ЭКОНОМИКА РОССИИ И РЕГИОНОВ

УДК 330.354
ГРНТИ 06.52.13:06.52.17

Цифровая экономика: уязвимость к сетевым атакам и возможности обеспечения устойчивости управления

Е.Л. Логинов, *д.э.н., профессор РАН*
e-mail: *loginovel@mail.ru*

А.Н. Райков, *д.т.н., профессор*
e-mail: *Alexander.N.Raikov@gmail.com*

Аннотация
Рассматривается создание Системы систем обеспечения безопасности объектов в цифровой экономике (технологии «больших данных», квантовые компьютеры, цифровые предприятия, элементы искусственного интеллекта и пр.). При этом для обеспечения безопасности используются информационно-вычислительные гиперконвергентные матрицы, обеспечивающие устойчивую сходимость процессов решения задач обеспечения безопасности таких объектов к заданным целям. Цели могут охватывать вопросы предупреждения нештатных ситуаций в системах управления организационными структурами различного профиля, использующими интеллектуальные управленческие сервисы. Применяются инструментарии ситуационной осведомленности, сетевой экспертизы и когнитивного моделирования. Гиперконвергентные матрицы позволяют управлять эмерджентными эффектами, возникающими в системе систем защиты. Они включаются в процесс сетевого ситуационного анализа для выявления в отношении объектов в цифровой экономике явных и неявных (латентных) характеристик их функционирования и управления. Системным итогом предлагаемого подхода является устойчивое целенаправленное функционирование всей цифровой экономики нашей страны.

Статья подготовлена при выполнении федерального задания по теме «Научно-технологическое развитие экономики отраслевых рынков» (№ 0163-2016-0007)

Ключевые слова: *цифровая экономика, гиперконвергентность, оперативная экспертиза, ситуационный анализ, мониторинг, прогноз, Система систем, управление*

Введение

В России и за рубежом растет потребность в повышении эффективности процессов формирования и развития систем обеспечения информационной, специальной и т.п. безопасности на объектах, относящихся к цифровой экономике [1, 13]. Так, в аналитическом отчете компании Positive Technologies проанализированы автоматизированные системы управления технологическими процессами (АСУ ТП) на предприятиях транспорта, водоснабжения, энергоснабжения и др. [3]. В рамках этого исследования были рассмотрены уязвимости компонентов более 500 производителей АСУ ТП. Количество уязвимостей в компонентах АСУ ТП различных производителей представлено на рис. 1.

Из 743 выявленных уязвимостей практически половина (47%) имеют высокую степень риска.

В сложившихся условиях актуализируется проблема улучшения защиты объектов цифровой экономики (искусственный интеллект, распределенные реестры, робототехника, квантовые вычисления и пр.) с большой ситуационной составляющей, в том числе критически быстрого каскадного развития эффекта ущерба, например, от сетевой террористической атаки. Это, прежде всего, объекты в цифровой экономике, например, объекты атомного энергопромышленного комплекса или интегрированный топливно-энергетический и жилищно-коммунальный комплекс крупного города.

В этом контексте все более актуальным становится вопрос конструирования комплексной системы (Системы систем) мониторинга и управления для обеспечения безопасности, в том числе прогнозирования и упреждения нештатных ситуаций в системах управления организационными структурами различного профиля, использующими интеллектуальные управленческие сервисы, в цифровой экономике с гетерогенными (разнород-

ными) компонентами. При этом обостряется вопрос целенаправленного и быстрого решения поставленных задач обеспечения безопасности такой инфраструктуры.

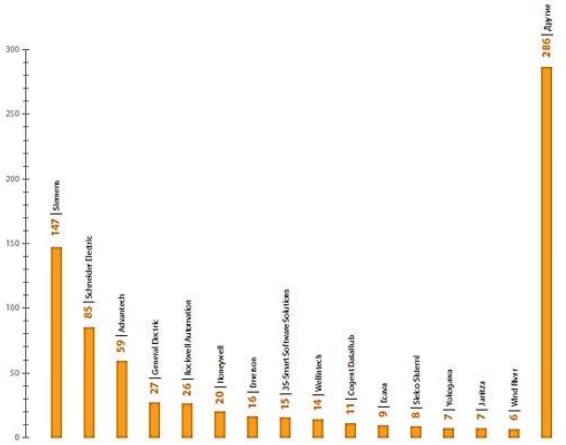

Рис. 1. Количество уязвимостей в компонентах АСУ ТП различных производителей [3].

