

КОНЦЕПТУАЛЬНЫЕ АСПЕКТЫ ПОСТРОЕНИЯ ДОВЕРЕННЫХ НЕОДНОРОДНЫХ БЛОКЧЕЙН-СРЕД НОВОГО ТЕХНОЛОГИЧЕСКОГО УКЛАДА

¹ Андрианова Е.Г., ² Головин О.Л.

¹ Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технологический университет», 119454, Россия, Москва, Проспект Вернадского, д. 78. dtghmflysq@gmail.com

² Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский Экономический Университет им. Г.В. Плеханова», 117997, Российская Федерация, Москва, Стремянный пер., 36. mifioleg@gmail.com

Переход к новому технологическому укладу связан с возрастающим совместным применением таких технологий, как блокчейн-алгоритмы публичных и частных распределенных реестров для организации доверенной среды; сети вещей и машин (IoT/IIoT/M2M); нейросетевые методы распознавания паттернов, анализа ситуаций и принятия решений; хранение, обработка и передача больших массивов данных; виртуальные облачные платформы. Их интегрированная аппаратно-программная реализация на основе полностью специфицированных компонент позволит обеспечить необходимый уровень конкурентоспособности и безопасности российской экономики, её оптимального развития, защиту интересов отечественных производителей, имеющих собственные компетенции и применяющих новые бизнес-модели. В этих условиях необходимы особые подходы к построению неоднородных доверенных сред нового технологического уклада, а также к разработке для них требований, регламентов и стандартов.

Ключевые слова: блокчейн, доверенная среда, сеть вещей и машин IoT/IIoT/M2M, нейронная сеть, центр обработки данных, облачные технологии, ассиметричная криптография, управление рисками, гиперконвергентность, программно-определяемые сети SDN/SD-WAN, технологический уклад, непосредственное макетирование.

CONCEPTUAL ASPECTS OF BUILDING A TRUSTED HETEROGENEOUS BLOCKCHAIN-ENVIRONMENTS OF A NEW TECHNOLOGICAL STRUCTURE

¹ Andrianova E.G., ² Golovin O.L.

¹ Federal State Budget Educational Institution of Higher Education "Moscow Technological University", 119454, Russia, Moscow, Vernadsky pr., 78. dtghmflysq@gmail.com

² Federal State Budget Educational Institution of Higher Education "Plekhanov Russian University of Economics" Stremyanny lane, 36, Moscow, 117997, Russia. mifioleg@gmail.com

The transition to the new technological structure is connected with the increasing joint use such technologies as blockchain-algorithms of public and private distributed registries for the organization of a trusted environment; networks of things and machines (IoT/IIoT/M2M), neural network pattern recognition methods, case analysis and decision making, storage, processing and transmission of big data; virtual cloud platforms. Their integrated hardware-software implementation based on fully specified components, allows ensuring the necessary level of competitiveness and security of the Russian economy, its optimum development, protecting the interests of domestic producers, with their own competence and new business models. In these circumstances, specific approaches are required to build heterogeneous trusted environments of a new technological structure, as well as for the development of new requirement, rules and standards for them.

Key words: blockchain, trusted environment, network of things and machines IOT/IIOT/M2M, neural network, data center, cloud technologies, asymmetric cryptography, risk management, hyperconvergence, program-defined networks SDN/SD-WAN, technological structure, rapid prototyping.

Введение

В настоящее время происходят качественные изменения в мировой экономике, сравнимые с изменениями за последние 30-40 лет, а именно смена очередного технологического уклада, технико-экономической парадигмы и соответствующих управленческо-организационных методов. Фактически идет переход к новому 6-му технологическому укладу, что также рассматривается как 4-я промышленная (научно-техническая) революция или Индустрия 4.0.

Технологический уклад можно описать как доминирующую в экономике совокупность производств и соответствующих им институтов, связанных общим техническим уровнем и развивающихся синхронно. Неравномерность научно-технического прогресса, дискретность инновационного процесса, синхронность перехода к новым технологиям одного уровня давно известны в экономической науке и практике. При переходах к новым укладам, как правило, имеют место особо сильные экономические кризисы и депрессии, военные конфликты, а стоимость перехода может быть велика. Ранее военные технологии были важным катализатором создания ядра нового уклада, но сейчас приоритетны именно гражданские технологии. Страны и структуры, первые перешедшие к новому укладу, имеют принципиальные конкурентные преимущества в условиях технологического лидерства.

