Принципы разработки прикладных мультиагентных систем управления жизнеспособностью критических инфраструктур*

А.В. Маслобоев

Институт информатики и математического моделирования им. В.А. Путилова, Федеральный исследовательский центр «Кольский научный центр Российской академии наук», г. Апатиты, Россия

Аннотация. Работа направлена на развитие информационных технологий интеллектуальной поддержки принятия решений в области организационного управления жизнеспособностью региональных критических инфраструктур. Исследование базируется на систематизации, анализе и обобщении известных методологических подходов к обеспечению надежности, безопасности и жизнеспособности сложных динамических объектов, а также методах общей теории систем, принципах сетецентрического управления и мультиагентного моделирования. Дана общая классификация методов и средств анализа и моделирования, используемых на практике в целях поддержки управления жизнеспособностью критических инфраструктур. Обоснована необходимость применения парадигмы мультиагентных систем для поддержки управления жизнеспособностью критических инфраструктур. Для этого определены преимущества и возможные ограничения их использования. Предложены принципы построения прикладных мультиагентных систем поддержки принятия решений по управлению жизнеспособностью критических инфраструктур, основанные на сопряжении общей методологии проектирования мультиагентных систем и методических подходов к организации систем обеспечения комплексной безопасности критически важных объектов.

Ключевые слова: *мультиагентная система, управление, информационная поддержка, моделирование, жизнеспособность, критическая инфраструктура.*

DOI: 10.14357/20790279240208 **EDN: OYAAOQ**

Введение

В настоящее время технологии мультиагентных систем [1-3] по-прежнему широко применяются в задачах управления и системах поддержки принятия решений в различных предметных областях (транспорт, энергетика, экономика, производство и т.д.), характеризующихся структурной сложностью, динамичностью, неоднородностью объектов и многоаспектностью. Среди всего многообразия динамичных областей отдельное внимание заслуживают так называемые «критические сферы», к которым относятся, например, региональная безопасность, государственное управление, экологическая устойчивость, организационная жизнеспособность и другие. Объекты этих предметных областей являются стратегически значимыми для развития общества и государства и в совокупности образуют критические инфраструктуры, нарушение нормального функционирования которых может нанести значительный ущерб здоровью населения, экономике и обороноспособности страны.

Управление рисками и жизнеспособностью критических инфраструктур по структуре многофункционально и представляет собой сложный многоуровневый процесс, требующий специализированных знаний, подходов и средств автоматизированной обработки и анализа больших объемов

* Работа выполнена в рамках государственного задания ИИММ КНЦ РАН (НИР № FMEZ-2022-0023).

разноплановой информации о динамике состояния объектов критических инфраструктур. Распределенность объектов, сетецентрический характер организационного управления и неопределенность в ситуационной осведомленности, в свою очередь, требуют более эффективного использования ресурсов и оперативного реагирования на возникающие угрозы и критические события. Мультиагентный подход позволяет учесть эту специфику и особенности критических инфраструктур для реализации эффективного управления ими в условиях неполноты оперативных данных и воздействия множественных угроз различной природы. Однако в реальных приложениях мультиагентные системы редко применяются для управления критически важными объектами и инфраструктурами. Зачастую это связано, во-первых, с непредсказуемостью поведения агентов, автономно принимающих решения на основе локальной информации, и, как следствие, самой системы управления в целом, что может приводить к нежелательным последствиям. Во-вторых, перекладывание ответственности за принимаемые решения на агентов в условиях критических ситуаций, а также сложность координации деятельности агентов и интеграции со сторонними системами вызывают недоверие риск-менеджеров, системных аналитиков и операторов ситуационных центров. И, в-третьих, жесткие завышенные требования к надежности и устойчивости систем управления критическими инфраструктурами склоняют разработчиков систем безопасности к выбору известных стандартных решений, что не всегда приемлемо и обосновано в ущерб обеспечению гибкости и адаптивности средств управления.

Несмотря на противоречивость мнений российских и зарубежных экспертов в области безопасности по вопросам оценки применимости мультиагентных систем для управления критически важными объектами, использование мультиагентных технологий в управлении жизнеспособностью критических инфраструктур обусловлено следующими решающими факторами, которые нивелируют указанные выше субъективные ограничения в той или иной степени:

– необходимость обеспечения управляемости системы в условиях высокой динамичности среды функционирования и состава участников процессов принятия решений по управлению жизнеспособностью критических инфраструктур;
– необходимость учета сетецентрической, социотехнической и киберфизической природы управления критическими инфраструктурами для поддержания их жизнеспособности;
– необходимость координации децентрализованного управления жизнеспособностью на всех уровнях принятия решений;
– необходимость учета человеческого фактора в системе управления, то есть постоянного активного влияния управляемой системы на процесс управления;
– необходимость быстрой реакции на изменения внешней среды и адаптации к этим изменениям без потери функциональности управляемой системы;
– необходимость наличия способности системы управления к реконфигурации, обучению и самоорганизации;
– необходимость сквозного процессного управления жизненным циклом жизнеспособности критических инфраструктур и комбинирования горизонтальных и вертикальных связей в структуре распределенного управления жизнеспособностью.

Вместе с тем, мультиагентные системы являются эффективным средством реализации сетецентрического управления жизнеспособностью критических инфраструктур и средством системной интеграции гетерогенных программных и физических объектов (систем), которые выполняют заданные функции, взаимодействуют друг с другом и с окружающей средой по определенным правилам, обмениваясь информацией, для достижения глобальной цели – обеспечения и повышения безопасности и жизнеспособности критических инфраструктур в условиях воздействия множественных угроз.

Согласно выводам исследований [4, 5] высокая степень автоматизации процессов принятия управленческих решений и адаптивность управления достигаются за счет использования в мультиагентных системах алгоритмов машинного обучения и методов искусственного интеллекта, которые позволяют агентам быстро адаптироваться к изменяющимся условиям и оперативно принимать решения на основе анализа больших объемов разнородных данных. Мультиагентные системы также учитывают социальные и организационные аспекты процессов управления безопасностью и жизнеспособностью, включая индивидуальные особенности конкретного класса критических инфраструктур, важные для адекватного решения задач мониторинга, сценарного анализа и прогнозирования проблемных ситуаций в этих системах.

В данной работе предпринята попытка обосновать необходимость и целесообразность применения парадигмы и технологии мультиагентных систем для поддержки управления жизнеспо-

собностью критических инфраструктур, а также разработать принципы построения прикладных мультиагентных систем поддержки принятия решений в этой сфере на основе обобщения известных методологических подходов к обеспечению надежности, безопасности и устойчивости сложных динамических систем, положений концепции жизнеспособности и общей теории безопасности, методологий сетецентрического управления и проектирования агентно-ориентированных систем, основанных на знаниях, а также анализа организационно-технических и нормативных аспектов создания, интеграции и внедрения систем обеспечения безопасности критически важных объектов и инфраструктур. Определены преимущества и возможные ограничения применения мультиагентного подхода к решению задач управления жизнеспособностью критических инфраструктур. Приводится общая классификация методов и средств моделирования, анализа, автоматизации и управления, используемых на практике в целях обеспечения жизнеспособности критических инфраструктур.

1. Методологические основы исследования

Классифицировать известные на сегодняшний день методы и средства поддержки управления жизнеспособностью критических инфраструктур можно по их функционально-целевому назначению и лежащему в их основе методическому подходу к моделированию данного класса динамических систем.

Первая категория средств включает следующие классические методы:

– выявления уязвимостей и анализа рисков, которые могут негативным образом отразиться на рабочих характеристиках функционирования системы или качественных свойствах ее отдельных элементов, а также нанести определенный ущерб;
– оценки величины риска и его приемлемости в разрезе вероятности возникновения рисковых событий, степени возможных последствий и затрат на восстановление работоспособности системы в случае потери функциональности в результате влияния негативных факторов;
– приоретизации и минимизации риска, нацеленные на планирование и выбор наилучших для заданных условий превентивных мер по смягчению последствий реализации угроз на основе ранжирования рисковых событий по степени критичности, и применения решающих правил;
– управления рисками и аудита безопасности сложных систем, предполагающие разработку адекватных программ снижения идентифицированных рисков и реализацию релевантных ситуаций защитных контрмер по противодействию множественным угрозам;
– стратегического анализа и оценки эффективности проводимых мероприятий по обеспечению безопасности и устойчивости исследуемых объектов, направленные на переосмысление риска и пересмотр превентивных мер по его снижению.

Вторая категория средств, используемых в процессе управления жизнеспособностью критических инфраструктур, согласно исследованиям [6,7], объединяет методы, которые различаются методологическими подходами к моделированию сложных систем, а именно:

– эмпирические методы, основанные на глубоком каузальном анализе статистических данных и экспертных знаний о типовых источниках угроз, инициирующих неблагоприятные события в работе критических инфраструктур, и характере их реализации в этих системах, что позволяет выявлять закономерности сбоев и отказов, а также установить и количественно оценить степень взаимозависимости показателей качества функционирования системы и влияющих ситуационных факторов;
– метод системной динамики, основанный на нисходящем подходе к анализу сложных динамических систем с взаимозависимыми параметрами и моделирующий поведение этих систем через уровни, потоки и петли обратной связи;
– методы сетевого планирования и когнитивного моделирования, позволяющие проводить анализ рисков нарушения безопасности критических инфраструктур на графе (сетевой модели), узлы которого представляют собой критически важные объекты этой инфраструктуры, а дуги - физические и относительные взаимосвязи между этими объектами, что обеспечивает за счет имитации воздействия на узлы системы негативных факторов оценку возмущения и реакции элементов критической инфраструктуры на системном уровне, а также возможность исследования каскадных сбоев и отказов в работе системы в целом;
– методы агентного имитационного моделирования, основанные на восходящем подходе к анализу сложных динамических систем [8, 9] и описывающие функционирование критических инфраструктур в виде совокупности взаимодействующих друг с другом и внешней средой

автономных агентов с заданными правилами поведения, имитирующих как логику работы реальных элементов критических инфраструктур, так и их реакцию на внутренние и внешние воздействия.

