200 случаев киберпреступлений;

- 1998 г. - 12-летний хакер проник в компьютерную систему, которая контролирует паводковые шлюзы плотины Т.Рузвельта в Аризоне - под угрозу затопления попали два города с населением 1 млн человек; мощная кибератака на индийский Центр ядерных исследований им. Баба, в результате которой возникла угроза системе управления реактором;

- 1999 г. - широкомасштабная компания КБА Китая и Тайваня друг против друга, в результате которой пострадали порталы госучреждений, финансовых компаний, университетов и т.д.; хакеры захватили управление американским военным спутником серии *Skynet* и изменили его орбиту; за год ФБР расследовало 800 киберпреступлений[7];

- 2000 г. - из пригорода Манилы в Интернет запущен вирус «*I love you*» (другое название - «*Love Bug*»), который быстро распространился по всему миру и заразил более 45 млн компьютерных сетей, в т.ч. сети Белого дома, ЦРУ, министерства обороны и Конгресса США, британского парламента и т.д.; масштабная *DoS*-атака (*Denial of Service* - хакерская атака на вычислительную систему с целью довести её до отказа) сделала недоступными в течение 2-3 часов серверы крупных компаний *Yahoo*, *eBay*, *CNN* и *ZDNet*; кибератака от имени чеченских националистов на сервер «Росбизнесконсалтинг»; группа пакистанских хакеров «Мусульманский онлайн-синдикат» атаковала более 500 индийских интернет-сайтов в знак протеста против военных действий в Кашмире;

- 2001 г. - крупнейшая атака на военные компьютеры: шотландский хакер Г.Маккинон сломал десятки компьютеров оборонных ведомств своей страны; 15-летний канадский хакер *Mafia Boy* успешно провел *DoS*-атаку на несколько крупных сетевых компаний - нанесенный им ущерб оценивается более чем в $1 млрд;

- 2002 г. - в первые сутки года зарегистрировано 79 мощных кибератак;

- 2003 г. - появление червяка *Blaster*, использующего уязвимость *Windows*;

- 2004 г. - массированная кибератака на электронные ресурсы правительства Южной Кореи; зафиксировано 75 тыс. попыток взлома серверов Пентагона;

- 2005-2006 гг. - по всему миру зафиксировано более 2 млн кибератак на информационные ресурсы органов государственной власти;

- 2007 г. - массированная кибератака на Рунет; мощная кибератака на сайты государственных структур Эстонии;

- 2008 г. - мощная кибератака на информационные компьютерные системы Грузии привела к изоляции грузинского правительства и народа от внешнего мира; миллионы рабочих станций на базе *Windows* по всему миру стали жертвами червя *Win32 /Conficker*;

- 2009 г. - китайская шпионская кибероперация *Ghostne* с проникновением в компьютерные сети более чем 100 стран мира;

- 2010 г. - кибератака перед саммитом «Большой двадцатки» в Париже; первая межконтинентальная кибератака *Stuxnet* в Иране; мощная *DoS*-атака на информационную инфраструктуру Мьянмы; на страницах сайта *Wikileaks* опубликовано огромное число секретных документов по войнам США в Афганистане и Ираке, а также более 250 тыс. документов переписки американских дипломатов; в результате КБА выведены из строя сайты крупнейших международных платежных систем *Visa*, *MasterCard* и *PayPal*; группа хакеров провела *DoS*-атаку на «Аэрофлот», в результате чего в течение недели была заблокирована услуга покупки электронных билетов[8];

- 2011 г. - беспрецедентная утечка данных в результате кибератаки на серверы Пентагона; кибератака на серверы *Sony* и «Банка Америки» с последующей публикацией конфиденциальной информации в Интернете; широкомасштабная кибератака перед саммитом Евросоюза в Брюсселе;