Важными элементами нового технологического уклада (НТУ) являются активное и разностороннее внедрение киберфизических устройств; когнитивных технологий и искусственного интеллекта, включая нейросетевые алгоритмы; аддитивных производств; разработки материалов, структур и организмов с заданными свойствами; нанотехнологии (наноэлектроники, нанохимии, нанофотоники); высоких социогуманитарных технологий; восстановительной медицины; новых образовательных технологий; интеллектуальных сетей вещей, объектов и машин; глобальных информационных систем; массовой робототехники и др.

В рамках НТУ информация становится фактором экономики и источником цифрового капитала. При этом разрабатываются новые бизнес-модели и новые подходы к организации межкорпоративных и внутрикорпоративных неиерархических пиринговых в информационно-телекоммуникационных систем связи и управления, принятия решений. В таких системах принципиально важным становится функциональная надежность, что требует создания соответствующей доверенной среды.

В данной работе рассматриваются возможности и перспективы реализации проектов НТУ с применением концепции доверенной неоднородной среды на технологии блокчейна и включающей сети вещей и машин IoT/IIoT/M2M, центры обработки данных (ЦОД/bigdata), облачные сервисы и др.

В этих проектах могут использоваться технологии искусственного интеллекта, в том числе нейронные сети, асимметричная криптография, программно-определяемые сети SDN/SD-WAN, программно-определяемые хранилища SDS, непосредственное макетирование (rapid prototyping). При этом необходимыми требованиями являются обеспечение заданных уровней безопасности и доверенности, а также гиперконвергентности среды [1,2,3].

Доверенные неоднородные блокчейн-среды

Доверенная среда – распределенная информационная программно-аппаратная система с заданными характеристиками функциональной надежности. Само понятие доверенности среды имеет вероятностный характер и требует использования критериев оценки доверенности, надежности, безопасности. В рамках НТУ применение доверенных неоднородных сред на основе блокчейн-технологий позволяет принципиально повысить эффективность и безопасность проектов в различных областях, включая промышленность и строительство, транспорт и энергетику, ЖКХ, агропромышленный комплекс, здравоохранение, государственные структуры, корпоративное управление, финансово-банковский сектор. То есть там, где инфраструктура, в том числе критическая, может быть связана информационно-телекоммуникационной сетью. Также перспективным направлением является создание персональных доверенных блокчейн-сред, включающих, например, умный дом.

Ключевые вопросы доверенных сред: гиперконвергентность, функциональная эффективность и надежность, включая коммуникации между доверенными средами и передачу доверенности, управление рисками и безопасность, согласованное применение компонентов при формировании доверенной среды, защиты информационных и финансово-инвестиционных потоков независимо от юрисдикций.

До недавнего времени для неоднородных систем было достаточным обеспечение конвергентности разнотипных составляющих. Однако в рамках нового уклада требования включают необходимость соблюдения конвергентности в условиях динамичной конфигурации и масштабирования среды, то есть гиперконвергентности, для чего необходимы дополнительные системы виртуализации, а также программные средства, позволяющие из одного интерфейса (контроллера) управлять системами хранения, средой виртуализации и дополнительной функциональностью.

Архитектура и структура, сетевая топология доверенной среды зависят от многих факторов, включая её области применения, и могут динамично меняться. Важными составляющими являются высокий уровень виртуализации и применение блокчейн-технологий при хранении, обработке и передаче данных, а также единый контроллер среды, обеспечивающий управление виртуализацией, сетевыми и вычислительными ресурсами и включающий механизмы анализа ситуации и принятия решений (рис.1). В рамках данной концепции в доверенной неоднородной блокчейн-среде могут использоваться:

- блокчейн пиринговая P2P сеть;

- облачные системы/сервисы;
- ЦОД – центр обработки данных с программно-определяемым хранилищем SDS;
- хеш-код – уникальный криптографический код, получаемый преобразованием данных функцией свертки;
- контроллер доверенной среды - система технологического управления сетевыми и вычислительными ресурсами с использованием нейросетевых алгоритмов, с сопроцессорами для защиты данных при работе в критически ответственной инфраструктуре;
- RC – резервируемые коммуникации, созданные по технологии программно-конфигурируемых (определяемых) сетей SDN/SD-WAN и обеспечивающие бесперебойные соединения при плановых разрывах и при неустойчивой связи [4];
- сети вещей, объектов и машин IoT/IIoT/M2M.

