

УДК 004.89, 004.942, 338.24

**АРХИТЕКТУРА И ТЕХНОЛОГИИ ФОРМИРОВАНИЯ ИНТЕГРИРОВАННОЙ
ИНФОРМАЦИОННОЙ СРЕДЫ ПОДДЕРЖКИ УПРАВЛЕНИЯ
БЕЗОПАСНОСТЬЮ РАЗВИТИЯ РЕГИОНА**

А.В. Маслобоев, М.Г. Шишаев

Рассматриваются задачи информационно-аналитической поддержки управления безопасностью развития социально-экономических систем регионального уровня и пути их решения на основе когнитивных информационных технологий и инструментов моделирования. Разработана концептуальная модель интегрированной информационной среды поддержки управления безопасностью развития региона. Предложены архитектура и технологии построения проблемно-ориентированных распределенных информационных систем поддержки управления региональной безопасностью на базе одноранговых телекоммуникационных сетей и мультиагентного подхода, обеспечивающие возможность интеграции разнородных информационных ресурсов и систем в рамках единого информационного пространства региона.

Ключевые слова: интегрированная информационная среда, когнитивный подход, информационная поддержка, управление, глобальная безопасность, региональное развитие, агентные технологии, одноранговая распределенная система.

Введение

В настоящее время особую значимость для арктических регионов РФ, превращающихся в одну из основных баз будущего развития страны, приобретают проблемы внешнего и внутреннего характера, связанные с обеспечением безопасности в различных сферах и уровнях организации социума. На современном и последующих этапах развития общественных отношений глобальная безопасность выступает важнейшим фактором устойчивого развития. Развиваемая авторами работы и их коллегами теория управления безопасностью регионального развития [1, 2], также как и концепция устойчивого развития [3], базируется на системном подходе, т.е. рассматривает объект управления (страну, регион, город, конкретную отрасль и т.п.) как систему. Это, в свою очередь, обеспечивает возможность использования современных достижений в сфере компьютерных технологий и методов моделирования для исследования функционирования региональных социально-экономических систем (СЭС) с целью разработки эффективных методов и средств поддержки управления безопасностью их развития.

Настоящая работа посвящена проблемам безопасности развития арктических регионов РФ. Отдельное внимание уделяется задачам создания моделей и технологий формирования целостной информационной среды поддержки управления безопасностью регионального развития. Предлагаемые решения основаны на когнитивном подходе, который заключается в комбинировании современных научных концепций и инструментов моделирования, таких как концептуальное моделирование, системная динамика, теория мультиагентных систем, математическая теория безопасности и др.

**Современное состояние исследований в области информационных технологий поддержки
управления глобальной безопасностью**

Существенным импульсом интенсификации отечественных исследований в рассматриваемой проблемной области во многом послужила разработка «Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2020 г.», а также принятие постановления Правительства РФ «Основы государственной политики Российской Федерации в Арктике на период до 2020 г. и дальнейшую перспективу» (от 18.09.2008 г., Пр.1969). В данных документах декларируется, что одной из главных целей государственной политики РФ в Арктике с точки зрения обеспечения безопасности и укрепления национальных интересов является развитие сферы информационных технологий и связи. Единое информационное пространство (ЕИП), сформированное с учетом специфических особенностей Арктической зоны (АЗ), должно обеспечить системообразующую основу при подготовке, планировании и реализации мероприятий государственной политики в Арктике [4]. Для этого необходима организация и проведение отдельных комплексных исследований в сфере создания и развития когнитивных компьютерных технологий информационно-аналитической поддержки управления безопасностью развития арктических регионов. Под когнитивными технологиями, согласно [5], в данном случае понимается широкий спектр технологий рационализации и формализации интеллектуальных систем создания и функционирования знаний, экспертизы, коммуникации и принятия решения. В настоящее время когнитивные технологии широко применяются в сфере прогнозирования и стратегического планирования развития сложных динамических систем.