- 2012 г. - хакерская группа *Anonymous* атаковала сайты госучреждений Израиля - в результате пострадали сайты «Моссада», армии и спецслужб; в Швеции осуществлена мощная КБА на министерство обороны, «Сведбанк» и Управление железных дорог; американские киберэксперты успешно атаковали пропагандистский сайт «Аль-Каиды» в Йемене; осуществлены мощные вирусные кибератаки на ряд энергетических компаний США[9];

- 2013 г. - неизвестные хакеры получили доступ и опубликовали персональные данные 40 тыс. солдат армии США и более 2 млн партийных функционеров правящей партии Республики Корея; активисты хакерской группировки *WikiCrew* с помощью *DoS*-атаки вывели из строя официальный сайт Агентства национальной безопасности США; хакерская группа *Syrian Electronic Army* провела кибератаку на информационную инфраструктуру системы водоснабжения израильского города Хайфа;

- 2014 г. - атаке анонимных хакеров подверглась программа, управляющая электронными деньгами - биткоинами; в конце февраля - начале марта 2014 г. произошел взлом базы данных американской компании *eBay*, владеющей одной из основных онлайн-площадок по купле-продаже товаров; 15 марта 2014 г. в результате масштабной хакерской атаки, предпринятой группой украинских хакеров «КиберБеркут», свыше 10 часов были практически недоступны сайты НАТО; в начале июня 2014 г. в результате взлома базы данных французского подразделения международной сети ресторанов *Domino Pizza* хакерской группой *Rex Mundi* были похищены персональные данные 592 тыс. французских и 58 тыс. бельгийских клиентов компании[10];

- 2015 г. - взлом аккаунтов военного командования США в социальных сетях группировкой «Киберхалифат», связанной с террористической организацией «Исламское государство»; направленная атака на «Лабораторию Касперского» с применением вредоносного ПО *Duqu 2*.

в социальных сетях. Так, с помощью социальных сетей можно организовывать различного рода протесты, митинги и демонстрации, причем организаторы подобных мероприятий могут находиться в любом месте мира, эффективно манипулируя массами.

«АРАБСКАЯ СПЕЦИФИКА» ИТ-ТЕХНОЛОГИЙ

Будучи частью цивилизованного мира, арабское общество не может игнорировать все вышеперечисленное, и в нем есть силы, стремящиеся взять на вооружение технику и приемы киберпреступности. Хотя по уровню развития информационных технологий (ИТ) страны Арабского Востока значительно уступают развитым странам Севера, однако с каждым годом проникновение Интернета и цифровых технологий в эти государства ощущается все сильнее.

Появление Интернета открыло новые возможности самым разным кругам арабского общества[11]. «Всемирную паутину» наполнили исламские сайты с текстами из Корана и их трактовкой различными онлайн-проповедниками. Отсутствие цензуры в Интернете позволяет появляться сайтам в Интернете, которые размещают тексты достаточно вольной трактовки Корана, вызывая недовольство консервативных исламских кругов по всему миру. Ряд мусульманских институтов, включая Каирский университет Аль-Азхар, считающийся самым авторитетным учреждением по изучению ислама, основали собственные веб-сайты для онлайн-ответа «неисламским», по их мнению, сайтам[12].

Развитие кибертерроризма и активное использование информационных технологий, социальных сетей террористами в Арабском мире в своей основе имеют следующие основные причины (см. *схему*).

Мы наблюдаем также, что Интернет становится инструментом в религиозном противостоянии суннитов и шиитов. Представители обоих течений ислама систематически атакуют сайты друг друга, используя хакерство как эффективное средство религиозной борьбы. Хакерским атакам в последнее время подверглись в общей сложности 77 шиитских сайтов. Со своей сторо-

