НИОКР АГЕНСТВА DARPA В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Петренко Александр Анатольевич, *кандидат технических наук, старший научный сотрудник, доцент кафедры математических методов в экономике МГИУ, г. Москва*
E-mail: aapetr@rambler.ru
Петренко Сергей Анатольевич, *доктор технических наук, профессор, профессор кафедры информационной безопасности СбГТУ (ЛЭТИ), г. Санкт-Петербург*
E-mail: s.petrenko@rambler.ru

В октябре 1957 года в СССР был успешно осуществлен запуск первого искусственного спутника Земли (ИСЗ) "Спутник–1". Незамедлительной ответной реакцией США стало создание в 1958 году агенства по перспективным оборонным научно–исследовательским разработкам, Defense Advanced Research Projects Agency, DARPA (http://www.darpa.mil/), для достижения и сохранения технологического превосходства вооруженных сил США. Среди значимых достижений DARPA в области информационных технологий – создание в 1969 году глобальной сети Интернет, тогда еще ARPANET. Эта сеть позволила объединить в единую информационную систему университеты, работающие по военным заказам и находящиеся на западном и восточном побережьях США. В настоящее время DARPA проводит широкий спектр научных исследований, направленных на предотвращение внезапного для США появления новых технических средств вооруженной борьбы и преодоление разрыва между фундаментальными исследованиями и их применением в военной сфере. За последние десятилетия пример DARPA способствовал созданию подобных научно–исследовательских организаций и агенств по всему миру: DRDO (Индия), MAFAT (Израиль), SASTIND (Китай), GDA (Франция), Фонд перспективных исследований (Россия) и пр. Давайте познакомимся с поисковыми исследованиями DARPA в области кибербезопасности подробнее.

Ключевые слова: *научные исследования, управление проектами, технологии кибербезопасности, эволюция программ кибербезопасности.*

R&D OF AGENCY OF DARPA IN THE FIELD OF CYBERSAFETY

Aleksandr Petrenko, *Ph.D., Associate Professor, Associate Professor at Department of Mathematical Methods in Economics (213) of MSIU, Moscow*
E-mail: aapetr@rambler.ru
Sergey Petrenko, *Doctor of Science (Comp.), Professor, Professor at Information Security Department of ETU (LETI), St. Petersburg*
E-mail: s.petrenko@rambler.ru

In October, 1957 in the USSR start of the first artificial satellite of Earth (ASE) "Satellite–1" was carried successfully out. Creation in 1958 of perspective defensive research development agency, Defense Advanced Research Projects Agency, DARPA (http://www.darpa.mil/), for achievement and preservation of technological superiority of armed forces of the USA became immediate response of the USA. Among significant achievements of DARPA in the field of information technologies – creation in 1969 of the global Internet, then still ARPANET. This network allowed to unite the universities working by military orders and being on the western and east coasts of the USA in uniform information system. Now DARPA conducts a wide range of the scientific researches directed on prevention of emergence of new technical means of armed struggle, sudden for the USA, and overcoming of a gap between basic researches and their application in the military sphere. For the last decades the example of DARPA promoted creation of the similar research organizations and agencies worldwide: DRDO (India), MAFAT (Israel), SASTIND (China), GDA (France), Fund of perspective researches (Russia) and so forth. Let's get acquainted with basic researches of DARPA in the field of cybersafety in more detail.

Keywords: *scientific researches, management of projects, technologies of cybersafety, evolution of programs of cybersafety.*

Состояние вопроса

Следует констатировать, что в настоящее время фундаментальные и прикладные исследования в области кибербезопасности в силу неделимости глобального информационного пространства и масштабности вызовов и угроз в этой сфере являются одним из приоритетных направлений обеспечения глобальной безопасности и мировой стабильности. Здесь США пока занимают лидирующее положение и последовательно проводят на системной основе широкий спектр научно-исследовательских и опытно-конструкторских работ (НИОКР) в области кибербезопасности для получения преимуществ в международных отношениях и мировой экономике. При этом все многообразие упомянутых НИОКР (например, см. табл. 1) можно условно разделить на три больших класса. Первый класс это фундаментальные исследования в области кибербезопасности. Названные исследования проводятся крупными государственными и частными университетами. Второй - прикладные исследования, подтверждающие фундаментальные исследования на практике. Как правило, исследования данного класса проводятся предприятиями оборонно-промышленного комплекса, возможно, под научным руководством некоторого университета. Третий - прикладные исследования на этапе эксплуатации и сопровождения вооружения и военной техники. Данные работы обычно выполняют производственные предприятия, иногда в партнерстве со службой эксплуатации заказчика.

***Таблица 1**. Синергетический результат междисциплинарных НИОКР*

№	Направление НИОКР	Название программ
1.	Технологии человека	• Биологическая защита от неизвестных ранее патогенов; • Терапия нейротравм центральной нервной системы; • Фундаментальные механизмы старения организма; • Системы автоматизированного проектирования живых существ
2.	Технологии робототехники	• Высокоэффективные транспортные средства доставки персонала и грузов; • Автономные операции роботов (подводные, наземные, воздушные); • Энергообеспечение длительных автономных действий; • Навигация в условиях радиоэлектронного противодействия; • Робототехнический транспорт для воздушного и водного пространства, пересеченной местности и дорог общего пользования.
3.	Сетевые технологии	• Обработка структурированных и неструктурированных данных больших объёмов и значительного многообразия для получения человекочитаемых результатов; • Программные реализации концепции «системы систем»; • Игровые модели управления операциями на боевом пространстве.
4.	Технологии интеграции возможностей человека и робота для действий в реальном мире	• Роботы для снижения физической нагрузки на человека; • Автоматические средства мониторинга и коррекции здоровья; • Расширение возможностей органов чувств за счет использования электронных сенсорных систем.
5.	Технологии автоматической коммутации событий реального и виртуального миров	• Групповое управление «роем» роботов; «Информационные сети вещей»; • Адаптивные производственные линии и «микрофабрики»; • Системы дополненной реальности и электростимуляции ЦНС.
6.	Технологии интеграции и взаимного усиления возможностей человека и компьютерных сетей	• Системы ускоренного обучения человека; • Системы поддержки принятия решений в науке и медицине; • Системы искусственного интеллекта в проведении кибероперациий; • Нестандартные аппаратные средства (нейроморфные чипы, и др.) обработки сложноструктурированных данных.
7.	Интегрированные сетевые технологии преобразования реального мира за счет взаимодействия человека и роботов	• Управление конфигурацией когнектома мозга человека и животных; • Единое боевое пространство (объединяющее как виртуальное, так и реальное) с универсальным протоколом проведения операций; • Автономная ресурсо-независимая робототехника и обеспечивающая инфраструктура.

Для выполнения упомянутых НИОКР привлекаются военно-научные коллективы и подразделения (Ливерморская лаборатория, Национальная лаборатория в Лос-Аламосе, Лаборатория Линкольна, исследовательский центр армии США и др.), а также гражданские организации – государственные и частные университеты, предприятия военно-промышленного комплекса, опытно-конструктурские бюро и различные творческие коллективы и пр. Как правило, в роли заказчика выступают следующие подразделения Министерства обороны США (DoD):

- Управление научно-исследовательских работ ВВС (Air Force Office of Scientific Research - AFOSR);
- Управление исследований ВМС (Office of Naval Research - ONR);
- Научно-исследовательское управление Сухопутных войск (Army Research Office - ARO);
- Агентство передовых оборонных исследовательских проектов (Defense Advanced Research Projects Agency - DARPA);
- Управление исследований и разработок Инженерного корпуса Армии США (Army Corps of Engineers Research and Development Directorate - USACE R&D);
- Управление исследований и разработок Агентства национальной безопасности (National Security Agency/Central Security Service Research Directorate (NSA/CSS - Research);
- Управление медицинских исследований и медицинской техники Сухопутных войск США (US Army Medical Research & Materiel Command);
- Агентство по сокращению военной угрозы (DTRA – Defense Threat Reduction Agency) и пр.

Среди перечисленных организаций выделим агенство DARPA (см. рис. 1,2), под управлением которого разработано и внедрено большинство технологических новинок Вооруженных сил США[1-7], среди которых можно выделить: ракеты-носители «Сатурн 5»; самолеты-невидимки F117 «стелс»; навигационная система GPS и ее новый аналог; новый беспилотный летательный аппарат; перспективное высокоточное оружие; новейшие средства разведки и наблюдения; современные приборы ночного видения; новый беспроводной стандарт связи на смену CDL со скоростью 100 Гб/с при радиусе покрытия 200 км.; самоорганизующиеся системы кибербезопасности и пр. (см. рис. 3).