На сегодняшний день создано большое количество ресурсов и технологий, обеспечивающих информационно-аналитическую поддержку ряда задач в области управления глобальной и региональной безопасностью. Современные отечественные и зарубежные системы информационной поддержки управления глобальной безопасностью разрабатываются, как правило, под конкретные задачи. Большинство из них реализовано в виде узкоспециализированных диспетчерских информационных систем, информационно-прогностических систем мониторинга социально-экономического развития, информационно-аналитических систем кризисного реагирования и поддержки принятия решений, систем пространственного позиционирования, а также web-ресурсов (Интернет-порталов), предоставляющих средства информационного взаимодействия субъектов и структур безопасности и обеспечивающих доступ к информационно-справочным ресурсам и нормативным документам на основе соответствующих информационных технологий.

Несмотря на столь широкий спектр существующих решений, перечисленные типы систем являются разнородными по своей технологической платформе, функциональному назначению и компонентному составу. Большинство из них традиционно имеют централизованную архитектуру, свои специфические протоколы информационного взаимодействия и форматы хранения и представления данных, что обуславливает их слабую интегрируемость и невозможность совместного использования для комплексного решения задач управления и обеспечения экологической, экономической, социальной и техногенной безопасности развития систем регионального или федерального уровня, реализации концепции приемлемого риска и своевременного предотвращения внутренних и внешних угроз безопасности на основе согласованного взаимодействия субъектов и организационных структур безопасности независимо от их организационной и административной разнородности и территориальной распределенности. Таким образом, существующие прикладные разработки в исследуемой проблемной области, ориентированные на решение частных задач управления безопасностью развития отдельных региональных подсистем, носят бессистемный и локальный характер и не обеспечивают достижение комплексного эффекта при решении рассматриваемого класса задач. Современные тенденции исследований в области создания и развития методов и средств интеграции разнородных информационных ресурсов и систем выводят задачу управления безопасностью интегрируемых систем на принципиально новый уровень, требующий развития концепции интегрируемости и разработки специализированных решений для создания единых информационных сред поддержки проблемно-ориентированной деятельности с учетом открытости, разнородности, про-активности и распределенности, интегрируемых в рамках их компонентов.

Концептуальная модель интегрированной информационной среды поддержки управления безопасностью региона

Реализация проекта по созданию на территории Мурманской области специализированного Центра исследований и обеспечения безопасности в Арктике предполагает формирование ЕИП региона для повышения эффективности согласованного взаимодействия организационных структур, на которые возложены функции по обеспечению безопасности функционирования конкретных региональных подсистем и их компонентов. В работе [6] под ЕИП понимается интегрированная информационная среда, которая рассматривается как комплекс проблемно-ориентированных, взаимоувязанных и взаимодействующих информационных подсистем. В рамках проводимых исследований поэтапное формирование ЕИП региона предполагает в итоге создание открытой расширяемой многофункциональной информационно-аналитической среды (инфраструктуры), ориентированной на поддержку управления комплексной безопасностью развития региональной СЭС, наделенной потенциалом к саморазвитию и способностью адаптации к динамичному стохастическому характеру функционирования внешнего и внутреннего окружения региона. В качестве технологической платформы для практической реализации и развертывания такой инфраструктуры предлагается использовать современные технологии одноранговых распределенных информационных систем (РИС) и интеллектуальные информационные технологии, в частности, технологию мультиагентных систем [7].

Использование технологии мультиагентных систем на основе сервис-ориентированной архитектуры (SOA – service-oriented architecture) позволит создать адекватную среду информационно-аналитической поддержки управления безопасностью развития региона, учитывая распределенность, динамичность и структурную сложность образующих его подсистем. Основу сервис-ориентированного подхода составляет принцип агентной ориентации, который заключается в использовании в качестве компонентов РИС интеллектуальных агентов, автономно функционирующих и обладающих целенаправленным поведением. При таком подходе агенты реализуются в виде web-сервисов. На интеллектуальных про-активных агентов могут быть возложены функции управления отдельными аспектами безопасности регионального развития, а на основе проблемно-ориентированных коалиционных взаимодействий агентов можно будет обеспечить эффективное функционирование самоорганизующейся инфраструктуры безопасности региона и ее отдельных компонентов, а также поддержание приемлемого уровня безопасности развития на перспективу. Техноло-

гии разработки распределенных мультиагентных систем на основе SOA и преимущества использования web-сервисов для реализации агентов представлены в работе [8].

