УДК 551.466

ОСНОВНЫЕ НАПРАВЛЕНИЯ ЗАРУБЕЖНЫХ НАУЧНЫХ ИССЛЕДОВАНИЙ В ОБЛАСТИ ТЕХНИЧЕСКИХ СРЕДСТВ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

© 2016 В.Ю. Корчак, И.Л. Борисенков, С.В. Куприянов, Г.И. Леонович

Секция прикладных проблем при Президиуме РАН

Статья поступила в редакцию 11.11.2016

Приведены результаты аналитического обзора зарубежных научных публи-каций. Дана краткая характеристика современных направлений и форм ин-формационного противоборства (ИПБ). Показана роль технических средств ИПБ в кибернетических и сетецентрических операциях, в создании информационной инфраструктуры. Отмечен приоритет фундаментальных и прикладных исследований, связанных с прогнозом усиления роли технических средств в ИПБ, связанным с интенсификацией развития многоуровневых информационных сетей. Особое значение зарубежные специалисты придают поиску и синтезу новых сенсорных и мультифункциональных материалов, освоению терагерцового радиодиапазона, формированию резервированных автономных робототехнических комплексов, маскированию и защите технических средств от широкого спектра деструктивных воздействий.
Ключевые слова: информационное противоборство, технические средства, фундаментальные и прикладные исследования.

ВВЕДЕНИЕ

Информационное противоборство (ИПБ), как правило, включает комплексное деструктивное воздействие на информацию, информационные системы и информационную инфраструктуру противоборствующей стороны с одновременной защитой собственной информации, информационных систем и информационной инфраструктуры от подобного воздействия. По мнению ведущих зарубежных специалистов в области информатики, основные понятия всех известных концепций ИПБ не являются новыми. Новизна заключается в использовании теоретических разработок, основанных, в том числе, на непрерывной модернизации существующих и создании новых высокоэффективных технических средств (ТС) [1, 2].

В статье приведены результаты аналитического обзора современного состояния и тенденций развития технических средств ИПБ за рубежом, тематики фундаментальных и прикладных исследований в США, Китае и странах Западной Европы.

1. СОВРЕМЕННОЕ СОСТОЯНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

К направлениям ИПБ, ведущая роль в которых отводится техническим средствам (ТС), зарубежные эксперты относят противоборство в электромагнитном диапазоне, обеспечение безопасности информационной инфраструктуры, информационные операции военной поддержки, космические операции, операции в киберпространстве (кибервойны) и специальные технические операции. Кроме того, ИПБ – неотъемлемая составляющая современных форм боевого противоборства – сетецентрических операций (СЦО), основанных на приоритете информационно-когнитивной сферы над физической. СЦО предусматривают развертывание функциональных сетей, содержащих комплекс ТС различного назначения: управления, разведки (сенсоры) и поражения (акторы). Ключевыми принципами ИПБ в СЦО, определяющими облик и параметры ТС, считаются своевременность, внезапность, скрытность и затрудненность противодействия [3].

Успех направлений и соответствующих форм противоборства в современных и будущих конфликтах определяется наличием и соответствием текущим требованиям трёх ключевых компонент информационной инфраструктуры [2-5]:

- высоконадежной коммуникационной среды, обеспечивающей эффективное функционирование компьютерных сетей и их объединение в глобальную специализированную информационную сеть;
- распределенных в пространстве точечных и групповых сенсоров - управляемых, достаточно информативных, надежных, долговечных и малозаметных для оппонентов;
- распределенной программной среды, обеспечивающей в реальном времени комплексную многоуровневую интеллектуальную обработку

Корчак Владимир Юрьевич, доктор экономических наук, профессор.
Борисенков Игорь Леонидович, кандидат технических наук.
Куприянов Сергей Васильевич, кандидат технических наук.
Леонович Георгий Иванович, доктор технических наук, профессор.

потоков малоинформативных в отдельности (а зачастую и противоречивых) первичных сведений о проявлениях объектов, а также позволяющей, при необходимости, оперативно изменять логику этой обработки по мере изменения состава и возможностей сенсоров, получения новых знаний о контролируемых объектах и т.п.

К техническим средствам ИПБ, включая программно-аппаратные средства, с определенной степенью дифференциации можно отнести [1-7]:

- источники электромагнитного излучения, предназначенные для реализации открытого и скрытого информационного воздействия, создания активных помех и деструктивного воздействия на радиоэлектронную аппаратуру (РЭА);
- пассивные средства защиты РЭА и инженерно-технических объектов в целом, основанные на поглощении, отражении и рассеивании излучений;
- аппаратуру технической разведки, в том числе различные записывающие и передающие закладные устройства, сенсорные устройства и сети;
- аппаратуру программно-математической защиты и активного воздействия, направленного на блокировку, шифрование, дешифрование, изменение, копирование и другие манипуляции с различного рода информацией;
- средства скрытого программно-технического воздействия, предназначенные для внедрения в автоматизированные системы управления специальных программ (вирусов), разрушающих программное обеспечение и базы данных (знаний), а также встроенные в типовую серийную аппаратуру микрочипы с широким спектром возложенных функций;
- средства контроля, предназначенные для выявления физических и иных каналов утечки информации, демаскирующих признаков собственной деятельности по одному или нескольким из контролируемых физических полей и химических веществ, а также для контроля соблюдения мер по обеспечению электромагнитной совместимости собственных радиотехнических средств и др.