Агенство DARPA подчинено Директору по оборонным исследованиям и технике, который в свою очередь выполняет задачи Замминистра обороны США по обеспечению, технологиям и логистике. Ежегодный перечень актуальных поисковых программ DARPA формируется соответствующими подразделениями Министерства обороны США. При этом часть программ Агентство может разрабатывать самостоятельно. На практике направления научных исследований DARPA конкретизируются специальными предписаниями и распоряжениями вышестоящего руководства (министра обороны США, его основных заместителей, директора по оборонным исследованиям, командующими видов войск и пр.), а также предложениями и указаниями соответствующих государственных и военных организаций.

№ п/п	Характеристика	Значение
1	Сотрудники	240 чел.
2	Из них менеджеры программ	33,6 %
3	Средний возраст	37 лет
4	Годовой доход, макс.:	
	• менеджер программ	130 000 долл.
	• дирекция	90 000–150 000 долл.
5	Образование сотрудников:	
	• топ-университеты США	20 %
6	Бюджет:	
	• общий	2,8 млрд
	• административные расходы	57 млн.
7	Год создания	1958
8	Сайт	www.darpa.mil

Рис.1. *Краткая характеристика DARPA*

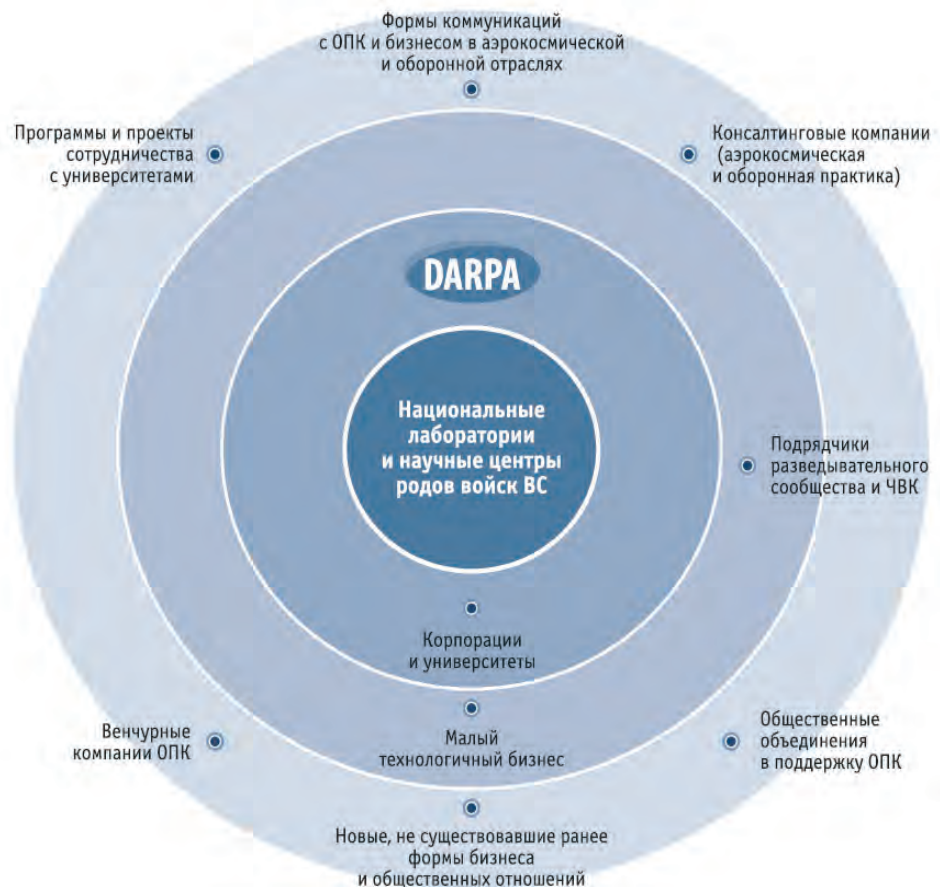

Рис. 2. *Роль и место DARPA в НИОКР США*

Яркой отличительной особенностью DARPA от других заказывающих подразделений Министерства обороны США (DoD) является выполнение ранее не проводившихся уникальных поисковых исследований (см. табл. 2), а именно:

• концептуальных исследований для выработки направлений исследований и постановки новых военно-прикладных задач;

• комплексных межведомственных и междисциплинарных исследований;

• научных исследований с большим риском достижения декларируемого результата и пр.

Следует константировать, что масштабы деятельности DARPA по уровню финансирования сравнительно небольшие и составляют не более 0,7-1,2% от 100% оборонных расходов США и не

Таблица 2. *Особенности поисковых исследований DARPA*

№	Критерии сравнения	DARPA	Научные подразделения МО США (DoD
1	Самостоятельность постановки научных задач	Творческий подход и возможность экспериментирования	Жесткий регламент выполнения поставленных задач согласно утвержденным планам и программам.
2	Системность научных исследований	Комплексные системные исследования.	Исследования в рамках поставленных целевых программ.
3	Цели и задачи	Поддержка прорывных исследований с потенциально значимым результатом.	Плановое совершенствование вооружения и военной техники.
4	Подчиненность	Центральному аппарату МО США	Стратегическим и тактическим командованиям МО США
5	Риски	Высокий риск получения результата	Гарантированное достижение результата

более 1% от общих расходов на военно-прикладные исследования и разработки (примерно 3-5 млрд. долл. в год). Однако влияние DARPA на развитие военных технологий и технологий двойного назначения США существенно и его трудно переоценить (см. рис. 3).

Выбор приоритетов

В истории DARPA можно выделить пять основных этапов развития агентства. Первый – 1958-1960 годы - становление тогда еще агентства ARPA как нового творческого научного коллектива. Основная задача агентства – выработка действенных способов технологического опережения СССР в космонавтике. Второй – 1960-1972 годы - сопровождался передачей космической темы в NASA и переориентацией на достижение значимых результатов в фундаментальных научных исследованиях. Третий – 1972-1991 годы - ARPA становится Defense. Этот этап характеризовался подписанием международных соглашений с СССР, эскалацией войны во Вьетнаме и, как следствие, приоритетом оборонных технологий. Четвертый – 1991-2001 годы - окончание «холодной войны», снижение расходов на оборону и приоритет технологий двойного назначения, прежде всего в области электроники и инфокоммуникаций. Пятый – 2001 год и по настоящее время - начало эпохи войны с международным терроризмом, не скрываемое прямое доминирование США в международных отношениях. Для упомянутого этапа характерно создание новейших военных технологий на основе современных достижений в оборонных исследованиях. Подробнее эволюционный путь развития DARPA, приоритеты программ НИОКР и характеристика деятельности его руководителей приведены в таблице 3.

