Киберугрозы и защита информации

Алексей Кухаркин

За последние пару десятилетий компьютеризация стала обязательным условием эффективности деятельности, а революция в информационных технологиях (ИТ) преобразила все стороны жизни человека. Но переход к ИТ на базе вычислительной техники несет с собой не только огромные преимущества, но и новые риски, и возможные сопутствующие негативные последствия. В целом производственная, управленческая и другие стороны деятельности организаций и предприятий представляются сейчас немыслимыми без широкого внедрения прогрессивных цифровых ИТ, а появляющиеся при этом новые риски и угрозы требуют своевременного парирования.

Столкнувшись с новыми вызовами, в индустриально-развитых странах в последние годы стали уделять повышенное внимание проблеме растущих угроз национальной безопасности, порождаемых недостаточной защищенностью информационных компонентов национальной инфраструктуры от кибернетических атак, исходящих не только от недружественных государств, но даже от частных лиц. В государствах стали изыскивать возможности для проведения дорогостоящих широкомасштабных организационно-технических мероприятий для нейтрализации новых угроз.

Так, в Официальном заявлении президента США Б.Обамы говорится о нарастающей тенденции роста кибершпионажа и преступлений в информационно-коммуникацион-

---

КУХАРКИН Алексей Валерьевич – аспирант ФГУП «Научно-исследовательский центр информатики при Министерстве иностранных дел Российской Федерации». *E-mail:* akuharkin@ya.ru

Ключевые слова: киберпреступность, информационная защита, информатизация здравоохранения.

ных сетях, включающих Интернет, телекоммуникационные и компьютерные структуры. Вследствие этого угрозы федеральным информационно-технологическим сетям вполне реальны и серьезны, а кибербезопасность становится высшим приоритетом национальной безопасности страны в XXI в.

Эксперты из Министерства внутренней безопасности США также считают, что архитектура национальной цифровой инфраструктуры страны, базирующейся в значительной степени на Интернете, далеко не безопасна. Это подтверждается тем, что в последние годы она многократно подвергалась вторжениям, что позволило хакерам красть деньги, интеллектуальную собственность и военную информацию.

Ежегодный ущерб американских коммерческих предприятий от хищений и разнообразных мошенничеств, совершаемых с помощью информационных технологий только через Интернет, достигает 5–7 млрд долл.; еще не менее 3 млрд теряются из-за взломов и повреждений локальных сетей. Специально проведенные имитационные исследования скрытого проникновения в информационные системы военного назначения, обычно лучше защищенные, чем гражданские, показали, что в среднем в 88% случаев такие атаки увенчались успехом и лишь 4-5% попыток удаленного несанкционированного доступа были своевременно обнаружены и пресечены1.

Согласно результатам исследований авторитетной аналитической организации *RAND Corporation* (США), следует сосредоточиться на защите критических компьютерных сетей, так как в будущем, имея в виду быстрое развитие кибертехнологий и рост кибершпионажа, будет все труднее предотвратить нападения на важные гражданские и военные объекты. По их оценке, ежегодный ущерб, наносимый американским информационным системам, составляет порядка 100 млрд долл.[1]

Подавляющее большинство случаев кибератак остаётся неизвестным широкой публике[2–4].

Вот перечень самых «резонансных» в мире крупномасштабных кибератак:

– в 2007 г. в связи с народными волнениями из-за переноса монумента «Бронзовый солдат» в Таллине, Эстония испытала хакерскую атаку на правительственные сайты, функционирование которых было блокировано;

– в 2008 г. массированная кибератака на Грузию была произведена во время военных действий против Южной Осетии;

– в конце 2008 г. программный червь проник в сеть сухопутных войск США. Как следствие, пришлось запретить использование сменных носителей информации (в частности, дискет) в Министерстве сухопутных войск, а затем и в министерстве обороны США. Вскоре ввели соответствующие ограничения в Национальном управлении США по аэронавтике и исследованию космического пространства (НАСА);

– в 2008–2009 гг. группа хакеров из китайской провинции Сычуань на протяжении 8 месяцев неоднократно взламывала компьютеры высокопоставленных сотрудников Министерства обороны Индии и скачива-