В условиях распределенности и открытости информационной среды безопасности особенную важность приобретает задача обеспечения единого структурного представления и формализации такой среды. Эту задачу позволяет решить технология концептуального моделирования [9]. Формально агентно-ориентированная модель интегрированной информационной среды поддержки управления региональной безопасностью может быть задана в виде теоретико-множественных отношений и определяет состав и взаимосвязи основных компонентов региональной инфраструктуры безопасности. Модель информационной инфраструктуры безопасности региона (ИИБР) представляется в виде композиции множеств:

$$E_{\text{ИИБР}} = \{O, S, R, SS, CS, A, Z, P, U, I, Attr\}.$$

Основными элементами, образующими ее состав, являются: *O* – множество объектов безопасности (люди, предприятия, региональные подсистемы и т.д.); *S* – множество субъектов обеспечения безопасности; *R* – множество информационных ресурсов; *SS* – множество организационных структур (территориально-распределенных групп субъектов безопасности, объединенных общей целью), ответственных за обеспечение безопасности функционирования региональных подсистем и их компонентов; *CS* – множество виртуальных когнитивных центров управления безопасностью функционирования конкретных региональных подсистем, объединяющих агентов с общими целями и областями интересов, ориентированных на групповое решение задач управления безопасностью; *A* – множество когнитивных агентов субъектов обеспечения безопасности, представляющих интересы своих хозяев в распределенной мультиагентной виртуальной среде поддержки управления безопасностью; *Z* – множество задач в области обеспечения определенных видов безопасности регионального развития; *P* – множество процессов взаимодействия субъектов обеспечения безопасности при решении различных классов задач управления региональной безопасностью; *U* – множество серверных и клиентских узлов системы, на которых функционируют когнитивные программные агенты; *I* – отношения на множествах объектов модели; *Attr* – множество атрибутов объектов модели.

В модели явно представлены когнитивные программные агенты субъектов региональной безопасности как специальный тип объектов. Агенты обеспечивают имитацию деятельности субъектов безопасности в интегрированной информационной среде поддержки управления безопасностью, реализуют поиск потенциальных субъектов совместной деятельности и участвуют в формировании виртуальных организационных структур безопасности для решения задач управления безопасностью функционирования конкретных региональных подсистем. Отношения, представленные в модели, обеспечивают формализацию взаимосвязей и взаимодействия компонентов реальной социально-экономической среды и виртуальной среды безопасности региона.

Множество атрибутов объектов модели описывается следующим образом:

$$Attr = \langle T_A, T_R, T_O, F \rangle,$$

где T_A – множество типов агентов (web-сервисов); T_R – множество типов информационных ресурсов; T_O – множество типов (режимов) доступа к информационным ресурсам, например, on-line или off-line режимы; F – множество функций агентов.

Концептуальная модель интегрированной информационной среды поддержки управления региональной безопасностью за счет формального задания отношений на множествах объектов модели обеспечивает возможность автоматического логического вывода в процедурах формирования виртуальных организационных структур, объединяющих агентов субъектов безопасности для решения общих задач.

Архитектура и технологии формирования интегрированной информационной среды поддержки управления безопасностью региона

При выборе архитектуры построения открытой расширяемой информационно-аналитической среды поддержки управления безопасностью региона принимались во внимание следующие основные факторы, определяющие специфику требований к ее функциональным возможностям и эксплуатационным характеристикам:

- территориальная распределенность и организационная разнородность субъектов безопасности;
- симметричность информационных взаимодействий субъектов безопасности;
- существование большого количества разнородных проблемно-ориентированных РИС поддержки управления различными видами безопасности регионального развития (унаследованных систем).