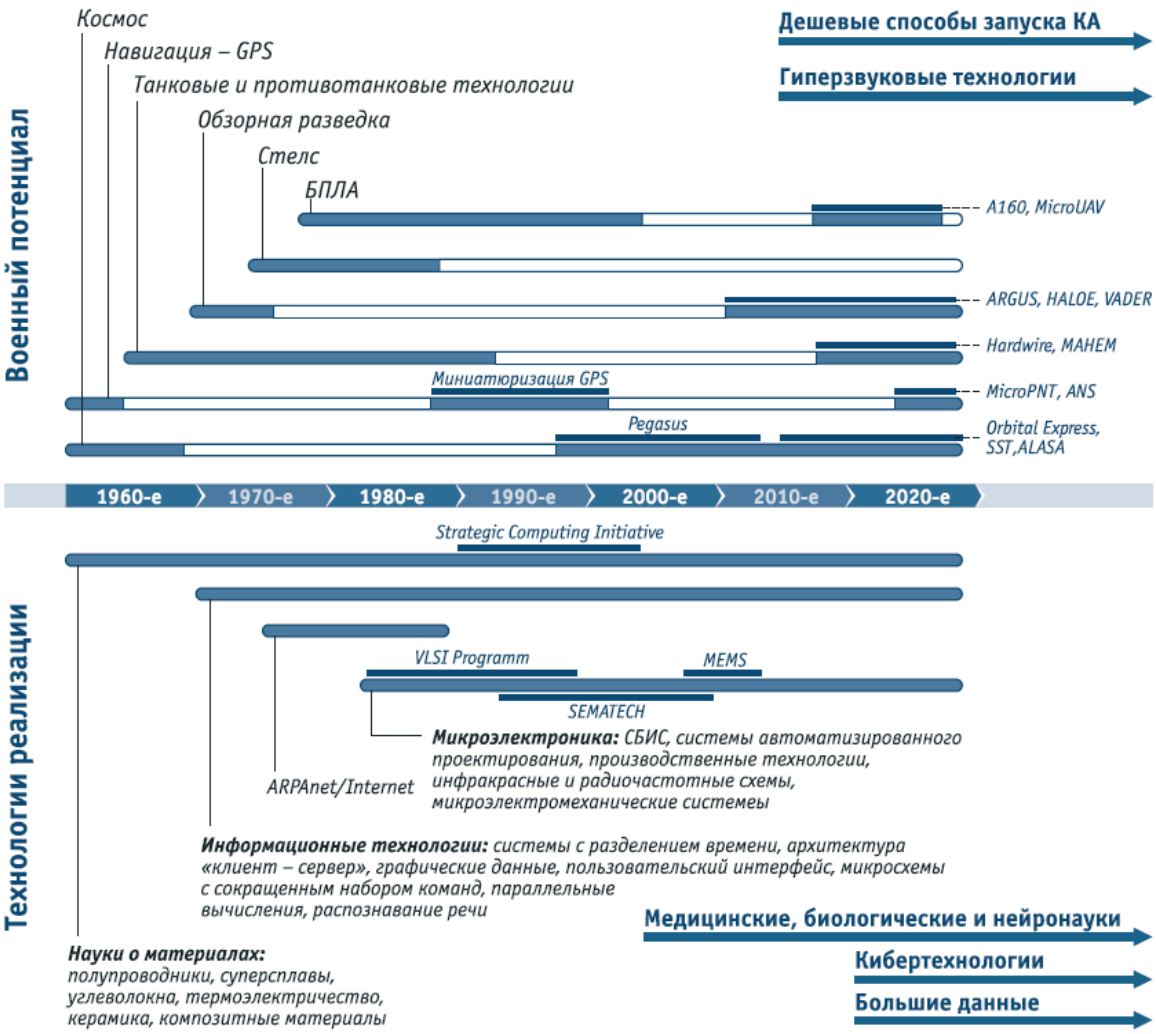

Рис. 3. *- Результативность DARPA*

Таблица 3. *Эволюция DARPA*

Этапы развития	Директор DARPA	Приоритеты НИОКР
I Этап 1958-1959 гг.	1 апреля 1958 года первым директором ARPA назначен вице-президент компании General Electric Рой Джонсон. В дальнейшем под его руководством был создан космический отдел Министерства Обороны США – родоначальник NASA.	Технологии исследования космоса. Тесная работа с исследовательской группой Вернера фон-Брауна. Участие в создании американской космической программы и ракеты «Юпитер-С».
II Этап 1960-1961 гг.	Бригадный генерал Остин Беттс, единственный кадровый военный, руководившим агентством. Холодная война. Гонка вооружений в космосе. Война во Вьетнаме (1959 - 1975).	Фундаментальные исследования для совершенствования вооружения и военной техники. Ставка на талантливых инженеров-исследователей.
1961-1963 гг.	Профессор электротехники Университета Иллинойса, Джек Руина. Закрепил децентрализованное управление проектами в ARPA, и сформировал систему самостоятельности в реализации научно-технических программ директорами отделов и руководителями проектов.	Долгосрочные научно-технические проекты. Ставка на научно-технический потенциал проекта, превышающий возможности его военного применения. Поощрялось творческое использование сотрудниками Агенства существующих в Министерстве обороны США управленческих и экономических механизмов, включая бессрочные ассигнования на НИОКР, инициативные проекты, закупки у единственного поставщика и авансирование долгосрочных контрактов.
1963-1965 гг.	Ученый Роберт Спрулл.	Организация новых форм сотрудничества между научными кругами, правительством и промышленностью для удовлетворения потребностей США в создании оборонных технологий и активной конкуренции с СССР.
1965-1967 гг.	Чарльз Херцфилд. Разгар войны во Вьетнаме.	Поддержка долгосрочных фундаментальных исследований (необязательно военного назначения).
1967-1970 гг.	Визионер в области телекоммуникаций, в том числе создании космических систем связи, Эберрхард Рецин. Считал, что только проекты с высоким риском могут быть по-настоящему прорывными.	Выполнение высокорисковых научных исследований.
III Этап 1970-1975 гг.	Стив Лукасик. При Президенте США Никсоне Конгресс запретил военным финансирование исследований, не имеющих прямого отношения к военным задачам. В 1972 году подписан договор с СССР об ограничении Стратегических наступательных вооружений и Договор по противоракетной обороне. ARPA становится официально Defense – появляется DARPA.	Ориентация на оборонные исследования, имеющие непосредственное военно-прикладное значение.

Этапы развития	Директор DARPA	Приоритеты НИОКР
1975-1977 гг.	Джордж Хаймлер. Известен формулировкой пяти основных вопросов к программам и проектам DARPA:	Системный подход к планированию и управлению исследовательскими проектами. Введена система планирования научного результата, ориентации на конкретный результат и соответствие плану-графику исследований. При этом основной целью DARPA стало финансирование прикладных исследовательских проектов, практическая польза от которых для Пентагона была очевидной.
1981-1985 гг	Роберт Фоссум. Окончание Вьетнамской войны. К концу 1980-х годов японские вендоры – производители полупроводниковой техники – активно расширяли свой рынок. При этом американские корпорации планировали большинство своих электронных комплектующих закупить именно в Японии. В США началась кампания по требованию активных действий со стороны правительства, в частности в области изменения законодательства.	Оборонные задачи уступили место вопросам повышения конкурентноспособности американской экономики, в частности промышленности. Борьба за приоритет в разработке микроэлектроники и компьютерных технологиях.
	Роберт Купер. Концепция Рональд Рейгана звездных войн подстегнула развитие на бумаге фантастических проектов, а в реальной практике – успех миниатюризации GPS и развитие портативных электронных устройств	В 1984 году из-под действия антимонопольного законодательства США выводятся кооперации по организации совместных научно-исследовательских работ и консорциумов, содействие обмену научно- техническими достижениями в рамках таких структур и иная кооперация в области развития НИОКР.
1985-1988 гг.	Роберт Дункан. В 1987 году 14 предприятий электронной промышленности объединились в консорциум SEMANTECH для кардинального улучшения качества выпускаемой продукции. В следующем 1988 году федеральное правительство ассигновало 100 млн. долларов ежегодно в течение 5 лет на финансирование электронной индустрии.	Успех DARPA в области разработки технологий промышленного производства интегральных схем сделал рентабельным массовое изготовление программируемых кристаллов сложных СБИС-устройств и обеспечил простой интерфейс доступа к производству разработчикам новых электронных устройств американских дизайн-центров.
1989-1990 гг.	Рэймонд Коллдэй. Министерство обороны США рекомендовало наделить DARPA полномочиями для заключения инновационных контрактных соглашений с самыми лучшими и яркими научно-исследовательскми коллективами и компаниями.	Новые, гибкие правила заключения контрактов на НИОКР. Привилегия менеджера программы DARPA на основании представленных документов формировать политику в области интеллектуальной собственности по контракту – от условий неограниченных прав правительства на результат до полного отказа от прав на интеллектуальную собственность, полученную в рамках проекта (в соответствии с разделом 845 Закона о национальной обороне).
1989-1990 гг.	Государственный чиновник Крэйг Филдс. В 1990 году Филдс был уволен за слишком активную, по мнению администрации Буша, поддержку проектов «промышленной политики», в ущерб новым военным технологиям. Считается, что он перешагнул неписаные правила допустимой эксплицитности в военно-промышленной политике.	Ставка на поддержку инструментов «промышленной политики», когда DARPA выступала заказчиком коммерчески значимых конкуретноспособных на внешнем рынке (прежде всего, по сравнению с Японией) технических решений, как например телевидения высокой четкости (HDTV) и электроники на основе арсенида галлия.

Этапы развития	Директор DARPA	Приоритеты НИОКР
IV Этап 1990-1992 гг.	Виктор Рэйс. Завершение Холодной войны и распад СССР.	Закрепление доминирования США в мире, повышение конкурентноспособности национальной экономики, обеспечение для США выхода за рамки международного контроля, в условиях снижения финансирования военных программ и трансформации инфраструктуры военно- промышленного комплекса.
1992-1995 гг.	Гари Денман. В 1993 году DARPA снова становится ARPA. В США начинается общая тенденция снижения расходов на оборону.	Большее внимание уделяется разработке технологий двойного назначения.
1995-1998 гг.	Ларри Линн.	Закрепление в мире приоритета американской экономики и ориентация на создание глобальных технологий вооруженной борьбы.
1998-2001 гг	Фернандо Фернандез, директор DARPA в 1998-2001 гг. 20 января 2001 года в должность Президента США вступил Джордж Буш и период увлечения технологиями двойного назначения и чисто гражданскими разработками подошел к концу	Интересно, что еще в июне 2001 года приоритетной задачей обороны США, решение которой возлагалась на DARPA, были «развитие космических технологий и обеспечение безопасности спутниковых систем и ближнего космоса».
V Этап 2001-2009 гг.	Энтони Тазер. Теракты 11 сентября коренным образом изменили миссию исследовательской деятельности DARPA. Под руководством Энтони Тазера прошла одна из самых значительных трансформаций DARPA за все время ее существования. Проблематика была переориентирована на задачи развития оборонно-промышленного комплекса США.	Ставка на решение тактических задач вооруженных сил, системы высокоточного оружия, информационной безопасности и т.д. Были произведены серьезные структурные изменения, формализованы сложившиеся процедуры, контрактная система DARPA стала значительно более регламентированной, изменились требования к срокам и структуре финансирования проектов.
2009-2012 гг.	В 2009 году DARPA возглавила Регина Дуган, ранее – основатель стартапа RedXDefense в области технологий обнаружения и деактивации взрывчатых веществ и основатель венчурного фонда Dugan Ventures.	Приоритет в сторону борьбы с терроризмом, обеспечения национальной безопасности, включая информационную безопасность.
с 2012 г. – по настоящее время.	Арати Прабхапар, директор DARPA с 2012 г.	DARPA имеет возможность переключиться с доминировавших прежде проблем национальной разведки и информационного контроля – на проблемы нарождающихся технологий в области биологии, медицины и микроэлекромеханических систем.