Среди прочих методических подходов можно выделить: методы нечеткой логики, сценарного анализа и информационного управления, в том числе «концептуальные рамки» [10, 11]; методы аналогового и дискретно-событийного моделирования; вероятностные методы моделирования в реальном масштабе времени; методы теории клеточных автоматов; методы экономической теории; метод Монте-Карло; деревья решений; аналитические и численные математические модели и методы, описывающие зависимости характеристик, режимы работы и поведение исследуемого класса систем; другие гибридные методы и инструменты моделирования, используемые, например, в современных геоинформационных и интеллектуальных информационно-аналитических системах.

Вместе с тем, ситуационное управление [12] такими сложными трудноформализуемыми объектами информатизации, как критические инфраструктуры, требует проведения регулярной оценки и анализа состояния защищенности и устойчивости компонентов этих инфраструктур в условиях воздействия множественных угроз различной природы. Для этих целей необходим соответствующий аналитический инструментарий оценки системных рисков нарушения жизнеспособности и безопасности критических инфраструктур.

Классификация моделей и средств анализа жизнеспособности сложных систем предложена в работах [7,13], в которых рассматриваются качественные и количественные подходы к управлению и оценке жизнеспособности. Первый класс оперирует методами, позволяющими получить интегральные оценки жизнеспособности системы на качественном уровне без учета количественных измерений характеристик функционирования системы. В этом классе дополнительно выделяют методы концептуального анализа жизнеспособности сложных систем, основанные на зарубежных практиках управления риском и безопасностью, а также определяющие принципы и характеристики жизнеспособных систем, и методы полуколичественного анализа, обеспечивающие оценку жизнеспособности систем на основе коллективных экспертных знаний о различных качественных аспектах жизнеспособности в заданных условиях и ограничениях.

Второй класс оперирует количественными методами, основанными на детерминированных и стохастических моделях оценки жизнеспособности, описывающих характер поведения статических и динамических систем соответственно, а также определяющими выбор стратегии управления жизнеспособностью путем сравнения общей эффективности функционирования системы до и после возникновения критической ситуации, не сосредотачиваясь на конкретных рабочих характеристиках системы. В этом же классе отдельно выделяют структурные методы анализа, исследующие влияние системы на ее жизнеспособность посредством наблюдения за динамикой структуры системы, поведением системы и моделирования ее динамических характеристик во времени.

Еще одна классификация существующих подходов к управлению рисками и анализу жизнеспособности сложных систем представлена в работе [14]. Согласно этой классификации принято выделять индикаторные методы, основанные на измерении показателей (метрик) жизнеспособности систем, и моделирующие инструменты, предполагающие исследование характеристик жизнеспособности на различных типах моделей. Первый класс использует индикаторную систему оценки измеряемых характеристик жизнеспособности, построенную на основе общих и специфических групп показателей жизнеспособности для конкретных условий, и обеспечивает получение агрегированной оценки жизнеспособности системы по совокупности этих показателей с учетом целей и ограничений на управление. Второй класс включает методы сценарного анализа и моделирования жизнеспособности, обеспечивающие определение общей эффективности системы по совокупности обобщенных показателей качества функционирования и конфигурации системы. Эти методы основаны на использовании математических и физических моделей реальной системы и ее окружения, а также требуют знаний о критических функциях системы, ее задачах, целях, временных закономерностях, предельно-допустимых значениях рабочих характеристик, способностях системы к запоминанию, обучению и адаптации в меняющихся условиях обстановки.

Согласно материалам исследования [13], известные подходы к решению проблем обеспечения жизнеспособности критических инфраструктур методологически являются либо централизованными с позиций теории управления, либо основанными на резервировании с точки зрения теории надежности. Учитывая реальную природу критических инфраструктур и децентрализацию функций управления различными аспектами жизнеспособности этого класса систем, централизованные подходы зачастую недостаточно эффективны, а ре-

ализация механизмов резервирования, требующая существенных затрат и приводящая, как правило, к избыточности системы, не всегда технически осуществима на практике, в частности, при управлении распределенными системами, включающими большое количество физических объектов и управляющих элементов, в том числе участников процессов принятия решений.

Исходя из рассмотренных выше классификаций, агентно-ориентированный подход и мультиагентные системы относятся к классу средств управления жизнеспособностью критических инфраструктур, основанных на методах моделирования и исследования модельных представлений сложных взаимосвязанных объектов управления, имеющих распределенную гетерогенную структуру. Агентные технологии обеспечивают возможность повышения жизнеспособности таких объектов за счет поддержания высокой степени про-активности/автономности принятия решений элементами системы управления, что позволяет своевременно обнаруживать критические ситуации и реагировать на них, а также оперативно адаптировать поведение объекта управления к этим ситуациям, используя арсенал методов искусственного интеллекта и социальные метафоры (модели) киберфизических систем [15]. Мультиагентная парадигма [16] на протяжении последних десятилетий вполне успешно зарекомендовала себя на практике как эффективный инструмент поддержки управления организационными и техническими системами различного уровня и, следовательно, может быть адаптирована для класса задач обеспечения жизнеспособности сложных систем, в нашем конкретном случае - критических инфраструктур.

Функциональная структура управления жизнеспособностью и рисками нарушения безопасности критических инфраструктур с использованием мультиагентных систем поддержки принятия решений приведена на рис. 1.

Мультиагентный подход обеспечивает децентрализованное решение проблемы единой точки отказа (когда потеря функциональности хотя бы

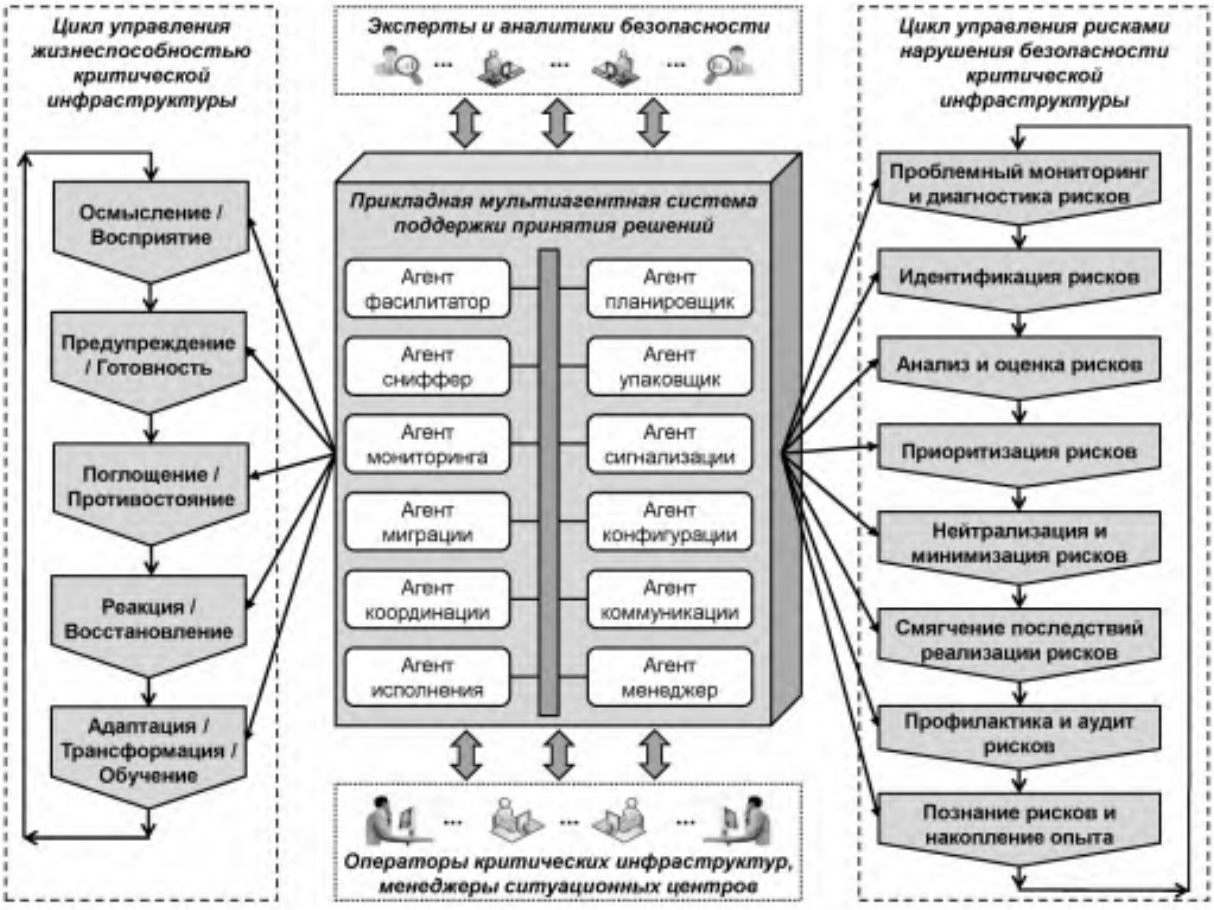

Рис. 1. Структура мультиагентного управления жизнеспособностью и безопасностью критических инфраструктур

одного элемента системы приводит к неработоспособности системы в целом), присущей централизованным решениям. Подход подразумевает, что каждый агент автономен и выполняет определенную роль в системе, в которой отсутствует иерархия контроля (глобальная управляемость), данные распределены, а локальные решения принимаются независимо и децентрализовано. За счет свойства автономности и способности к самоорганизации мультиагентные системы могут поддерживать свою работоспособность в случае потери функциональности ее отдельных элементов или связи между ними, а также в случае потери данных или масштабирования системы, что позволяет избежать избыточности (дублирования) программных компонентов и технических средств, используемых в управлении физическими объектами реального мира. Кроме того, по сравнению с традиционными методами, мультиагентный подход опирается на когнитивную науку и психологию для имитации когнитивных функций управляющих агентов, как в процессе принятия решений, так и в групповой самоорганизации.

