БЕЗОПАСНОСТЬ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

SAFETY IN EMERGENCY SITUATIONS

УДК 004.75, 004.89 **DOI 10.21685/2307-4205-2020-1-11**

А. В. Маслобоев

СРЕДСТВА ПОДДЕРЖКИ ИНТЕРОПЕРАБЕЛЬНОСТИ СЕТЕЦЕНТРИЧЕСКИХ СИСТЕМ УПРАВЛЕНИЯ РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТЬЮ

A. V. Masloboev

INTEROPERABILITY SUPPORT FACILITIES FOR NETWORK-CENTRIC CONTROL SYSTEMS OF REGIONAL SECURITY

Аннотация. *Актуальность и цели*. Целью исследования является повышение эффективности функционирования и взаимодействия информационно-управляющих систем региональных ситуационных центров. *Материалы и методы*. Объектами исследования являются архитектура и технологии реализации сетецентрических информационно-управляющих систем ситуационных центров региона, ориентированных на решение задач управления региональной безопасностью, а также свойство интероперабельности этих систем. Рассмотрены проблемы и средства обеспечения интероперабельности распределенных информационных систем ситуационных центров на технологическом, семантическом и организационном уровнях взаимодействия. *Результаты и выводы*. Предложены технологические решения по обеспечению интероперабельности компонентов сетецентрических систем управления региональной безопасностью, основанные на сервис-ориентированном подходе и совместном использовании мультиагентных технологий и семантических моделей представления знаний. Это обеспечивает интеграцию системных компонентов в единую виртуальную сетецентрическую среду и унификацию представления совместно используемых информационных ресурсов и сервисов, что способствует повышению эффективности управления региональной безопасностью на базе системы распределенных ситуационных центров.

Abstract. *Background*. The objective of our research is functioning and intercommunication efficiency enhancement of information-management system of the regional situational centers. *Materials and methods*. The subjects of inquiry are architecture and implementation technologies of the network-centric information system of situational centers of the region, oriented to regional security management problem-solving, as well as its interoperability characteristics. Interoperability support problems and facilities of the distributed information system of situational centers at technological, semantic and organizational interaction level are considered. *Results and conclusions*. Engineering solutions for component interoperability support of the network-centric control system of regional security based on service-oriented methodology and joint use of multi-agent technologies and knowledge representation semantic models are proposed. That provides system component integration within the unified virtual network-centric environment and representation unification of shared information resources and services that further regional security management efficiency enhancement on the basis of distributed situational centers.

© Маслобоев А. В., 2020

Ключевые слова: сетецентрическая система, управление, региональная безопасность, интероперабельность, архитектура, информационное взаимодействие, ситуационный центр.

Keywords: network-centric system, control, regional security, interoperability, architecture, intercommunication, situational center.

Введение

Стратегической задачей государственного значения является интенсификация широкомасштабных процессов автоматизации и информатизации различных отраслей экономики и жизнедеятельности населения страны на основе внедрения и комплексного использования новых информационно-аналитических систем и технологий обработки больших данных. В современных условиях темпы данных процессов определяют уровень развития цифровой экономики страны. В настоящее время важная роль в реализации государственных программ перехода к цифровой экономике и в решении проблем обеспечения национальной безопасности отводится системе распределенных ситуационных центров, функционирующих в режиме повседневной деятельности по единому регламенту взаимодействия. Эта система строится по сетецентрическому принципу из разнотипных по своей структуре и ведомственной принадлежности ситуационных центров (СЦ) различного уровня – федерального, регионального, муниципального, отраслевого и корпоративного. Интеграция распределенных СЦ в единую систему и организация их взаимодействия на основе общих организационных и технических регламентов нацелены на совершенствование системы государственного управления и структуры обеспечения комплексной безопасности за счет проблемно-ориентированной информационно-аналитической поддержки принятия управленческих решений в условиях возникновения кризисных ситуаций в социально-экономической и военно-политической сферах развития страны.

Большинство СЦ, созданных в регионах страны, являются уникальными, как с точки зрения информационно-технологической архитектуры, так и программно-аппаратной реализации аналитического обеспечения ситуационного управления критически важными объектами региональной экономики. Вместе с тем сегодня наблюдаются потребности в проектировании новых и модернизации существующих СЦ, а также в их последующей интеграции и адаптации в рамках уже созданной сети СЦ. Это является серьезной проблемой, которая до сих пор остается недостаточно проработанной с научно-методической точки зрения, что на практике приводит к снижению эффективности управления социально-экономическими системами с использованием существующих и вновь создаваемых СЦ.