Актуальная программа поисковых исследований DARPA на 2014/2015 финансовый год опубликована по адресу http://www.darpa.mil/NewsEvents/Budget.aspx и содержит тематические карточки актуальных НИОКР и размеры финансирования (см. табл. 4). При этом большая часть документов по планируемым направлениям исследований (за исключением секретной части программ, составляющий около 5% от бюджета DARPA) являются открытыми. Это позволяет потенциальным исполнителям ознакомиться с программами исследований заранее, а также подготовить и представить свой проект в рамках выбранной программы. Как правило, типовой проект рассчитан на 2-3 года с бюджетом от 10 до 40 млн. долл. К работе могут быть привлечены до 10 организаций-подрядчиков и 1-2 университета. Управление проектами осуществляют соответствующие менеджеры, обладающие достаточной финансовой и операционной самостоятельностью.

Таблица 4. *Динамика финансирования поисковых программ DARPA*

Тип	Направление программ	Объем финансирования за период			
		2013	2014	2015	2014–2015**
6.1. Фундаментальные	Оборонные исследования	273 750*	315 033	312 146	–0,9 %
	Фундаментвльные исследования в области военной медицины	37 143	49 500	49 848	+0,7 %
6.2. Прикладные исследования	Биомедицинские технологии	98 097	114 790	112 242	–2,2 %
	Инфокоммуникационные технологии	348 530	399 597	334 407	–16,3 %
	Когнитивные компьютерные системы	27 538	16 330	—	—
	Технологии биологической защиты	15 131	24 537	44 825	+82,7 %
	Тактические технологии	209 578	218 209	305 484	+40 %
	Технологии материалов и биотехнологии	158 175	166 654	160 389	–3,8 %
	Электронные технологии	192 349	233 469	179 203	–23,2 %
6.3. Технологические разработки	Перспективные аэрокосмические системы	168 376	144 804	129 723	–10,4 %
	Космические программы и технологии	136 427	142 546	179 883	+26,2 %
	Перспективные элекктронные технологии	92 291	107 080	92 246	–13,9 %
	С3: системы навигации, управления и связи	189 909	239 078	243 265	+1,8 %
	Секретные программы	2 760	—	—	—
	Технологии сетецентрической вооруженной борьбы	221 490	259 006	386 926	+49,4 %
	Сенсорные технологии	272 095	276 364	312 812	+13,2 %
Обеспечение	Информационная безопасность	1 961	—	—	—
	Программа поддержки малого бизнеса	70 839	—	—	—
	Штаб-квартир	64 248	71 659	71 362	–0,4 %
	Всего:	2 580 656	2 778 656	2 914 770	+4,8 %

** Суммы приведены в тыс. долл. США.*
*** Период с 01.10.2014 по 30.09.2015.*

Рис.4. *Текущая структура DARPA*

Для достижения поставленных целей и решения задач поисковых программ сформирован современный облик агенства DARPA (см. рис. 4), ядро которого составляют уникальные научно-исследовательские подразделения агентства (см. табл. 5).

Таблица 5. *Характеристика научно-исследовательских подразделений DARPA в 2014 году*

№	Отдел	Состав	Направления исследований
1	Тактические технологии (Tactical Technology).	24 сотрудника: - 6 PhD - 13 без степени; - 5 офицеров.	Современные высокоточные системы вооружения, лазерное оружие, беспилотные средства вооружений на базе воздушных, космических, наземных и морских платформ, перспективные космические системы мониторинга и управления.
2	Инновации в информационных технологиях (Information Innovation)	23 сотрудника: - 12 PhD - 10 без степени; - 1 офицер.	Информационные системы мониторинга и управления, технологии высокопроизводительных вычислений, интеллектуальный анализ данных, системы распознавания образов, когнитивные системы машинного перевода.
3	Стратегические технологии (Strategic Technology)	24 сотрудников: - 14 PhD - 10 без степени.	Системы связи, средства защиты информационных сетей, средства радиоэлектронной борьбы (РЭБ), устойчивость систем к кибератакам, системы обнаружения замаскированных целей на новых физических принципах, энергосбережение и альтернативные источники энергии.
4	Адаптивное управление (Adaptive Execution)	8 сотрудников: - 1 PhD - 6 без степени; - 1 офицера.	Исследования в области построения адаптивных платформ и архитектур, включая универсальные программные платформы, модульные аппаратные средства, многофункциональные информационные системы и средства разработки и проектирования.
5	Оборонные исследования (Defense Sciences)	16 сотрудников: - 12 PhD - 4 без степени.	Исследования в области фундаментальной физики, новых технологий и приборов на новых физических принципах, энергетики, новые материалы и биотехнологии, прикладной и вычислительной математики, медико-биологические средства защиты, биомедицинские технологии.
6	Микросистемные технологии (Microsystems Technology)	17 сотрудников: - 13 PhD - 4 без степени.	Технологии электроники, фотоники, микромеханических систем, перспективной архитектуры интегрированных микросхем и алгоритмов распределенного хранения данных.
7	Биологические технологии	12 сотрудник: - 8 PhD - 2 без степени; - 2 офицера.	Исследования в области инженерной биологии, включая омиксные технологии, синтетическую биологию, метаболическую инженерию, генную терапию (включая искусственную хромосому человека), прикладные аспекты нейронаук.

Особенности управления проектами

В основе успешной научно-исследовательской деятельности агенства DARPA лежат выполненные с высоким качеством НИОКР, общей продолжительностью 3-5 лет. По мнению DARPA для достижения успеха в реализации проекта необходимы оригинальные новые научные идеи и соответствующая команда проекта, обладающая всеми необходимыми навыками и компетенциями. Схема управления программами поисковых исследований DARPA представлена на рис. 6.

По мнению руководителей DARPA [1-2] все технологические проекты следует оценивать в координатах «уровень риска – уровень значимости для вооруженных сил США» (Technical risk – Potential military utility). При этом преимущество отдается проектам, которые имеют одновременно и высокие риски, и высокую отдачу (High risk – High pay-off) и обеспечивают, таким образом, прорывные достижения. Как правило, это крупные долгосрочные концептуальные проекты, в которые вовлечены различные научно-исследовательские отделы DARPA. В эти проекты вкладывается основная часть финансирования – около 60% инвестиций. На проекты с низким риском и высокой отдачей (Low risk – High pay-off) (глав-

Рис. 6. *Схема управления программами DARPA*

ным образом, адаптация и применение готовых коммерческих продуктов к актуальным оборонным потребностям, лежащим на пересечении сфер ответственности военных ведомств) в общем случае отводится 20% и более инвестиций. Проекты с высоким риском и низкой отдачей (High risk – Low pay-off) получают также примерно 20% инвестиций. К таким проектам относятся разработка технологий двойного назначения, занятие ниш на коммерческом рынке безопасности, создание новых технологий военного назначения.

Отметим, что еще в 1975 году директор DARPA Джордж Хейлмейер сформулировал следующий актуальный вопросник для проводимых НИОКР, который не потерял своей актуальности и в настоящее время:

1. Что мы пытаемся сделать? Какова проблема, которую мы пытаемся решить?
2. Как это делается сегодня? Какие ограничения накладывает существующий опыт?
3. Что нового в нашем подходе, и почему мы думаем, что он будет успешным? Каковы доказательства того, что новый подход будет работать?
4. Предполагая, что мы добьемся успеха, к каким изменениям это приведет?
5. Как много времени это займет? Сколько это будет стоить? Каковы среднесрочные и целевые показатели?

В агенстве DARPA различают следующие этапы реализации проектов:

• от идеи к концепту – осуществление опытно-конструкторских разработок, демонстрирующих принципиальную возможность реализации технологии;

• от концепта к прототипу – разработка опытного или демонстрационного прототипа образца, возможно масштабированного;

• от демонстрационного прототипа к промышленному прототипу и мелкосерийному производству;

• от мелкосерийного производства к массовому производству промышленного прототипа военного назначения.