Обзор научной литературы показал, что исследования вопросов применения технологии мультиагентных систем для управления жизнеспособностью критических инфраструктур носят точечный характер, то есть ориентированы на узкие приложения, например, анализ и решение проблем повышения жизнеспособности социотехнических, киберфизических, энергетических и контрольно-измерительных систем с иерархической или сетевой структурой [8, 17, 18].

2. Принципы построения мультиагентных систем управления

Для всех типов критических инфраструктур (мягкие/жесткие), классифицируемых как крупномасштабные системы, имеющие конкретные физические характеристики и свои индивидуальные особенности, опираясь на анализ современной научной литературы, можно сформулировать достаточно общие принципы построения прикладных мультиагентных систем поддержки управления жизнеспособностью этих инфраструктур в независимости от рассматриваемой области жизнеспособности - технологической, организационной и т.д. К этим принципам относятся следующие:

1. *Принцип изоморфизма*. Архитектура мультиагентной системы, включающая агенты и отношения между ними, должна взаимно-однозначно соответствовать моделируемой структуре организационного управления (участники, объекты/процессы и связи между ними) критической инфраструктурой.

2. *Принцип независимости*. Состав и физические характеристики критической инфраструктуры определяют минимальное количество независимых активных управляющих элементов (агентов), необходимых для полного и адекватного описания функционирования и степеней свободы этой инфраструктуры с учетом наложенных ограничений на управление.

3. *Принцип существования*. Для каждого участника процесса принятия решений по управлению жизнеспособностью критической инфраструктуры или физического элемента этой инфраструктуры в мультиагентной системе управления должен существовать хотя бы один активный элемент – агент, определяющий его целеполагание и выполняющий заданные функции, направленные на поддержание жизнеспособности критической инфраструктуры с учетом определенной ресурсоемкости и имеющихся физических возможностей.

4. *Принцип функционального разнообразия*. По своей структуре агенты должны быть многофункциональными и поддерживать весь спектр операций в рамках жизненного цикла управления жизнеспособностью критических инфраструктур: от проблемного мониторинга и предобработки информации о нештатных ситуациях до оценки рисков и анализа последствий реализации угроз нарушения жизнеспособности критических инфраструктур. При выборе конкретной функции агенты должны учитывать неоднородную структуру инфраструктурных систем, детерминированную и стохастическую природу, протекающих в них процессов, ресурсные возможности и ограничения на управление. Агенты должны моделироваться через определенный набор признаков (критериев), например: качество выполнения задания (высокое, среднее, низкое); скорость выполнения задания (высокая, средняя, низкая); используемый ресурс (малый, средний, большой) и т.п.. В результате, подбор подмножества агентов для выполнения конкретного задания становится нетривиальной задачей: какой выбрать агент, который быстро выполняет задание, но расходует большой ресурс, или же агент, который выполняет задание медленно, но при этом ресурс расходует экономно. Ответить на эти вопросы помогают многокритериальные методы для описания неоднородных агентов [19, 20].

5. *Принцип интеграции*. Для эффективной информационной поддержки управления жизнеспособностью критических инфраструктур агенты должны объединяться в коллективы (коалиции) на

разных уровнях принятия решений, а сама мультиагентная система должна отражать физическую интеграцию управляющих элементов (центров управления или отдельных акторов), деятельность которых она моделирует в виртуальной среде.

6. *Принцип пригодности*. Мультиагентная система поддержки принятия решений должна обеспечивать возможность использования функционала агентов для моделирования и анализа процессов управления жизнеспособностью критической инфраструктуры в условиях неопределенности, высокой динамики степеней свободы инфраструктурной системы и заданных ограничений.

7. *Принцип взаимодействия*. Для совместной деятельности при решении задач управления жизнеспособностью критической инфраструктуры агенты должны взаимодействовать друг с другом на всех уровнях управления и принятия ращений, а мультиагентная система должна поддерживать стандартные языки, модели и средства коммуникации агентов, независящие от выбранной методологии разработки мультиагентной системы и ограничений на управление. К специализированным агентным языкам, применяемым в имитационных моделях, относятся, например, РДО, Microsoft Axum [8, 9] и другие языки программирования агентов [21]. В виртуальной среде управления глобальное поведение системы однозначно определяется взаимодействием между распределенными агентами.

8. *Принцип самоорганизации*. В условиях динамически меняющейся внешней среды и показателей функционирования критических инфраструктур мультиагентная система должна обладать потенциалом к самоорганизации, то есть способностью к реконфигурации своих ресурсов и активных элементов (агентов) под новые условия исходной задачи, в том числе при наложении дополнительных ограничений на управление жизнеспособностью. При этом система не должна становиться избыточной и терять управляемость в области воздействия на физические элементы моделируемой критической инфраструктуры. Кроме того, запуск адекватных ситуаций механизмов перенастройки и реконфигурации, например, механизма самоорганизации агентов на основе градиентных вычислительных полей [22], должен быть предусмотрен как на уровне агентов, так и мультиагентной системы в целом. Поскольку один и тот же процесс реконфигурации может потребовать существенных ресурсных затрат в зависимости от выбранного механизма самоорганизации, мультиагентная система должна обеспечивать полноту и разнообразие используемых информационных ресурсов и сервисов агентов, что непосредственно влияет на способность системы управления к реконфигурации. Это особенно важно в поддержке управления жизнеспособностью на этапах восстановления и адаптации критических инфраструктур после воздействия множественных угроз.

9. *Принцип свободы действий*. Возможности, область действий и намерения агентов должны ограничиваться целями и сферой ответственности участников процессов управления жизнеспособностью критических инфраструктур, деятельность которых агенты имитируют в виртуальной среде, и согласовываться с реальной картиной, отражающей физическое состояние элементов критических инфраструктур на всех этапах жизненного цикла управления жизнеспособностью. Чем выше функциональная и информационная мощность агентов и чем выше динамичность их взаимодействия друг с другом, тем выше степень свободы агентов, а также вариативность действий и гибкость, которыми они обладают для поиска и генерации оптимальных решений ситуационного управления в условиях неполноты и нечеткости информации о состоянии жизнеспособности критических инфраструктур.

10. *Принцип инкапсуляции*. Агент, моделирующий конкретный физический объект критической инфраструктуры или акторов, управляющих жизнеспособностью этой инфраструктуры, должен быть реализован как программная сущность, основанная на знаниях и способная агрегировать внутри себя разноплановую информацию о состоянии жизнеспособности критических инфраструктур и их элементов, а также применять методы и средства автоматизированной обработки и анализа этих данных для решения задач, стоящих перед мультиагентной системой. При этом агент должен иметь возможность предоставления доступа к своим ресурсам и сервисам другим агентам по запросу, если возможности последних ограничены в силу каких-либо обстоятельств.

12. *Принцип интероперабельности*. Для совместного использования разнородных информационных ресурсов и сервисов, а также их интеграции в единую виртуальную среду управления, мультиагентная система должна поддерживать современные стандарты интероперабельности активных компонентов распределенных информационно-управляющих систем на технологическом, семантическом и организационном уровнях взаимодействия агентов и связанных с ними веб-сервисов. К таким стандартам относятся, например, специализированные FIPA [23] и IEC61499 [24], а также общепринятые ГОСТ Р 55062-2012, LISI, SCOPE

и DODAF, подробно рассмотренные в научных работах [25, 26]. Формирование профилей интероперабельности на уровне протоколов, интерфейсов и процессов является важной задачей при разработке агентов и прикладных мультиагентных систем управления жизнеспособностью критических инфраструктур. Кроме того, при создании данного класса систем необходимо применять единые подходы, основанные на отечественных и зарубежных методиках и открытых стандартах инфокоммуникационных технологий, регламентирующих обеспечение функциональной совместимости элементов этих систем.

Вместе с тем, стоит отметить, что структурная сложность объектов, образующих различные типы критических инфраструктур, моделируемых и управляемых агентами, в совокупности с динамическими характеристиками жизнеспособности этих инфраструктур во многом предопределяют структуру и состав проектируемых прикладных мультиагентных систем управления, однако архитектура агентов и самих систем может быть в общем случае унифицированной.

12. *Принцип системной динамики*. Жизнеспособность – это динамичная предметная область, а критические инфраструктуры – это пространственно-распределенные сложные динамические системы, развивающиеся во времени. Мультиагентные системы, нацеленные на мониторинг и управление поведением таких комплексных объектов, должны оперировать развитыми моделями принятия решений и средствами прогнозирования, учитывающими как динамические характеристики критических инфраструктур, так и саму динамику показателей жизнеспособности, изменяющихся в реальном масштабе времени. Кроме того, используемые модели должны максимально подробно описывать поведение критических инфраструктур во всех измерениях жизнеспособности, для которых требуется эффективное принятие решений, и моделировать динамику показателей жизнеспособности и управляющих воздействий как в непрерывном, так и в дискретном времени.

13. *Принцип дискретизации*. Область действий агентов должна быть ограничена во времени, то есть агент-регулятор или агент-исполнитель вырабатывают управляющие воздействия на элементы критических инфраструктур строго в определенные дискретные моменты времени. При этом в мультиагентной системе динамические характеристики моделируемой критической инфраструктуры должны контролироваться в реальном времени как минимум одним агентом, способным принимать своевременные решения при заданных условиях в пределах своих полномочий и компетенций.