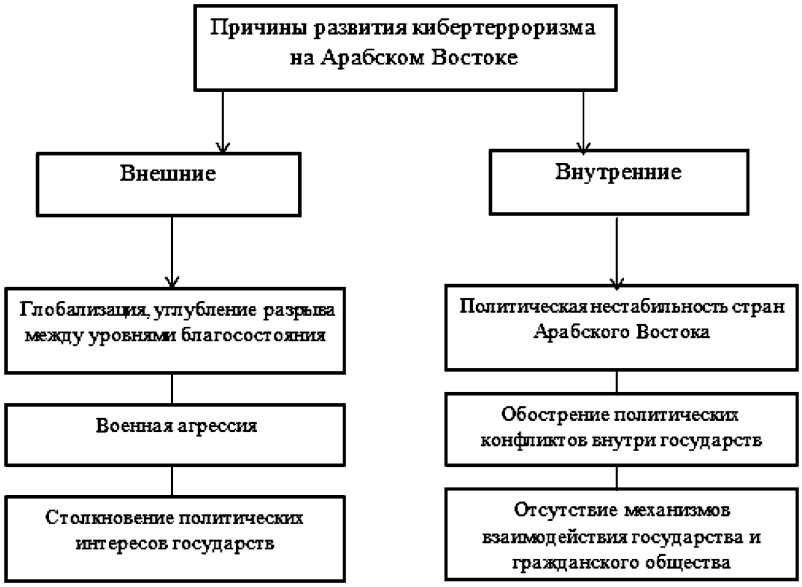

Схема. Причины кибертерроризма в Арабском мире.

Составлено автором по: *Клименский М.М.* Кибертерроризм как угроза национальной безопасности государства: тенденции развития // Сборники конференций НИЦ Социосфера. 2014. № 33. С. 22-24.

ны, шииты атаковали около 900 суннитских сайтов, среди которых оказались сайты муфтия Саудовской Аравии и группы известных саудитских ученых[13].

Благодаря интернет-сети деятельность радикальных исламистских группировок и террористических организаций приобрела глобальный характер. С появлением кибертерроризма появилось и понятие «электронный джихад». Кибератаки, направленные на компьютерные системы министерств обороны, торговых центров и биржевых рынков, несут в себе не менее серьезную угрозу, а может, и бóльшую, чем классические теракты с использованием взрывчатки. При этом они не требуют больших материальных затрат[14].

Блогосфера быстро стала инструментом политической борьбы значительной части населения арабских стран. Так, развитию блогосферы в Египте в значительной степени способствовало появление политического движения «Кифайя» («Хватит!»). К этому движению потянулись и другие оппозиционные активистские движения, создав свои блоги в Интернете. Появившиеся в начале нового века медиаплатформы - *Twitter*, *Flikr* и *Facebook* - дали новый толчок развитию египетской блогосферы. Киберактивисты с их помощью присылают сообщения журналистам и правозащитным организациям о незаконных арестах, нарушениях прав и т.д.[15]

По мнению чешского исследователя Вита Сислера, значительную роль в формировании общественного мнения в арабском мире, кроме Интернет-сети и электронных СМИ, стали играть видеоигры, влияющие на процесс восприятия и интерпретации современных реалий, в то время как европейские и американские видеоигры обычно представляют Ближний Восток в квазиисторической манере или как источник потенциального терроризма, создавая стереотипное восприятие арабов как врагов[16].

Производство видеоигр в арабских странах пока только начинается, поэтому большинство игр на арабском рынке представлено западными производителями и часто несет антиарабское и антиисламское содержание. Играя в такие игры, арабы «атакуют» собственную культуру, религию и образ жизни. Из-за этого, по мнению исполнительного директора сирийской компании «Афкар Медиа» Радвана Касмии, молодежь, играющая в такие видеоигры, испытывает комплекс вины перед остальным миром[17].

ЛИДЕРЫ - ОАЭ И ЕГИПЕТ

Арабский мир активно участвует в процессе строительства информационного общества. Интернет-сеть, электронные СМИ и видеоигры стали важными инструментами формирования общественного мнения. Темпы информационного развития арабских государств в последние годы существенно выросли. Их правительства считают сектор информационных технологий одним из наиболее приоритетных направлений развития своих экономик. По данным исследователей *The Arab Advisors Group*, сегодня около 20 арабских стран имеют электронные правительственные порталы; среди них: Бахрейн, Египет, Иордания, Кувейт, Ливан, Мавритания, Марокко, Катар, Саудовская Аравия, Сирия, Тунис и ОАЭ[18].