ла с них секретные документы. Специалисты, учитывая уровень квалификации злоумышленников, а также характер их целей, не исключают вероятности того, что хакеры действовали с ведома и одобрения китайского правительства, что китайцы категорически отрицают;

– в апреле 2009 г. пришло сообщение о неизвестных хакерах, проникших в сеть компании *Lockheed Martin* (США), занятой разработкой новейшего истребителя 5-го поколения *(Air Force's Joint Strike Fighter – JSF)*, и похитивших терабайты информации;

– корпорация *Google* (США) вместе примерно с 20 другими крупнейшими компаниями подверглась кибернападению со стороны Китая в конце 2009 г.;

– вирусные атаки на ядерные объекты в Иране в 2010-2011 гг.[2–12]

В материалах конгресса США летом 2010 г. использована следующая типизация кибератак:[6,7] отказ обслуживания, распределенный отказ обслуживания, инструменты взлома («отмычки»), логические бомбы, фишинг, сниффер, «трояны», вирусы, вишинг, «военное катание», «черви», «атака нулевого дня». Кроме того, выделяют также киберугрозы, ставящие целью захват контроля над компьютером, управляющим какой-либо реальной инфраструктурной или иной функциональной системой.

Появление сложных компьютерных вирусов, способных проникать в управляющие схемы объектов, свидетельствует о том, что угроза кибертерроризма в мире весьма реальна.

Об этом заявил президент компании *McAfee Inc.* (США), занимающейся разработкой антивирусного программного обеспечения [4], добавив: «Когда становится известно об атаках, нацеленных на жизненно важные объекты инфраструктуры, которые способны вызвать аварию на атомном предприятии, появляется повод для серьезного беспокойства».

Участились случаи возникновения труднообъяснимых аварийных ситуаций на предприятиях нефтегазовой и электроэнергетической промышленности.

Одним из потенциально опасных подозрительных инцидентов стало внезапное, практически одновременное нарушение работы сразу двух американских АЭС (ноябрь 2010 г.).

Сначала из-за отказа дистанционно-управляемых систем охлаждения, утечек радиоактивных вод и неисправности насосов первого контура была на неделю остановлена АЭС в штате Вермонт.

Меньше чем через час после этого происшествия неожиданно взорвался и сгорел один из мощных силовых трансформаторов на территории АЭС в штате Нью-Йорк, что вызвало аварийное отключение ее реакторов.

В обоих случаях были зарегистрированы сбои компьютерных систем управления и несанкционированный удаленный доступ к программному обеспечению[2].

К настоящему времени уже выявлено несколько десятков новых компьютерных вирусов модульного типа, наиболее опасным из которых признан вирус (вернее, троянский вирусный червь) *Stuxnet*, который нанес вред иранской программе обогащения урана на Бушерской АЭС и производственном комплексе Натанз по разделению изотопов урана[9, 10]. Такие вирусы специально предназначены для внедрения в промышленные, энергетические и финансовые сети или для несанкционированного доступа к конфиденци-

альной информации, а также для удаленного осуществления определенных вредоносных действий, например, вывода из строя оборудования автоматизированных систем управления технологическими процессами (АСУ ТП).

Stuxnet относится к практически не имевшему аналогов в прошлом классу программного обеспечения, разработанного на высокопрофессиональном государственном уровне для диверсионных кибернетических атак. Он является результатом совместной тайной работы большой интернациональной команды специалистов из США, Великобритании и Израиля[11].

В 2010 г. было зафиксировано проникновение программы *Stuxnet* в сотни тысяч производственных компьютерных систем по всему миру, а к апрелю 2011 г. он был найден в неактивизированном, но вполне работоспособном состоянии в более чем половине компьютерных систем немецких энергетических фирм и коммунальных служб. Подтверждено также подобное же вирусное заражение компьютерных систем во Франции, Индии и многих других странах.

