ПРИНЦИПЫ ФОРМИРОВАНИЯ ЕДИНОГО АЛГОРИТМИЧЕСКОГО ПРОСТРАНСТВА РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ И ОБЕСПЕЧЕНИЯ ЕГО КИБЕРБЕЗОПАСНОСТИ

Ю.С. Затуливетер, Е.А. Фищенко

Введение

Миллиарды компьютерных устройств всех классов, связанных сетями (от встраиваемых систем, интеллектуальных датчиков, смартфонов, ПК до суперкомпьютеров), образуют глобальную компьютерную среду. Она обладает колоссальным функциональным и вычислительным потенциалом, системообразующие возможности которого не имеют исторических прецедентов. Глобально сильносвязное информационное пространство, носителем которого она является, охватывает практически все сферы жизнедеятельности. Наше нынешнее и будущее благополучие становится всё более зависимым от способности компьютеров своевременно и качественно перерабатывать лавинно растущие потоки информации, а также от возможностей индустриального производства следующих поколений компьютеров, способных взять на себя новые задачи управления устойчивым развитием глобальной социосистемы в едином, сильносвязном информационном/алгоритмическом пространстве [1].

Наряду с рассмотрением вопросов функциональной интеграции сетевых ресурсов посредством единого алгоритмического пространства в работе анализируются общесистемные причины растущей уязвимости компьютерных сред в связи со стихийным ростом размеров и системной сложности крайне разнородной компьютерной среды. В условиях разнородности комбинаторная системная сложность функциональной интеграции сетевых ресурсов становится непреодолимым барьером. В том числе и поэтому с увеличением размерности задач и размеров систем распределённой обработки информации обеспечение должных уровней кибербезопасности становится практически невозможным.

Приводятся отдельные примеры киберугроз, которые могут дестабилизировать функционирование глобального информационного пространства компьютерной среды, а через него и мировой социосистемы, включая важнейшие её части – электроэнергетику, водоснабжение и т.д. вплоть до провоцирования социальных волнений и военных конфликтов.

Обсуждаются принципы построения новой ЭБ в виде однокристальных сетевых компьютеров с немикропроцессорной архитектурой, которые позволят устранить причины непрерывного воспроизводства разнородности компьютерной среды и бесшовным образом распространить свойство универсальной программируемости с внутрикомпьютерных ресурсов на сетевые.

Новая ЭБ позволит с минимальными затратами средств и времени сформировать в ресурсах глобальных сетей свободно масштабируемое/ конфигурируемое и бесшовно программируемое алгоритмическое пространство. В этом пространстве устраняется разнородность форм представления данных и программ, поэтому сложность систем распределённой обработки информации перестаёт зависеть от количества и состава вовлекаемых компьютеров, что кардинально снижает трудоёмкость их создания и программирования. В рамках немикропроцессорной архитектуры за счёт исполнения ключевых системных функций управления вычислительными ресурсами и процессами на аппаратном уровне может быть достигнуто кардинальное снижение сложности компьютерной среды и её системного ПО. Такое решение позволит избавляться от многослойного, разнородного, потому крайне сложного и, во многих случаях, ненадёжного и неэффективного системного программного обеспечения.

1. О проблемах формирования единого алгоритмического пространства

В условиях глобально сильносвязного информационного пространств компьютерная среда становится общеиспользуемым инструментом решения практически неограниченного разнообразия задач управления функционированием и развитием мировой социосистемы и её частей [1]. В сильносвязном информационном пространстве глобально распределённая компьютерная информация (данные и программы) становится универсальным посредником в регулировании техногенных, экономических, политических и других социально значимых процессов нашей жизни.

Основным инструментом раскрытия системного и алгоритмического потенциала компьютерной среды служат системы распределённых вычислений, реализуемые в сетевых ресурсах. Такие системы решают разнообразные задачи переработки глобально распределённой информации с вовлечением большого количества связанных сетями компьютерных устройств а различных классов – от "умной пыли", смартфонов и ПК до суперкомпьютеров.

