

З.У. Меджидов

---

## КИБЕРБЕЗОПАСНОСТЬ В ЕДИНОМ АЛГОРИТМИЧЕСКОМ ПРОСТРАНСТВЕ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ И В УСЛОВИЯХ ГЛОБАЛЬНОЙ КОМПЬЮТЕРНОЙ СРЕДЫ

---

**Аннотация.** Цель статьи – исследовать кибербезопасность в едином алгоритмическом пространстве распределенных вычислений с учетом особенностей развития глобальной компьютерной среды. Для достижения цели исследования использованы методы обобщения, анализа, синтеза. Выделяются фундаментальные проблемы интеграции разнородных ресурсов глобальной компьютерной среды. Показаны причины разнородности и пути устранения ее негативных последствий. В применении к распределенным социотехническим системам определены основные понятия сетевидного управления. Излагаются принципы формирования в глобальной компьютерной среде математически однородного алгоритмического пространства распределенных вычислений и сетевидного управления. Обсуждаются системообразующие возможности нового пространства: бесшовная программируемость, кибербезопасность и надежность распределенных вычислений. Обосновывается необходимость построения новой элементной базы в виде массовых однокристальных сетевых компьютеров с немикропроцессорной архитектурой. После устранения фундаментальных причин разнородности открываются возможности формирования в глобальной компьютерной среде математически однородного, бесшовно программируемого и кибербезопасного алгоритмического пространства распределенных вычислений для целостного решения сильно связанных задач сетевидного управления сколь угодно большими социотехническими системами.

**Ключевые слова:** глобальная компьютерная среда, кибербезопасность, разнородность, глобальная информационная сильносвязанность, модель распределенных вычислений, сетевидное управление, математически однородное алгоритмическое пространство, бесшовное программирование, надежность распределенных вычислений.

Z.U. Medzhidov

---

## CYBERSECURITY IN A SINGLE ALGORITHMIC SPACE OF DISTRIBUTED COMPUTING AND IN A GLOBAL COMPUTER ENVIRONMENT

---

**Abstract.** The purpose of the article is to study cybersecurity in a single algorithmic space of distributed computing, taking into account the developmental features of the global computer environment. To achieve the goal of the study, the methods of generalization, analysis, and synthesis were used in the work. Fundamental problems of integration of heterogeneous global computer environment resources are singled out. The causes of heterogeneity and ways to eliminate its negative consequences are shown. As applied to distributed socio-technical systems, the basic concepts of network-centric control are defined. The principles of formation in the global computer environment of a mathematically homogeneous algorithmic space of distributed computing and network-centric control are outlined. The system-forming possibilities of the new space are discussed: seamless programmability, cybersecurity and reliability of distributed computing. The necessity of building a new element base in the form of mass single-chip network computers with a non-microprocessor architecture is substantiated. It is shown that, by eliminating the fundamental causes of heterogeneity, they open up the possibility of forming in the global computer environment a mathematically homogeneous, seamlessly programmable and cyber-safe algorithmic space of distributed computing for a holistic solution of strongly connected network-centric control problems by arbitrarily large sociotechnical systems.

**Keywords:** global computing environment, cybersecurity, heterogeneity, global informational tightness, distributed computing model, network-centric control, mathematically homogeneous algorithmic space, seamless programming, reliability of distributed computing.

**Меджидов Заур Уруджалиевич**

кандидат экономических наук, доцент кафедры информационных технологий и информационной безопасности; доцент кафедры информационных технологий и безопасности компьютерных систем, Дагестанский государственный университет, город Махачкала. Сфера научных интересов: информационная безопасность, защита информации, кибербезопасность, киберугрозы. Автор более 50 опубликованных научных работ.