Еще один феномен, который набирает популярность в арабском регионе с развитием информационных технологий - создание т.н. медиагородков - индустриальных центров, где сосредоточиваются и функционируют медиакомпании. Египетский *Media Production City* был первым медиагородком, основанным в арабском регионе еще в 1997 г., по образцу ко-

торого в 2001 г. появились *Dubai Media City* (Дубай, ОАЭ) и *Jordan Media City* (Иордания). Сейчас в регионе действуют 8 медиагородков, 5 из них находятся в ОАЭ и по одному - в Египте, Иордании и Омане[19].

ОАЭ остаются несомненным лидером в арабском регионе «в ИТ-измерении». Они занимают 1-е место среди остальных арабских государств по многим показателям ИТ, а именно: индексу сетевой готовности, индексу развития ИТ, пропускной способности международного потенциала Интернет, важности ИТ-сектора для правительства и т.п.[20] Правительство страны видит в ИТ-инфраструктуре удачный сектор для зарубежных инвестиций и диверсификации экономики.

Дубай - это, безусловно, ведущий региональный центр развития новых ИТ-технологий в арабском мире. В 2000 г. здесь была создана свободная зона *TECOM* (*The Dubai Technology E-Commerce & Media Freezone*), включающая в себя более 650 компаний, функционирующих в отраслях телекоммуникации, медиа и информационных технологий. В рамках *TECOM* были созданы такие крупные и ныне известные во всем мире компании, как «Дубай Интернет Сити», «Дубайский Идейный Оазис», «Деревня знаний»[21].

Велики амбиции в сфере развития информационных технологий у Египта. Несмотря на жесткий политический режим и недостаток демократических свобод, в стране проводится активная политика в секторе массмедиа. Именно Египет запустил еще в 1990 г. первый арабский спутниковый телевизионный канал, а затем и еще два: *Nilesat-1* - в 1996 г. и *Nilesat-2* - в 2000 г. Спутники транслируют 117 телевизионных каналов. 32 радиостанции распространяют информацию о Египте по всему миру[22].

Кроме того, сами страны Арабского Востока зачастую становятся источниками распространения кибератак. Так, в 2014 г. компания *FireEye* обнаружила волну атак, созданную группой злоумышленников из Ближнего Востока и направленную на несколько европейских государственных организаций и, по крайней мере, одно финансовое учреждение в США. Атаки известны как *Operation Molerats*. Их жертвами стали правительственные ведомства Израиля, Словении, США, а также Британская вещательная корпорация BBC[23].

По данным интервью главы подразделения киберзащиты Армии обороны Израиля, опубликованном в *Financial Times*, Иран и противостоящие ему страны в 2016 г. развернут настоящую кибервойну. По словам израильских официальных лиц, иранским хакерам в августе 2012 г. удалось вывести из строя тысячи компьютеров саудовской и катарской национальных нефтяных компаний. В сентябре того же года иранцам удалось нарушить работу электронных сетей нескольких американских банков[24].

Остро стоит вопрос с кибербезопасностью в Сирии. По данным газеты *New York Times*, у Пентагона и Агентства национальной безопасности США уже давно есть план кибератаки против Сирии. В 2011 г. он был заблокирован президентом Обамой. В 2015 г. военные предложили Белому дому еще раз рассмотреть этот вопрос. Благодаря Эдварду Сноудену известно, что в 2011 г. американцы совершили 200 с лишним кибератак, большинство из которых были направлены против Ирана, Китая, КНДР и России[25].

Развитие информационных технологий в арабском мире идет по многим направлениям при существенной поддержке со стороны правительств и часто на основе специально разработанных государственных ИТ-стратегий. Однако, как было сказано выше, арабские страны именно благодаря современным ИТ-технологиям уязвимы к внешним киберугрозам. Здесь налицо определенная опасность возникновения информационных войн, угрожающих нормальному развитию как отдельных государств, так и функционирующим в регионе международным организациям.