14. *Принцип координации*. Принимаемые решения агентами системы на всех уровнях управления жизнеспособностью критических инфраструктур должны быть согласованными во времени и в пространстве, а также не противоречить логике функционирования реальной физической системы. Для этого в мультиагентной системе должны быть реализованы методы согласования распределенного управления, основанные на моделях активных систем [27] и принципах координации путем «развязывания» и прогнозирования взаимодействий, известных в теории иерархических многоуровневых систем [28, 29]. Таким образом, агенты должны действовать согласованно для достижения глобальной цели системы.

15. *Принцип децентрализации*. Каждый агент в мультиагентной системе управления должен строго иметь свою зону ответственности, регулировать конкретные характеристики моделируемой физической системы и выполнять возложенные на него функции независимо от других агентов. Несмотря на то, что иерархическое подчинение агентов неизбежно, но малоэффективно, при управлении жизнеспособностью таких крупномасштабных систем, как критические инфраструктуры, агенты должны иметь возможность делегировать часть своих функций другим агентам в случае, когда требуется реализовать групповое принятие решений в условиях многокритериальности или большой размерности глобальной задачи системы. Для этого мультиагентная система должна обеспечивать сетевой принцип организационного управления с выделенными управляющими центрами. При этом агенты, распределяющие подзадачи внутри локально сформированных иерархий агентов, выступают в роли центров координации и контролируют эквивалентность иерархии агентов декомпозиции глобальной задачи системы, а также процессы дискретизации действий агентов во времени на основе анализа связей между агентами и динамики рабочих характеристик управляемой системы (критической инфраструктуры). Децентрализация функций управления позволяет агентам системы поддерживать приемлемую для заданных условий работоспособность элементов критических инфраструктур в случае возникновения непредвиденных событий и нештатных ситуаций.

16. *Принцип автономности и про-активности*. В распределенной мультиагентной системе поддержки принятия решений, моделирующей процессы ситуационного управления жизнеспособностью критических инфраструктур, агенты должны функционировать как целеустремленные автоном-

ные программные сущности и активно реагировать на возможные изменения внешней среды и действия других агентов, на основе чего планировать стратегию своего поведения в будущем. У агентов должна быть предусмотрена собственная внутренняя логика или интеллектуальный механизм принятия решений, что не требует тотального контроля над их деятельностью в процессе достижения глобальной цели системы или решения конкретной задачи, то есть агенты работают по гетерархическому принципу [30].

17. *Принцип открытости.* Для обеспечения возможности системной интеграции новых программных компонентов в единую мультиагентную систему, ее модификации и обновления интерфейсы агентов системы и спецификации интегрируемых компонентов должны быть реализованы с использованием непроприетарных средств и открытых стандартов. Открытые мультиагентные системы ориентированы на работу в динамических распределенных средах и поддерживают совместимость и переносимость агентов и внешних приложений (сервисов). При этом агенты свободно обмениваются данными, взаимодействуют друг с другом и имеют доступ к внешним ресурсам за счет унификации регламентов и форматов коммуникации. Здесь стоит также отметить большой потенциал специальных языков программирования агентов [8, 9, 21] в обеспечении указанных возможностей.

18. *Принцип репликации*. Общесистемная (глобальная) информация и знания должны быть доступны всем агентам системы и использоваться централизованно, что положительно влияет на эффективность процесса принятия решений. Специфичная информация, требуемая для решения конкретной задачи, генерируется самими агентами локально, тиражируется и предоставляется другим агентам по запросу в ходе распределенного принятия решений. Для этих целей в мультиагентной системе, как правило, реализуются специальные сервисы обмена данными и стандартные модели коммуникации, например, «витрина задач», «доска объявлений», «круглый стол» и др. [31], позволяющие в той или иной степени удовлетворить информационные потребности агентов.

19. *Принцип «дружественности»*. В идеале агенты системы не должны находиться в антагонизме по отношению друг к другу, а должны придерживаться рационального и альтруистичного поведения, несмотря на конкуренцию в вопросах распределения и использования ресурсов системы. Для реальных задач управления безопасностью и жизнеспособностью критических инфраструктур на практике не всегда удается достичь однотипного поведения всех акторов, поэтому в мультиагентной системе должна быть реализована возможность гибкой настройки поведения управляющих агентов, цели и предпочтения которых могут естественным образом меняться в процессе индивидуальной адаптации к изменению ситуации. Кроме того, стоит отметить, что асимметрия намерений субъектов управления и их стремление доминировать в информационном поле характерны для большинства децентрализованных систем принятия решений в этой сфере. Однако при этом сохраняются риски потери управляемости и не достижения глобальной цели системы.

20. *Принцип самовосприятия*. Для анализа собственного состояния и потенциала других агентов системы, а также адаптации к меняющимся условиям архитектура агентов должна включать имитационный аппарат [32] или упрощенные модели внутреннего состояния и внешней среды. Это позволяет агентам строить и выбирать стратегию своего поведения, опираясь на прогноз деятельности других агентов и изменений внешней среды, а также находить баланс между имеющимися в их распоряжении возможностями и системными ресурсами при выполнении заданных функций и задач. Агентное имитационное моделирование [8, 9] хорошо зарекомендовало себя для исследования природоподобных и социальных систем. Поэтому, при агентном моделировании процессов управления жизнеспособностью критических инфраструктур прослеживаются определенные аналогии с моделями биологических систем.

21. *Принцип локализации (размещения).* Любая мультиагентная система должна быть развернута на агентной платформе, которая встроена в существующую информационно-коммуникационную инфраструктуру, а агенты системы должны функционировать в рамках определенной вычислительной или физической среды, имея возможность косвенно или напрямую воздействовать на ее составные части или процессы, а также воспринимать возмущения этой среды и ее отдельных элементов.

22. *Принцип «качества обслуживания»*. Работоспособность мультиагентной системы поддержки принятия решений для таких сложных объектов управления, как критические инфраструктуры, должна максимально не зависеть от обстоятельств непреодолимой силы, то есть форс-мажорных событий, например, отключение электроэнергии, что приведет к потере связи между агентами, нарушению функциональности системы в целом и будет замедлять процесс принятия решений в условиях критических ситуаций. Особенно ощутимо это от-

разиться на уровне оперативного управления. Для предотвращения подобных инцидентов в мультиагентной и соответственно физической системах должны быть предусмотрены резервные каналы связи, чтобы взаимодействие между агентами не прерывалось. Однако это может быть технически сложно реализовать и является весьма ресурсозатратным с точки зрения сервисной поддержки и регулярного обслуживания. Потеря актуальной информации и управляющих сигналов в результате сбоев в работе информационно-коммуникационной инфраструктуры снижает общую эффективность деятельности агентов системы кризисного реагирования. Вместе с тем, время жизни агентов может быть ограничено сроком решения поставленных перед ними задач или продолжительностью оказания информационных услуг (предоставление сервисов) другим агентам системы. Таким образом, требования обеспечения эксплуатационной надежности и живучести элементов моделируемой физической системы должны быть заложены в логику работы мультиагентной системы управления на этапе ее проектирования.

Приведенные принципы обеспечивают общую методологическую основу разработки прикладных мультиагентных систем поддержки принятия решений и призваны повысить эффективность управления жизнеспособностью сложных динамических систем, в частности, критических инфраструктур, за счет практической реализации и внедрения этих систем. На практике рассмотренные принципы нашли применение при проектировании мультиагентных приложений, например, в сфере управления жизнеспособностью транспортных, банковских, энергетических, телекоммуникационных и производственных инфраструктурных систем [33, 34], представляющих собой совокупность взаимосвязанных критически важных объектов и коммуникаций, нацеленных на обеспечение устойчивого функционирования городов и даже регионов. Обобщенная методология и принципы разработки прикладных мультиагентных систем управления жизнеспособностью критических инфраструктур представлены на рис. 2.

В дополнение к перечисленным принципам должны применяться базовые подходы организации систем обеспечения безопасности сложных социально-экономических объектов, которые лежат в основе теории и методологии управления жизнеспособностью критических инфраструктур, а именно [35]:

1. *Принцип локальности*. Этот принцип заключается в парировании и локализации возможных угроз и опасностей на начальной фазе их зарождения (до развития) посредством создания особых условий, препятствующих возникновению и распространению негативных факторов и тенденций и, в то же время, выгодных с экономической точки зрения. Данный принцип применяется однократно или многократно в зависимости от специфики постановки решаемой задачи обеспечения безопасности/жизнеспособности критических инфраструктур.

2. *Принцип глобальности*. Этот принцип состоит в более широкой многоуровневой организации управления безопасностью/жизнеспособностью критических инфраструктур и реализуется в тех случаях, когда нарушается принцип локальности, либо применение последнего недостаточно эффективно. Данный принцип представляет собой надстройку над принципом локальности и призван обеспечить благоприятные условия существования и функционирования системы (критической инфраструктуры) при возникновении глобальных угроз за счет упорядочивания и регулирования взаимодействия элементов критической инфраструктуры и внешней среды.