Учитывая требования к доверенным средам, необходимы специализированные инструментarii/платформы для их создания, модификации и расширения, изменения параметров и обеспечения гиперконвергентности, принимая во внимание также взаимодействие доверенных систем, обеспечение заданного уровня доверенности, изменения в технологиях, применяемых в доверенных средах. Одним из перспективных вариантов является метод непосредственного (быстрого) макетирования (rapid prototyping), включая динамическое макетирование – для обеспечения заданных характеристик доверенности, функциональной эффективности и надежности, безопасности в доверенных блокчейн-средах.

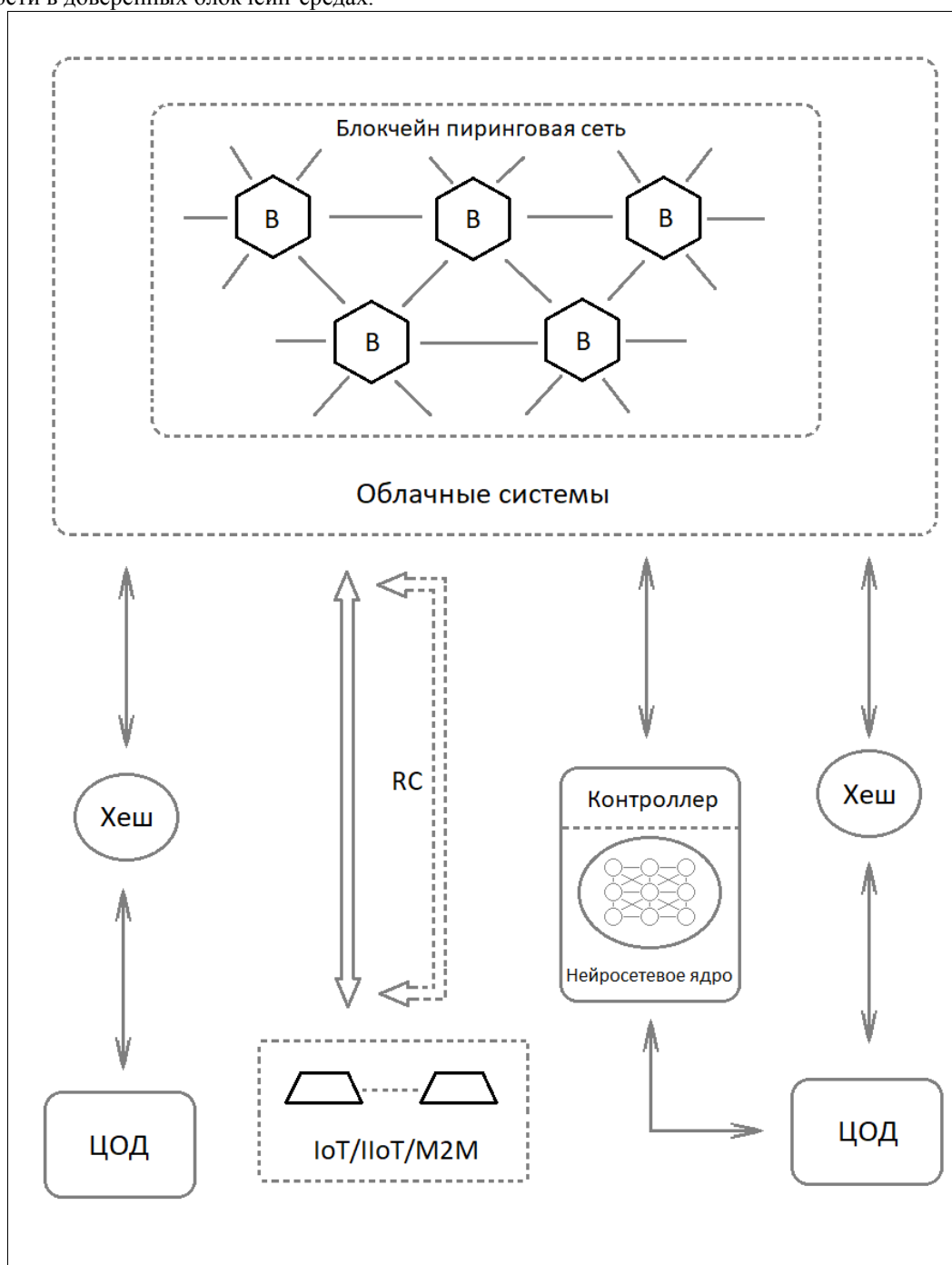


Рис.1. Структурная модель доверенной неоднородной блокчейн-среды.

