А.М. Белевцев, доктор технических наук
В.А. Балыбердин, доктор технических наук, профессор
А.А. Белевцев
Е.Б. Маркелов, кандидат технических наук

Некоторые тенденции развития информационных технологий для систем сетецентрического управления

В статье рассмотрены тенденции развития информационных технологий в свете реализации концепции сетецентрического управления (СЦУ) как логической основы перспективных систем и комплексов автоматизированного управления военного назначения. За основу приняты исследования и разработки, осуществляемые в США как государстве, занимающем ведущие позиции в исследованиях по данной тематике. Рассмотрены работы, осуществляемые федеральными исследовательскими центрами, а также национальными лабораториями и лучшими IT(ИТ)-компаниями. Выделены наиболее важные направления исследований, отмечено акцентированное внимание федеральных исследовательских центров на тематику, связанную с формированием «ударной компоненты» информационных технологий, включая вопросы создания кибероружия и программных средств боевого применения с высокими качественными характеристиками.

В последние годы в известной литературе большое внимание уделяется вопросам развития идеологии «сетецентрической войны». Практическая реализация этой идеологии основана на интеграции всех сил и средств в рамках единого информационного пространства, что позволяет многократно увеличить эффективность их боевого применения за счет информационного превосходства над противником[1]. Основные пути достижения информационного превосходства изложены в концепции «Ведение боевых действий в едином информационном пространстве» (NCW – Network-Centric Warfare). Эта концепция более известна под наименованием «сетецентрических войн». Применяют также термин «сетецентрическое управление» [1].

Концепция СЦУ определяет архитектуру системы проведения операций в виде взаимоувязанных в единую сеть трех видов сетевых структур: разведки и наблюдения, информационно-управляющей, средств поражения [2-4]. При этом ведущую роль играет информационно-управляющая структура, обеспечивающая взаимосвязанное функционирование элементов всего войскового организма в едином информационном пространстве (ЕИП).

По замыслу зарубежных военных специалистов, объединение средств разведки и поражения посредством ЕИП обеспечит [2-4]:

- значительное сокращение цикла управления «обнаружение – оценка – принятие решения – удар» при одновременном повышении качества принимаемого решения;
- повышение эффективности использования высокоточного оружия;
- интегрированное оперативное управление на ТВД силами и средствами, принадлежащими к разным видам и родам войск.

1 Буренок В.М. Базис сетецентрических войн – опережение, интеллект, инновации // Независимое военное обозрение, 02.04.2010 // http://nvo.ng.ru/concepts/2010-04-02/1_bazis.html

Это позволяет применять развертываемые на ТВД вооруженные формирования в качестве единой пространственно-распределенной разведывательно-ударной системы, использующей тактику ведения боевых действий без образования непрерывной линии боевого соприкосновения.

Работы по созданию единого информационного пространства проводятся достаточно интенсивно в ведущих странах мира, хотя единый системный взгляд на сетецетрическое развитие системы вооружения окончательно не сформирован. Важным шагом в эволюционном развитии концепции СЦУ стала практическая реализация стратегии гибридных войн и использование мягкой силы в обеспечении глобального геополитического превосходства США. Вместе с тем практическая реализация рассматриваемой концепции замыкается на широкое использование перспективных информационных технологий, обеспечивающих функционирование систем СЦУ[1].

На решение главной задачи разработки новых информационных технологий для систем СЦУ – достижение информационного превосходства над противником – направлены усилия федеральных научно-исследовательских центров (DARPA, IARPA, DISA), федеральных венчурных фондов, ведущих университетов и национальных исследовательских лабораторий США, Европы, а также многочисленных IT-компаний по всему миру. Интерес представляет проведение анализа тенденций развития информационных технологий, обеспечивающих различные аспекты практической реализации систем сетецентрического управления. В качестве характерного примера целесообразно рассмотреть ситуацию на примере исследований, осуществляемых в США.

Отметим, что одним из наиболее активных организаторов исследований и разработок в области информационных технологий для СЦУ в США является DARPA – агентство передовых оборонных исследовательских проектов. Анализ имеющихся материалов позволил определить некоторые наиболее важные направления исследований DARPA в плане развития информационных технологий в интересах систем СЦУ[2]. На рисунках 1 и 2 приведены диаграммы, характеризующие соответствующие направления работ DARPA. При этом диаграмма на рисунке 1 характеризует активность исследований по числу реализуемых программ, а на рисунке 2 – по финансовому обеспечению.