Территориальная распределенность субъектов безопасности естественным образом заставляет использовать при построении целостной информационной среды поддержки управления безопасностью региона распределенную архитектуру. Субъект безопасности должен иметь возможность с собственного рабочего места получать доступ ко всем (или, по крайней мере, большей части) функциям распределенной информационной среды, т.е. в информационной системе должен быть реализован распределенный

доступ к информационно-вычислительным ресурсам. Наиболее распространенной архитектурой, реализующей распределенный доступ, является архитектура с централизованным (выделенным) сервером.

«Транскорпоративный» характер современных РИС увеличивает требования к модульности построения системы и максимально возможной независимости ее компонентов. Эти требования нашли отражение в современной тенденции к использованию слабосвязанных (loosely-coupled) архитектур РИС [8]. Поскольку деятельность субъектов и организационных структур безопасности характеризуется территориальной распределенностью и организационной разнородностью субъектов, слабосвязанные, в частности, сервис-ориентированные архитектуры являются эффективным способом реализации соответствующих проблемно-ориентированных распределенных систем информационной поддержки.

Важным аспектом, который необходимо учитывать при выборе архитектуры реализации информационной среды поддержки управления безопасностью, является симметричность информационных функций и продолжительный характер информационной активности субъектов безопасности. Функции компонентов системы симметричны, если они выступают как в роли серверов, так и в роли клиентов. Подобную симметричную функциональность обеспечивают одноранговые или пиринговые (от англ. peer-to-peer, P2P) РИС. В отличие от архитектур с выделенным сервером, логика функционирования всех узлов одноранговой системы (пиров) одинакова, а информационно-вычислительные ресурсы (в том числе – системная информация), напротив, распределены. Отличительными особенностями пиринговых систем, согласно [10], являются: отсутствие централизованной координации узлов, отсутствие централизованных баз управляющей информации, доступность всех имеющихся в системе данных и служб любому узлу. Перечисленные особенности делают одноранговые системы максимально открытой, легко масштабируемой и наращиваемой архитектурой РИС. Таким образом, одноранговая архитектура обеспечивает высокие эксплуатационные показатели функционирования РИС и соответствует симметричному характеру информационного взаимодействия субъектов безопасности.