Гиперконвергентная Система систем

Система систем (SoS) - это большая система, которая обеспечивает уникальные возможности, формируемые за счет интеграции независимых друг от друга полезных систем [17,19]. Концептуальной основой для определения характеристик Системы систем являются «пять критериев Майера»:

а) компоненты системы должны быть способны работать независимо друг от друга, когда они не интегрированы в SoS (то есть, полезны сами по себе);

б) компоненты системы продолжают оперировать независимо друг от друга до некоторой степени в то время, когда они интегрированы в SoS;

в) SoS растет и развивается со временем и опытом;

г) SoS способна выполнять функции, которые не могут быть найдены в любом из компонентов системы, и эти функции являются основными целями SoS;

д) SoS распределена по большой географической протяженности [19].

Приведенное определение декларирует новое качество функционирования совокупности систем, связанное с эмерджентностью, т.е. проявлением существенно новых особенностей у Системы систем, отсутствующих у каждой из отдельных ее составляющих. Вместе с тем приведенное определение не дает рекомендаций как это новое качество получить, какие условия должны быть предписаны Системе систем, чтобы процесс ее функционирования устойчиво сходился к намеченным целям, отражающих это новое качество.

Применительно к решению рассматриваемого вопроса такие, «устойчиво сходящиеся», Системы систем можно реализовать с использованием информационно-вычислительных гиперконвергентных матриц, а именно матриц, позволяющих получить целенаправленный синергетический эффект за счет специального управления процессами интеграции и взаимодействия информационных, телеметрических, аналитических сервисов поддержки систем обеспечения безопасности на инфраструктурных объектах.

Под *гиперконвергентностью* в данной работе понимается обеспечение устойчивой сходимости процессов управления сложными ситуациями за счет:

- использования методологии конвергентного управления;
- наиболее эффективного конфигурирования платформ и сервисов датацентров.

Основные положения по методологии конвергентного (устойчиво сходящегося) управления приведены в [16] и последующих работах автора настоящей работы. Такое сходящееся управление обеспечивается созданием необходимых условий по структурированию информации при взаимодействии участников процессов принятия решений на уровне «субъект – коллективный самоорганизующийся субъект» [21]. Эти условия формулируются на основе применения закономерностей преобразования информации, диктуемых, в частности, фундаментальной термодинамикой и методами решения обратных задач на топологических пространствах.

Гиперконвергентная инфраструктура объединяет вычислительные серверные возможности, хранение, сетевую коммутацию, гипервизор, защиту данных, эффективность использования данных, глобальное управление и другие функциональные возможности информационных технологий (см., например, [22]).

Гиперконвергентная Система систем в инфраструктурном объекте позволяет осуществлять *целенаправленно* и с постоянным *ростом эффективности:* мониторинг, накопление информации, анализ ситуаций и синтез решений, прогнозирование, идентификацию угроз, поддержку управленческих решений, планирование мер противодействия, их реализацию,

установление обратной связи и принятие мер по совершенствованию процессов и процедур, а также развитие самой Системы систем.

Сложность решения вопроса создания Системы систем для объектов цифровой экономики (искусственный интеллект, распределенные реестры, робототехника, квантовые вычисления и пр.) заключается в ее многогранности, так как требует рассмотрения в комплексе множества различных аспектов: субъективных, эмоциональных, коллективного принятия решений, организационных, технических, управленческих, информационных, безопасности и т.д. Необходим также учет факторов неустойчивости, беспричинности, стохастичности, неоднозначности и нелинейности как самих попыток перехвата управления, так и факторов, влияющих на их протекание во времени и пространстве.

Применение методологии конвергентного (устойчиво сходящегося) управления [16] и создание гиперконвергентной Системы систем именно и позволяет целенаправленно сосредоточиться на эффективном использовании современных научных и технических достижений, в том числе направленных на преодоление существующих сегодня барьеров (технических, ведомственных и пр.) для обеспечения совместной работы множества различных структур организационного, технологического и т.п. управления, имеющих отношение к работе цифровой экономики нашей страны.