3. *Принцип функциональной декомпозиции*. Применение этого принципа предполагает реализацию двух защитных механизмов (специальных мер, выстроенных по системному принципу): внутренний механизм обеспечения безопасности/жизнеспособности критической инфраструктуры, интегрированный в потенциально уязвимые области ее функционирования, и внешний механизм противодействия множественным угрозам. Внешний механизм защиты реализует модели и методы, обеспечивающие приемлемые условия для нормального функционирования и поступательного развития критической инфраструктуры, то есть минимально допустимый уровень воздействия на нее негативных факторов, приводящих к отклонению показателей жизнеспособности от нормативных значений. Внешний механизм обеспечения жизнеспособности нацелен на достижение состояния защищенности критических инфраструктур от воздействия множественных угроз и их проникновения в критически важные объекты, образующие эти инфраструктуры. Внутренний механизм защиты обеспечивает парирование и локализацию внутренних угроз жизнеспособности (структурных трансформаций и возмущений, порождаемых элементами критических инфраструктур в результате самоорганизации), а также внешних угроз жизнеспособности (воздействий, продуцируемых окружающей средой и преодолевших внешний защитный механизм). Другими словами, внутренний механизм

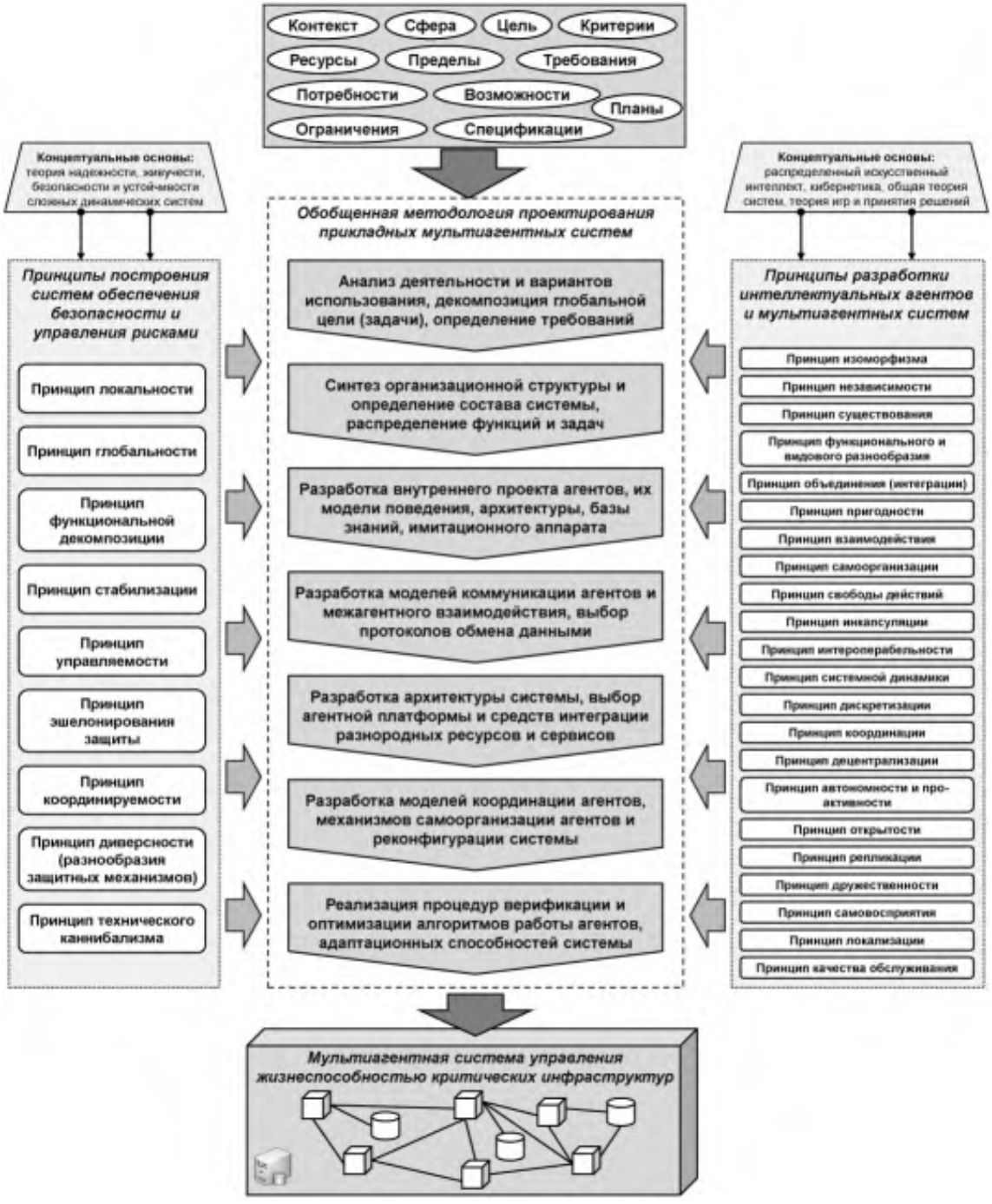

Рис. 2. Концептуальные основы и принципы разработки мультиагентных систем управления жизнеспособностью критических инфраструктур

обеспечения жизнеспособности ориентирован своими мерами на поддержание динамического равновесия элементов критической инфраструктуры (системного гомеостаза) и удержание их критических параметров в области безопасности/устойчивости за счет саморегуляции и адаптации системы. Использование принципа, базирующегося на рассмотренных механизмах защиты, в теории жизнеспособности позволяет более глубоко исследовать природу происхождения внутренних и внешние угроз, а также различать их при решении проблем управления безопасностью/жизнеспособностью критических инфраструктур и других сложных систем.

4. *Принцип стабилизации*. Этот принцип может рассматриваться применительно как к исследуемому классу систем (критических инфраструктур), так и к конкретной ситуации при взаимодействии отдельных элементов системы друг с другом и с внешней средой в условиях действия параметрических возмущений. Критические инфраструктуры относятся к классу сложных развивающихся целеустремленных систем, структура и функции которых изменяются с течением времени. При этом с позиции общей теории систем и теории управления в процессе анализа их устойчивости на некотором фиксированном временном интервале такие системы можно рассматривать, как системы стабилизации типа «объект - регулятор», вследствие наличия органов управления, противодействующих внутренним и внешним возмущениям. Тогда задачи теории жизнеспособности сложных систем можно отождествить с задачами стабилизации. Принцип стабилизации предполагает реализацию комплекса мер по сохранению и движению системы в пространстве устойчивых состояний (области жизнеспособности), наблюдаемые характеристики которых в критических условиях могут динамически меняться и предопределять характер поведения системы. Как правило, на практике приходиться иметь дело с несколькими, функционально связанными областями безопасности/жизнеспособности в пространстве состояний критических инфраструктур, соответствующими множеству источников и каналов инициализации угроз в этих системах.

В качестве регулятора для компенсации возмущений используются механизмы управления, обеспечивающие формирование благоприятных условий для целенаправленного поведения объекта управления (в данном исследовании - критической инфраструктуры) [36]: «жесткое» институциональное управление через контроль ограничений и норм деятельности (координация управления на метауровне); «мягкое» мотивационное управление через изменение функций полезности и предпочтений субъектов управления путем введения системы штрафов и поощрений за выбор тех или иных действий (стимулирование деятельности субъектов); «гибкое» информационное управление через изменение информации (ситуационной осведомленности), которой оперируют субъекты управления в процессе выработки и реализации решений (адекватная ситуации информационно-аналитическая поддержка принятия решений). Нарушение стабильности системы приводит к неполадкам и коллизиям в ее функционировании, обусловленным развитием критических ситуаций и случайных процессов, которые на деле могут не поддаваться корректирующим управляющим воздействиям.

5. *Принцип управляемости*. Этот принцип характеризует достижение поставленных целей системой обеспечения безопасности/жизнеспособности критических инфраструктур. Для реализации данного принципа, как известно из практики, необходимо, чтобы органы управления безопасностью и жизнеспособностью критических инфраструктур имели возможность целенаправленно воздействовать на параметры состояния критически важных объектов, образующих эти инфраструктуры, а также, чтобы ресурсное обеспечение процесса управления было достаточным для решения задач на пути к цели и адекватным ей. Вместе с тем, для реализации управления критическими инфраструктурами должны быть выполнены требования наблюдаемости системы, обеспечивающие получение и доступ к информации о состоянии системы. Для этого широко применяются средства мониторинга и идентификации состояния функционирования критических инфраструктур. Для нелинейных динамических систем условие управляемости сопряжено с большими трудностями, тогда, как для линейных систем оно известно.

6. *Принцип эшелонирования защиты*. Этот принцип базируется на сетецентрическом подходе [36] к управлению жизнеспособностью критических инфраструктур и реализации механизма обеспечения жизнеспособности системы «в глубину» посредством развертывания многоуровневых распределенных систем ситуационного управления безопасностью. Примерами сетевой инфраструктуры безопасности на федеральном и региональном уровне являются системы распределенных ситуационных центров и центров управления регионом [37], соответственно. Сеть большая, решающих центров много и всем необходимо предоставить информацию, точно соответствующую текущей ситуации, для согласования управленческих решений и координации совместных действий. Содержательно принцип сетецентричности в теории жизнеспособности сложных систем подразумевает реализацию полностью или частично децентрализованной структуры организационного управления жизнеспособностью критически важных объектов, входящих в состав критических инфраструктур, с выделенными управляющими центрами, взаимодействие между которыми осуществляется на базе их интеграции в единое информационное пространство. Управляющие центры выполняют функции мониторинга, превентивной аналитики, фильтрации и контроля рисков, связанных с нарушением безопасности функционирования кри-

тических инфраструктур, а на основе прогнозов неблагоприятных событий формирует антикризисные меры по минимизации возможных последствий реализации угроз в каждой области жизнеспособности системы и обеспечению приемлемого уровня риска защищенности критически важных объектов.

7. *Принцип координируемости*. Этот принцип в теории жизнеспособности сложных систем реализуется путем контроля ограничений на управление. При таком способе координации должны выполняться принципы согласования взаимодействий и функций качества, а также постулат совместимости задач, решаемых элементами системы, по отношению к общей задаче системы. Под координацией понимается достижение согласованности в работе всех звеньев системы путем установления рациональных связей между ними, что обеспечивает получение оптимального решения общей задачи системы при оптимизации подзадач, решаемых подсистемами. Система координируема, если существует координирующий сигнал, обеспечивающий согласованность связующих входов и согласованность ожидаемых и фактических значений локальных функций соответственно.