Электронный адрес: zaур-medzhidov@mail.ru

*Введение*

Глобальная компьютерная среда (далее – ГКС) привнесла беспрецедентный феномен глобальной информационной сильносвязности, который меняет условия устойчивого развития социумов и мировой социосистемы в целом. Этот новейший и потому малоизученный наукой феномен сформировался в ходе стихийного роста и развития ГКС. Она стала принципиально новым киберобъектом, оказывающим тотальное воздействие на социальные и техногенные системы.

Сложившиеся ранее (в отсутствие глобальной сильносвязности) принципы, методы и механизмы управления функционированием и развитием социотехнических систем [1] утрачивают действенность, так как не были предназначены для переработки в реальном времени экспоненциально растущих потоков и объемов глобально распределенной информации. В этом кроются причины снижения качества управления на разных уровнях, нарастания кризисных явлений, дестабилизирующих мировую социосистему. В условиях глобальной сильносвязности распределенных социотехнических систем необходимы новые принципы и модели их функционирования и развития, а также массово доступный инструментарий сетецентрического управления (далее – СЦУ) для их реализации в ГКС.

Дальнейшее развитие ГКС во многом связывается с развитием важных технологий цифровой экономики (далее – ЦЭ) – Internet of Things и Internet of Everything, а также с зарождением и развитием ЦЭ в целом, в которой управление всё большей части бизнес-процессов возлагается на компьютерно-сетевые технологии ГКС.

Посредством автоматического сбора и переработки глобально распределенной информации в ГКС, поступающей в реальном времени, достигается эффективное, в заметной части автоматическое, управление бизнес-процессами. Доля ЦЭ в 2016 году в Великобритании составляет 12,4 % от ВВП, в Китае – 6,9 %, в США – около 5,4 %, в России – 2,8 %, и этот сектор растет каждый год [2].

Однако следует отметить, что из-за разнородности ГКС ее совокупный системообразующий и алгоритмический потенциал в настоящее время раскрывается лишь в малой степени. Для полномасштабного решения задач с вовлечением всей совокупности ресурсов ГКС необходимо формирование универсального, свободно масштабируемого, бесшовно программируемого и кибербезопасного алгоритмического пространства распределенных вычислений и СЦУ. Формирование такого пространства в ГКС позволит снять ограничения на количество вовлекаемых в распределенные вычисления и процессы управления компьютеров, а также предельно снизить затраты на функциональную интеграцию вычислительных и информационных ресурсов ГКС.

*Глобальная компьютерная среда и феномен глобальной информационной сильносвязности*

ГКС – это миллиарды компьютерных устройств разных классов связанных сетями, от встраиваемых систем, интеллектуальных датчиков, смартфонов и ПК до суперкомпьютеров. Она стала качественно новым киберобъектом искусственного происхождения, воплотившим феномен глобальной информационной сильносвязности («всё влияет на всё и сразу»). Посредством ГКС мир разрозненных вещей и слабо связанных субъектов спонтанным и слабо предсказуемым образом трансформируется в сильносвязную киберсистему.

Современные компьютерно-сетевые технологии, такие как Grid- и Cloud-системы, используются, главным образом, для решения отдельных классов узкопрофилированных комплексов задач. Из-за комбинаторной сложности интеграции разнородных ресурсов ГКС они имеют принципиальные ограничения на количество компьютеров, которые осуществляют распределенную обработку (как правило, примерно  $10^4$ ) и позволяют лишь фрагментарно осваивать низовые этажи массовых применений методов и средств СЦУ. Пользователи либо не имеют, либо ограничены в возможностях программировать собственные алгоритмы решения задач. Их применение приводит к неконтролируемому росту числа разнородных сетевых систем решения узкопрофильных задач СЦУ. В условиях глобальной сильносвязности это ведет к предельному обострению проблем интеграции.

Переход от стихийного роста ГКС к ее упорядоченному развитию в целях дальнейшего развития систем СЦУ требует новых архитектурных принципов, общих методов и инструментария для исследования закономерностей ее развития, а также для практических разработок в целях качественного совершенствования ее функциональных и системообразующих возможностей.