Однако, вследствие крайней разнородности аппаратных, системных и программных средств совокупный системообразующий и алгоритмический потенциал компьютерной среды в настоящее раскрывается лишь в крайне незначительной степени.

Ведущие технологии в этой сфере – Grid-системы и "Облачные" вычисления. Они позволяют интегрировать для осуществления распределённых вычислений от десятков до десятков тысяч компьютерных устройств в отдельно взятом решении. Однако это составляет ничтожную часть совокупного вычислительного потенциала компьютерной среды, что не позволяет удовлетворять опережающий спрос на расширение масштабов массового применения систем переработки экспоненциально растущих потоков и объёмов распределённой компьютерной информации, циркулирующей в ресурсах глобальных сетей. Очевидно, что эти технологии в принципе не могут охватить своим влиянием совокупные ресурсы компьютерной среды.

Одна из главных причин ограничения размеров существующих систем распределённых вычислений, является разнородность глобально распределённой компьютерной информации и способов её переработки – данных, программ, процессов и систем. Интеграция и программирование вычислительных систем в условиях крайней разнородности сетевых ресурсов является многовариантной задачей, которые, как хорошо известно, обладают комбинаторной сложностью своих решений. Уровни сложности таких систем крайне быстро растут с увеличением размеров вычислительных сред, что нашло выражение в термине "комбинаторное проклятие" размерности.

Преодоление комбинаторной сложности в ходе интеграции и программирования сетевых ресурсов с увеличением размеров требует неограниченного роста средств и времени. Отсюда следует, что в условиях разнородности компьютерной среды полномасштабное раскрытие совокупного потенциала компьютерной среды практически невозможно.

По мере увеличения масштабов интеграции разнородных сетевых ресурсов системная сложность систем распределённых вычислений растёт опережающими темпами. В отсутствие формально строгих методов и средств композиции единого целого из разнородных фрагментов внутренняя структура таких систем обретает вид "лоскутного" одеяла. В отсутствии системной гарантии полноты и непротиворечивости функций в таких системах неизбежно накапливаются неучтённые ошибки и нестыковки, которые повышают не только вероятность аварийных ситуаций. На разных уровнях – от аппаратных средств, инструментов программирования, операционных систем и сетевых протоколов, в них неизбежно возникают каналы нелегального доступа к вычислительным ресурсам.

Ввиду неконтролируемого роста системной сложности компьютерная среда становится всё менее защищённой от вредоносного вмешательства и всё более подверженной киберугрозам, которые всё сложнее идентифицировать и нейтрализовывать. Такая ситуация способствует нагнетанию агрессивных намерений и наращиванию усилий в подготовке регулярных средств ведения глобальных кибервойн [2]. Уголовно преследуемое хакерство теперь легализуется в военных структурах [3].

Накапливаемая в сетевых ресурсах компьютерная информация всё в более полно отражает текущее состояние мировой социосистемы и её частей [1]. В условиях растущей нестабильности мировой социосистемы в сильносвязном пространстве взаимодействий необходима своевременная алгоритмическая переработка этой информации в целях управления устойчивым функционированием и развитием. Доступность полномасштабной переработки информации о текущем состоянии социосистемы в едином алгоритмическом пространстве посредством совокупных ресурсов компьютерной среды открывает возможности для кардинального повышения качества управления социально значимыми процессами.

На пути к единому алгоритмическому пространству остаются такие фундаментальные проблемы, как

- устранение причин непрерывного воспроизводства разнородности компьютерной среды и форм представления компьютерной информации;
- бесшовное распространение свойства универсальной программируемости с внутренних ресурсов компьютерных устройств на совокупные сетевые ресурсы [4];
- разработка элементной базы (ЭБ) с новой архитектурой, обеспечивающей формирование в сетевых ресурсах свободно масштабируемого/конфигурируемого и бесшовно программируемого алгоритмического пространства распределённых и параллельных вычислений [5, 6];
- кардинальное решение вопросов обеспечения кибербезопасности единого алгоритмического пространства на аппаратном уровне, который не подвержен деструктивным воздействием со стороны исполняемых программ.