Важными составляющими информационных инфраструктур СЦО являются физические каналы формирования и передачи данных, системы сбора и обмена информацией, их возможности по взаимодействию с системами управления. В частности, СЦО опираются на высокую пропускную способность магистральных коммуникаций на базе оптико-волоконной и спутниковой связи, скрытность, обеспечиваемую атмосферной оптической связью, фрагментарной связью с БПЛА и др. Отсюда следует одна из основных особенностей СЦО - сильная зависимость эффективности операций от интеллектуального уровня и надежности технических и программно-аппаратных средств и технологий, задействованных в формировании и поддержании сетевой инфраструктуры. Даже короткие перебои в работе сети могут стать катастрофическими для всей операции. При этом необходимо учитывать, что противник будет пытаться использовать потенциальную уязвимость инфраструктуры с использованием всего арсенала доступных средств [4]. Кроме того, имеют место неконтролируемые и трудно прогнозируемые угрозы техногенного характера. Например, серьезные помехи спутниковой связи оказывает космический мусор. Так, при запуске средней ракеты–носителя регистрируется свыше 3000 предметов размером более 1 см. Только 6% фрагментов входит в атмосферу Земли в течение года, а остальные находятся на орбите до трех лет [6].

К средствам ИПБ с высокой степенью технической уязвимости эксперты относят полностью и частично импортируемые из других стран или из международного сектора собственной экономики электронные системы, устройства, узлы и комплектующие, а также программные продукты. Серьезные проблемы возникают при использовании COTS/GOTS/MOTS продуктов, закупки которых способствуют сокращению затрат на НИОКР и обслуживание систем, особенно в области ICT-продуктов. Это, с одной стороны, повышает рентабельность и темпы производства новых изделий, а с другой - возрастает риск внедрения трудно обнаруживаемых и купируемых закладок и вирусов в системы с высоким уровнем конфиденциальности [8].

К другим источникам угроз технического характера относят конструктивно-алгоритмическое несовершенство аппаратуры, неадекватную реакцию аппаратной защиты на внешние воздействия, недостаточность или, наоборот, необоснованную избыточность автономности и интеллекта устройств при решении различных задач в конкретных условиях функционирования, а также ряд других причин, связанных с человеческим фактором, как, например, запаздывание или ошибки при модернизации и введении в инфраструктуру новых ТС [9].

2. ФУНДАМЕНТАЛЬНЫЕ И ПРИКЛАДНЫЕ ИССЛЕДОВАНИЯ В ОБЛАСТИ ТЕХНИЧЕСКИХ СРЕДСТВ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

В целях достижения превосходства над потенциальными противниками и предотвращения террористических угроз за рубежом ведется ряд долгосрочных программ фундаментальных и прикладных исследований, опытно-конструкторских работ, осуществляется модернизация и

переоснащение информационной инфраструктуры новыми ТС [3-11].

Фундаментальные исследования ориентированы на решение следующих задач ИПБ [8-12]:

- совершенствование известных и создание новых систем с искусственным интеллектом, разработка адаптивных систем распознавания образов, алгоритмов мультикритериального принятия решений,
- создание групповых робототехнических комплексов;
- расширение и углубление сфер применения нейроинформатики и биоинформатики, в в том числе, на основе синтетической биологии;
- развитие многоуровневых интегрированных информационно– телекоммуникационных систем и сетей;
- разработка малогабаритных энергоэффективных сенсорных сетей с высокой степенью адаптивности, автономности, интеллектуальности, скрытности и живучести;
- развитие архитектуры информационно-вычислительных комплексов, создание принципиально новых системных решений и программного обеспечения;
- формирование и развитие новой элементной базы микроэлектроники, наноэлектроники и квантовых процессоров;
- активный поиск и применение эффективных способов и средств получения материалов для перспективной микро - и наноэлектроники, сенсорных устройств, маскировочных и защитных покрытий, устойчивых к широкому спектру воздействующих факторов;
- опережающее развитие опто -, радио - и акустоэлектроники, оптической, СВЧ и КВЧ-связи, освоение терагерцового диапазона.