Основные проблемы фундаментального характера на путях дальнейшего развития ГКС и систем СЦУ состоят в следующем:

- разнородность на уровнях аппаратных, системных, программных средств и информационных ресурсов;
- невозможность бесшовного программирования распределенных вычислений в сколь угодно больших разнородных сетях;
- неконтролируемая сложность создания и интеграции разнородных систем ведёт к росту неучтённых ошибок и нестыковок, снижению надёжности систем и их устойчивости к киберугрозам.

*Принципы формирования алгоритмического пространства сетецентрического управления*

Сферы применения СЦУ – большие распределенные системы из разнопрофильных подсистем стационарных и/или мобильных объектов со встроенными компьютерными средствами, взаимодействующими между собой в сетевом сильносвязном информационном пространстве. СЦУ обеспечивает циклическое повторение следующих действий [3; 4]:

- многоканальный сбор и накопление в сетевой памяти разноплановой информации, поступающей с различных компонентов системы, которые в различных аспектах фрагментарно отражают состояние внешней среды, а также значения внутреннего состояния распределенных компонентов;
- компьютерная переработка накапливаемой в распределенной памяти информации (формирование из информационных фрагментов полной, согласованной в пространстве и времени картины, которая определяет текущее состояние системы и служит основой выработки управляющих воздействий);

Кибербезопасность в едином алгоритмическом пространстве распределенных вычислений ...

- выработка согласованной управляющей информации для всех компонентов систем на основе полной динамической картины (таким образом, чтобы каждый из них выполнял свой набор функций, чем достигается эффективность их совместного использования в достижении целей управления).

Использование распределенной памяти для формирования единой динамической картины происходящих событий является отличительным признаком СЦУ. Полнота собираемой в реальное время информации и выработка согласованного управления обеспечивают кардинальное повышение качества управления в распределенных социотехнических системах. Стратегическая цель развития таких систем в ресурсах ГКС – достижение преимуществ за счет полномасштабной (без ограничений на размеры) функционально-сетевой интеграции всех компонентов систем с использованием растущего разнообразия сенсоров и факторов, видов и способов их многоканального взаимодействия между собой и внешним миром.

Совокупная глобально распределенная информация, которая накапливается в ГКС, при определенных условиях способна во всё большей мере отражать текущее состояние социотехнических систем. Это требует сетецентрической глобализации парадигмы управления [3; 4] посредством формирования в ГКС универсального алгоритмического пространства распределенных вычислений с преобладанием децентрализованных универсально и бесшовно программируемых вычислительных систем, относящихся к одноранговым сетевым архитектурам Peer-to-Peer (P2P).

Архитектуры P2P в сравнении с архитектурами «клиент – сервер» обладают максимальным потенциалом пропускной способности в сетях (в отношении передаче, распределённого хранения и обработке информации). Они позволяют практически неограниченно повышать надежность хранения, передачи и обработки глобально распределенной информации, обеспечивать устойчивость к деструктивным воздействиям, максимально раскрывать функциональный потенциал ГКС. Однако для таких архитектур, допускающих высокую гибкость распределения функций по универсальным вычислительным узлам, пока нет моделей вполне распределенных, универсально и бесшовно программируемых вычислений, что ограничивает сферы их применения узкопрофильными системами.

В основу предлагаемого алгоритмического пространства СЦУ положена модель универсально и бесшовно программируемых распределённых вычислений в сколь угодно больших одноранговых сетях. Она построена путем математического обобщения классической модели Дж. фон Неймана, которая осуществлена на основе компьютерного исчисления древовидных структур (далее – ИДС) [3; 4]. Универсальный объект исчисления в этом базисе – двоичные деревья, которые являются математически однородным структурным объектом универсального представления данных и программ. Для реализации алгоритмического пространства распределённых вычислений в ГКС на основе модели ИДС необходимо формирование сквозного адресного пространства, охватывающего, прежде всего, оперативную память вовлекаемых в это пространство компьютеров. При этом данные и программы в виде древовидных структур могут своими частями распределяться по памяти различных компьютеров этого пространства. Важно отметить, что при этом логика работы с деревьями в процессе составления и исполнения программ остается инвариантной относительно способов размещения компонентов деревьев в распределенной памяти.