При разработке Системы систем обеспечения безопасности в цифровой экономике на основе информационно-вычислительных гиперконвергентных матриц, авторами настоящей работы были приняты во внимание и использованы также результаты ряда известных зарубежных проектов, реализуемых DARPA (Terrorism Information Awareness (TIA), Wargaming the Asymmetric Environment (WAE), Rapid Analytical War Gaming (RAW), Future Markets Applied to Prediction (FutureMAP), Graph-theoretical Research in Algorithm Performance & Hardware for Social networks (GRAPHS), Visual Media Reasoning (VMR) и пр.) [2, 5, 8, 15].

Для создания гиперконвергентной матрицы информационных, телеметрических, аналитических сервисов поддержки систем мониторинга и обеспечения информационной, специальной и т.п. безопасности, а также повышения оперативности и эффективности мер по защите от сетевых или аналогичных им атак [10], на инфраструктурных объектах предлагается применить многофункциональный аппаратно-программный комплекс, осуществляющий мультиагентное интеллектуальное управление автоматизированным процессом сбора данных, анализа и принятия решения, использующий соответствующий фреймворк управления знаниями.

Мониторинговые механизмы

Мониторинговые механизмы в работе создаваемой Системы систем должны обеспечивать выявление таксономии и мерономии взаимосвязей в системе работы изучаемых объектов [13]. Для этого требуется формирование пакета моделей ситуационного анализа обстановки, управления знаниями и обеспечения ситуационной осведомленности участников управления и принятия решений, динамично адаптируемых к индивидуализированному профилю потенциальных объектов сетевых атак для постоянного уточнения оценки динамично меняющейся ситуации.

Предметно-адаптированная конфигурация базовых компонент Системы систем обеспечения безопасности формируется путем идентификации атрибутивно-семантических взаимосвязей (отношений), которые оператор системы должен выявить (в интерактивном режиме) между выбранными им блоками связанных сложноструктурированных данных электронного контента, сформированного по результатам этапа мониторинга и первоначального ситуационного анализа изучаемого объекта. При этом используются методы сетевой экспертизы [20], управления знаниями, когнитивного моделирования, эволюционных вычислений и анализа Больших Данных. Обобщенный фреймворк управления знаниями имеет вид, приведенный на рис. 2.

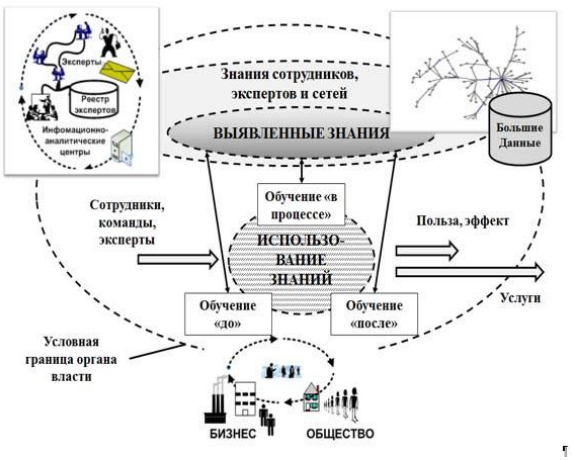

Рис. 2. Фреймворк управления знаниями

Создаваемая Система систем обеспечит автоматизированный ситуационный анализ массивов Больших Данных и соответствующее когнитивное и эволюционное моделирование для обнаружения атак и аномалий в процессах функционирования объектов цифровой экономики (искусственный интеллект, распределенные реестры, робототехника, квантовые вычисления и пр.), а также поддержки управленческих действий и принятия решений, в том числе в условиях быстрого каскадного развития эффекта ущерба от террористической атаки и острой нехватки ресурсов для обеспечения работы объекта инфраструктуры в контролируемом режиме.