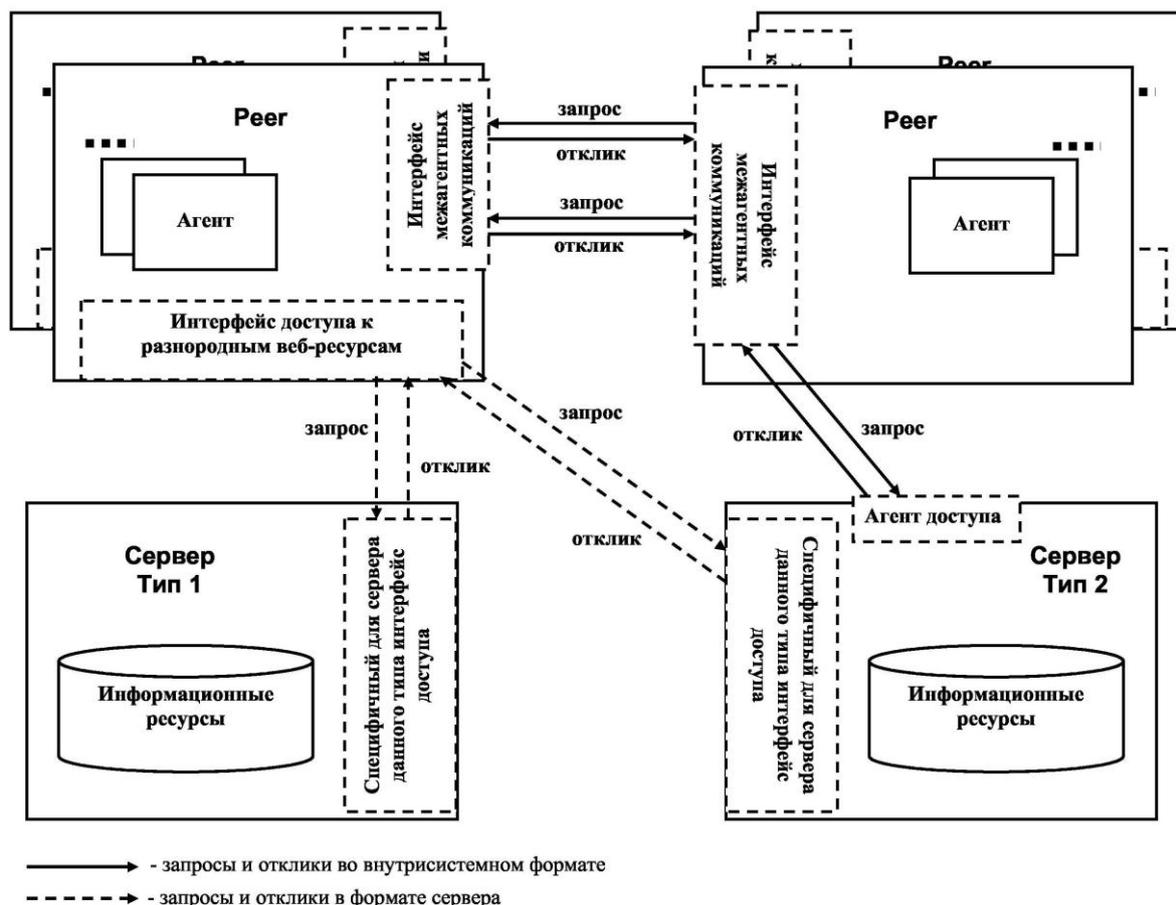


Рисунок. Обобщенная архитектура интегрированной информационной среды поддержки управления безопасностью региона на базе агентных и P2P-технологий

Обеспечение симметричного и продолжительного во времени информационного взаимодействия между субъектами безопасности может быть достигнуто на основе реализации агентной модели организации информационной среды [11]. Симметричная функциональность агентов создает предпосылки для более эффективного формирования возможных виртуальных организационных структур для решения

конкретных задач управления безопасностью, а их реактивность, про-активность и автономность делает распределенную среду «живой», активно функционирующей при минимальном участии пользователя. Таким образом, мультиагентный подход является адекватным средством создания открытой расширяемой саморазвивающейся информационной среды поддержки управления безопасностью.

Обобщенная архитектура интегрированной информационной среды поддержки управления безопасностью региона представлена на рисунке.

Основная функциональность системы реализуется узлами одноранговой сети (на рисунке – Peer), выполняющими также роль агентной платформы. Взаимодействие между агентами, дислоцирующимися на пирах, симметрично: каждый из них может как быть источником информационного запроса, так и играть роль сервера, обслуживающего запрос со стороны другого агента.

Серверы 1-го и 2-го типов представляют в составе единой информационной среды существующие системы информационной поддержки управления безопасностью. К первому типу относятся системы, не допускающие инсталляции на стороне сервера дополнительных программных модулей, реализующих агентов доступа к серверным данным. Для работы с серверами такого типа используются обычные механизмы и протоколы передачи запросов и получения результатов их обработки, например, протокол HTTP. Согласование общесистемных форматов запросов и откликов, а также используемых схем данных осуществляется на стороне пира в рамках интерфейса доступа к разнородным веб-ресурсам. Такой подход к интеграции унаследованных систем, очевидно, наиболее гибок, однако сопряжен с потенциально большей нагрузкой на коммуникационную сеть, так как исключает возможность предварительной обработки извлеченных данных на стороне сервера и отправки в рамках отклика более компактного результата. Второй тип сервера, напротив, допускает инсталляцию программного обеспечения агента доступа, осуществляющего все необходимые преобразования форматов данных и используемых схем локально, на стороне сервера, и взаимодействующего с другими агентами с использованием общесистемных коммуникационных протоколов и форматов данных. Для согласования разных технологий хранения и представления данных на стороне информационных серверов предлагается использовать программные адаптеры ресурсов, реализующие специфичные для каждого конкретного ресурса механизмы доступа и извлечения данных.