2. Примеры киберугроз

Для решения задач кибербезопасности предпринимаются всё более дорогостоящие, но далеко не всегда эффективные, меры. Например, связанные с созданием международных стандартов кибербезопасности [7] или с применением экономических санкций против стран с агрессивными компьютерными взломщиками, не прекращающими кибератаки даже после того как их обнаружили [8].

Апофеозом подготовки к глобальным сражениям в сетях можно считать "доктрину кибервойны", которая устанавливает, что компьютерная диверсия может считаться актом военной агрессии, к которой применимы законы военных действий: "Президент США вправе отдавать распоряжения о нанесении превентивного виртуального удара по любым объектам в интернет-пространстве, действия которых США сочтут опасными" [9].

Примерами крупных кибератак являются [10]:

- использование компьютерного вируса Stuxnet, который вывел из строя компьютеры ядерных объектов Ирана, но автора вируса не обнаружили.
- DDOS-атаки на серверы правительств Эстонии в 2007 г. (во время событий с памятником советским солдатам) и Грузии в 2008 г.

Обеспечить киберзащиту сетей промышленного масштаба, которые используются для управления критически важными отраслями, такими как транспортное сообщение, энергоснабжение и другие, целиком достаточно сложно [11]. Здесь установка традиционных антивирусов и межсетевых экранов не всегда возможна и резонна. За последнее десятилетие эти критически важные системы управления стали все чаще прибегать к использованию информационных технологий, таких как Ethernet, TCP/IP и web услуги. К сожалению, вместе с этим системы промышленного управления, включающие программируемые логические контроллеры, распределённые системы и системы SCADA все больше подвергаются атакам вирусов, хакеров и террористическим атакам по всему миру.

3. О причинах уязвимости компьютерных сред

В [11] сделана попытка анализа кибербезопасности с позиций теории управления. Кибератака считается "возмущающим воздействием" на объект, при этом "система управления объектом должна компенсировать эти возмущения, а в целом объект+ система управления должны обладать устойчивостью к этим возмущениям, т.е. быть киберустойчивыми". В этой работе вводится, на наш взгляд, важное понятие скрытых функций: "Скрытыми функциями объекта будем называть те, что не входят в перечень штатных функций, но могут выполняться в силу физических особенностей объекта и наличия возможности внесения изменений в систему управления".

Первые поколения систем управления объектами строились на основе аналоговых средств. В таких системах "скрытые функции", проявляли себя сначала на этапах проектирования и доводки изделий, затем – при выходе за границы штатных режимов эксплуатации. Границы штатных режимов новых изделий тщательно выверялись и документировались на этапах испытаний. В практике применения влияние "скрытых функций" исключалось строгими регламентами эксплуатации.

С переходом на цифровые средства объекты и алгоритмы управления ими стали усложняться. Сложность поведения объектов определяется числом его внутренних степеней свободы. Для расширения функций управляемых объектов стали широко использоваться программируемые компьютерные средства, вместе с этим пришли операционные системы (ОС). Сами программы представляют собой сложные системы, обладающие собственными степенями свободы.

С использованием компьютерных сетей стали широко применяться распределённые системы сильносвязных объектов. Функционирование сетей основывается на сетевых протоколах с многослойной программной реализацией. Сложность системных программных решений в виде ОС, сетевых протоколов и разнообразных, так называемых, промежуточных программных слоёв (middle ware) стала быстро расти. Это означает, что растёт количество их внутренних степеней свободы. В настоящее время сложность систем в значительной, а во многих случаях, и в подавляющей части определяется сложностью программных решений.