С целью обеспечения скоординированного взаимодействия внутри доверенных сред, между ними и с внешними объектами необходимы согласования регламентов/стандартов на государственном, региональном, отраслевом и корпоративном уровнях, вырабатываемые с участием профессиональных сообществ. Такие регламенты/стандарты должны учитывать аналогичные требования, действующие или разрабатываемые для технологий, входящих в доверенные среды. Что может привести к необходимости создания специальных инструментов формата доверенной среды для разработки адаптивных регламентов/стандартов и определения соответствия данной среды действующему на момент сертификации регламенту/стандарту.

Особым вопросом является нормативно-правовое обеспечение доверенных блокчейн-сред с учетом возможной кросс-юрисдикции элементов среды.

Блокчейн-технологии в доверенных неоднородных средах

Применение технологий публичного или частного распределенного консенсуса блокчейн при обработке, хранении и передаче метаданных без нарушения приватности является принципиальным для данной концепции доверенной неоднородной среды. При этом уязвимости блокчейн-технологий могут быть компенсированы их взаимодействием с нейросетевым ядром контроллера сетевых и вычислительных ресурсов доверенной среды.

Неиерархические пиринговые P2P блокчейн-структуры можно использовать для доверенной обработки данных/документов, например, помещая уникальный криптографический определитель хеш в блокчейн-среду. Блокчейн-алгоритмы и их гибридные программно-аппаратной реализации также употребляются для защиты информационных и финансово-инвестиционных потоков независимо от юрисдикций, включая трансграничные платежи и комплаенс-контроль. При этом отдельной темой являются блокчейн-механизмы перевода этих потоков под российскую юрисдикцию.

В данной концепции блокчейн-механизмы применяются для обеспечения доверенности среды, защиты от фальсификации информации, исключения человеческого фактора. В сочетании с нейросетевым ядром контроллера сетевых и вычислительных ресурсов доверенной среды блокчейн-механизмы обеспечивают также восстановление искаженных или нечётких данных, в том числе при транзакциях в SDN/SD-WAN сетях. При сопряжении с сетью вещей, объектов и машин IoT/IIoT/M2M и облачными сервисами, предоставляемыми ЦОД, блокчейн-технологии обеспечивают доверенную идентификацию и аутентификацию. Еще одной действующей в доверенной среде функцией блокчейн-технологий являются умные блокчейн-контракты, гарантирующие, что контракт будет выполнен надлежащим образом без раскрытия лишней информации посторонним.

Телекоммуникационные технологии для доверенных неоднородных блокчейн-сред

При реализации доверенных сред ключевым моментом являются телекоммуникационные связи с заданными параметрами надежности и безопасности, что может быть обеспечено применением программно-конфигурируемых (программно-определяемых) сетей SDN (software-defined networking). Тип сетей с программно реализуемым управлением, разработанный около 10 лет назад, позволяет отделить собственно передачу данных с помощью соответствующих устройств (каналы передачи данных, коммутаторы и пр.) от управления этими устройствами (контроллер), что гарантирует необходимые для доверенных блокчейн-сред параметры. Программно реализуемый уровень управления в SDN физически отделен от уровня инфраструктуры, на котором действуют каналы передачи данных и сетевые коммутаторы. Для SDN уже созданы различные интерфейсы между логическим контроллером сети и сетевым транспортом. SDN сети оптимальны для обеспечения гиперконвергентности, гибкости и адаптивности доверенных неоднородных сред.

Программно-определяемые сети особо эффективны для облачной инфраструктуры, позволяющей автоматически формировать виртуальные сетевые ресурсы по требованиям потребителей доверенной среды. Ещё одной частью доверенной среды являются центры обработки данных, где применение программно-определяемых сетей также обосновано с учетом характерной централизации при помощи унифицированным программных средств и динамичного управления сетью и её ресурсами. Технологии SDN перспективны и для применения в сетях вещей и машин IoT/IIoT/M2M с особыми требованиями по взаимодействию между вещами/машинами, входящими в сеть, а также с внешними объектами.