Анализ публикаций, позволяет выделить ряд тенденций и приоритетных направлений прикладных НИР и ОКР, проводимых за рубежом, на ближайшее десятилетие [7-15]:

- исследования будут ориентироваться в первую очередь на создание и применение квантовой вычислительной техники, широкое внедрение нанотехнологий, направленных на совершенствование робототехники, дистанционно управляемых мобильных автономных платформ, миниатюрного оружия с поддержкой защищенными высокоскоростными когнитивными системами связи;
- предполагается существенный скачок в радиофизике, направленный на кратное увеличение пропускной способности физических каналов передачи данных;
- формируется тенденция взаимодополняющего развития обычного и кибероружия, направленного на повышение эффективности перенастройки, деструкции и уничтожения ТС ИПБ;
- существенно расширяется номенклатура интеллектуальных датчиков физических и химических величин, способных оперативно интегрироваться в сетевые структуры различного, в том числе смешанного, базирования;
- сохраняется тенденция ускоренного совершенствования систем сбора данных, расширения возможностей при обработке, хранении, передаче и отображении данных с учетом дополненной реальности;
- расширяется интеграция общедоступных и специализированных мобильных беспроводных и облачных сетей с глобальными сетями.

Ряд НИОКР успешно воплощается в национальные программы в области ИПБ. В частности, в США формируется глобальная информационная сеть LandWarNet, которая рассматривается в качестве базовой основы перехода к сетецентрическому принципу управления, обеспечивающему на основе совместного использования информационных ресурсов и надежного сетевого обеспечения высокую степень согласованности и синхронизации действий всех видов вооруженных сил [7].

При создании тактических систем связи особое внимание уделяется обеспечению непрерывности управления для любых условий рельефа местности, надежности связи при высокой мобильности абонентов, гарантированной защищенности каналов от воздействия средств РЭБ, а также гарантированное качество обслуживания пользователей. Цель – создание комплексного аппаратно-программного решения со специальным стеком протоколов и набором унифицированных служб, которое бы позволяло развертывать беспроводную сеть с возможностью динамического конфигурирования ее характеристик. Приоритетная проблема – необходимость надежно защищенной связи с применением адаптивного программного обеспечения. Пример такой связи – программно-определяемая радиосистема (Software-*defined radio,* SDR) с адаптивным кодированием и модуляцией (АСМ), которой, в частности, можно компенсировать индуцированный погодой эффект затухания более чем на 15 дБ. В НАТО в настоящее время внедряется адаптивная сеть с распределенным управлением (Control-Based Mobile Ad Hoc Networking - CBMANET), которая в общих чертах отвечает указанным требованиям.

Планируется более широкое использование высокоскоростной оптической спутниковой связи со стационарных орбит. Например, Лунная лазерная система связи (LLCD) НАСА в 2013 году показала при применении импульсного инфракрасного лазера для связи между Землей и

Луной на расстоянии 385,000 км нисходящий поток 622 Мбит/с и безошибочный восходящий 20 Мбит/с. Протоколы для обмена данными в сетях должны быть в состоянии адаптироваться к изменяющимся видам и каналам связи, например, с наземных коммуникаций на радиооптические спутниковые. Поэтому они должны взаимно коррелироваться по скорости передачи данных и по функциям коррекции ошибок с учетом характерных задержек и дрожаний. При работе в условиях космического мусора предполагается упрочнение корпусов спутников, введение активной защиты, создание группировок из взаиморезервированных наноспутников. В соответствии с программой HELLADS разрабатывается высокоэнергетическая сеть бортовых лазерных систем передачи данных с многократным уменьшением массогабаритных показателей по сравнению с существующими лазерными системами. Кроме того, HELLADS должна быть способна к применению в качестве атакующего оружия [14].

Продолжает меняться операционная среда для морских и подводных сетей тактического взаимодействия, которые получили новый толчок для развития благодаря техническим достижениям в области акустических коммуникаций, оптических и волоконно-оптических линий связи. Это инициировало появление следующего поколения интеллектуального оружия, встроенного в сетевую структуру, которое может устанавливаться на типовых и беспилотных подводных средствах с дистанционно управляемыми поражающими платформами. Ведущаяся программа Distributed Agile Submarine Hunting (DASH) - предназначена для создания распределенной сетевой системы подводного слежения. Узлы-сонары DASH будут работать на больших глубинах в открытом океане и на больших площадях пеленговать объекты, проплывающие над сетевой структурой [14, 15].

ЗАКЛЮЧЕНИЕ

Анализ зарубежных публикаций показывает, что тематика научных исследований в области ИПБ все в большей степени ориентируется на достижения фундаментальной и прикладной науки, связанные с обеспечением технического превосходства в создании сетевых инфраструктур сенсорного уровня, защищенных каналов передачи информации и эффективных высокопроизводительных программно-аппаратных средств.