Этот вирус, выявленный в 2010 г., теперь уже не представляет очень большой опасности. Однако по аналогии с ним могут создаваться гораздо более сложные и эффективные инструменты вредоносного кибернетического воздействия, первым из которых, возможно, стал полиморфный компьютерный вирус модульного типа с условным названием *Stars*, об обнаружении которого заявили иранские власти в апреле 2011 г. и который мог быть нацелен против новой секретной иранской программы по разработке опытного реактора для управляемого термоядерного синтеза.

Существует точка зрения, что *Stuxnet* является одним из первых образцов высокоточного вирусного оружия избирательного действия. Быстро развивающееся «компьютерное оружие» отличает относительная дешевизна и простота применения, скрытность использования, избирательность зон поражения национальных систем жизнеобеспечения и прямая нацеленность на дезорганизацию техногенной среды обитания развитых государств, полагающихся на технически прогрессивные сети и системы электронной цифровой связи и автоматического управления.

В системе кибероборoны США ключевые позиции занимают профильные центры[6]. Основную роль будет играть вновь создаваемый Национальный центр кибербезопасности *(National Cybersecurity Center)*, в задачи которого войдет координация шести других центров. Основные работы по осуществлению разработанной программы повышения эффективности противодействия кибератакам на американские информационно-коммуникационные сети и базы данных разворачиваются под руководством Совета национальной безопасности США в соответствии с комплексным секретным документом «Всеобъемлющая инициатива национальной кибербезопасности» *(The Comprehensive National Cyber Security Initiative)*.

Документ был подготовлен и принят к исполнению во времена президента Д.Буша-мл., гриф секретности с него был снят президентом Б.Обамой[6].

На реализацию «Инициативы» предполагается израсходовать от 40 до 100 млрд долл.

В целом предусмотрено проведение работ по 12 основным инициативным направлениям, которые должны стать ключевыми элементами системы всесторонней защиты национального информационного пространства и определить основополагающие черты общей комплексной стратегии обеспечения кибербезопасности США. Важнейшей задачей должна стать защита баз данных от всего спектра вероятных киберугроз. Большое внимание уделено улучшению профессиональной подготовки специалистов в области информационной безопасности.

В настоящее время в США разворачивают комплексную систему слежения за кибернетическими атаками на инфраструктуру страны[9, 12], создаваемую по программе, получившей название «Безупречный гражданин» *(Perfect Citizen)* и нацеленной на обнаружение кибернападений на частные американские компании и правительственные агентства критически важного значения, например, управляющие эксплуатацией электрогенерирующих мощностей, включая АЭС.

В соответствие с программой особое внимание будет обращено на крупные, обычно старые, компьютерные системы, которые в свое время разрабатывались без учета выхода в Интернет и без соответствующих мер безопасности. Многие из таких систем, которые широко распространены и эксплуатируются до сих пор, принимают участие в управлении всем – от оборудования в метро до авиадиспетчерских служб. Впоследствии они были связаны с Интернетом, что сделало их более эффективными, но вместе с тем и более уязвимыми перед кибернападением.

В министерстве обороны (МО) США отмечают эскалацию попыток вторжения в компьютерные системы, сети и базы данных военного назначения, которые постоянно подвергаются кибератакам со стороны иностранных спецслужб, а также различных негосударственных структур, в том числе террористических, и хакеров. Многие военные высокого ранга рассматривают сложившуюся ситуацию как характерную для состояния кибервойны. Большое значение в информационной войне придается Интернету, который становится мощным стратегическим ресурсом.

МО США отведена лидирующая роль в обеспечении информационной безопасности всей национальной инфраструктуры, включая гражданскую и коммерческую. В составе Объединенного стратегического командования США в 2009 г. сформировано Киберкомандование *(U.S. Cyber Command)*, которое возглавил по совместительству руководитель Агентства национальной безопасности.

В своем официальном выступлении он сообщил о том, что в распоряжении американских военных находится свыше 7 млн компьютеров, объединенных в 15 тыс. сетей. Ежечасно фиксируется примерно 250 тыс. попыток взлома этих систем – более 6 млн в сутки. Национальные интересы подвергаются опасности вследствие чрезвычайной уязвимости компьютерных сетей и нарастающих угроз со стороны других стран, террористов, криминальных группировок и хакеров[13].