Большие программные решения наряду с легальными внутренними состояниями, связанными со штатными режимами работы управляемых объектов, обладают и многими неучтёнными ("нелегальными"), которые становятся основой для внедрения "скрытых функций" и несанкционированных манипуляций ими. Поэтому исполнение каждой штатной команды управления объектом становится зависимым от большого количества неучтённых факторов.

Неучтённые степени свободы становятся объектом кибератак. Посредством "скрытых функций" управления нелегальными степенями свободы производится вредоносное воздействие. Цель – нарушение работоспособности системы управления или несанкционированной перевод объекта в те или иные режимы работы.

В разработках больших программных систем, как правило, преобладают эвристические методы. Функциональная полнота и непротиворечивость программных решений в ходе проектирования практически недоказуема. В условиях крайней разнородности компьютерной среды (аппаратных платформ, а также форм представления данных, программ и процессов) уровни сложности системного ПО достигли таких уровней, что никакими испытаниями уже невозможно их идентифицировать в полной мере. Такие решения неизбежно содержат внутренние нестыковки.

Примером таких нестыковок является недавнее обновление для Windows [12]. Оно может приводить к синему экрану смерти на раннем этапе загрузки системы, а также вызвать проблемы у пользователей некоторых антивирусных программ.

Современные способы обеспечения защиты посредством многослойных обновлений (патчей) носят несистемный характер "латания дыр". При этом из-за чрезмерной сложности разнородных решений вносимые фрагменты изменений в отсутствие полнотой картины могут вступать в противоречия с существующим контекстом. Методы нанесения заплаток на заплатки явно не адекватны темпам катастрофического роста системной сложности компьютерной среды. Эта сложность является главным барьером на путях

полномасштабного использования практически неограниченных возможностей потенциала многих и многих миллиардов связанных сетями компьютерных устройств.

Обстоятельство неконтролируемой системной сложности больших и сверхбольших систем является основой для несанкционированного использования сетевых ресурсов. Поэтому чем масштабнее системы распределённой обработки, тем сложнее обеспечивать их кибербезопасность. Защита таких систем от несанкционированного вмешательства обретает чрезвычайную остроту.

4. Общий системный подход к преодолению сложности и обеспечению кибербезопасности

Известные технологии функциональной интеграции сетевых ресурсов и борьбы с киберугрозами достигли пределов. Для устранения причин кризиса развития компьютерной среды необходимо выявление и устранение причин непрерывного воспроизводства разнородности, а значит и комбинаторной сложности.

Кибербезопасность - это не только защита от зловредных программ, но и борьба с причинами чрезмерной системной сложности, которая приводит к утрате контроля над внутренними степенями свободы больших программных систем. Одна из главных таких причин – разнородность данных, программ, процессов и систем в сетевых ресурсах. Чем сложнее объекты и системы распределённых объектов, тем труднее обеспечивать работоспособность и контроль над ними.

Совершенно ясно, что дальнейшая борьба с системной сложностью за кибербезопасность путём лобового преодоления комбинаторной сложности разнородных программных решений посредством добавления новых, всё более дорогостоящих и менее надёжных слоёв "промежуточного ПО" в условиях глобальной сильносвязности не имеют долгосрочных перспектив. Огромное количество частных, крайне затратных решений по созданию и последующего обеспечения кибербезопасности больших и всё более разнообразных систем распределённой обработки, только наращивают многослойность и разнородность компьютерной среды в целом.

В условиях глобальной сильносвязности необходим общий системный подход к решению проблем сложности разнородной компьютерной среды. Он состоит в следующем:

- выявление и устранение первопричин непрерывного воспроизводства разнородных форм представления и способов работы с компьютерной средой;
- перенос системных функций управления вычислительными ресурсами и процессами с программного уровня на аппаратные [4-6];
- формирование в сетевых ресурсах математически однородного алгоритмического пространства распределённых и параллельных вычислений [1, 4-6, 13].