На каждом этапе DARPA размещает предложения (solicitations) на реализацию соответствующей разработки с заданными тактико-техническими характеристиками. Организации, отвечающие заявленным критериям выбора исполнителей НИОКР, получают определенное «поощрение» и право на заключение дальнейшего контракта. В целом правительство США применяет от 40 до 50 различных типов федеральных контрактов. Различают следующие группы контрактов: контракты «фиксированных цен» и контракты «возмещения издержек производства подрядчика». При этом выделяются контракты «поощрительного» или «многократно-поощрительного типа», которым присущ сложный механизм ценообразования и широкое варьирование размера материального поощрения подрядчика в зависимости от достигнутых результатов.

DARPA уделяет большое значение управлению рисками НИОКР. Для каждого проекта подбирается индивидуальный подход и методика управления рисками. Кроме того проводятся тщательные ревизии со стороны контролирующих органов.

Непосредственно перед заключением контракта на НИОКР проводится разработка программы исследований. Как отмечается в [2-3] по результатам взаимодействия со всеми заинтересованными сторонами, а также ознакомления с существующи-

ми технологиями и достижениями в данной области - менеджер программ объявляет процедуру запросов о представлении предложений (requests for competitive proposals - RFP). Затем, после окончания сбора предложений, менеджер программы формирует техническое задание на НИОКР (Broad Agency Announcement – BAA). При этом условия и требования BAA являются закрытыми до момента объявления конкурса и не подлежат разглашению.

Отметим высокую самостоятельность менеджера программы, который уполномочен самостоятельно принимать решения о допуске к конкурсу различных исполнителей, в том числе, финансируемых из бюджета Мининстерства обороны США, продливать срок проведения конкурса для более тщательной подготовки заявок предполагаемыми исполнителями и формирования соответствующих команд проекта, определять цену контракта, принимать решение о форме сотрудничества – государственный контракт, грант (субсидия), соглашение о совместных НИОКР и пр., формировать политику в области интеллектуальной собственности по контракту – от условий неограниченных прав до полного отказа от прав на интеллектуальную собственность согласно разделу 845 Закона о национальной обороне (section 845 the National Defense Authorization Act). По времени процедура оценивания заявок может длиться до 3-4 месяцев, контрактование с победителем конкурса до 2-х месяцев. При этом большинство контрактов заключается на срок 1-3 года.

Отметим, что DARPA наделена специальными полномочиями (Special authorities), упрощающими бюрократические процедуры, распространяющиеся на другие оборонные агентства. В частности, осуществлять упрощенный наем сотрудников из коммерческих структур (Experimental Personnel Authority, EPA), например, руководителей проектов, предлагая им достойную заработную плату. Ранее наем сотрудников производился исключительно из государственных структур согласно акту Interagency Personnel Act (IPA). Отметим, что EPA и IPA являются специальными исключениями по отношению к своду правил Civil Service rules, установленных для государственных служащих. В результате это позволило существенно упростить заключение контрактов (Other transaction authority) в отличие от большинства других государственных агентств, которые руководствуются требованиями Federal Acquisition Regulations FAR (Федеральное регулирование закупок). Кроме того, DARPA имеет возможность существенно стимулировать ход выполнения проекта денежными премиями (Grand challenge) для скорейшего получения итоговых результатов НИОКР.

DARPA регулярно проводит научно-технические семинары для выявления существующих проблем в различных технологических областях и для поиска возможных путей их решения. Кроме того, Агентство регулярно участвует в специализированных мероприятиях, конференциях и круглых столах[3-5].

Примеры проектов DARPA

Начиная с 2002 года, приоритет поисковых программ DARPA плавно сместился в новую и перспективную область кибербезопасности. Дело в том, что в середине XX века «оборонные» НИОКР включали в себя разработку различных систем вооружения, оружия массового поражения, тяжелой техники и составляли обособленную часть экономики США как отдельно взятого государства. На рубеже XX и XXI века проблема борьбы с международным терроризмом поставила на первый план вопросы обеспечения внутренней безопасности с учетом внешней политической обстановки, в том числе вопросы обеспечения кибербезопасности критически важных объектов государственного и военного управления. В результате современные НИОКР DARPA направлены на разработку критически важных технологий, от которых зависит безопасность систем сообществ public network, а не только государства в целом. При этом актуальны именно *фундаментальные междисциплинарные исследования* в области инфокоммуникационных технологий, нанотехнологий и материалов, биомедицины, когнитивных технологий, универсальных систем связи, систем интеллектуального анализа данных, информационной безопасности и новой электроники. Проведем критический анализ упомянутых НИОКР, начиная с 2002 г. по настоящее время.

Катастрофические последствия 11 сентября продемонстрировали неспособность США к отражению подобных терактов, беспрецедентных как по своему масштабу, так и асимметричности вызовов безопасности. Для разрешения сложившейся ситуации DARPA инициировала ряд специальных НИОКР с бюджетом финансирования от 500 млн (2002-2005 годы) до 1 млрд долл. (2002-2009 годы).

Проект «Предупреждение террористических актов» (Terrorism Information Awareness - TIA) позволил на основе анализа большого количества разнородных данных о слабо связанных между собой событиях, таких как покупка авиа- и желез-

нодорожных билетов, бронирование номеров в гостиницах, покупка химикатов и взрывчатых веществ, приобретение огнестрельного оружия и др., выявлять преступные группы лиц, готовящихся совершить террористический акт с применением оружия массового уничтожения (ядерного, химического, биологического) на территории США. Для реализации проекта были привлечены модели и методы системного анализа, исследования операций, теории игр, теории вероятности и статистического анализа, теории принятия решений и пр.

Другой проект DARPA был направлен на разработку специализированного программного обеспечения так называемого «ситуационного анализа» (Software for Situational Analysis), который позволил в автоматизированном режиме: распознавать людей на расстоянии, обнаруживать противника, осуществляющего наблюдение за целями (объектами критической инфраструктуры) на территории США; автоматически находить, извлекать и связывать между собой отрывочные и фрагментарные представления о намерениях и деятельности групп людей, содержащиеся в больших массивах открытых и закрытых источников информации; достаточно точно моделировать субъективные представления и социальное поведение малочисленных по составу групп для имитации и проигрывания асимметричных действий противника; обеспечивать более эффективные средства анализа и принятия решения для пресечения преступной деятельности.

Проект «Моделирование асимметричных воздействий» (Wargaming the Asymmetric Environment - WAE) позволил выявлять мотивы и своевременно раскрывать замысел террористических действий. В результате были созданы имитационные модели поведения отдельных людей и небольших групп с учетом их психологии, культуры, политических взглядов, уровня образования и жизненного опыта (Scalable Social Network Analysis - SSNA). Также были разработаны имитационные модели поведения отдельных враждебно настроенных стран, их ключевых политических лидеров и террористических групп. Кроме того, построены аналитические модели для принятия решений, позволяющие прогнозировать различные ситуации в реальном масштабе времени (Rapid Analytical War Gaming - RAW). Здесь был применен математический аппарат теории игр со смешанными стратегиями, а также теория принятия решений в условиях неопределенности.

Для повышения эффективности и координации совместных действий американских спецслужб по своевременному обнаружению террористов, раскрытию их замыслов и предотвращению терактов DARPA инициировала проекты «Генуя» и «Генуя-2». В результате была создана так называемая «динамическая виртуальная среда» для снятия возможных организационных и технических барьеров в совместной работе специалистов различных ведомств и организаций. В основу были положены модели и методы нечеткого структурирования аргументов, трехмерной цветной визуализации и организации адаптивной памяти.

Для обеспечения устойчивости и живучести критически важных объектов государственного и военного управления в чрезвычайных условиях DARPA инициировала долгосрочную программу - «Научные и инженерные методы» (Information Assurance Science and Engineering Tools - IASET), - которая объединила усилия специалистов в смежных областях знаний (исследование операций, системотехника, вычислительные системы и сети, кибербезопасность, операционные системы, базы данных и др.).

Проект «Безопасные и живучие информационные системы» (Organically Assured and Survivable Information Systems - OASIS) позволил выработать новые архитектурные решения комплексной системы защиты критических важных информационных систем. В результате была создана новая клиент-серверная технология обеспечения устойчивости и живучести вычислительных систем на основе современных методов обнаружения вторжений, адаптивной защиты, отказоустойчивости и реконфигурации.

Для оперативного контроля и прогнозирования состояния критически важных информационных систем реализован проект «Новые методы обнаружения кибератак» (Advanced Network Surveillance), в рамках которого созданы новые технологии обнаружения массовых и групповых кибератак. Создан прототип самообучающейся системы контроля и прогнозирования состояния критически важных информационных систем в условиях воздействия противника.

В рамках проекта «Корреляционный анализ кибернападения» (Cyber Attack Data Correlation) были разработаны адаптивные методы корреляционной обработки и классификации регистрируемых данных о состоянии критически важных информационных систем в условиях массовых враждебных программно-математических воздействий. Основное назначение – использова-

ние в крупных территориально-распределенных вычислительных сетях для определения фактов скоординированного широкомасштабного кибернападения и последующего адекватного противодействия.