Он утверждает, что «диверсии и вывод из строя сетей сейчас возможны, и надо относиться к этому со всей серьезностью». Он за-

явил о том, что до сих пор ущерб от хакерских атак был в основном экономическим, но ситуация быстро меняется и не за горами то время, когда кибертеррористы смогут угрожать системам жизнеобеспечения городов и стран[1].

В 2011 г. МО США выпустило документ Стратегия операций в киберпространстве, в котором киберпространство трактуется как еще одна сфера оперативной деятельности, наравне с четырьмя известными прежде (сушей, воздухом, водой, космосом). В «Стратегии» предлагается увеличить финансовые и материальные ресурсы, вкладываемые в развитие научно-технической базы кибербезопасности, а также в подготовку профильных высококвалифицированных специалистов. Введено понятие «информационное оружие», под которым понимается арсенал средств несанкционированного доступа к информации и выведения из строя электронных систем управления противника.

В военных кругах США высказывается даже предложение считать США как бы находящимися в состоянии кибервойны[14], хотя это мнение не разделяют в Администрации президента США. Разрабатываются концептуальные положения по подготовке и ведению операций в киберпространстве. По утверждению главы комитета начальников штабов ВС США, кибератаки быстро перемещаются в начало списка приоритетных угроз. Эта угроза, сравнимая с ядерной, должна, по его мнению, занимать центральное место в американском военном планировании[15]. Составляются среднесрочные и долгосрочные планы по созданию и совершенствованию методов, аппаратно-программных средств информационной самозащиты и нападения. Выделяются инвестиции на проведение профильных научно-исследовательских и конструкторских работ. Ведутся поиски и обучение высококвалифицированных, разносторонне подготовленных специалистов.

На слушаниях в Конгрессе США директор ФБР также говорил о том, что к традиционным угрозам национальной безопасности США добавилась еще одна – кибертерроризм. Кроме того, за последние годы существенно выросло число мошеннических схем и финансовых преступлений с использованием Интернета. ФБР вынуждено увеличить до тысячи человек количество сотрудников, непосредственно занимающихся противодействием этой угрозе, и запрашивает выделения ассигнований в размере 8,2 млрд долл. на 2013 финансовый год[16].

Директор ФБР добавил, что глобальной сетью охотно пользуются иностранные разведки для добывания политической, военной и экономической информации, а также в промышленном шпионаже, сославшись на дела по технологиям бомбардировщика B-2 и биотехнологиям.

Соединенные Штаты Америки прилагают усилия на международной арене по урегулированию кибербезопасности и рассматривают возможность нанесения даже военного удара в ответ на кибератаку[17]. Кибератака, как причина для коллективного военного ответа, обсуждается также в НАТО, которое провело в 2010 г. киберучения и готовило к выпуску в июне 2011 г. основные концептуальные положения по кибероборoне[18–20].

Проблемой кибербезопасности обеспокоены не только в США, но и во многих других странах, например

в Великобритании, Израиле, Китае, Индии, Иране и т. д., откуда поступают тематически сходные сообщения.

Так, в авторитетном аналитическом Международном институте стратегических исследований (Лондон) высказано предположение, что в ближайшие годы кибернетика может вообще стать «решающим оружием» в межгосударственных конфликтах[21].

В Великобритании, как и в НАТО, проблеме кибербезопасности придается приоритетное значение, было запланировано выделение 650 млн фунтов стерлингов (1,05 млрд долл.) на 4 года (первоначально называлась более значительная сумма, которую пришлось уменьшить из-за сокращений бюджета).

В министерстве обороны в апреле 2011 г. образована специальная команда, группа, по разработке идеологии и политики в области кибербезопасности (*Cyber Security Policy Team*).

5 июля 2011 г. в Лондоне объявлено о создании Международного альянса обеспечения кибербезопасности (*The International Cyber Security Protection Alliance — ICSPA*)[22]. Новая некоммерческая структура призвана объединить государственные организации, международный бизнес и правоохранительные органы в борьбе с киберпреступностью в глобальном масштабе и в партнерстве с полицейской службой ЕС (Европолом)[23].