В предложенной модели в универсальном алгоритмическом пространстве сетевые архитектуры P2P становятся универсально и бесшовно программируемыми. При этом

открываются возможности ситуативной аккумуляции совокупного функционального потенциала и вычислительных мощностей ГКС для целостного решения задач СЦУ. Новое пространство должно обеспечить согласованную работу ресурсов, связанных глобальными сетями, – от датчиков и смартфонов до суперкомпьютеров. Это путь к полному раскрытию функционально вычислительного и системообразующего потенциала ГКС.

Бесшовная программируемость алгоритмического пространства открывает возможности обеспечения требуемой надежности исполнения распределенных вычислительных процессов путем автоматического внесения информационной, коммуникационной и вычислительной избыточности в программы на этапах их трансляции [5].

Надежность распределенных вычислений в ненадежных (недетерминированных) вычислительных средах обеспечивается посредством исполнения в идентичных копиях программ процедуры мажорирования. Она встраивается в коды исполняемых программ на этапе трансляции. В ходе параллельного исполнения всех копий ее процессов на различных компьютерах во всех одноименных контрольных точках осуществляется обмен промежуточными данными между всеми копиями с последующим их сравнением и мажорированием. Совпадение большинства промежуточных данных указывает на то, что компьютеры, в которых они получены, находятся в работоспособном состоянии. Отсутствие сведений в определенном промежутке времени ожидания или несовпадение с результатом большинства говорит о неработоспособности соответствующих компьютеров. Далее они заменяются на другие компьютеры сети из пула дееспособных (с передачей копии текущего состояния правильного процесса) [5].

Системный интеллект немикропроцессорной архитектуры, встроенный в «умную» память, аппаратно реализует:

- универсальный компьютерный базис ИДС [4], который открывает возможности формирования универсального, бесшовно программируемого и кибербезопасного алгоритмического пространства распределенных вычислений и СЦУ, нейтрализующего разнородность ГКС и устраняющего комбинаторную сложность интеграции ресурсов (системная сложность компьютерной среды перестает зависеть от её размера);
- полную защиту от несанкционированного доступа к физическому адресу пространству оперативной памяти каждой исполняемой программы со стороны других исполняемых программ (кибербезопасность);
- основные функции ядра операционных систем, среди которых: динамическое распределение памяти, управление вводом/выводом и многозадачным исполнением программ, виртуализация памяти (отпадает необходимость впрограммной реализации ключевых системных функций);
- сетевые взаимодействия по осуществлению распределенной обработки в сколь угодно больших сетях, в том числе маршрутизация и защищенные протоколы, поддерживающие бесшовную программируемость, масштабируемость, надежность вычислений (при отключениях узлов, отказах сетевых компонентов и деструктивных воздействиях на них) [5], санкционирование доступа и др.

Аппаратная реализация системных функций на порядок повышает эффективность их исполнения и обеспечивает им полную защиту от воздействия со стороны любых исполняемых программ. Математическая замкнутость компьютерного базиса ИДС делает достижимым полный контроль корректности аппаратной реализации ядра системных функций. Это гарантирует от противоречий и нестыковок (неустраняемых при программ-

Кибербезопасность в едином алгоритмическом пространстве распределенных вычислений ...

но-эвристической реализации системных функций), ведущих к появлению скрытых ошибок и побочных каналов нелегального воздействия на вычисления.

#### Заключение

Воплощение принципов формирования алгоритмического пространства СЦУ в ГКС открывает новые возможности бесшовной интеграции совокупных ресурсов ГКС и создания принципиально новых технологий построения систем СЦУ. Они позволят с минимальными издержками решать разнообразные задачи управления сколь угодно большими распределенными социотехническими системами, функционирующими в условиях глобальной информационной связности. Это особенно важно для решения всего разнообразия задач ЦЭ.