КИБЕРТЕРРОРИЗМ КАК ОРУЖИЕ «ИСЛАМСКОГО ГОСУДАРСТВА»

Сегодня кибертерроризм представляет собой использование сетей для организации террористической деятельности. При этом блокирование сайтов, как показала история откровений Сноудена, не решает проблемы[26].

Террористическая группировка ИГ постепенно вывела пропаганду в социальных сетях на достаточно высокий профессиональный уровень. Боевики стали настоящими профессионалами в сфере социального маркетинга, выкладывая в *Instagram* селфи с оружием, транслируя бои в *Twitter* с помощью собственного мобильного приложения и интернет-магазина, где продаются футболки с логотипом террористов. Еще один канал - фильмы, которые специально снимаются террористами; в частности, речь идет о пропагандистском полнометражном фильме «Звон мечей IV». Некоторые специалисты склоняются к мнению, что именно онлайн-тактика стала основой проведения террористами успешной кампании по привлечению к себе новых сторонников.

Во время штурма иракского города Мосул в общей

сложности было опубликовано около 40 тыс. твитов, поддерживающих ИГИЛ, что позволило выводить в верхние строки поиска нужные хештеги - *#ISIS*, *#AllEyesOnISIS*, *#Iraqwar* и фотографии, манипулируя новостной повесткой. Устрашающие видеоролики, твиты с пометкой «мы идём вас убивать», рассказы об убитых иракских военных, фотографии обезглавленных или распятых тел представляют собой виртуальную атаку на город, что является не менее устрашающим, чем реальность. В частности, в итоге такой информационной войны, по сообщениям британской *The Guardian*, защитники Мосула в панике оставляли свои позиции. Источник газеты *Washington Post* сообщал, что за первые недели наступления боевиков ИГ в Ираке свыше 90 тыс. военнослужащих правительственных войск дезертировали[27].

В докладе «*The New Terrorism and New Media*» Центра Вудро Вильсона в 2014 г. говорится, что аккаунты в *Twitter*, *YouTube* или *Facebook* позволяют группировкам стать частью мейнстрима, социальные сети удобны и просты в использовании, надёжны и бесплатны. Некоторые израильские специалисты уверяют, что число завербованных боевиками через социальные сети сильно недооценивается[28].

В 2015 г. террористы, принадлежащие к группировке «Исламское государство», открыто заявили, что вскоре начнут полноценную кибервойну против экономики и инфраструктуры США. Кроме того, исламисты сообщили о своих намерениях создать «киберхалифат» (*cyber caliphate*) с целью проведения постоянных кибератак и взлома американских государственных и частных структур[29].

Таким образом, распространение угроз кибертерроризма при поддержке группировки ИГ делает современный мир все более уязвимым в информационном пространстве и ставит его перед необходимостью консолидации в вопросах как борьбы с киберпреступностью и принятия единой слаженной политики в этой сфере, так и в целом консолидации усилий по борьбе с группировкой «Исламское государство».

ПУТИ ЗАЩИТЫ ОТ КИБЕРТЕРРОРИЗМА

Развитие информационных технологий способствует массовому распространению кибертерроризма в странах Арабского Востока. Препятствовать этому можно, только обобщив опыт более развитых в этом отношении стран, которые активно разрабатывают и применяют меры защиты от кибертерроризма[30].

В настоящее время мировым сообществом накоплен значительный опыт борьбы с кибертерроризмом. На международном уровне приняты несколько нормативно-правовых актов, которые регламентируют эту проблему. Генеральная Ассамблея ООН в резолюции 53/70 от 4 декабря 1998 г. затрагивает вопросы необходимости разработки международных принципов организации работы по противодействию кибертерроризму, которые, в свою очередь, предусматривают меры по усилению безопасности глобальных интернет- и информационных систем. Важный шаг в процессе формирования международной правовой базы в этом направлении - подписание 23 ноября 2001 г. странами - членами Совета Европы, а также США, Канадой и Японией Конвенции Совета Европы «О киберпреступности».