Здесь же, в Лондоне, вниманию властей и бизнеса представлен так называемый интернет-телескоп. Этот программный инструмент предназначен для непрерывного мониторинга трафика интернет-сети и выслеживания ее проблемных областей с зараженными зловредным кодом компьютерами. Кибератака должна будет пресекаться автоматически без вмешательства человека.

В 2010 г. открыт имитационный киберобъект, на котором можно производить моделирование режимов функционирования реальных компьютерных сетей и оценку нештатных ситуаций в Интернете, а также разрабатывать кибероперации и проводить испытания аппаратных и программных изделий в условиях стресса.

Вслед за опубликованием весной 2010 г. группой американо-канадских экспертов доклада *Shadows in the Cloud* («Тени в облаке»), в котором говорилось об обнаружении свидетельств тайного насильственного доступа китайских хакеров к секретной индийской документации, вооруженные силы Индии выпустили тревожное предупреждение о возможных крупномасштабных кибератаках на правительственные организации или крупные корпорации.

В директиве ВС Индии содержится указание на то, что необходимо ограничить использование компьютеров, имеющих прямой выход в Интернет. Принято решение о создании командования по кибероборонe, задачей которого является защита правительственных и военных цифровых сетей от угрозы нападения, в особенности со стороны Китая. Со временем оно должно быть преобразовано в командование по ведению боевых действий в киберпространстве в целом[24].

Характерно, что предусмотрена передача ответственности из министерства информации и технологии в министерство обороны.

Многими специалистами отмечена склонность Китая к нелегальному вторжению в информационные цифровые сети других стран.

Как предполагают, согласно китайской военной доктрине хорошо развитые кибератакующие способности необходимы Китаю, чтобы уравнять свои боевые возможности с лидирующими индустриальными странами Запада, вооруженные силы которых гораздо лучше оснащены технологически.

По оценке индийских военных специалистов, на службе в ВС Китая состоят более 10 тыс. киберпрофессионалов с научной степенью по ИТ.

В Китае уделяют большое внимание созданию единой государственной информационно-вычислительной системы, базирующейся на сверхмощных суперкомпьютерах собственной разработки. По быстродействию они должны будут соответствовать уровню американского суперкомпьютера *IBM «Roadrunner»*, имеющего пиковую вычислительную мощность около 1460 трлн операций в секунду. Ожидается прокладка новых оптико-волоконных магистралей.

Планируется, что в 2012 г. будет завершено развертывание крупнейших национальных центров суперкомпьютеров и соединение их закрытыми каналами передачи информации. К 2015 г. к ним будут добавлены другие информационно-вычислительные центры, а к 2020 г. формирование и устойчивое функционирование системы должно быть обеспечено.

Отмечается заинтересованность китайских разработчиков в получении зарубежных алгоритмов организации сетевой защиты.

Центральный военный совет КНР выпустил руководящий документ об усилении информационной безопасности в ВС Китая.

Израиль готовится к переходу на новую стратегию противодействия растущим киберугрозам, в разработке которой принимает участие новая Национальная киберадминистрация, образованная при канцелярии премьер-министра[25].

Появление нового органа знаменует собой заметное изменение курса, так как прежде предпочтение отдавалось наступательной кибертактике. Теперь же из-за резкого роста компьютерной преступности необходимо укрепление оборонительной компоненты для подавления потенциальных угроз экономике и вооруженным силам страны, широчайшим образом применяющим современные высокие технологии и поэтому особенно уязвимым.

За недавней волной электронных атак на Израиль подозревают Иран. Помимо спонсируемых правительствами разных стран атак растет число кибервторжений, организуемых индивидуалами или группами хакеров из арабских стран или самого Израиля, в частности, с палестинских территорий.

Подобная атака в 2008 г. парализовала на несколько дней работу одной из министерских сетей связи.

Хотя в таких инцидентах не пострадала «критическая инфраструктура», все же необходимо признать постоянное быстрое совершенствование мастерства атакующей стороны. Огромные наступательный и оборонительный потенциалы сетевых операций делают эту тему особо актуальной, привлекают все большие ресурсы, стимулируют создание новых специализированных подразделений в ВС и разведке Израиля, несмотря на то что, по их собственной субъективной оценке, киберзащита Израиля в целом находится в хорошей форме по сравнению с другими странами.