СПИСОК ЛИТЕРАТУРЫ

1. Collins English Dictionary - Complete & Unabridged 10th Edition. URL: http://www.dictionary.com/browse/information-warfare. (дата обращения 11.10.2016).
2. *Stupples D.* What is information warfare? URL: https://www.weforum.org/agenda/2015/12/what-is-information-warfare (дата обращения 11.10.2016).
3. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. - Washington D.C.: The White House, 2009. URL: https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (дата обращения 11.10.2016).
4. *Libicki M.* Conquest in Cyberspace: National Security and Information Warfare, Cambridge University Press, Cambridge, 2007. URL: http://www.garykessler.net/library/libicki.pdf (дата обращения 12.10.2016).
5. Joint Publication 3-57. Civil-Military Operations. 11 September 2013. URL: http://www.dtic.mil/doctrine/new_pubs/jp3_57.pdf (дата обращения 12.10.2016).
6. *Robert Koch and Mario Golling* , Blackout and Now? Network Centric Warfare in an Anti-Access Area Denial Theatre, in *M. Maybaum, A.-.M. Osula, and L. Lindström* (eds), 2015 7th International Conference on Cyber Conflict: Architectures in Cyber Cyberspace, Tallinn: NATO CCDCOE, 2015, 169-184, 178-180. URL: https://ccdcoe.org/cycon/2015/proceedings/12_koch_golling.pdf. (дата обращения 12.10.2016).
7. Hybrid Warfare JSOU Report 13-4 The JSOU PressMacDill Air Force Base, Florida 2016. URL: http://www.ndia.org/Divisions/Divisions/SOLIC/Documents/JSOU16-4_Various_SpecialOpsEssays_final.pdf (дата обращения 18.10.2016).
8. Defence Committee. Acquisition—Fundamental Principles / Written evidence from *Christopher Donnelly*, July 2012. URL: http://www.parliament.uk/ (дата обращения 18.10.2016).
9. *Anton P.S., Anderson R.H., Mesic R., Scheiern M.* Finding and Fixing Vulnerabilities in Information Systems. The Vulnerability Assessment and Mitigation Methodology/ Monograph Reports. 2004, URL: https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1601.pdf (дата обращения 12.10.2016).
10. Report of the Defense Science Board Task Force on Basic Research/ Office of the Under Secretary of Defense for Acquisition, Technology and Logistics Washington, D.C. 20301-3140, January 2012. URL: http://www.acq.osd.mil/dsb/reports/BasicResearch.pdf (дата обращения 18.10.2016).
11. DoD Agency Strategic Plan, Fiscal, Years 2015-2018. URL: http://dcmo.defense.gov/Portals/47/Documents/Publications/ASP/FY2016_2018ASP.pdf (дата обращения 18.10.2016).
12. Journal of Information Warfare (JIW). Copyright 2014-2016. URL: http://www.Jinfowar.com. (дата обращения 19.10.2016).
13. Modern Militaries and a Network Centric Warfare Approach, *Jonjo Robb*, Jan 9 2014, 4042 views. URL: http://www.e-ir.info/2014/01/09/modern-militaries-and-a-network-centric-warfare-approach/ (дата обращения 19.10.2016).
14. PE 0603766E: Network-centric warfare technology unclassified, Defense Advanced Research Projects Agency, 2015. URL: http://www.globalsecurity.org/

military/library/budget/fy2016/dod-peds/0603766e_3_pb_2016.pdf (дата обращения 19.10.2016).
15. *Rogers P.* Unmanned Air System: the future of air & sea power? / Focus strategique, No 49, 2014. URL: https://www.ifri.org/sites/default/files/atoms/files/fs49rogers.pdf (дата обращения 19.10.2016).

THE MAIN FOREIGN SCIENTIFIC RESEARCH DIRECTIONS IN THE TECHNICAL MEANS FIELD OF INFORMATION CONFRONTATION

© 2016 V.Yu. Korchak, I.L. Borisenkov, S.V. Kupriyanov, G.I. Leonovich

Section of Applied Problems at the Presidium of RAS

Analytical review results of international scientific publications. Modern trends and forms of informational confrontation (IC) brief description. The technical means role in cyber and network-centric operations, creating the information infrastructure. Marked priority fundamental and applied research associated with the forecast strengthening of the role of technical means in the IC related to the intensification of the development of multi-level information networks. Of particular importance to foreign experts give the search and synthesis of new multi-touch and multi-functional materials, development of terahertz radio range and the formation of redundant autonomous robotic systems, masking and protection of technical means against a wide range of destructive impacts.
Keywords: information warfare, technical tools, fundamental and applied research.

Vladimar Korchak, Doctor of Economics, Professor.
Igor Borisenkov, Candidate of Technics.
Sergey Kupriyanov, Candidate of Technics.
Georgy Leonovich, Doctor of Technics, Professor.