Набор автоматизированных операций по обнаружению атак и аномалий процессов функционирования объектов цифровой экономики (искусственный интеллект, распределенные реестры, робототехника, квантовые вычисления и пр.), а также работа экспертов, коллективные процессы моделирования и принятия решений осуществляются в рамках распределенной (сетевой) информационно-вычислительной среды [7, 9, 20]. При этом каждая из гиперконвергентных матриц определяет набор динамических паттернов (в виде фреймов, семантической сети, исчисления предикатов) формируемых с помощью механизмов управления знаниями и когнитивного моделирования. Паттерны могут образовывать иерархические и сетевые системы отношений, быть подпаттернами других паттернов. Паттерны отражают атрибутивно-семантические взаимосвязи в рамках совокупности блоков сложноструктурированных данных, характеризующих адекватность или неадекватность поведения наблюдаемых отдельных индивидуумов и групп людей с элементами идентификации неявных террористических универсалий, которые с определенной вероятностью представляют опасность для цифровой экономики.

Таким образом, гиперконвергентные матрицы в рассматриваемой системе систем используются для ситуационного анализа и принятия решений в сетевой среде с подключением территориально распределенных участников. При этом обеспечивается идентификация соответствия предметно-адаптированной конфигурации базовых характеристик Системы систем обеспечения безопасности критериям и стандартам построения таких систем [14,17].

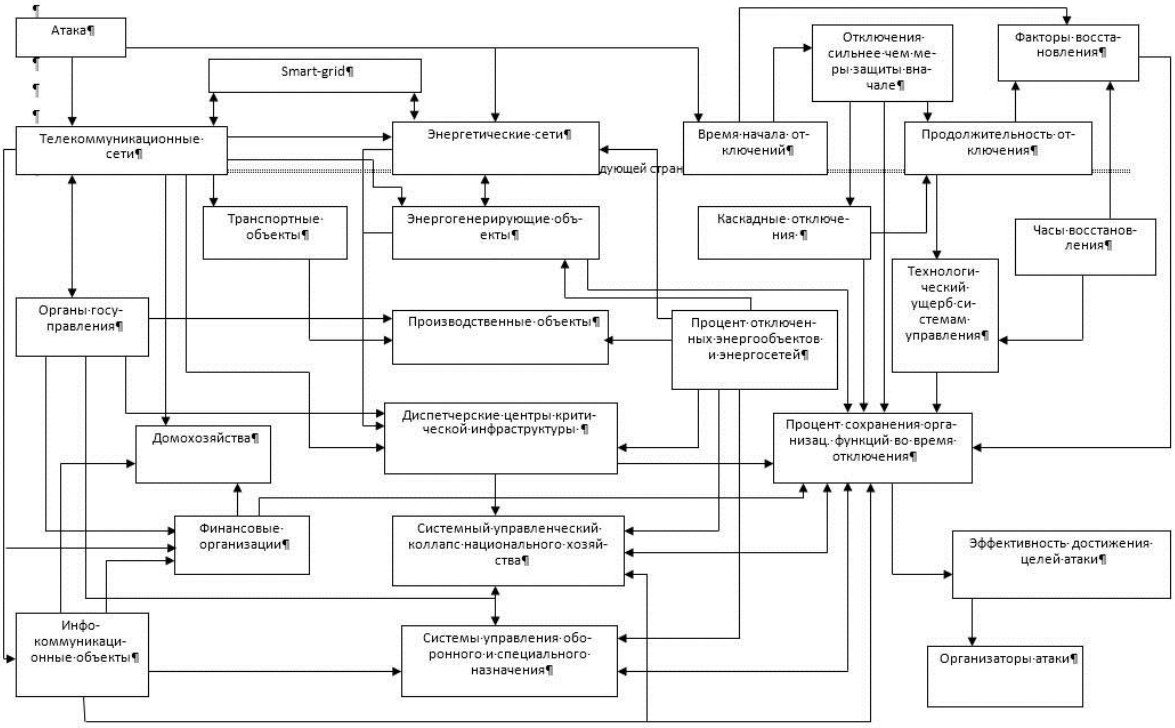

Рис. 3. Модель взаимосвязей при осуществлении атак на объекты цифровой экономики

Моделирование развития латентной ситуации

Мониторинговые сервисы должны позволять моделировать и осуществлять прогноз развития ситуации в условиях быстрого изменения окружающей реальности с сохранением процесса развития ситуации в рамках управляемого профиля [12]. Модель взаимосвязей при осуществлении атак на информационно-коммуникационных линиях в цифровой экономике, позволяющая поддерживать такое прогнозирование, приведена на рис. 3.