Причины незащищённости вычислительных процессов на уровне машинной среды кроются в классической модели универсальной вычислений фон Неймана. Это однозадачная модель, в которой изначально отсутствует защита памяти от прямого вмешательства одной программы со стороны другой (незащищённое адресное пространство). Многозадачность привносится специальными программами – операционными системами (ОС). Работа сетей также опирается на системные программы, обеспечивающие реализацию сетевых протоколов обмена данными. В условиях крайней разнородности ресурсов глобальных сетей комбинаторная сложность программных системных слоёв достигла критических уровней. Дальнейшее развитие компьютерной среды из-за опережающего роста сложности (а значит трудоёмкости и себестоимости) становится практически невозможным – ни в части функциональной интеграции, ни в части обеспечения безопасности.

Путь к общему системному решению начинается с обновления классической компьютерной аксиоматики в модели фон Неймана, которое на уровне классических постулатов универсального счёта, посредством перехода к новому компьютерному базису в виде исчисления древовидных структур, устраняет имеющиеся в них избыточные степени свободы, открытые на программистов [1,4].

Стратегическим направлением совершенствования глобальной компьютерной среды, которая станет носителем универсального алгоритмического пространства, является полное разнесение системных и прикладных функций. При этом системный базис и ключевые системные функции высокоэффективного и защищённого управления машинными ресурсами должны реализоваться на аппаратном уровне. Прикладные функции обработки распределённой информации реализуются на уровне инструментальных средств программирования в математически замкнутом базисе операций исчисления древовидных структур [1,4].

Для общего и кардинального решения проблем системной сложности компьютерной среды и функциональной интеграции связанных сетями компьютеров необходимо формирование в ресурсах глобальных компьютерных сетей математически однородного, универсально и бесшовно программируемого алгоритмического пространства распределённых вычислений, которое без ограничений на размеры реализуемых систем обеспечит свободно масштабируемую функциональную интеграцию сетевых ресурсов и бесшовное программирование задач высокой структурной сложности [1,4,6,13].

Для реализации математически замкнутого компьютерного базиса [4] операций нового алгоритмического пространства, в котором отпадает необходимость в многослойных, крайне разнородных и трудно контролируемых средствах программной поддержки системных функций компьютерной среды, необходим переход на новую элементную базу с немикропроцессорной архитектурой [6].

Универсальные функции системной поддержки распределённых вычислений в новом компьютерном базисе будут реализовываться на аппаратном уровне [4,6]. Математическая замкнутость компьютерного базиса позволяет, во-первых, в полной мере контролировать внутренние степени свободы его аппаратных реализаций, во-вторых, при определённых условиях и архитектурных решениях в ходе исполнения прикладных операций автоматически осуществлять все необходимые системные функции управления машинными ресурсами. При этом доступ к системному уровню со стороны прикладного полностью закрывается, что означает устранение "неучтённых" степеней свободы и "скрытых функций" манипуляции с ними.

Аппаратная реализация математически замкнутого компьютерного базиса [4] полностью защищает системные функции от попыток внесения несанкционированных изменений посредством программных средств прикладного назначения. Прикладные функции, реализуемые в этом базисе, в едином алгоритмическом пространстве распределённых вычислений в полной мере изолированы от системных функций управления машинными ресурсами компьютерной среды.

Перенос ключевых системных функций, которые сегодня реализуются в ядре ОС, на аппаратный уровень посредством математически замкнутого базиса позволяет устранить причины непрерывного воспроизводства разнородности форм представления компьютерной информации, а вместе с ними и необходимость в непомерно раздувшемся и неконтролируемом системном ПО. В этом состоит стратегия кардинального решения вопросов кибербезопасности компьютерной среды.

Устранение многослойного, крайне разнородного и сложного системного ПО (ОС, промежуточное ПО, а в перспективе и ПО сетевых протоколов) не только кардинально снизит системную сложность и повысит системную эффективность компьютерной среды, но выведет её на качественно новые уровни кибербезопасности.