Даже беглый взгляд на представленные обобщенные материалы позволяет отметить определенное смещение акцентов на тематику, связанную с решением вопросов «мягкого» воздействия на противника, а также противодействия соответствующим воздействиям со стороны противника.

Анализ количественных аспектов приведенных диаграмм свидетельствует о том большом внимании, которое уделяется в США вопросам развития новых информационных технологий для повышения боевых возможностей вооруженных формирований. Анализируя данные, представленные на рисунках 1 и 2, необходимо учитывать следующие соображения.

В позиции, связанной с работами в области искусственного интеллекта (ИИ), отражены лишь те исследования, которые связаны в основном с методологией и методами реализации систем ИИ. В более широком плане тематика ИИ присутствует и в других позициях, таких как кибероружие и кибербезопасность, анализ больших объемов неструктурированных данных, технологии

1 [1]; [2]; Российская компания победила Google в распознавании лиц // http://lenta.ru/news/2015/12/07/megaface/.

2 [1]; Отчет DARPA за 2015 год // https://mipt.ru/education/chairs/theor_cybernetics/government/upload/3af/Program_darpa2015_rus.pdf; The US government is not spending enough on cybersecurity // http://www.businessinsider.com/us-government-cybersecurity-spending-2015-9;Клабуков И.Д., Алехин М.Д., Мусиенко С.В. Сумма технологий национальной безопасности и развития // https://mipt.ru/education/chairs/theor_cybernetics/government/upload/512/summa_technologies-arphxczeanv.pdf; «Ростех», ФРИИ и «Ай-теко» вложат миллиард в кибербезопасность // http://www.vedomosti.ru/technology/articles/2015/10/16/613179-rostekh-frii-ai-teko-vlozhat-kiberbezopasnost

системного анализа и прогнозирования, технологии РЭБ и др. Значительный интерес в плане рассматриваемой тематики представляют исследования, проводимые Агентством передовых исследований в сфере разведки (Intelligence Advanced Research Projects Activity, IARPA)[1].