8. *Принцип диверсности (разнообразия)*. Принцип диверсной защиты является одним из центральных как в теории безопасности, так и теории жизнеспособности сложных систем. Он реализуется как на объектовом (локальная диверсность), так и на инфраструктурном (глобальная диверсность) уровне организации крупномасштабных систем. Данный принцип нацелен на рациональное сочетание и распределение различных видов ресурсов и средств обеспечения безопасности на всех уровнях ситуационного управления жизнеспособностью критических инфраструктур. Это необходимо для уменьшения вероятности (риска) нарушения работы группы критически важных объектов по общей причине. При создании систем ситуационного управления жизнеспособностью критических инфраструктур этот принцип подразумевает наличие и запуск многоверсионных механизмов резервирования (генерация двух или более резервных систем), оптимизирующих функционирование критически важных объектов по критериям «надежность - стоимость» или «безопасность (приемлемый риск) – готовность парирования», в случае деструктивного воздействия множественных внутренних и/или внешних угроз, в том числе необратимого характера. Принцип диверсной защиты ориентирован на адаптивные системы управления жизнеспособностью критических инфраструктур, способные к самоорганизации и работающие по непрограммируемой логике. Разнообразие в защите достигается за счет использования взаиморезервирующих каналов и элементов обеспечения безопасности, либо путем расширения существующей системы дополнительными средствами управления жизнеспособностью, построенными на принципиально иных методах и подходах. Параметрическое разнообразие, как правило, является программируемым и предполагает активацию и запуск адекватных ситуаций алгоритмов управления (регуляторов) на основе данных мониторинга за состоянием показателей жизнеспособности управляемой системы и контроля их допустимых значений. Применение принципа диверсности позволяет учитывать влияние человеческого фактора при решении задач управления безопасностью и жизнеспособностью критических инфраструктур.

9. *Принцип «технического каннибализма»*. Этот принцип предполагает использование ресурсов системообразующих элементов критических инфраструктур, деградировавших или утративших свою функциональность в результате воздействия множественных угроз, в интересах восстановления работоспособности других элементов этих инфраструктур для поддержания их жизнеспособности и системы в целом. Данный принцип реализуется в процессе трансформации и эволюции элементов критических инфраструктур, что зачастую обусловлено изменением их свойств, системных требований, высокой динамикой внешней среды и т.д., для адаптации систем управления жизнеспособностью к новым вызовам и меняющимся условиям функционирования. Это способствует рациональному выбору сил и средств по обеспечению безопасности и жизнеспособности критических инфраструктур в целях минимизации рисков потерь функциональности критически важных объектов этих инфраструктурных систем.

3. Преимущества мультиагентного подхода

При решении задач ситуационного управления мультиагентный подход, основанный на взаимодействии групп распределенных автономных агентов, и методы многокритериальной оптимизации, широко используемые в системах поддержки принятия решений, гармонично дополняют друг друга. При этом, по сравнению с другими инструментами информационной поддержки, мультиагентные системы обеспечивают такие неотъемлемые преимущества, как масштабируемость, расширяемость, локальную устойчивость, релевантность, прозрачность, автономность, контекстуальность, социальность и адаптивность:

– *Масштабируемость*. Мультиагентный подход обеспечивает более высокую гибкость при масштабировании системы информационной поддержки управления за счет интеграции дополнительных поставщиков информационных услуг, программных компонентов или веб-сервисов в общую структуру системы управления. При этом существенных изменений в концептуальную модель и логику работы этой системы в целом вносить не потребуется.
– *Расширяемость*. Мультиагентный подход обеспечивает более высокую гибкость при расширении (наращивании) функциональных возможностей системы управления за счет включения в процессы распределенного принятия ращений новых участников (агентов) «под задачу», обладающих требуемыми функциями и компетенциями для мониторинга и контроля состояния новых типов объектов управления в моделируемой физической системе. При этом реконфигурация информационной структуры принятия решений в целом не потребуется. Однако в случае, если внедряемые про-активные элементы влияют определенным образом на деятельность существующих агентов, то может потребоваться модификация структуры взаимосвязей между управляющими элементами мультиагентной системы или перераспределение функций управления.
– *Локальная устойчивость*. В процессе решения задач агенты объединяются в проблемно-ориентированные коалиции, образуя устойчивые центры принятия локальных решений в системе децентрализованного управления. Эти центры представляют собой виртуальные сети агентов, информационных ресурсов и сервисов, работающие по сетецентрическому принципу [38]. За счет этого мультиагентный подход обеспечивает более высокую гибкость при самоорганизации и адаптации системы управления в условиях возмущения внешней среды и изменения характеристик функционирования элементов моделируемой физической системы. Кроме того, это позволяет в целом отказаться от централизованного управления и изолированности локальных ресурсов, а также повышает ситуационную осведомленность и доступность сервисов агентов, что, в свою очередь, способствует быстрой реакции системы на изменение обстановки и выработке согласованных решений ситуационного управления.
– *Релевантность*. Серьезной проблемой для лиц, принимающих решения, при управлении сложными динамическими объектами является оперирование (получение, анализ, поиск, генерация) достоверной и релевантной информацией о состоянии рабочих характеристик этих объектов. Как автоматизированные средства поддержки управления, агенты призваны частично нивелировать эту проблему в части своевременной актуализации, регулярного обновления, анализа и контроля достаточной полноты управляющей информации, поступающей в систему из разнородных источников, как в дискретном режиме, так и в режиме реального времени, а также необходимой операторам для принятия обоснованных решений. Для этого агенты непрерывно взаимодействуют друг с другом и с внешней средой, оценивая влияние наблюдаемых ситуационных факторов и обмениваясь информацией о состоянии контролируемых параметров в зависимости от происходящих в системе событий. Кроме того, агентами обеспечивается оперативность распределенного принятия решений с минимальными задержками, которые могут быть вызваны продолжительным откликом централизованных служб или других элементов системы управления на целевые информационные запросы.
– *Прозрачность*. Автономные агенты, используемые для поддержки и оптимизации управления сложными системами, взаимодействуют в открытой децентрализованной виртуальной среде. Прозрачность этой среды определяется тем, что вся управляющая информация об агентах, о самой среде и моделируемых в ней объектах и процессах, открыта. Это достигается за счет коммуникации агентов, которые предоставляют друг другу информацию о своем текущем состоянии, имеющихся в их распоряжении ресурсах и собственных намерениях в ходе совместного решения задач управления. Несмотря на то, что агенты являются независимыми сущностями и ориентированы на самостоятельное принятие решений, за счет такого взаимодействия, восприятия среды и самообучения, обеспечивается более эффективное функционирование всей системы управления в целом. Вместе с тем, обобщенная модель деятельности агентов представляет собой «прозрачный ящик» [32], в котором отражаются внутренние механизмы функционирования агентов путем анализа собственного поведения, опыта других агентов, процессов саморегуляции и моделирования внешней среды.
– *Автономность*. Агентные технологии в управлении сложными объектами различной природы обеспечивают автономность активных программных компонентов систем управления этими объектами на оперативном, тактическом и стратегическом уровнях принятия решений, а также инкапсуляцию алгоритмов управления, но не дан-

ных, внутри агентов, что в целом снижает сложность управления крупномасштабными системами, характеризующимися высокой внутренней динамикой, полицентризмом, вариативностью и распределенностью структурных элементов этих систем, а также динамичностью параметров операционной и внешней среды.

– *Эксплицитная ситуативность (контекстуальность)*. Несмотря на вполне естественную ограниченность знаний агентов о всей управляемой системе и внешней среде, агентно-ориентированный подход обеспечивает полное погружение в контекст ситуации и ее всестороннее восприятие при управлении сложными распределенными объектами за счет взаимодействия групп управляющих агентов и связанных с ними сенсоров (датчиков), а также вариативность моделирования сценариев управления этими объектами в условиях ограниченности ресурсов на управление и ситуационной неопределенности. Встроенность агентов в среду, способность изменения ее состояния и учет контекста, в свою очередь, вкупе с последним позволяют строить более адекватную модель принятия решений для каждой конкретной ситуации и проводить более глубокую детализацию (декомпозицию) глобальной задачи системы, что уменьшает трудоемкость решения отдельных подзадач для достижения целей управления.

– *Социальность*. Мультиагентный подход позволяет гибко организовать высокоуровневое одноранговое взаимодействие между динамичными про-активными элементами кибер-физических и социотехнических систем (агентами, людьми, сенсорами, роботами и т.п.) за счет цифрового отображения физических объектов реального мира в виртуальное пространство с сохранением внутренней динамики, особенностей социального поведения, структуры взаимосвязей, логики и сценариев функционирования в процессе имитации этих объектов средствами цифровых двойников – интеллектуальных агентов.

– *Адаптивность*. Мультиагентный подход обеспечивает синтез адаптивных систем управления сложными распределенными объектами, обладающих способностью к самонастройке и самоорганизации. В процессе инициативных взаимодействий между агентами происходит обмен опытом и взаимообучение, а адаптационные способности системы управления в целом развиваются, что позволяет адекватно реагировать на изменения условий функционирования управляемого объекта с приемлемыми потерями его функциональности и расширить заранее запрограммированный репертуар возможных вариантов поведения для ситуаций, характеризующихся новизной и неопределенностью.

Заключение

В работе исследованы: стратегическая для обеспечения региональной безопасности предметная область – жизнеспособность критических инфраструктур, а также потенциал и перспективы применения мультиагентных систем для поддержки принятия управленческих решений в этой сфере. По результатам проведенного анализа современного состояния исследований в области разработки прикладных мультиагентных систем поддержки принятия решений установлено, что вопросы приложения агентных технологий для задач управления жизнеспособностью региональных критических инфраструктур недостаточно изучены как в теоретическом плане, так и на практике, в связи с чем требуют более детальной научной проработки. Вместе с тем, комплексная информационная поддержка всего жизненного цикла управления жизнеспособностью критических инфраструктур на базе мультиагентного подхода ранее не проводилась. В отечественной и зарубежной практике известны лишь независимые друг от друга фрагментарные технологические решения этой проблемы с применением средств мультиагентного моделирования и виртуальных анализаторов (агентов) для отдельных этапов жизненного цикла, например, связанные с мониторингом, сценарным анализом, аудитом и прогнозированием потенциальных угроз нарушения безопасности и устойчивости критических инфраструктур.