Заключение

В ходе проведенных исследований были получены следующие основные результаты.

1. Обоснована необходимость адаптации и развития существующих, а также создания новых научно-методических разработок для решения задач в области информационно-аналитической поддержки управления безопасностью развития арктических регионов с учетом специфических особенностей АЗ РФ.
2. Разработана агентно-ориентированная модель интегрированной информационной среды поддержки управления безопасностью развития региона, обеспечивающая технологическую основу для решения задач информационной поддержки согласованной деятельности организационных структур в области обеспечения безопасности функционирования региональных подсистем.
3. Предложены архитектура и технологии формирования целостной информационной среды поддержки управления безопасностью развития региона на базе одноранговых телекоммуникационных систем и мультиагентного подхода.

Литература

1. Маслобоев А.В., Путилов В.А. Обеспечение глобальной безопасности регионального развития: постановка задачи // Труды Института системного анализа РАН: Прикладные проблемы управления макросистемами. – 2010. – Т. 59. – С. 29–44.
2. Смирнов А.И., Агеев А.И., Кретов В.С., Котов Н.М., Котов М.Н., Кохтюлина И.Н., Куроедов Б.В., Сандаров О.В. Глобальная безопасность: инновационные методы анализа конфликтов. – М.: Общество «Знание» России, 2011. – 272 с.
3. Путилов В.А., Горохов А.В. Системная динамика регионального развития. – Мурманск: НИЦ «Пазори», 2002. – 306 с.
4. Маслобоев А.В., Путилов В.А. Информационно-аналитическая поддержка управления безопасностью развития Арктических регионов России: задачи, методы, технологии // Научно-технический вестник СПбГУ ИТМО. – 2011. – № 3 (73). – С. 143–145.
5. Десятов И.В., Малинецкий Г.Г., Маненков С.К., Митин Н.А., Отоцкий П.Л., Ткачев В.Н., Шишов В.В. Когнитивные центры как информационные системы для стратегического прогнозирования // Информационные технологии и вычислительные системы. – 2011. – № 1. – С. 65–81.
6. Юсупов Р.М., Заболотский В.П. Концептуальные и научно-методологические основы информатизации. – СПб: Наука, 2009. – 542 с.

7. Маслобоев А.В., Шишаев М.Г. Одноранговая распределенная мультиагентная система информационно-аналитической поддержки инновационной деятельности // Научно-технический вестник СПбГУ ИТМО. – 2009. – № 4 (62). – С. 108–114.
8. Путилов В.А., Шишаев М.Г., Олейник А.Г. Технологии распределенных систем информационной поддержки инновационного развития региона // Труды Института системного анализа РАН: Прикладные проблемы управления макросистемами. – М.: Книжный дом «ЛИБРОКОМ», 2008. – Т. 39. – С. 40–63.
9. Емельянов С.В., Попков Ю.С., Олейник А.Г., Путилов В.А. Информационные технологии регионального управления. – М.: Едиториал УРСС, 2004. – 400 с.
10. Сухорослов О.В. Принципы самоорганизации в пиринговых системах // Труды Института системного анализа РАН: Прикладные проблемы управления макросистемами. – 2004. – Т. 8. – С. 141–174.
11. Швецов А.Н., Яковлев С.А. Распределенные интеллектуальные информационные системы. – СПб: СПбГЭТУ «ЛЭТИ», 2003. – 318 с.

- Маслобоев Андрей Владимирович** – Институт информатики и математического моделирования технологических процессов Кольского научного центра РАН, кандидат технических наук, доцент, докторант, masloboev@iimm.kolasc.net.ru
- Шишаев Максим Геннадьевич** – Институт информатики и математического моделирования технологических процессов Кольского научного центра РАН, доктор технических наук, профессор, зав. лабораторией, shishaev@iimm.kolasc.net.ru