Следующий важный шаг - консолидация государственного и частного секторов внутри государств в целях борьбы с кибертерроризмом. Так, после многочисленных высококлассных атак на корпорации по всей Великобритании Национальное агентство по борьбе с преступностью (*National Crime Agency - NCA*) стало активно помогать сетевым администраторам осуществлять управление ключевыми частями британской интернет-инфраструктуры.

Британское правительство приняло участие в нескольких международных операциях, направленных на борьбу с киберпреступлениями. *NCA* совместно с европейскими агентствами по преступлению остановило работу нескольких серверов. Был произведен ряд арестов в 140 аэропортах разных стран. В ходе международной правоохранительной операции задержано около 130 подозреваемых.

В 2015 г. мировым сообществом были приняты следующие меры по борьбе с кибертерроризмом:

- представлен второй доклад Контртеррористического комитета «Об исполнении резолюции 2178 СБ ООН по иностранным террористам-боевикам» (Implementation of Security Council Resolution 2178 (2014) by States Affected by Foreign Terrorist Fighters);

- генеральный секретарь Интерпола Юрген Шток провёл в Пекине переговоры с министром общественной безопасности КНР Го Шэнькунем, заместителем секретаря Центральной комиссии по проверке дисциплины Чжао Хунджу и некоторыми другими высокопоставленными чиновниками о развитии сотрудничества в борьбе с транснациональной преступностью и киберпреступностью; о борьбе с терроризмом; о поддержке глобальных и региональных инициатив Интерпола;

- объявлено о начале ряда совместных мероприятий Интерпола и Европола с возможностью присоединения к ним партнёров со всего мира, в частности: создание объеди-

ненной целевой группы по сотрудничеству в сфере киберпреступности и совместимости (*Joint Cybercrime Cooperation and Compatibility Taskforce*) в целях гармонизации различных правовых систем для оперативного взаимодействия по вопросам отмывания денег в глобальном масштабе; развитие партнерства против злоупотребления виртуальной валютой для незаконных операций и отмывания денег;

- Федеральная торговая комиссия США и семь международных партнеров - регуляторы из Австралии, Канады, Ирландии, Нидерландов, Новой Зеландии, Норвегии, Великобритании - выступили с новой инициативой, призванной усилить сотрудничество в деле защиты конфиденциальных данных потребителей[31].

* * *

В заключение подчеркнем, что решение проблемы борьбы с распространением кибертерроризма требует объединения усилий не только государств арабского мира, но также интеллектуального потенциала и политической воли всего мирового сообщества[32].

---

[1] *Корченко О.Г.* Признаковый принцип формирования классификации кибератак // Вестник Восточноукраинского национального университета им. Владимира Даля. 2010, № 1. С. 32-38.

[2] *Харченко В.П.* Кибертерроризм на авиационном транспорте // Проблемы информатизации и управления: Сб. науч. пр. Вып. 4 (28). К., НАУ, 2009. С. 131-140.

[3] Потери от кибератак в 2015 году составили $158 млрд - http://versii.com/news/341903/

[4] Information technology - Security techniques-Guidelines for cybersecurity. ISO/IEC 27032. 2012.

[5] Anti-Malware - http://www.anti-malware.ru/

[6] *Бурячок В.Л.* Основы формирования государственной системы кибернетической безопасности. К., НАУ. 2013.

[7] Супертерроризм: новый вызов нового века // Научные записки ПИР-Центра / Под общ. ред. Федорова А.В. М., Изд-во «Права человека». 2002. С. 92-109.

[8] Информационные вызовы национальной и международной безопасности / Под общ. ред. Федорова А.В. и Цыгичко В.Н. М., ПИР-Центр. 2001.

[9] *Мельник С.В.* К проблеме формирования понятийно-терминологического аппарата кибербезопасности // *Мельник С.В., Тихомиров О.О., Ленков О.С.* Сборник научных трудов Военного института КНУ им. Тараса Шевченка. К., ВИКНУ, 2011. Вып. 30. С. 159-165.