В 2014 году на сайте DARPA (www.darpa.mil/Our_Work/I2O/Programs) был опубликован следующий актуальный перечень поисковых программ исследований:

- Профилирование поведения пользователей (Active Authentication);
- Активная киберзащита с ложными целями (ACD);
- Обнаружение аномальных процессов в обществе (ADAMS);
- Автоматизированный анализ кибербезопасности (APAC);
- Инфракрасный страж (ARGUS-IR);
- Интеллектуальный РЭБ (BLADE);
- Высоконадежный семантический транслятор (BOLT);
- Адаптивная система (CRASH);
- Поисковая компьютерная система (CSSG);
- Формальная верификация (CSFV);
- Новая киберзащита (Cyber Genome);
- Контроль изменений (CGC);
- Противодействие инсайдерам (CINDER);
- Глубокая очистка контента (DEFT);
- Психофизическая защита (DCAPS);
- Вымоконадежная киберзащита беспилотных летательных аппаратов (HACMS);
- Семантический анализ (ICAS);
- Поиск контента (Memex);
- Повышение устойчивости программного обеспечения (MUSE);
- Транспарентные вычисления (Transparent Computing);
- Создание «живучего облака» (MRC);
- Рубрикация и семантическая классификация документов (MADCAT);
- Боевые операции в киберпространстве (Plan X);
- Надежное программирование (PPAML);
- Криптозащита вычислений ((PROCEED);
- Автоматизированный перевод речи (RATS);
- Безопасные коммуникации (SAFER);
- Работа в социальных СМИ (SMISC);
- Позиционирование в городских условиях (ULTRA-VIS);
- Программа контроля НДВ в закупаемом для нужд Минобороны США ПО (VET);
- Наглядная визуализация (VMR);
- Распознавание сетей (WAND);
- Большие данные (XDATA) и пр.

Выборочно прокомментируем ряд поисковых программ DARPA.

Наример, *программа MUSE* предназначена для повышения надежности и безопасности прикладного программного обеспечения на основе методов надежности программ, машинного обучения и формальной верификации программного обеспечения.

Другая программа «Автоматизированный анализ кибербезопасности мобильных приложений» (*Automated Program Analysis for Cybersecurity - APAC)* позволяет осуществлять контроль недекларируемых возможностей (НДВ) в мобильных приложениях в автоматизированном режиме.

Программа (*Power Efficiency Revolution For Embedded Computing Technologies -PERFECT)* направлена на решение проблемы дефицита вычислительных ресурсов для компьютерных систем производительностью 75 Гфлопс/Вт. Предполагается оптимизировать архитектуру соответствующих вычислительных систем, разработать трансляторы для параллельной обоаботки данных, обеспечить устойчивость и живучесть программного обеспечения к программным ошибкам и вредоносным воздействиям, оптимизировать трафик передаваемых данных, а также выработать новые алгоритмы обработки данных с требуемой устойчивостью и энергопотреблением.

Программа (*Integrated Cyber Analysis System - ICAS)* посвящена разработке новых методов автоматического обнаружения и нейтрализации кибератак на основе интеллектуального анализа данных и выявления скрытых закономерностей.

Программа *(Safer Warfighter Computing - SAFER)* предусматривает создание программных средств компьютерной разведки и преодоления средств защиты информации противоборствующей стороны.

Программа «Контроля качества средств вычислительной техники» *(Supply Chain Hardware Intercepts for Electronics Defense - SHIELD).* В последние два года в Минобороны США выявлено более миллиона электронных компонентов сомнительного качества и подлинности. Это и бывшие в употреблении детали, продающиеся под видом новых, и микросхемы с подправленной в сторону улучшения характеристик маркировкой, и излишки, которые производители продают полулегально, и откровенные подделки.

В рамках программы Supply Chain Hardware Intercepts for Electronics Defense предполагается разработать миниатюрный (100X100 мкм) и недорогой (меньше одного цента за штуку) чип, кото-

рый будет подтверждать аутентичность электронных компонентов. Чип будет находиться внутри корпуса микросхемы, но никак не будет электрически связан с ее функциональной начинкой и не должен требовать существенных изменений процесса производства. Ожидается, что эта разработка будет иметь большой успех и на рынке потребительской электроники, где производители не всегда способны проконтролировать качество всех необходимых компонентов (учитывая огромные темпы развития полулегального китайского фабричного производства).

Программа *«Защиты АСУ ТП» (Protecting Cyber Physical Systems – PCPS*) предусматривает создание технологий для обнаружения, нейтрализации и пресечения известных и не известных ранее кибератак.

Программа *Plan X* направлена на разработку интуитивно понятного (игрового) интерфейса для управления боевыми действиями в киберпространстве. Например, создание технологий, упрощающих обучение и ведение кибервойн. В частности, очки дополненной реальности Oculus Rift позволяют виртуально погрузиться в интернет, перемещаться в информационных потоках, видеть информацию вокруг и манипулировать ею. По мнению исследователей, Oculus Rift может оказаться эффективным инструментом для оборонительных и наступательных информационных операций. В 2014 году в Пентагоне была проведена видеодемонстрация, позволяющая получить представление о целях, преследуемых DARPA. Симуляция была разработана при участии компаний Frog Design и Infinic, помимо Oculus Rift для навигации использовались два контроллера Razer Hydra. Были смоделированы типовые информационные операции в киберпространстве. Отметим, что завершение НИОКР по программе *Plan X* намечено на 2017 год.

Программа (*Crowd Sourced Formal Verification - CSFV*) направлена на решение сложных аналитических задач в игровой форме. Сложные математические задачи можно представить в виде интересных и увлекательных онлайн-игр.

Программа-конкурс (*Cyber Grand Challenge - CGC*) направлена на разработку приложений для автоматического исправления уязвимостей так называемого нулевого дня, 0-day, в том числе для тестирования программного обеспечения, выявления уязвимостей, генерации патчей и установки их в компьютерной сети. Сегодня поиск уязвимостей и так частично автоматизирован. Есть методы статичного и динамичного анализа, которые способны обнаружить характерные уязвимости в коде. Но вот исправлять эти ошибки автоматически компьютеры пока не научились. Задача программы - совместить анализ кода и защиту сетей в единый программно-аппаратный комплекс. Задача чрезвычайно сложная, но и 2 миллиона — достойная награда за победу в названной программе-конкурсе. Заметим, что название Cyber Grand Challenge связано с известным конкурсом Grand Challenge, который трижды проводился для автономных транспортных средств в 2004-2007 гг. Десятки автомобилей-роботов пытались проехать по незнакомой пересеченной местности, прокладывая маршрут и объезжая препятствия, включая канавы, камни и узкие тоннели. Маршрут объявляли за два часа до начала конкурса. Если в первый год проведения DARPA Grand Challenge ни одна машина не доехала до финиша (собственно, только 8 из 15 машин смогли уйти со старта, а лучшая команда преодолела 11,8 км из 230), то потом они уже начали соревноваться на скорость. Прогресс был очевиден. По аналогии и с Cyber Grand Challenge — поначалу задача кажется неразрешимой, но в дальнейшем ожидается получить первые самообучающиеся прототипы, которые действительно смогут автоматически генерировать патчи и закрывать уязвимости нулевого дня, 0-day, в течение нескольких секунд после обнаружения. Конкурс Cyber Grand Challenge пройдет в несколько этапов и будет продолжаться несколько лет. В ближайшее время опубликуют информацию о грантах на разработку технологий для проведения этого конкурса, в том числе на создание набора задач. Финал соревнований состоится в первой половине 2016 года.

Программа (*Vanishing Programmable Resources - VAPR*) направлена на создание средств вычислительной техники нового класса. Сегодня микропроцессоры широко используются для управления военной техникой и вооружением. Настоящая программа разрабатывает физически самоуничтожающиеся микросхемы, превращающиеся по команде в «неспособные к воссозданию элементы». Другими словами речь идет о создании средств вычислительной техники с заранее заданным сроком эксплуатации. Функция самоуничтожения может быть активирована как посредством внешнего сигнала, так и под воздействием окружающей среды, например, в определенных температурных условиях. В частности, компания IBM будет экспериментировать

Hadoop), оптимизирующий компилятор Numba для Python, разработанный Continuum Analytics, Inc. под лицензией BSD и пр.