В ходе исследования предложены принципы построения прикладных мультиагентных систем поддержки принятия решений по управлению жизнеспособностью региональных критических инфраструктур, основанные на сопряжении общей методологии разработки мультиагентных систем и методических подходов к организации систем обеспечения комплексной безопасности критически важных объектов и ситуационному управлению их жизнеспособностью.

С теоретической точки зрения, полученные результаты развивают общую теорию безопасности сложных систем в части расширения потенциала применения мультиагентного подхода к управлению жизнеспособностью критических инфраструктур и разработки новых принципов синтеза адаптивных систем сетецентрического ситуационного управления безопасностью и жизнеспособностью критически важных объектов.

С практической точки зрения, полученные результаты в случае успешной реализации и верификации на практике могут быть использованы для повышения эффективности средств информационной поддержки стратегического и оперативного управления безопасностью и жизнеспособностью критических инфраструктур за счет обеспечения более высокого уровня автоматизации управленческой деятельности операторов региональных ситуационных центров, наряду с повсеместно применяемыми стандартными инструментами мониторинга и контроля для данного класса задач и объектов информатизации.

Вместе с тем, стоит отметить некоторые ограничения мультиагентных систем для управления жизнеспособностью критических инфраструктур, которые могут оказать влияние на эффективность их применения в реальной практике:

– системная сложность и, как следствие, сложность координации взаимодействий между большим числом агентов, моделирующих процессы функционирования критических инфраструктур в мультиагентной системе управления жизнеспособностью, что создает определенные трудности на этапах разработки, тестирования и технического обслуживания такой системы после введения в эксплуатацию;

– невысокая надежность в случае непредсказуемого поведения автономных агентов и несогласованности действий при совместном решении задач управления жизнеспособностью критических инфраструктур, по сравнению с централизованными системами обеспечения безопасности;

– уязвимость активных элементов (агентов) мультиагентных систем в плане рисков нарушения информационной безопасности, то есть вероятности возникновения кибератак или реализации других видов угроз, что недопустимо для таких объектов управления как критические инфраструктуры и что может привести к потере их управляемости средствами мультиагентных систем, а также к частичной или полной утрате своей жизнеспособности;

– высокая стоимость разработки, оценки рисков и внедрения мультиагентных систем управления жизнеспособностью критических инфраструктур, включая специализированные программно-технические средства, поддерживающих корректную работу этих адаптивных систем, отвечающих всем требованиям и стандартам обеспечения безопасности, надежности и устойчивости, принятых для данного класса объектов информатизации и управления;

– высокая трудоемкость непрерывного обучения/самообучения агентов и сложность организации этого процесса, что необходимо для принятия обоснованных решений агентами и что отражается на общей эффективности работы мультиагентной системы управления жизнеспособностью критических инфраструктур.

Дальнейшие исследования будут направлены, главным образом, на разработку научно-методологических основ проектирования прикладных мультиагентных систем поддержки принятия решений в сфере управления жизнеспособностью критических инфраструктур на базе предложенных принципов, а также их апробацию в структуре управления региональных ситуационных центров.

Литература

1. *Goonatilleke S.T., Hettige B.* Past, Present and Future Trends in Multi-Agent System Technology // Journal Européen des Systèmes Automatisés. 2022. Vol. 55, No. 6. P. 723-739.
2. *Dorri A., Kanhere S.S., Jurdak R.* Multi-Agent Systems: A Survey // IEEE Access. 2018. Vol. 6. P. 28573-28593.
3. *Wooldridge M.* An Introduction to MultiAgent Systems. 2nd Edition. John Wiley & Sons, 2009. 484 p.
4. *Поспелов Д.А.* Многоагентные системы – настоящее и будущее // Информационные технологии и вычислительные системы. 1998. № 1. С. 14-21.
5. *Сохова З.Б., Редько В.Г.* Моделирование поиска инвестиционных решений автономными агентами в прозрачной конкурентной экономике // Искусственный интеллект и принятие решений. 2019. № 2. С. 98-108.
6. *Ouyang M.* Review on modeling and simulation of interdependent critical infrastructure systems // Reliability Engineering and System Safety. 2014. Vol. 121. P. 43-60.
7. *Маслобоев А.В.* Формальные модели жизнеспособности региональных критических инфраструктур // Труды ИСА РАН. 2022. Т. 72. № 3. С. 59-80.
8. *Макаров В.Л., Бахтизин А.Р.* Социальное моделирование – новый компьютерный прорыв (агент-ориентированные модели). М.: Экономика. 2013. 295 с.
9. *Емельянов В.В., Ясиновский С.И.* Введение в интеллектуальное имитационное моделирование сложных дискретных систем и процессов. Язык РДО. М.: АНВИК. 1998. 432 с.
10. *Serfilippi E., Ramnath G.* Resilience measurement and conceptual frameworks: A review of the literature // Annals of Public and Cooperative Economics. 2018. Vol. 89. Iss. 4. P. 645-664.

11. *Andersson J., Grassi V., Mirandola R., Perez-Palacin D.* A conceptual framework for resilience: fundamental definitions, strategies and metrics // Computing. 2021. Vol. 103. P. 559-588.
12. *Поспелов Д.А.* Ситуационное управление. Теория и практика. 2 изд. М.: УРСС. 2021. 288 с.
13. *Hosseini S., Barker K., Ramirez-Marquez J.E.* A review of definitions and measures of system resilience // Reliability Engineering & System Safety. 2016. Vol. 145. 47-61.
14. *Linkov I., Kott A.* Fundamental concepts of cyber resilience: Introduction and overview // Cyber resilience of systems and networks. Risk, Systems and Decisions. Springer, Cham. 2019. P. 1-25.
15. *Kouicem E., Raiievsky C., Occello M.* Artificial emotions for distributed cyber-physical systems resilience // Proceedings of the Cyber-Physical systems PhD Workshop. 2019. P. 84-95.
16. *Ferber J., Weiss G.* Multi-agent systems: an introduction to distributed artificial intelligence. 1st Edition. Addison-Wesley Longman Publishing Co., Inc. Boston, MA USA. 1999. 509 p.
17. *Janu´ario F., Cardoso A., Gil P.* Multi-agent framework for resilience enhancement over a WSAN // 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON'2018). Chiang Rai, Thailand. 2018. P. 110-113.
18. *Janu´ario F., Cardoso A., Gil P.* A distributed multi-agent framework for resilience enhancement in cyber-physical systems // IEEE Access. 2019. Vol. 7. P. 31342-31357.
19. *Ройзензон Г.В.* Синергетический эффект в принятии решений // Системные исследования. Методологические проблемы. Ежегодник / Под ред. Ю.С. Попкова, В.Н. Садовского, В.И. Тищенко. № 36. 2011-2012. М.: УРСС, 2012. С. 248-272.
20. *Фоминых И.Б., Романчук С.В., Алексеев И.П.* Модель целеполагания в многоагентной системе с ограниченным ресурсом времени // Вестник МЭИ. 2018. № 5. С. 73-78.
21. *Cardoso R.C., Ferrando A.* A Review of Agent-Based Programming for Multi-Agent Systems // Computers. 2021. Vol. 10. No. 2. 16.
22. *Masloboev A.V.* A technology for dynamic synthesis and configuration of multi-agent systems of regional security network-centric control // Reliability and Quality of Complex Systems. 2020. No. 3(31). P. 112-120.
23. *Poslad S., Charlton P.* Standardizing Agent Interoperability: The FIPA Approach // Multi-Agent Systems and Applications. ACAI 2001. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2001. Vol. 2086. P. 98-117.
24. *Zoitl A., Lewis R.* Modeling control systems using IEC 61499 (Control, Robotics and Sensors). Second Edition. London: The Institution of Engineering and Technology. 2014. 248 p.
25. *Макаренко С.И.* Интероперабельность организационно-технических систем. Санкт-Петербург: Изд-во Наукоемкие технологии. 2024. 313 с.
26. *Маслобоев А.В.* Средства поддержки интероперабельности сетецентрических систем управления региональной безопасностью // Надежность и качество сложных систем. 2020. № 1(29). С. 91-105.
27. *Бурков В.Н., Новиков Д.А.* Теория активных систем: состояние и перспективы. М.: Синтег. 1999. 128 с.
28. Методы и модели согласования иерархических решений / Под ред. А.А. Макарова. Новосибирск: Наука. 1979. 240 с.
29. *Месарович М., Мако Д., Такахара И.* Теория иерархических многоуровневых систем. М.: Мир. 1973. 343 с.
30. *Ou-Yang C., Lin J.S.* The development of a hybrid hierarchical/heterarchical shop floor control system applying bidding method in job dispatching // Robotics and Computer-Integrated Manufacturing. 1998. Vol. 14. Iss. 3. P. 199-217.
31. *Тарасов В.Б.* От многоагентных систем к интеллектуальным организациям. Серия «Науки об искусственном». М.: УРСС. 2002. 352 с.
32. *Маслобоев А.В.* Гибридная архитектура интеллектуального агента с имитационным аппаратом // Вестник МГТУ: Труды Мурманского государственного технического университета. 2009. Т. 12. № 1. С. 113-124.
33. *Городецкий В.И., Скобелев П.О.* Многоагентные технологии для индустриальных приложений: реальность и перспектива // Труды СПИИРАН. 2017. № 6(55). С. 11-45.
34. *Baig Z.A.* Multi-agent systems for protecting critical infrastructures: A survey // Journal of Network and Computer Applications. 2012. Vol. 35. Iss. 3. P. 1151-1161.
35. *Masloboev A.V.* An overview of the regional security theory and methodological foundations // Reliability and Quality of Complex Systems. 2022. No. 2(38). P. 102-118.
36. *Маслобоев А.В.* Модель и технология поддержки принятия решений в условиях сетецентрического управления региональной безопасностью // Надежность и качество сложных систем. 2019. № 2(26). С. 43–59.