Таким образом, программно-определяемые сети оптимальны для доверенных неоднородных блокчейн-сред и обеспечивают комплексное решение телекоммуникационных задач в облачных сервисах, ЦОД и IoT/IIoT/M2M.

Для телекоммуникационного обеспечения доверенных блокчейн-сред, особенно корпоративных, перспективно применение SD-WAN сетей (software-defined - wide area network»; программно определяемая – глобальная компьютерная сеть), изначально основанных на идеях и базовой архитектуре SDN, однако имеющих важные для доверенных блокчейн-сред, особенно распределенных корпоративных, отличия. Основа SD-WAN – туннелирование в глобальных сетях, с автоматической конфигурацией сети, бесперебойной передачей данных с участием резервных соединений, агрегацией каналов сети, мониторингом качества услуг.

В частности, в SD-WAN, по сравнению с SDN, более сложная аппаратная и программная реализация, целью которых является дополнительная защита (безопасность), самонастраивающиеся сети (особая сетевая аналитика) и др. Механизмы повышения быстродействия в SD-WAN при реализации доверенных блокчейн-сред могут быть сделаны, например, на базе масштабируемых многопротокольных MPLS – решений (multiprotocol label switching — многопротокольная коммутация по меткам). Причём MPLS является независимым от протоколов механизмом передачи данных только на основании меток без анализа самих данных, что позволяет реализовать сквозной виртуальный канал, не ограниченный средой передачи данных.

Нейросетевое ядро контроллера доверенной блокчейн-среды

Контроллер сетевых и вычислительных ресурсов доверенных блокчейн-сред должен включать нейросетевое ядро для определения и ликвидации конфликтных и кризисных ситуаций в среде, для анализа достоверности информации, распознавания в условиях неполной и/или недостоверной информации с коррекцией ошибок и помех. Такой подход обеспечивает действительно параллельную обработку информации с выдачей согласованных последовательных решений/управленческих действий.

В настоящее время большая часть используемых алгоритмов нейронных сетей основывается на так называемых глубинных или сверточных нейронных сетях. Они представляют собой каскады или многослойные структуры из нескольких десятков или сотен более простых нейронных сетей. Каждая из них обрабатывает исходные данные, а продукты анализа, полученные сетью, расположенной выше, что позволяет упрощать очень сложные проблемы и решать их при помощи сравнительно скромных вычислительных ресурсов. Традиционно используются различные вариации, восходящие к нейронным сетям Хопфильда [5], первым действительно работоспособным, после оказавшихся не эффективными и ограниченными перцептронов.

Одним из дополнительных способов обеспечения безопасности является использование нестандартных нейросетевых алгоритмов с оригинальными нейронами с необычным поведением (behavior). Интерес могут представлять нейронные сети осцилляторного типа, изначально создававшиеся для вычислительных систем на основе новых физических принципов, в частности, для оптических компьютеров [6]. Такие сети стремятся к равновесному состоянию, в котором каждая следующая итерация сети близко к предыдущему и отличается от него не более, чем на размер установленного предела (threshold), определяющего точность решения, что также может быть использовано для корректировки уровня доверенности.

Некоторые аспекты разработки доверенных неоднородных блокчейн-сред

Для доверенных блокчейн-сред предлагается использовать асимметричную криптографию с нетривиальной эмпирической оценкой рисков и с последующим переходом к квантовой криптографии по мере появления её коммерческой реализации, решения вопросов сертификации и оценки рисков. Важен отказ от классических «тяжелых» криптографических протоколов и принятие низкоресурсных криптографических механизмов.

Для ЦОД, используемых в доверенных блокчейн-средах, необходимо развитие дополнительных сервисов по обеспечению функционирования доверенных сред, включая обеспечение конфиденциальности при хранении, обработке и передаче больших массивов данных с использованием программно-определяемого хранилища SDS (software-defined storage). Так как конвергентные решения уже применяются в ЦОД, SDS позволят перейти к гиперконвергентной модели в ЦОД для реализации облачных сервисов, что обеспечит дополнительную отказоустойчивость, масштабируемость, управляемость в доверенной блокчейн-среде.