Отметим, что в 2014 году приоритет в программах DARPA был отдан развитию специальных биотехнологий. По мнению нового директора DARPA Арати Прабакар, «Биология является величайшим естественным инноватором, и любому научно-исследовательскому коллективу просто необходимо обращаться к этому *величайшему мастеру* сложных систем за вдохновением и вариантами решения проблем». И если 2013 год прошел в DARPA под флагом создания боевых роботов, солдат-киборгов и военизированных дронов, то создание в 2014 году нового отдела Biological Technologies Office, BTO, означает, что была сделана ставка на следующее поколение оборонных технологий, которое будет брать пример с естественных форм жизни. При этом одним из основных направлений военного развития станет синтетическая биология, а технологии робототехники постепенно будут переданы в Научно-исследовательскую лабораторию BMC или Лабораторию Линкольна МТИ. BTO займется изучением биотехнологий на стыке биологии и машиностроения. Цель заключается в создании искусственных живых сверхматериалов, которые можно использовать для следующего поколения механической и электротехнической продукции, самовосстанавливающихся материалов, возобновляемого топлива, солнечных батарей и так далее. Стоит отметить, что DARPA объявило о создании программы по синтетической биологии Living Foundries три года назад, чтобы трансформировать современное производство. Бюджет программы на 2015 год составляет от 18 до 28 миллионов долларов. Заметим, что еще в 2010 году агентство создало программу BioDesign, которая изучала способы создания синтетических существ, которые были бы генетически запрограммированы на бессмертие и оснащены своего рода «выключателем», позволяющим в случае необходимости «выключать» их. Помимо создания новых живых материалов и живых организмов, BTO будет проводить долгосрочные исследования в области эпидемиологии, неврологии, протезирования и пр. Упомянутый отдел продолжит исследование искусственных конечностей, управляемых силой мысли. Уже сегодня некоторыми протезами можно управлять непосредственно при помощи мозговых волн. Парализованным добровольцам вживляли чипы в мозг, которые были способны принимать нервные сигналы и управлять двигательными функциями автоматизированных конечностей. Далее исследователи предполагают исследовать обратные связи для возможности ощущать физическое прикосновение при взаимодействии отчуждаемых устройств с внешним миром. Согласно официальному заявлению DARPA, Biological Technologies Office также займется НИОКР в области искусственного интеллекта для разнообразных машин и автоматизированных приспособлений на поле боя и пр.

В целом программы DARPA направлены на создание новых технологий в нескольких конкретных приложениях: подчинение тела человека его намерениям, расширение возможностей человека в реальном мире за счет робототехнических средств, использование человеком виртуального мира как полностью управляемой части «дополненной реальности» и, как результат, комбинации методов управления и преобразования объектов из живого, неживого и виртуального миров на пути достижения военного технологического превосходства. Таким образом, разрабатываемые новые передовые исследовательские программы условно можно разделить на триплет технологий: *технологии человека, технологии робототехники и сетевые технологии*.

Отмечается[2], что предлагаемый набор технологий в полной мере соответствует ожиданиям в области технологических прорывов и экспоненциального роста в ближайшие 20 лет. «Технологии человека – создание передовых биомедицинских технологий, способных предотвратить смерть человека в результате ранений, заболеваний или инфекций – от диагностики до восстановления или даже полного воссоздания тканей и органов тела. Сетевые технологии – оперирование совокупностью объектов, средств и систем, как единым управляемым пространством, в частности сведением информации (технологии C4ISR+), развитием технических средств связи, разведки и обработки информации, в том числе на новых физических принципах. Технологии робототехники – создание техники, способной к выполнению широкого спектра механических операций, наблюдения и доставки полезной нагрузки в любую точку на Земле, включая миниатюрные манипуляции, высотные перемещения и подводные операции»[2].

Заключение

Сравнительно недавно произошел крупный международно-политический скандал, вызван-

ный разоблачениями Э. Сноудена и ряда других журналистов, в ходе которого было выявлено следующее. Агентство национальной безопасности, АНБ США, имеет прямой доступ к центральным серверам и дата-центрам крупнейших интернет-компаний – «Google», «Yahoo!», «Microsoft», «Facebook", «Skype", «YouTube" и «Apple". Перехват информации осуществляется в каналах мобильной и фиксированной связи по всему миру. Используется более 85 тысяч специальных аппаратно-программных закладок. Только в Германии АНБ ежемесячно отслеживает 500 миллионов электронных и компьютерных соединений, во Франции за один месяц в конце 2012 года – свыше 70 миллионов, количество отслеживаемых аккаунтов в социальных сетях за год составило более 250 миллионов. По мнению одного из экс-сотрудников АНБ У. Бинни, АНБ располагает данными о 40-50 триллионах телефонных переговоров и сообщений электронной почты со всего мира. Установлено, что АНБ ведет «киберразведывательную» деятельность в отношении более 35 глав государств и правительств, включая канцлера Германии, президентов Бразилии и Мексики, а также уполномоченных представителей Совета министров ЕС и Европейского совета, 38 посольств и дипмиссий, Евросоюза и стран – членов ЕС в здании штаб-квартиры ООН в Нью-Йорке, ООН и МАГАТЭ.

Страны Европы, Азии и Латинской Америки незамедлительно отреагировали и заявили о продвижении своей собственной и независимой от США технической политики в области кибербезопасности. 12 государств Латинской Америки, входящих в Союз южноамериканских наций (УНАСУР), заявили о намерении создания собственной сети аналога Интернет. Власти Бразилии начали разработку своей «безопасной» электронной почты. Правительство Германии запретило прохождение интернет-трафика между немецкими пользователями через сетевые узлы, расположенные за пределами страны с целью исключения прослушки зарубежными спецслужбами. Крупнейший оператор Европы «Deutsche Telekom» призвал немецкие компании объединиться в проекте по созданию «национальной маршрутизации» и пр.

В настоящее время ряд технологически развитых государств (более 120 стран) продекларировали разработку «кибероружия». В США в декабре 2011 года от Конгресса было получено разрешение на развитие «наступательного» кибероружия. «Международная стратегия по действиям в кибер-пространстве» США 2011 года признала киберпространство таким же потенциальным полем боя как сушу, море, воздух и космос. Во Франции в 2008 году в «Белой книге по обороне и национальной безопасности» введено понятие «кибервойна» и раскрыты ее составляющие –»кибероборона» и «наступательные возможности для кибервойны». В Германии в феврале 2011 года принята «Стратегия безопасности в киберпространстве». Аналогичный документ введен в действие в Великобритании с ноября 2011 года. В 2011 году официально было объявлено о создании в Народно-освободительной армии Китая «интернет-войск». В Индии стратегия в области кибербезопасности принята в мае 2013 года, предполагающая в том числе создание индийского Национального координационного центра по контролю за информацией в Интернете с целью предотвращения иностранного кибершпионажа и хакерских атак. В «Белой книге» Министерство обороны Японии за 2013 год отмечена исключительная важность кибербезопасности для обеспечения безопасности государства и его вооруженных сил. В частности, обращается внимание на то, что: «Участились кибератаки на информационные и коммуникационные сети правительственных и военных институтов различных стран». В самой Японии за 2012 год было зафиксировано более 1000 кибератак на японские учреждения. В НАТО в 2011 году утверждены новая редакция программного документа «Политика НАТО в области киберзащиты» и «План действий НАТО в области киберзащиты», который содержит практические рекомендации по действиям в данной области. 19 июня 2013 года стратегия кибербезопасности вступила в силу в Евросоюзе. В начале 2013 года стратегию кибербезопасности разработала Финляндия.

Начиная с 2010 г. в технологически развитых странах созданы специальные организационно-штатные структуры, призванные осуществлять планирование и управление кибероперациями как в мирное время, так и в состояниях повышенной боевой готовности. Например, в США в АНБ еще в 1997 году из высококвалифицированных хакеров было создано специализированное подразделение под названием ТАО (Tailored Access Operations), способное «достигать недоступного». В госдепартаменте США с 2011 года существует отдельный департамент по вопросам киберпространства, руководитель которого объявил кибербезопасность «императивом внешней политики США». В июне 2009 году создано специальное **Киберкомандование ВС США** (USCYBERCOM),

основными задачами которого являются «проведение операций, направленных на обеспечение свободы действий США и их союзников в киберпространстве, а также ограничение этой свободы для стран-противников». Примечательно, что в 2013 году Пентагон учредил специальную «Медаль за боевые отличия» для военнослужащих, отличившихся при проведении кибероперациий. В Великобритании с июня 2010 года в составе одной из секретных служб – Центре правительственной связи и коммуникаций (GCHQ) – функционирует центр операций кибербезопасности. Национальные центры кибербезопасности созданы в июне 2011 года в Германии, в январе 2012 года в Нидерландах в январе 2013 года в Дании. Во Франции подобное подразделение входит в состав главного управления внешней безопасности, в ФРГ в составе Федеральной разведывательной службы (BND) функционирует специальный отдел по противодействию хакерским атакам и кибершпионажу. В Латвии существует центр по противодействию киберугрозам, в Литве – национальный центр по предотвращению инцидентов в сфере информационных технологий. В Эстонии создан передовой центр НАТО - Центр кибероборонны (Cooperative Cyber Defense Center of Excellence), в работе которого участвует ряд стран (Венгрия, Великобритания, Германия, Испания, Италия, Латвия, Литва, Нидерланды, Польша, Словакия, США и Эстония и пр.). При этом координацией деятельности НАТО в области кибербезопасности занимается специальный отдел управления по новым вызовам и угрозам Международного секретариата блока в Брюсселе. В рамках Евросоюза действует Европейское агентство по сетевой и информационной безопасности (European Network and Information Security Agency), а с 1 января 2013 года начал работу Центр по борьбе с киберпреступностью (European CyberCrime Centre).