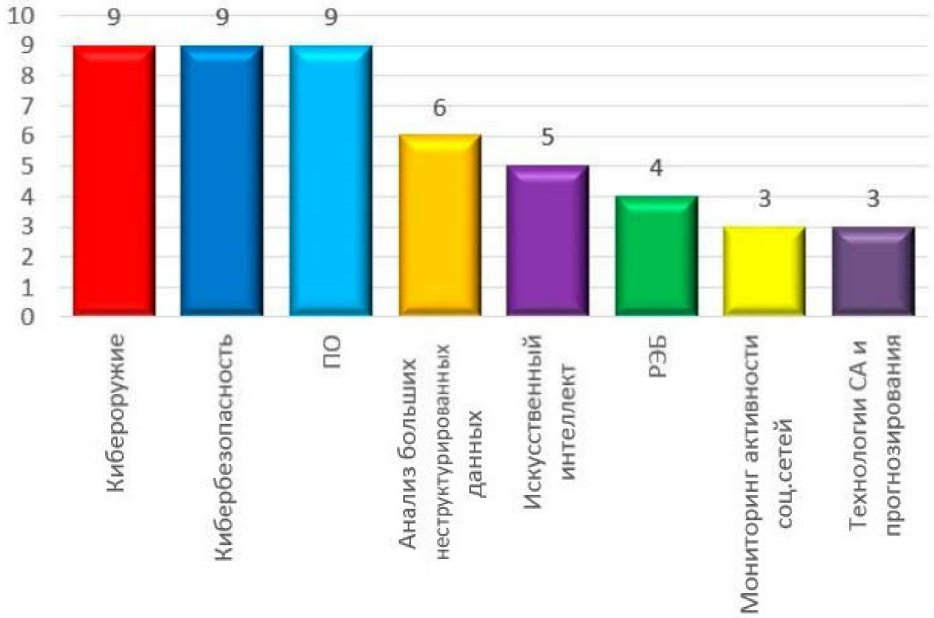

Рисунок 1 – Объединенная диаграмма активности исследований DARPA

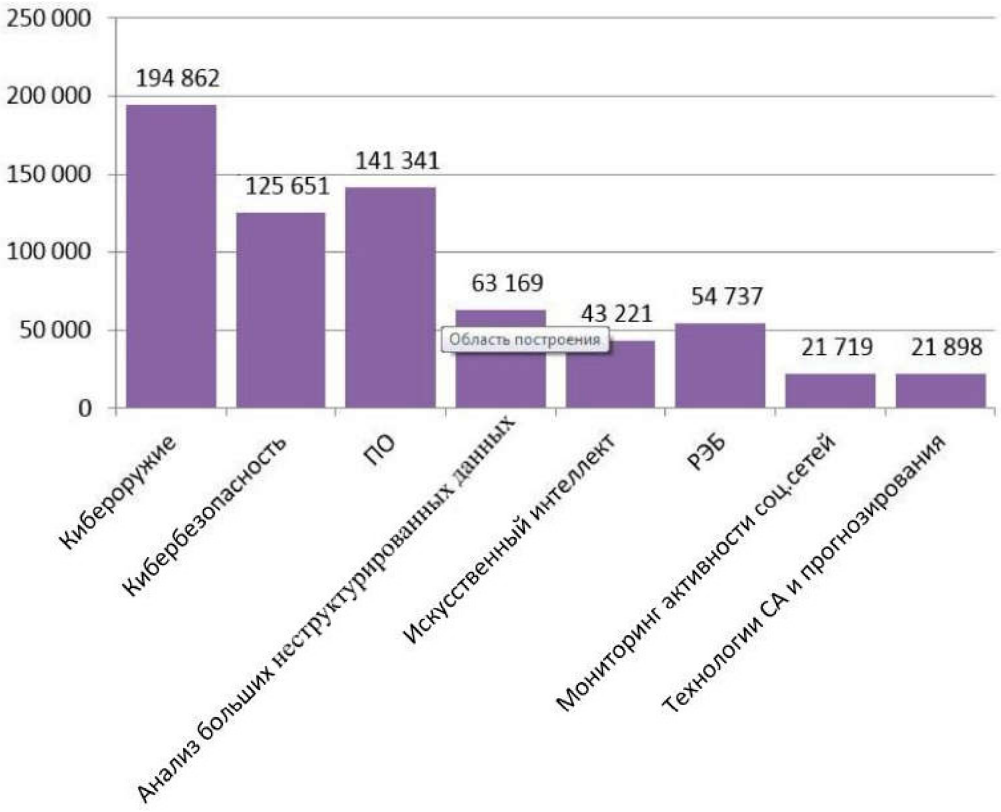

Рисунок 2 – Диаграмма суммарных затрат (у. е.)

1 Клабуков И.Д., Алехин М.Д., Мусиенко С.В. Указ. соч.; Берд К. «Кивино гнездо: Серьезные игры». – М.: «Компьютерра»,2015; «Ростех», ФРИИ и «Ай-теко» вложат миллиард в кибербезопасность // http://www.vedomosti.ru/technology/articles/2015/10/16/613179-rosteh-frii-ai-teko-vlozhat-kiberbezopasnost

Деятельность IARPA и ее бюджет засекречены, публикуется информация лишь о части проектов. В процессе анализа имеющихся материалов была получена структура научной деятельности агентства, из которой видно, что главное место IARPA отводит исследованиям, посвященным созданию искусственного интеллекта, технологиям стратегического анализа и прогноза, а также технологиям анализа больших неструктурированных данных, – критически важным технологическим направлениям для развития и автоматизации разведывательной деятельности (рисунок 3).