Заключение

Построение доверенных сред на основе блокчейн-технологий, программно-конфигурируемых сетей SDN/SD-WAN и единого контроллера сетевых и вычислительных ресурсов с нейросетевым ядром, при использовании облачных сервисов, ЦОД с SDS и алгоритмов асимметричной криптографии, обеспечивает заданный и контролируемый уровень их функциональной эффективности и надежности, безопасности и доверенности, в том числе для неоднородных систем, включающих сети вещей и машин IoT/IIoT/M2M, и при неустойчивых каналах связи.

При создании, модификации и масштабировании доверенных неоднородных блокчейн-сред важно применение специализированного инструментария, включая методы непосредственного макетирования rapid prototyping.

Адаптивные подходы к регулированию и регламентации доверенных блокчейн-сред должны учитывать требования гиперконвергентности и, возможно, разные юрисдикции частей среды, в том числе, при взаимодействии доверенных сред. Для доверенных блокчейн-сред существенна стандартизация их архитектуры, согласованная стандартизация используемых в средах технологий и требований к программно-аппаратным средствам.

Доверенные неоднородные блокчейн-среды обеспечат необходимый уровень конкурентоспособности и эффективности проектов в условиях нового технологического уклада.

Список литературы

1. Жданов С.Е. «Глобальная промышленная революция. Международный опыт стандартизации интернета вещей в рамках деятельности международного союза электросвязи» // Электронный научный журнал «ИТ-Стандарт», 2016, №1, 4 стр., URL: <http://www.itstandard.ru>

2. Головин О.Л., Варганов М.А., Сбоев А.Г. Интернет и инвестиции // Банковские технологии – 1997, №25 – с. 108-110

3. Е.Г. Андрианова, О.Л. Головин, Г.Б. Коняев, Д.А. Поликашечкин, А.В. Полторак. К вопросу о развитии и стандартизации технологий IoT/IIoT/M2M в России с участием российских компаний. // Электронный научный журнал «ИТ-Стандарт», 2016, № 4, 5 стр., URL: <http://www.itstandard.ru>

4. О.Л. Головин, А.В. Полторак. О подходе к обеспечению надежности и безопасности в информационно-коммуникационных системах промышленного и бытового интернета вещей и объектов IoT/IIoT/M2M». // XVI Научно-практическая конференция «Современные информационные технологии в управлении и образовании», 20 апреля 2017 года, Москва, стр. 124-130.

5. John J. Hopfield, «Neural networks and physical systems with emergent collective computational abilities», Proceedings of National Academy of Sciences, vol. 79, no. 8, pp. 2554–2558, April 1982.

6. Oleg L. Golovin. An artificial network based on unfixed states number oscillators. International Joint Conference on Neural Networks IJCNN'91 Singapore, Paper NO: S0163, Session: Hybrid system, 1991

References

1. Zhdanov S.E. Global industrial revolution. International experience standardization Internet of Things in the activities of the international telecommunication union. // Scientific e-magazine “IT-Standard”, 2016, №1, 4 pp., URL: <http://www.itstandard.ru>

2. Golovin O.L., Vartanov M.A., Sboev A.G. Internet and investments // Banking technologies – 1997, №25 – pages 108-110

3. Andrianova E.G., Golovin O.L., Konjaev G.B., Polikashechkin D.A., Poltorak A.B. Questions concerning development and standardization of technologies IoT/IIoT/M2M in Russia with participation of Russian companies. // Scientific e-magazine “IT-Standard”, 2016, № 4, 5 pp., URL: <http://www.itstandard.ru>

4. Golovin O.L., Poltorak A.B. About approach to providing reliability and security in information-telecommunicational systems industrial and common internet of things and subjects IoT/IIoT/M2M». // XVI Science-practical conference “Modern information technologies in management and education”, 20 April 2017, Moscow, pages 124-130.

5. John J. Hopfield, «Neural networks and physical systems with emergent collective computational abilities», Proceedings of National Academy of Sciences, vol. 79, no. 8, pp. 2554–2558, April 1982.

6. Oleg L. Golovin. An artificial network based on unfixed states number oscillators. International Joint Conference on Neural Networks IJCNN'91 Singapore, Paper NO: S0163, Session: Hybrid system, 1991