Напряженная ситуация в мире с защитой информационной инфраструктуры также осложняется и тем обстоятельством, что в соответствии с современными тенденциями развития ИТ можно с течением времени ожидать повсеместного перехода на прогрессивный метод безбумажной записи и хранения информации, а также массовое внедрение перспективных «облачных вычислений» *(Cloud Computing)*[26, 27].

«Облако» представляет собой большое количество серверов, объединенных в один мощный вычислительный механизм, использующий технологии виртуализации. Многие отечественные и зарубежные компании, имеющие представительства в России, уже сейчас заняты созданием внутренних виртуальных сред с расчетом на внешние «облачные» ресурсы.

Разработанное в компании «Оверсан» российское «облако» соответствует международному стандарту *NIST Cloud Computing v.15*. Это «облако» используют в настоящее время более 200 компаний реального сектора экономики; ежемесячный прирост спроса на «облачные» сервисы составляет 50%. На его основе в России введено в эксплуатацию первое «облако» корпоративного уровня.

В таких структурах, как Роскосмос, Федеральная налоговая служба, Росатом и АФК Система уже приступили к применению «облачных» технологий.

Однако не вполне ясен вопрос о надежности сохранения конфиденциальности информации при пользовании через Интернет «облачными» сервисами. Возможно, решением проблемы информационной защиты организаций и предприятий может стать подход, предусматривающий создание отделенных один от другого сетевым экраном внешнего «облака» и его защищенной копии, внутреннего «облака» в стенах учреждения.

Кстати, государственные службы США уже используют внутреннее «облако»[28].

В 2000 г. утверждена Доктрина информационной безопасности Российской Федерации, содержащая основные концептуальные и терминологические понятия и определения. Летом 2009 г. страны Шанхайской организации сотрудничества (ШОС), в том числе и Россия, заключили Соглашение о сотрудничестве по обеспечению международной информационной безопасности. В нем называются следующие основные угрозы в области международной информационной безопасности:

– разработка и применение информационного оружия, подготовка и ведение информационной войны;

– информационный терроризм;

– информационная преступность;

– использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств;

– распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств;

– угроза безопасному стабильному функционированию глобальных и национальных информационных инфраструктур, имеющих природный и (или) техногенный характер.

Несмотря на принципиальную российскую позицию избегать введения ограничений на Интернет, поскольку он способствует развитию демократии в стране, Россия, как и другие страны организации ШОС, вынуждена отвергнуть свободный доступ к своему киберпространству. Она не примет участия в Конвенции по киберпреступности Совета Европы *(Council of Europe Convention on Cybercrime)* и не намерена подписывать Европейский договор о кибер-

преступности (*European Cybercrime* Treaty), так как эти документы оговаривают в своих положениях разрешение зарубежным правоохранительным органам проводить интернет-поиск внутри российских границ, что является нарушением Конституции РФ.

Таким образом, у нас в стране понимают, как быстро возрастает опасность нелегитимных киберагрессивных действий в цифровых сетях, и стремятся предпринимать своевременные шаги для ее нейтрализации. Но обязательным продолжением и развитием глобальных общегосударственных усилий должно стать безотлагательное проведение соответствующих инициативных мероприятий аналогичной киберзащитной направленности на корпоративном уровне во всех отраслях, в частности, и в здравоохранении.

При Президенте России образована Комиссия по модернизации и технологическому развитию страны, одним из пяти магистральных направлений деятельности которой определена «Медицинская техника и фармацевтика»[29]. Другим направлением является «Компьютерные технологии и программы». Многообещающим признан синтез обоих направлений, чем обосновывается проведение под эгидой Комиссии в 2011 г. в Москве 7-го Международного форума MedSoft 2011 и выставки «Медицинские информационные технологии».

В России разработана и принята к исполнению концепция информатизации здравоохранения. В ней предусмотрено создание централизованных информационных ресурсов и каналов связи, а также модернизация медицинских учреждений, которые должны быть аппаратно и программно подготовлены к работе в новой информационной среде и новых производственных условиях.