[10] Крупные атаки хакеров в 2001-2014 гг. Хронология - http://tass.ru/info/1408961

[11] *Абрамова И., Поликанов Д.* Африка в век информационных технологий: возможность прорыва // Азия и Африка сегодня. 2001. № 8. С. 19. (*Abramova I., Polikanov D.* 2001. Afrika v vek informatsionnykh tekhnologiy... // Aziya i Afrika segodnya. № 8) (in Russian)

[12] *El-Kashef Injy*. Islam dot com - http: www.islamicity.com/AlAhram/20051014/fault.htm

[13] *Sadeq Adel Abdel*. Internet Hacking between Sunnis and Shia: when politics manipulate religion - http: www.acpss.ahram.org.eg/eng/ahram/2004/7/5/EGYP74.htm

[14] *Куприенко Е.Е.* Интернет как инструмент террористических и экстремистских организаций - http://www.iimes.ru/rus/stat/2005/03-10-05.htm

[15] *Radsch Courtney*. Core to Commonplace: The Evolution of Egypt's blogoshere // ArabMedia & Society, September 2008.

[16] *Sisler Vit*. Representation and Self-Representation: Arabs and Muslims in Digital Games - http: //www.digital-islam.eu/article.do?articleId=1423

[17] *Sisler Vit*. Digital Arabs: Representation in Video Games - http://www.digitalislam.eu

[18] e-Government on the march in the Arab World: 11 Arab countries have already launched e-Government portals - http://www.arabadvisors.com/Pressers/presser-021209.htm

[19] Eight media cities serve the Arab World's media industry with more cities on the horizon - http: // www.arabadvisors.com/Pressers/presser-011109.htm

[20] UAE Rankings in Various International Studies - http://www.tra.gov.ae/E_rankings.php

[21] *Peterson Jonathan D.* The Information & Communication Technology Landscape in the United Arab Emirates - http://www1.american.edu/carmel/jp2450a/author.htm

[22] Egypt and the Cultural Globalization - www.sis.gov.eg/En/Pub/magazine/spring2003

[23] Хакеры из Ближнего Востока совершают кибератаки на правительственные ведомства по всему миру - http://internetua.com/hakeri-iz-blijnego-vostoka-sovershauat-kiberataki-na-pravitelstvennie-vedomstva-po-vsemu-miru

[24] ЦАХАЛ: в 2016 г. мир ожидает мощная волна иранских кибератак - http://cursorinfo.co.il/news/novosti1/2016/01/23/cahal-v-godu-mir-ozhidaet-moshnaya-volna-iranskih-kiberatak/

[25] США готовят кибератаку против Сирии - http://oko-planet.su/politik/newsday/232591-ssha-gotovyat-kiberataku-protiv-sirii.html

[26] *Рогозинский Рафал.* Цель «Исламского государства» - создать халифат, в который должен войти и Казахстан - http://digital.report/rafal-rogozinskiy-tsel-islamskogo-gosudarstva-sozdat-halifat-v-kotoryiy-dolzhen-voyti-i-kazahstan/

[27] Джихад в *Twitter*: Как террористы осваивают приёмы социального маркетинга - http://apparat.cc/network/isis-social-war/

[28] Там же.

[29] Арабские террористы угрожают провести масштабную кибератаку против США - http://www.securitylab.ru/news/458038.php

[30] *Polikanov D., Abramova I.* Africa and ICT: a Chance for Breakthrough? // Information Communication and Society. 2003. Т. 6. № 1. С. 51.

[31] События по борьбе с киберпреступностью и кибертерроризмом в 2015 г. - http://d-russia.ru/sobytiya-po-borbe-s-kiberprestupnostyu-i-kiberterrorizmom-v-oktyabre-2015-goda.html

[32] *Пахарева Е.Н.* Кибертерроризм как технология воздействия на молодежную среду: причины и пути минимизации // Ученые записки Российского государственного социального университета. 2009. № 4. С. 77-81.