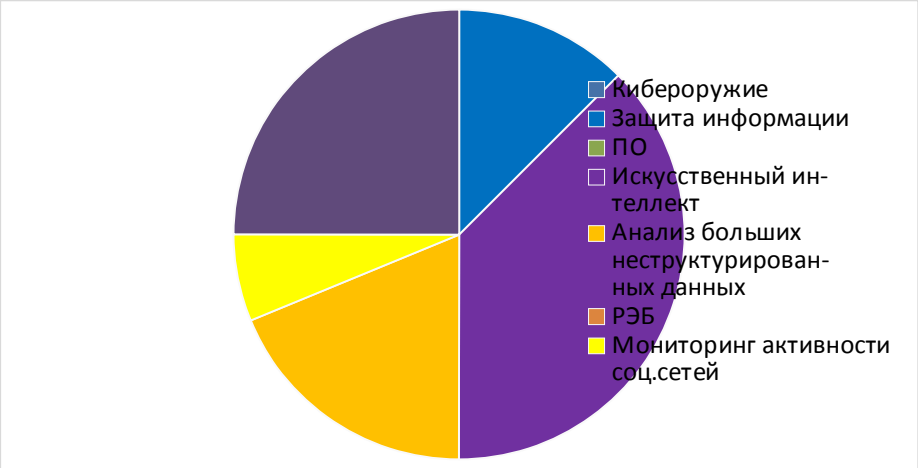

Рисунок 3 – Структура научной деятельности IARPA

Помимо DARPA и IARPA рассматриваемой тематикой исследований и разработок занимаются и другие федеральные исследовательские центры, такие как DISA (Defence Information System Agency) и венчурный фонд In-Q-Tel, созданный в 1999 году, сеть исследовательских лабораторий, созданных при поддержке курирующих министерств, а также целый ряд IT-компаний. Таблицы 1-3 дают общее представление о сфере научных интересов этих организаций.

Таблица 1 – Основные направления исследований федеральных исследовательских агентств США в области информационных технологий систем СЦУ

№ п/п	Направления исследований	DARPA	IARPA	DISA	In-Q-tel
1	Кибероружие	■			
2	Кибербезопасность	■	■	■	■
3	Методы разработки, программирования, тестирования и диагностики ПО	■		■	■
4	Анализ сложных неструктурированных данных	■	■		■
5	Радиоэлектронная борьба	■			
6	Мониторинг активности социальных сетей	■	■		
7	Прогноз и стратегический анализ	■	■		
8	Искусственный интеллект	■	■		■
9	Суперсистемы	■			

На основании проведенного мониторинга результатов исследований федеральных исследовательских центров, национальных лабораторий, крупных промышленных компаний была получена сводная диаграмма, отражающая суммарное количество организаций, занимающихся каждым технологическим направлением (рисунок 4).

Таблица 2 – Направления исследований национальных лабораторий США в области информационных технологий систем СЦУ

Направления исследований	Sandia National Laboratories	Los Alamos National Laboratory	The Ames Laboratory	Fermi National Accelerator Laboratory	Idaho National Laboratory	Pacific Northwest National Laboratory
Защита данных						
Большие данные						
Методы ПО						
Методы ИИ						
Технологии моделирования						

Таблица 3 – Сравнительный анализ направлений деятельности лучших IT-компаний в области кибербезопасности

№ п/п	IT-компании	Технологии сетевой защиты	Технологии защиты конечных устройств	Технологии защиты беспроводных сетей	Анализ и предотвращение угроз	Технологии обучения кибербезопасности	Идентификация	Биометрия
1	FireEye							
2	Lancope							
3	AlienVault							
4	Norse							
5	Easy Solutions							
6	IBM Corporatio							
7	Veracode							
8	Clearwater Compliance							
9	Palo Alto Networks							
10	SecuEra Technologies							
11	Trend Micro							
12	Nexusguard							
13	NuData Security							
14	Code Dx							
15	Sera-Brynn							
16	DFLabs							
17	BT							
18	Cavirin							
19	IT Security, Inc.							
20	Herjavec Group							

В целом по результатам проведенного анализа можно сделать следующие основные выводы:

1. Наиболее важными направлениями исследований в плане развития информационных технологий в интересах систем СЦУ являются работы в части создания кибероружия и обеспечения кибербезопасности, разработки высокоэффективных и надежных программных средств, систем и средств искусственного интеллекта, методов и средств анализа больших объемов неструктурированных данных, осуществления стратегического анализа и прогноза развития сложных ситуаций, мониторинга подозрительной активности в соцсетях, создания и совершенствования методов и средств радиоэлектронной борьбы, развития технологии построения суперсистем.

2. В США вопросы развития информационных технологий для обеспечения разработок в области систем сетецентрического управления находятся в центре внимания федеральных иссле-

довательских центров, национальных лабораторий, крупных промышленных компаний и проводятся широким фронтом.