Однако специфика информатизации медицинских учреждений состоит в том, что приходится сочетать якобы противоречивые требования по максимально широкому информационному раскрытию их для населения, с одной стороны, и по вынужденной информационной изоляции – с другой, с целью избежать разглашения персональных данных и нарушения врачебной тайны.

Примечания

[1] *Корсаков Г.Б.* Роль информационного оружия в военно-политической стратегии США // США и Канада. 2012. № 1.

[2] Безопасность энергетических сетей США: проблемы борьбы с кибернетическим терроризмом // Сб. Института США и Канады РАН. 2011. № 7.

[3] *Wright A.* National-Security Infrastructure Faces Relentless Cyberespionage Campaign // National defense. 2009. Dec.

[4] Кибератака на научную лабораторию США // Зарубежное военное обозрение*. 2011. № 8.

[5] Борьба с угрозой кибертерроризма // ЗВО. 2010. № 12.

* Дальше ЗВО.

[6] *Роговский Е.А.* Глобальные информационные технологии – фактор международной безопасности // Сб. института США и Канады. 2010. № 12.
[7] Использование за рубежом сети Интернет в интересах ведения информационных войн // ЗВО. 2010. № 4.
[8] Китайские хакеры взломали компьютеры и похитили секретную информацию минобороны Индии // Военно-техническое сотрудничество*. 2010. 5–11 апреля.
[9] Система слежения за кибернетическими атаками // ЗВО. 2010. № 8.
[10] Анализ причинно-следственных факторов применения компьютерного вируса «Стакснет» против ядерных объектов Ирана // ЗВО. 2011. № 8.
[11] *Fulghum D.A.* Digital Deluge // Aviation Week & Space Technology. 2011. № 18. May 23. Vol. 173.
[12] U.S. Cybersecurity Incentives // Defense News. 2010. № 14. Apr. 5. Vol. 25.
[13] США должны быть готовы к попыткам противника вывести из строя компьютерные сети // ВТС. 2010. № 23. 7–13 июля.
[14] An Online "War"? // Defense News. 2010. Apr. № 14. 5. Vol. 25.
[15] Иностранная военная хроника // ЗВО. 2011. № 8.
[16] ФБР просит у Конгресса 8,2 млрд долл. на борьбу с кибертерроризмом // ВТС. 2012. № 11. 12–18 марта.
[17] США не исключают возможности нанесения военного удара в ответ на кибератаки // ВТС. 2010. 10–16 мая.
[18] Кибератаки теоретически могут быть расценены НАТО как причина для военного ответа // ВТС. 2010. № 41. 11–17 октября.
[19] Кибератака на одного из членов НАТО может быть расценена как нападение на весь альянс // ВТС. 2010. № 48. 29 ноября – 5 декабря.
[20] НАТО приступило к созданию концепции кибернетической войны будущего // ВТС. 2010. 8–14 февраля.
[21] *Wall R.* Rule Change // Aviation Week & Space Technology. 2011. № 18. May 23. Vol. 173.
[22] Создание международного альянса обеспечения кибербезопасности // ЗВО. 2011. № 8.
[23] Кибернетическое оружие в ближайшие годы может стать решающим в международных конфликтах // ВТС. 2010. № 6. 8–14 февраля.
[24] India Plans Cyber Command // Defense News. 2010. Apr. 19.
[25] *Ben-David A.* Playing Defense // Aviation Week & Space Technology. 2011. № 23. June 27. Vol. 173.
[26] *Шаров П.* Облачные» технологии от РКС: возможности и перспективы // Новости космонавтики. 2011. Т. 21. № 8 (343).
[27] ИТ – будущее витает в «облаках» // Российский космос. 2011. № 8 (68). Август.
[28] Системы компьютерной безопасности минобороны США переходят на новую платформу // ВТС. 2011. 31 октября – 6 ноября.
[29] Комиссия по модернизации и технологическому развитию экономики России // URL: www.i-russia.ru

---

* Дальше ВТС.