Аппаратная реализация системных функций управления ресурсами ГКС, осуществляемая в новом алгоритмическом пространстве немикропроцессорной архитектурой, избавляет от необходимости создания многослойных, крайне разнородных и потому трудно контролируемых их программных реализаций. На этом пути открываются перспективы кардинального снижения разнородности совокупных ресурсов ГКС, а значит, чрезмерной системотехнической сложности и, как следствие, принципиального повышения уровней кибербезопасности ГКС.

Наследуя универсальность и простоту процедурного стиля программирования классической компьютерной аксиоматики, новая модель распределенных вычислений позволяет интегрировать в новое алгоритмическое пространство функциональные возможности и наработки существующих компьютерных и программных платформ, обеспечивая тем самым эволюционный переход в новое алгоритмическое пространство, охватывающее совокупные ресурсы ГКС.

#### Литература

1. David K., Geihs K., Leimeister J.M., Roßnagel A., Schmidt L. (eds.) (2014) Socio-technical Design of Ubiquitous Computing Systems. Springer Cham Heidelberg New York Dordrecht London (eBook). Library of Congress Control Number: 2014938066. Springer International Publishing, Switzerland, 2014, 353 p.
2. Банке Б., Бутенко В., Котов И., Рубин Г., Тушен Ш., Сычева Е. Россия онлайн? Догнать нельзя отстать // The Boston Consulting Group, Июнь 2016. URL: <http://www.bcg.ru/documents/file220967.pdf> (дата обращения: 04.03.2023).
3. Ogiela U., Ogiela L., Takizawa M. Cybersecurity of Distributed Systems and Dispersed Computing: Advanced Information Networking and Applications, Pp. 434–438. DOI: 10.1007/978-3-031-28451-9\_38
4. Ghosh S., Mishra A., Mishra B.K. (2019) Cyber-Security Techniques in Distributed Systems, SLAs and other Cyber Regulations. In Cyber Security in Parallel and Distributed Computing; Wiley: Hoboken, NJ, USA, 2019, Pp. 109–127.
5. Balabanov T., Zankinski I., Tomov P., Petrov P., Kostadinov G. (2020) Distributed computing cybersecurity in donated computing resources for evolutionary algorithms: Scientific Conf. Current Security Problems, Pp. 697–704.

#### Literature

1. David K., Geihs K., Leimeister J.M., Roßnagel A., Schmidt L. (eds.) (2014) Socio-technical Design of Ubiquitous Computing Systems. Springer Cham Heidelberg New York Dordrecht London (eBook).

Library of Congress Control Number: 2014938066. Springer International Publishing, Switzerland, 2014, 353 p.

2. Banke B., Butenko V., Kotov I., Rubin G., Tushen Sh., Sycheva E. Russia online? You can't catch up. *The Boston Consulting Group*, June 2016. URL: <http://www.bcg.ru/documents/file220967.pdf> (accessed: 04.03.2023) (in Russian).

3. Ogiela U., Ogiela L., Takizawa M. Cybersecurity of Distributed Systems and Dispersed Computing: Advanced Information Networking and Applications, Pp. 434–438. DOI: 10.1007/978-3-031-28451-9\_38

4. Ghosh S., Mishra A., Mishra B.K. (2019) Cyber-Security Techniques in Distributed Systems, SLAs and other Cyber Regulations. In *Cyber Security in Parallel and Distributed Computing*; Wiley: Hoboken, NJ, USA, 2019, Pp. 109–127.

5. Balabanov T., Zankinski I., Tomov P., Petrov P., Kostadinov G. (2020) Distributed computing cybersecurity in donated computing resources for evolutionary algorithms: Scientific Conf. *Current Security Problems*, Pp. 697–704.