5. К созданию однокристального сетевого компьютера с немикропроцессорной архитектурой

Для формирования в компьютерной среде свободно масштабируемого и конфигурируемого алгоритмического пространства с бесшовным программированием [1,4] требуется элементная база в виде однокристального сетевого компьютера (рис.1) с немикропроцессорной архитектурой [5], обеспечивающей аппаратную реализацию не только прикладного уровня программирования, но и ключевых системных функций. Аппаратная реализация системных функций в рамках математически замкнутого компьютерного базиса [1,4] не имеет "неучтённых" степеней свободы и "скрытых функций" управления машинными ресурсами, что позволяет устранить неконтролируемые системные каналы внешнего несанкционированного проникновения.

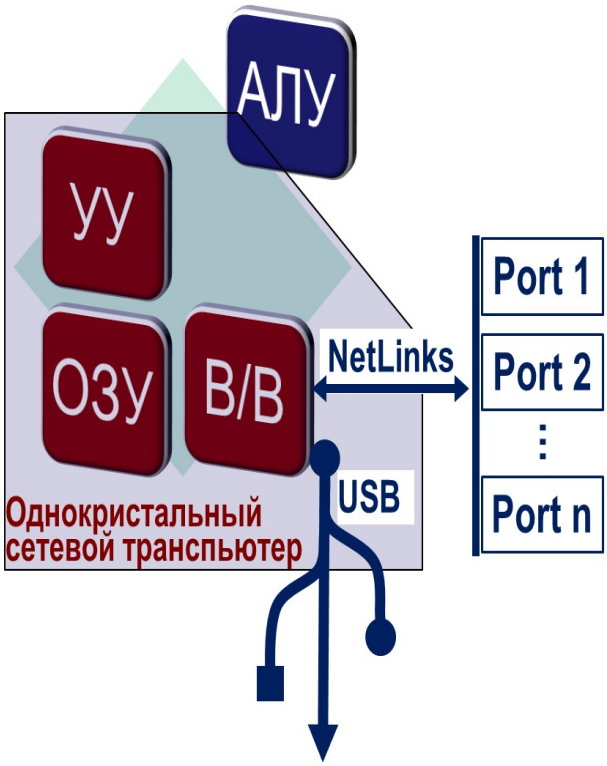

Рис.1. Универсальный сетевой компьютер с немикропроцессорной архитектурой

Немикропроцессорная архитектура принципиально отличается от классических микропроцессоров тем, что реализуя новый компьютерный базис на аппаратном уровне, устраняет причины непрерывного воспроизводства разнородных форм представления компьютерной информации (данных и программ) [1,4].

Отметим особенности её компоновки. В отличие от микропроцессоров в отдельном корпусе интегральной схемы заключены не арифметико-логическое устройство (АЛУ) и устройство управления (УУ), а оперативное запоминающее устройство (ОЗУ), УУ и устройство ввода/вывода (В/В) (рис.1). Устройство В/В реализует обмены данными с внешним миром через встроенные контроллеры, в том числе через сетевые порты (рис.1).

Функциональная особенность архитектуры однокристального сетевого компьютера - "умная" оперативная память большого объёма со встроенным на аппаратном уровне системным интеллектом, в которой реализуются:

- основные функции ядра операционных систем (управление вводом/выводом, динамическое перераспределение памяти, управление многозадачным исполнением программ, управление сетевыми обменами данных), чем достигается кардинальное снижение системной сложности функциональной интеграции сетевых вычислительных ресурсов;
- универсальный компьютерный базис бесшовного программирования распределённых структурно-сложных вычислений в сетевых ресурсах;
- встроенные средства маршрутизации и защищённые протоколы, поддерживающие свободно масштабируемые распределённые вычисления в сетевых ресурсах;
- реконфигурируемый набор устройств сопряжения с объектом, реализуемый посредством ПЛИС-технологии, который включает типовые блоки (библиотечный набор) и специфические блоки (программно конфигурируются с учётом уникальных особенностей конкретных объектов сопряжения);
- эффективная защита от несанкционированного доступа (обеспечение кибербезопасности посредством изоляции физического адресного пространства памяти от вредоносного вторжения).