Методы мониторинга позволяют выявлять наряду с явными также и латентные характеристики типичного или атипичного функционирования с выяснением соответствия ситуации критериям антитеррористической защищенности, вскрытие латентных отношений между внешне не связанными агентами активных действий. Для этого может быть использован авторский метод латентного синтеза решений [18], основанный на ситуационном анализе трафиков электронных сообщений в глобальных и локальных сетях. При моделировании и вскрытии латентных отношений между внешне не связанными агентами активных действий оператором Системы систем используется механизм управления знаниями [11].

При реализации рассматриваемого подхода требуется определить направления расширения контроля совокупных массивов данных в доступных для анализа Больших Данных в условиях внешних информационных атак. При этом формируется соответствующая система межведомственной координации мер безопасности с выделением ключевых операционных узлов, с помощью которых и производится выполнение технических или иных операций в отношении наиболее опасных форм сетевых или аналогичных им атак в отношении объектов в цифровой экономике.

Создаваемая Система систем рассматривается авторами как масштабируемое пространство с участием компаний и органов государственной власти, которые образуют соответствующую систему систем более высокого уровня, обладающую собственными свойствами.

Заключение

Необходимо принципиально изменить информационно-аналитические технологии поддержки процессов мониторинга и управления объектами цифровой экономики с опорой на внедрение подхода, основанного на создании гиперконвергентной Системы систем в рамках специализированной информационной платформы [6]. Такие системы и используемые в них гиперконвергентные матрицы создают необходимые условия для сходимости процессов управления, принятия и реализации управленческих решений к заданным целям обеспечения безопасности этих объектов [4].

Гиперконвергентная Система систем позволяет перейти от позадачного подхода к созданию комплексной технологии предоставления сервисов поддержки интеллектуального управления и принятия эффективных коллективных решений в сетевой среде в интересах повышения эффективности мер по обеспечению безопасности объектов цифровой экономики. Системным итогом предлагаемого подхода является устойчивое целенаправленное функционирование всей цифровой экономики нашей страны.

Литература

1. Ковальчук Ю.А., Степнов И.М. Цифровая экономика: трансформация промышленных предприятий // Инновации в менеджменте. 2017. № 1 (11). С.32-43.

2. Аналитический комплекс Security AS (Security Analyst's Station) [Электронный ресурс]. URL: http://irule.ru/reshenija/universalnoe-reshenie-security-as.html (дата обращения: 01.10.2017).

3. «Безопасность АСУ ТП в цифрах - 2016» [Электронный ресурс] Positive Technologies. URL: http://www.ptsecurity.ru/upload/ptru/analytics/ICS-Vulnerability-2016-rus.pdf (дата обращения: 01.10.2017).

4. Борталевич С.И., Логинов Е.Л., Чиналиев В.У. Проблемы стратегической перестройки организационных механизмов управления научно-техническим развитием России и ЕАЭС. – М.: Финансовый университет при Правительстве Российской Федерации, 2016. - 258 с.

5. В интересах национальной безопасности [Электронный ресурс] URL: http://www.agentura.ru/dossier/usa/darpa/ (дата обращения: 01.10.2017)

6. Куприяновский В.П., Синягов С.А., Климов А.А., Петров А.В., Намиот Д.Е. Цифровые цепи поставок и технологии на базе блокчейн в совместной экономике // International Journal of Open Information Technologies. 2017. Т. 5. № 8. С. 80-95.

7. Агеев А.И., Логинов Е.Л. Битва за будущее: кто первым в мире освоит ноомониторинг и когнитивное программирование субъективной реальности? // Экономические стратегии. 2017. Т. 19. № 2 (144). С. 124-139.

8. Исследовательская программа DARPA на 2015 год (Review of DARPA FY 2015 Research Programs). [Электронный ресурс] URL: https://mipt.ru/education/chairs/theorcyber

netics/government/upload/3af/Program_darpa2015_rus.pdf. (дата обращения: 01.10.2017).

9. Когаловский М.Р. Перспективные технологии информационных систем. – М.: ДМК. Пресс, 2008. – 288 с.