37. *Masloboev A.V.* Regional management center framework for G2C-feedback and public safety support // Reliability and quality of complex systems. 2021. No. 4(36). P. 127-138.
38. *Тихонов А.Н., Иванников А.Д., Соловьёв И.В., Цветков В.Я., Кудж С.А.* Концепция сетецентрического управления сложной организационно-технической системой. М.: МаксПресс. 2010. 136 с.

Маслобоев Андрей Владимирович. Институт информатики и математического моделирования им. В.А. Путилова, Федеральный исследовательский центр «Кольский научный центр Российской академии наук», г. Апатиты, Россия. Ведущий научный сотрудник. Доктор технических наук, доцент. Область научных интересов: системный анализ, моделирование социально-экономических систем, ситуационное управление, теория безопасности систем, мультиагентные системы. E-mail: masloboev@iimm.ru.

Principles of applied multi-agent system engineering for resilience management of critical infrastructures

A. V. Masloboev

Putilov Institute for Informatics and Mathematical Modeling of the Federal Research Centre “Kola Science Centre of the Russian Academy of Sciences”, Apatity, Russia

Abstract. The work is aimed at development of information technologies for intelligent decision-making support in the field of organizational management of the regional critical infrastructures resilience. This is urgent to enhance the efficiency of systems for ensuring the security and stability of these infrastructures under the influence of heterogeneous situational factors. The study is based on systematization, analysis and generalization of well-known methodological approaches to ensuring the reliability, security and resilience of complex dynamic entities, as well as methods of general system theory, principles of network-centric control and multi-agent modeling concepts. A general classification of analysis and simulation methods and techniques used in practice to management support of the critical infrastructures resilience is given. The crucial need for applying the multi-agent systems paradigm to management support of the critical infrastructures resilience is substantiated. For this purpose, the field-of-use advantages and potential restrictions of applying a multi-agent approach in management problems of critical infrastructures resilience are determined. Design principles of applied multi-agent decision support systems for overall resilience management of critical infrastructures, based on the conjugation of generic methodology for multi-agent systems engineering and technical approaches to organizing integrated security systems for critical facilities protection, have been proposed.

Keywords: *multi-agent system, management, information support, simulation, resilience, critical infrastructure.*
DOI: 10.14357/20790279240208 **EDN: OYAAOQ**

References

1. *Goonatilleke S.T., Hettige B.* Past, Present and Future Trends in Multi-Agent System Technology. Journal Européen des Systèmes Automatisés. 2022; 55(6): 723-739.
2. *Dorri A., Kanhere S.S., Jurdak R.* Multi-Agent Systems: A Survey. IEEE Access. 2018; 6: 28573-28593.
3. *Wooldridge M.* An Introduction to MultiAgent Systems. 2nd Edition. John Wiley & Sons. 2009; 484.
4. *Pospelov D.A.* Multi-agent systems – present and future. Information technologies and computing systems. 1998; 1: 14-21. (In Russ.)
5. *Sokhova Z.B., Redko V.G.* Modeling the search for investment decisions by autonomous agents in a transparent competitive economy. Artificial intelligence and decision making. 2019; 2: 98-108. (In Russ.)
6. *Ouyang M.* Review on modeling and simulation of interdependent critical infrastructure systems. Reli-

ability Engineering and System Safety. 2014; 121: 43-60.
7. *Masloboev A.V.* Formal models of the regional critical infrastructures resilience. Proceedings of the Institute of System Analysis of the Russian Academy of Sciences. 2022; 72(3): 59-80. (In Russ.)
8. *Emel'yanov V.V., Yasinovskiy S.I.* Introduction to intelligent simulation modeling of complex discrete systems and processes. RDO language. Moscow: ANVIK, 1998; 432. (In Russ.)
9. *Makarov V.L., Bakhtizin A.R.* Social modeling - a new computer breakthrough (agent-based models). Moscow: Ekonomika, 2013; 295. (In Russ.)
10. *Serfilippi E., Ramnath G.* Resilience measurement and conceptual frameworks: A review of the literature. Annals of Public and Cooperative Economics. 2018; 89(4): 645-664.
11. *Andersson J., Grassi V., Mirandola R., Perez-Palacin D.* A conceptual framework for resilience: fundamental definitions, strategies and metrics. Computing. 2021; 103: 559-588.
12. *Pospelov D.A.* Situational control. Theory and practice. 2nd Edition. Moscow: URSS, 2021; 288. (In Russ.)
13. *Hosseini S., Barker K., Ramirez-Marquez J.E.* A review of definitions and measures of system resilience. Reliability Engineering & System Safety. 2016; 145: 47-61.
14. *Linkov I., Kott A.* Fundamental concepts of cyber resilience: Introduction and overview. Cyber resilience of systems and networks. Risk, Systems and Decisions. Springer, Cham, 2019; 1-25.
15. *Kouicem E., Raiievsky C., Occello M.* Artificial emotions for distributed cyber-physical systems resilience. Proceedings of the Cyber-Physical systems PhD Workshop. 2019; 84-95.
16. *Ferber J., Weiss G.* Multi-agent systems: an introduction to distributed artificial intelligence. 1st Edition. Addison-Wesley Longman Publishing Co., Inc. Boston, MA USA. 1999; 509.
17. *Janu´ario F., Cardoso A., Gil P.* Multi-agent framework for resilience enhancement over a WSAN. 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON'2018). Chiang Rai, Thailand. 2018; 110-113.
18. *Janu´ario F., Cardoso A., Gil P.* A distributed multi-agent framework for resilience enhancement in cyber-physical systems. IEEE Access. 2019; 7: 31342-31357.
19. *Roizenzon G.V.* Synergetic effect in decision making. System Research. Methodological problems. Yearbook. In Yu.S. Popkov, V.N. Sadovsky, V.I. Tishchenko (eds.). Moscow: URSS, 2012; 36: 248-272. (In Russ.)
20. *Fominykh I.B., Romanchuk S.V., Alekseev I.P.* Model of goal setting in a multi-agent system with a limited time resource. Bulletin of MPEI. 2018; 5: 73-78. (In Russ.)
21. *Cardoso R.C., Ferrando A.* A Review of Agent-Based Programming for Multi-Agent Systems. Computers. 2021; 10(2): 16.
22. *Masloboev A.V.* A technology for dynamic synthesis and configuration of multi-agent systems of regional security network-centric control. Reliability and Quality of Complex Systems. 2020; 3(31): 112-120.
23. *Poslad S., Charlton P.* Standardizing Agent Interoperability: The FIPA Approach. Multi-Agent Systems and Applications. ACAI 2001. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2001; 2086: 98-117.
24. *Zoitl A., Lewis R.* Modeling control systems using IEC 61499 (Control, Robotics and Sensors). Second Edition. London, The Institution of Engineering and Technology, 2014; 248.
25. *Makarenko S.I.* Interoperability of organizational and technical systems. St. Petersburg: Publishing house Science-intensive technologies. 2024; 313. (In Russ.)
26. *Masloboev A.V.* Tools for interoperability support of network-centric systems for regional security management. Reliability and quality of complex systems. 2020; 1(29): 91-105. (In Russ.)
27. *Burkov V.N., Novikov D.A.* Theory of active systems: state and prospects. Moscow: Sinteg Publishing. 1999; 128. (In Russ.)
28. Methods and models for coordinating hierarchical decisions. In A.A. Makarov Eds. Novosibirsk: Nauka, 1979; 240. (In Russ.)
29. *Mesarovic M., Mako D., Takahara I.* Theory of hierarchical multi-level systems. Moscow: Mir Publishing. 1973; 343. (In Russ.)
30. *Ou-Yang C., Lin J.S.* The development of a hybrid hierarchical/heterarchical shop floor control system applying bidding method in job dispatching. Robotics and Computer-Integrated Manufacturing. 1998; 14(3): 199-217.
31. *Tarasov V.B.* From multi-agent systems to intelligent organizations. Series "Sciences of the Artificial". Moscow: URSS. 2002; 352. (In Russ.)
32. *Masloboev A.V.* Hybrid architecture of an intelligent agent with a simulation apparatus. Bulletin of MSTU: Proceedings of the Murmansk State Technical University. 2009; 12(1): 113-124. (In Russ.)
33. *Gorodetsky V.I., Skobelev P.O.* Multi-agent technologies for industrial applications: reality and

prospects. Proceedings of SPIIRAS. 2017; 6(55): 11-45. (In Russ.)
34. *Baig Z.A.* Multi-agent systems for protecting critical infrastructures: A survey. Journal of Network and Computer Applications. 2012; 35(3): 1151-1161.
35. *Masloboev A.V.* An overview of the regional security theory and methodological foundations. Reliability and Quality of Complex Systems. 2022; 2(38): 102-118.
36. *Masloboev A.V.* Model and technology of decision support in the conditions of network-centric management of regional security. Reliability and quality of complex systems. 2019; 2(26): 43–59. (In Russ.)
37. *Masloboev A.V.* Regional management center framework for G2C-feedback and public safety support. Reliability and quality of complex systems. 2021; 4(36): 127-138.
38. *Tikhonov A.N., Ivannikov A.D., Solov'ev I.V., Tsvetkov V.Ia., Kudzh S.A.* Concept of network-centric management of complex technical-organizational system. Moscow: MaksPress Publishing. 2010; 136. (In Russ.)

Masloboev Andrey V. Leading Researcher, Associate Professor, Doctor of Technical Sciences, Putilov Institute for Informatics and Mathematical Modeling of the Federal Research Centre «Kola Science Centre of the Russian Academy of Sciences», 14 Fersmana St., Apatity, Murmansk region, 184209, Russia.
E-mail: masloboev@iimm.ru.