Такая элементная база обеспечивает высокоэффективную реализацию функций автоматического управления машинными ресурсами на аппаратном уровне. Замена программной реализации функций ядра операционных систем на аппаратную обеспечит полную их защищённость от несанкционированного вмешательства через программные каналы влияния. Исключение системных степеней свободы управления машинными ресурсами с уровня прикладного программирования оставляет программисту только содержательные "степени свободы", связанные с придумыванием и программированием в математически замкнутом компьютерном базисе алгоритмов решения задач.

ЛИТЕРАТУРА:

1. Ю.С. Затуливетер. Проблемы глобализации парадигмы управления в математически однородном поле компьютерной информации // Проблемы управления. 2005. – № 1. – Ч. I. – С. 1-12; №2. – Ч. II. – С. 13-23. URL: http://zvt.hotbox.ru.
2. http://ru.wikipedia.org/wiki/кибервойна
3. http://rus.ruvr.ru/2013_02_05/Kiberarmii-SSHA-ne-hvataet-hakerov/
4. Ю.С. Затуливетер Компьютерный базис сетецентрического управления// Российская конференция с международным участием" Технические и программные средства в системе управления, контроля и измерения" (УКИ'10). Труды конференции. Москва, 18-20 октября 2010 г. Учреждение Российской Академии наук Институт проблем управления им. В.А. Трапезникова РАН. –С.17-37. URL: http://cmm.ipu.ru/proc/Затуливетер%20Ю.С.%20.pdf.
5. Ю.С. Затуливетер. ExaScale: на пути к единому пространству распределенных и параллельных вычислений // Научный сервис в сети Интернет: Экзафлопсное будущее: Труды Международной суперкомпьютерной конференции (20-25 сентября 2010 г., г. Новороссийск). – М.: Изд-во МГУ, 2011. С.10-14. URL: http://agora.guru.ru/abrau2011/pdf/10.pdf.
6. Ю.С. Затуливетер, Е.А. Фищенко К универсальному алгоритмическому пространству распределенных и параллельных вычислений на основе немикропроцессорных компьютерно-сетевых архитектур / Труды Международной суперкомпьютерной конференции "Научный сервис в сети Интернет: поиск новых решений" (17-22 сентября 2012 г. Новороссийск). М.: МГУ, 2012. С. 159-166. URL: http://agora.guru.ru/abrau2012/pdf/159.pdf.
7. http://global-standard.ru/novii_standart_iso_na_kiberbezopasnost/
8. http://itsec.ru/newstext.php?news_id=91853
9. http://rus.ruvr.ru/2013_02_05/SSHA-zavershajut-razrabotku-doktrini-kibervojni/
10. http://slavkina.ru/?p=1998
11. А.Г. Полетыкин, В.Г. Промыслов. Формальные определения и критерии устойчивости объектов с цифровыми системами управления к воздействиям кибератак // Шестая международная конференция "Управление развитием крупномасштабных систем" (MLSD'2012). Институт проблем управления, 2012.. URL: http://www31.ipu.rssi.ru/images/documents/plen_2012.pdf.
12. http://bugtraq.ru/rsn/archive/2013/04/06.html
13. Ю.С. Затуливетер, Е.А. Фищенко Графодинамические системы с сетецентрическим управлением в математически однородном поле компьютерной информации // Управление большими системами. 2010. Выпуск 30.1 "Сетевые модели в управлении". С. 567-604. URL: http://www.ipu.ru/sites/default/files/publications/5292/1174-5292.pdf.