10. Логинов Е.Л., Борталевич С.И., Баитов А.В. Сетецентрическое управление объектами атомного энергопромышленного комплекса России как многоагентной системы с большим числом квази-автономных организационных и технических элементов с собственными управленческими траекториями // Проблемы безопасности и чрезвычайных ситуаций. 2017. № 1. С. 112-119.

11. Цветков В.А., Логинов Е.Л., Райков А.Н. Формирование интеллектуального ядра сетевой инфраструктуры сферы высшего образования и науки // Образовательные технологии и общество. 2015. Т. 18. № 3. С. 372-379.

12. Логинов Е.Л., Райков А.Н. Стратегические тренды развития конвергентной информационно-телекоммуникационной инфраструктуры России и Евразийского экономического союза. // Межотраслевая информационная служба. 2015. № 1 (170). С. 5-10.

13. Логинов Е.Л., Райков А.Н., Эриашвили Н.Д. Аналитическое моделирование кризисных процессов: первоочередные подходы к удержанию российской экономико-политической системы в рамках управляемого контура // Вестник экономической безопасности. 2015. № 5. С. 91-96.

14. Логинов Е.Л., Борталевич С.И., Шкута А.А., Логинова В.Е. Подходы к использованию модели самоорганизации и распада нейронно-сетевых структур для повышения живучести информационных систем органов государственного управления вследствие природных, техногенных катастроф или военных атак // Вестник Московского университета МВД России. 2017. № 4. С. 187-194.

15. Callahan D., Shakarian P., Nielsen J., Johnson A. Shaping Operations to Attack Robust Terror Networks [Электронный ресурс] // URL: http://arxiv.org/pdf/1211.0709.pdf. (дата обращения: 01.10.2017).

16. Райков А.Н. Конвергентное управление и поддержка решений. -М.: Издательство ИКАР, 2009. – 245 с.

17. ISO/IEC/IEEE 24765:2010, 3.2991

18. Бугаев А.С., Логинов Е.Л., Райков А.Н., Сараев В.Н. Семантика сетевых контактов // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2009. №. 2. С. 33-36.

19. Maier, M. W. 1996. “Architecting Principles for Systems-of-Systems.” 6th Annual International Symposium of INCOSE, Boston, MA, USA, p. 567-574.

20. Gubanov, D., Korgin, N., Novikov, D., Raikov, A. E-Expertise: Modern Collective Intelligence, Springer. Series: Studies in Computational Intelligence, Vol. 558, 2014, XVIII, 112 p.

21. Юрьева А.А. Развитие информационного общества как условие формирования инновационной экономики // Проблемы рыночной экономики, 2016, №3. С.14-20.

22. Scott D.Lowe, David N.Davis. The Gorilla Guide to Hyperconvergent Infrastructure Implementation Strategies. USA. ActualTech Media. 2015. 122 h.

Digital Economy: Vulnerability to Network Attacks and Opportunities for Sustainability Management

***Evgeny L. Loginov**, Dr. of Sci (econ.), Professor of RAS*
e-mail: *loginovel@mail.ru*

***Alexander N. Raikov,** Dr. of Sci (tech.), Professor*
e-mail: *Alexander.N.Raikov@gmail.com*

Abstract

The creation of a System of Security Systems for objects in the digital economy ("large data" technologies, quantum computers, digital enterprises, elements of artificial intelligence, etc.) is being considered. In this case, information-computational hyperconvergent matrices are used, which ensure a stable convergence of the processes of solving the problems of ensuring the security of such objects to specified goals. Objectives can cover issues of preventing contingencies in the management systems of organizational structures of various profiles that use intelligent management services. The tools of situational awareness, network expertise and cognitive modeling are used. Hyperconvergent matrices allow you to manage emergent effects that arise in the system of protection systems. They are included in the process of network situation analysis to identify explicit and implicit (latent) characteristics of their functioning and management in relation to objects in the digital economy. The systemic outcome of the proposed approach is the stable, purposeful functioning of the entire digital economy of our country.

Keywords: *digital economy, hyperconversion, operational expertise, situational analysis, monitoring, forecast, system of systems, management*

Об авторах
Логинов Евгений Леонидович, д.э.н., профессор РАН, зам. директора, Институт проблем рынка РАН, Москва.
Райков Александр Николаевич, д.т.н., главный научный сотрудник, Институт проблем управления РАН, Москва.