В целом следует отметить, что в настоящее время проводится большой спектр НИОКР в области кибербезопасности, которые направлены на разработку специальных программно-аппаратных комплексов: *«PRISM» (сбор и обработка метаданных), «Feed through», «Gourmet through» и «Jet p low» (дистанционное внедрение «закладок» в персональные компьютеры), «Quantum Insert « (перенаправление трафика к ложным сайтам Интернета), «Dropout Jeep» (дистанционный съем информации с айфонов фирмы «Apple»), «Monkey calendar» (sms-сообщения о местонахождении мобильных телефонов), «Rage master» (перехват информации с экранов компьютеров), «Genie» (контроль функционирования 85000 «закладок-шпионов» по всему миру).*

Начиная с 2006 года в США регулярно проводятся крупномасштабные транснациональные киберучения «Cyber Storm» и с 2010 года в Евросоюзе «*Cyber Europe – CE),* в ходе которых на основе «предполагаемых действий противника» отрабатываются и проверяются различные аспекты обеспечения кибербезопасности, в т.ч. посредством моделирования в режиме реального времени «хакерских атак» и «кибернападений» на информационные системы критически важных объектов государственного и военного управления. Согласно публикации газеты «The Washington Post» на основе заявлений Э.Сноудена разведслужбы США в течение только 2011 года провели против других стран 231 кибератаку, были потрачены более 652 милл. долларов США. Три четверти кибератак, уточнило издание, были направлены против России, Ирана, Китая и Северной Кореи, в т.ч. ядерные программы этих стран. По мнению Э.Сноудена США провели более 61 тысячи хакерских кибератак по всему миру. Таким образом, представляется, что вопросы кибербезопасности как минимум до 2020 года будут входить в число приоритетных направлений обеспечения глобальной безопасности и мировой стабильности.

НИОКР в области кибербезопасности актуальны и для отечественных представителей военно-промышленного комплекса[8-12], ведущих военных и гражданских университетов и других представителей отечественной школы науки и образования. В частности в 2012 году в Российской Федерации был создан Фонд перспективных исследований РФ (ФПИ) для содействия осуществлению научных исследований и разработок в интересах обороны страны и безопасности государства, связанных с высокой степенью риска достижения качественно новых результатов в военно-технической, технологической и социально-экономической сферах.

К основным задачам упомянутого фонда относятся:

• разработка наиболее действенных методик определения важнейших тенденций в научно-технологической сфере и потребностей в инновационных решениях;

• построение системных эволюционных моделей технологического пространства и соответствующих баз знаний;

• выработка наиболее эффективных форм и способов взаимодействия с научными и экспертными сообществами;

• создание автоматизированных средств научно-технологического прогнозирования и поддержки принятия решений, использующих качественные и количественные подходы и оперирующих большими объемами неструктурированных и слабоструктурированных данных;

• разработка технологии управления в системах связи с произвольной маршрутизацией на основе динамической сети разнородных ретрансляторов; разработка технологии высокопроизводительных вычислений в распределенных гетерогенных сетях;

• разработка технологии создания элементной базы квантовых компьютеров; разработка технологий обучения и имитации мыслительного процесса человека;

• разработка технологий понимания техническими системами смысла и многозначного контекста информации;

• разработка технологий, обеспечивающих способность технических систем к обобщению и эффективной работе с неполными, неточными или искаженными данными;

• разработка технологий определения психоэмоционального состояния и прогнозирования поведения людей;

• создание демонстрационных образцов нейроинтерфейсов с возможностью обратной связи и персонифицированным усилением когнитивных способностей для управления роботизированными боевыми, разведывательными, транспортными и др. модулями и улучшение качества подготовки личного состава;

• создание цифровых моделей головного мозга и моделирование его работы в системах искусственного и гибридного интеллекта с использованием в когнитивных технических системах (когнитивные человеко-машинные интерфейсы, интерфейсы мозг-компьютер и глаз-мозг-компьютер, антропоморфные и нейроморфные роботы) и пр. Важнейшей задачей Фонда перспективных исследований является создание примера совершенно новой системы и модели управления разработкой передовых технологий для обороны и безопасности страны в условиях нарушенных производственных цепочек. Выделенный статус позволяет Фонду транслировать стратегические вызовы обороны и безопасности государства в конкретные научнотехнические проекты поверх границ ведомственных НИОКР осуществлять целеполагание и сопровождать развитие приоритетных межвидовых, междисциплинарных и межотраслевых научно-технических исследовательских проектов. Непрерывные коммуникации с научным сообществом, промышленностью, органами власти и институтами развития открывают новые возможности в области технологических прорывов в ближайшее десятилетие для обеспечения обороноспособности и промышленного развития государства на новом технологическом уровне, в том числе и в области кибербезопасности.

Литература:

1. Исследовательская программа DARPA на 2015 год. И.Д. Клабуков, М.Д. Алехин, А.А.Нехина, Москва, 2014.
2. И.Д. Клабуков, М.Д. Алехин, С.В. Мусиенко «Сумма технологий национальной безопасности и развития», Москва, 2014.
3. Сайт агенства по перспективным оборонным научно-исследовательским разработкам, Defense Advanced Research Projects Agency, DARPA (http://www.darpa.mil/)
4. Бюджет и программа перспективных исследований DARPA на 2014/2015 (http://www.darpa.mil/NewsEvents/Budget.aspx.)
5. Facebook - http://www.facebook.com/DARPA
6. Twitter - http://twitter.com/darpa_news
7. YouTube (видеоролики о достижениях DARPA) - http://www.youtube.com/DARPAtv
8. М.А. Мамаев, С.А. Петренко. Технологии защиты информации в Интернете. — СПб.:Питер, 2002. — 848 с.
9. А.А. Петренко, С.А. Петренко. Аудит безопасности Intranet. — М.: ДМК Пресс, 2002.— 416 с.
10. С.А. Петренко, С. В. Симонов. Управление информационными рисками. — М.: ДМК Пресс, 2004. — 420 с.
11. С.А. Петренко, В.А. Курбатов. Политики информационной безопасности. — М.: ДМК Пресс, 2005. — 400с.
12. С.А. Петренко, А.В. Беляев. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться. — М.: ДМК Пресс, 2011 . — 400с.

References

1. Evrosoiuz i SSHA provodiat sovmestny`e kiberucheniia [E`lektronny`i` resurs]. – Rezhimdostupa: http://www.itsec.ru/newstext.php?news_id=81407 (07.11.2011).

2. Obshchee prostranstvo vnutrennei` bezopasnosti v ES: politicheskie aspekty`. / Otv.red. – S. V. Utkin. – M.: IME`MO RAN, 2011. – 146 s.
3. Smirnov A. A. Obespechenie informatcionnoi` bezopasnosti v usloviiakh virtualizatcii obshchestva: opy`t Evropei`skogo Soiuza. Monografiia. – M.: IUNITI-DANA, 2011. – 196 s.
4. Fred Shrai`er, Barbara Viks, Theodore Ch. Vincler. Kiberbezopasnost`: doroga, kotoruiu predstoit nai`ti. – Zheneva: Zhenevskii` centr demokraticheskogo kontrolia nad vooruzhenny`mi silami, 2013. – 196 s.
5. Federal`ny`i` zakon RF ot 21.12.94 № 68-FZ «O zashchite naseleniia i territorii` ot chrezvy`chai`ny`kh situatcii` prirodnogo i tekhnogennogo haraktera».
6. Postanovlenie Pravitel`stva RF ot 30.12.03 № 794 «O edinoi` gosudarstvennoi` sisteme preduprezhdeniia i likvidatcii chrezvy`chai`ny`kh situatcii`».
7. Postanovlenie Pravitel`stva RF ot 04.09.03 № 547 «O podgotovke naseleniia v oblasti zashchity` ot chrezvy`chai`ny`kh situatcii` prirodnogo i tekhnogennogo haraktera».8. European Data Protection Supervisor [Электронный ресурс]. – Режим доступа:http://www.edps.europa.eu/EDPSWEB/edps/cache/off/pid/1.
9. Network and Information Security: Proposal for A European Policy Approach. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Brussels, 6.6.2001 [Электронный ресурс]. – Режим доступа: http://eurlex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf.
10. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March2004 establishing the European Network and Information Security Agency.
11. A strategy for a Secure Information Society – Dialogue, partnership and empowerment. Communication from the Commission to the Council, the European Parliament, the European economic and social Committee and the Committee of the Regions. Brussels, 2006 [Электронный ресурс]. – Режим доступа: http://ec.europa.eu/information_society/doc/com2006251.pdf.
12. Communication from the Commission to the European Parliament and the Council «The EU Internal Security Strategy in Action: Five steps towards a more secure Europe». Brussels, 22.11.2010. COM(2010).