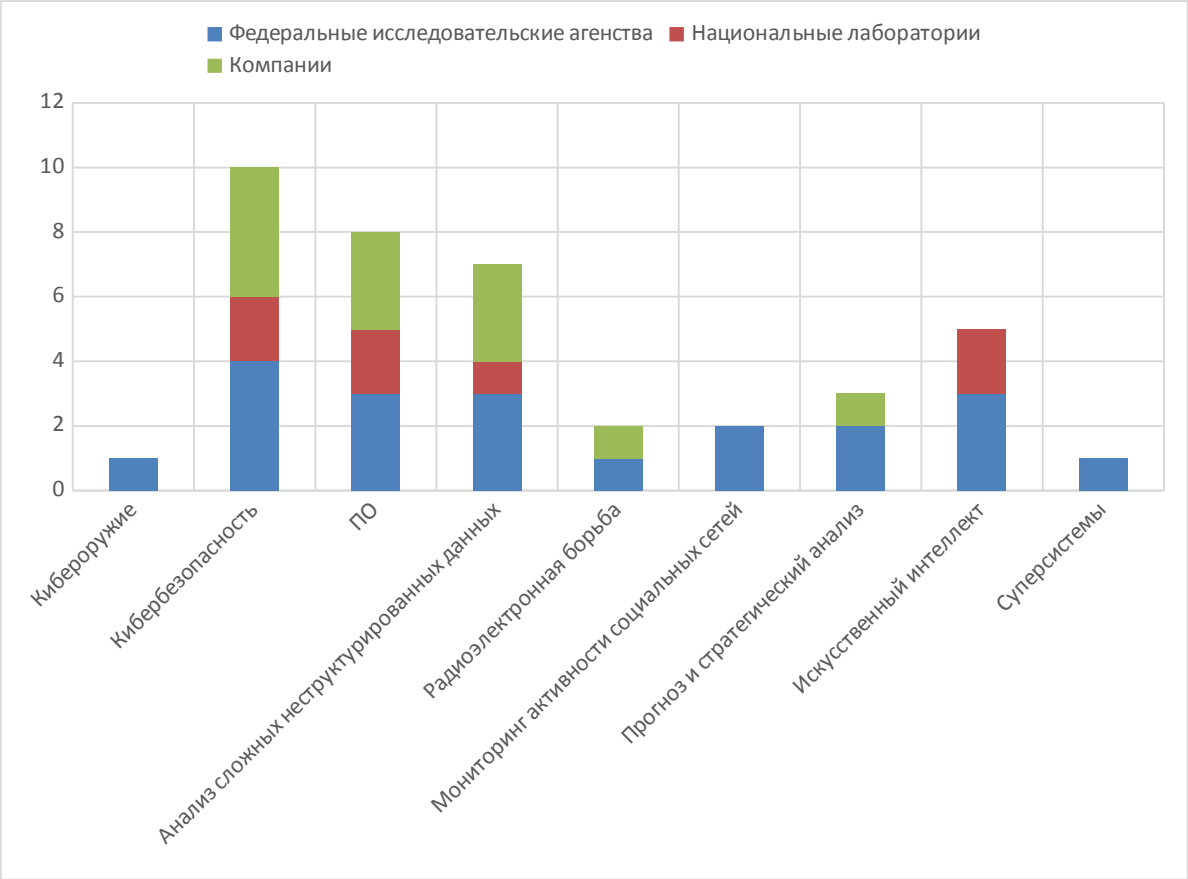

Рисунок 4 – Сводная диаграмма активности исследований федеральных исследовательских центров, национальных лабораторий, крупных промышленных компаний

3. Существует определенное акцентирование внимания федеральных исследовательских центров на тематику, связанную с формированием «ударной компоненты» информационных технологий, включая вопросы создания кибероружия и программных средств боевого применения с высокими качественными характеристиками.

4. Наличие широкого спектра организаций, участвующих в исследованиях и разработках по развитию информационных технологий для систем сетецентрического управления, обеспечивает практические гарантии возможности выбора и прикладного использования в соответствии с назначением наиболее качественных разработок по рассматриваемой тематике.

Список использованных источников

1. Хамзатов М.М. Влияние концепции сетецентрической войны на характер современных операций // Военная мысль. – 2006. – № 7. – С. 13-17.

2. Кондратьев А.Е. Проблемные вопросы исследования новых сетецентрических концепций вооруженных сил ведущих зарубежных стран // Военная мысль. – 2009. – № 11. – С. 61-74.

3. Долгополов А.В., Богданов С.А. Эволюция форм и способов ведения вооружтнной борьбы в сетецентрических условиях // Военная мысль. – 2011. – № 2. – С. 49-58.

4. Белевцев А.М., Балыбердин В.А., Бендерский Г.П., Белевцев А.А. Анализ направлений развития нано- и IT-технологий для построения специализированных сетевых коммуникационных систем нового поколения // Известия ЮФУ. Технические науки. – 2015. – № 3. – С. 35-45.