На этапе интеграции информационных и функциональных компонентов различных СЦ в рамках распределенной информационной среды возникает множество проблем, связанных с обеспечением их интероперабельности (совместимости) на концептуальном, модельном, программно-техническом и организационном уровнях детализации. Это порождает увеличение временных и ресурсных затрат на «стыковку» СЦ и адаптацию их инструментария к динамически меняющейся внешней среде, а также на корректировку системотехнических и методических ошибок, выявленных в процессе эксплуатации компонентов СЦ, и согласование форматов информационного взаимодействия.

Работа посвящена вопросам обеспечения интероперабельности компонентов ведомственных информационных систем и их интеграции в единую инфраструктуру региональных ситуационных центров на базе сетецентрического подхода, мультиагентных технологий и онтологий.

Основные понятия и определения

Под интероперабельностью в общепринятом смысле понимается способность к интеграции двух или более информационных систем или их компонентов в единую информационную среду (систему). Согласно утвержденному стандарту [1] при этом должны обеспечиваться обмен информацией между всеми элементами интегрированной среды и возможность использования информации, полученной в результате интеграции и обмена. Для обеспечения свойства интероперабельности гетерогенных систем на практике применяются современные стандарты информационно-коммуникационных технологий. Интероперабельность – это одно из свойств открытых систем [2].

Анализ отечественных и зарубежных исследований проблем интеграции распределенных информационно-управляющих систем для решения задач в разных областях, как в гражданской, так и

в военной сферах показывает, что интероперабельность является ключевым системообразующим принципом построения сетецентрических систем управления сложными объектами различной природы и масштаба – от технических до социально-экономических. Этот принцип служит основой современной концепции горизонтального и вертикального информационно-технологического сопряжения существующих и вновь создаваемых систем сетецентрического управления, предназначенных для реализации перспективных государственных проектов и программ в области цифровой экономики, промышленности, энергетики, космосе, здравоохранении, транспорте, национальной безопасности и в других стратегических сферах.

Сетецентрическая система представляет собой объединение всех субъектов, объектов и средств управления в единое информационное пространство (виртуальную сетецентрическую среду управления), в рамках которой обеспечивается полная функциональная совместимость всех элементов, координация децентрализованного принятия решений и свободный обмен информацией на всех уровнях иерархии управления независимо от выполняемых элементами функций. Виртуальная среда ориентирована не только на интеграцию человеческих и технических ресурсов для задач управления, но и средств автоматизации получения, обработки и анализа информации для принятия решений в процессе управления, что обеспечивает повышение эффективности совместной деятельности субъектов управления и согласованное информационное взаимодействие между ними. Под взаимодействием понимается не только обмен информацией в системе для поддержания ситуационной осведомленности, но и выработка общей стратегии и координации совместных действий в интересах решения некоторой целевой задачи.

Базовые функции и структура типовой сетецентрической среды управления изложены в концепции Net-Centric Environment Joint Functional Concept [3]. Сетецентрические системы управления, согласно работе [4], характеризуются слабой иерархией в контуре принятия решений, способностью порождать цели внутри себя, а также открытостью и самоорганизацией. При этом достоинством сетецентрического способа управления по сравнению с иерархическим является то, что при таком подходе к управлению уменьшается совокупная ошибка принятия неверного решения в условиях неопределенности, что приводит к стабильности и способности системы адаптироваться к динамически изменяющейся внешней среде, а также обеспечивает рациональное распределение ресурсов в процессе децентрализованного управления системой.

В настоящей работе рассматривается система сетецентрического управления региональной безопасностью, построенная на базе сети СЦ региона. Региональные СЦ представляют собой комплексный инструмент ситуационного управления, обеспечивающий проблемный мониторинг, прогнозирование рисков и стратегическое планирование устойчивого социально-экономического развития региона для поддержки принятия эффективных управленческих решений как в стабильных условиях, так и в критических ситуациях.

Сетецентрическое управление региональной безопасностью заключается в реализации сетевой структуры организационного управления с выделенными управляющими СЦ, взаимодействие между которыми осуществляется на базе интеграции их компонентов (средств мониторинга, субъектов управления, исполнительных ресурсов и т.д.) в единое региональное информационное пространство [5]. СЦ региона как центры группового принятия решений (пункты ситуационного управления), являясь узлами сетецентрической системы управления региональной безопасностью, реализуются физически в определенной точке пространства, а также виртуально, когда отдельные компоненты СЦ локализованы на других узлах сети. При этом в процессе решения конкретной задачи управления центры принятия решений способны перемещаться между узлами виртуальной среды. Решение о миграции центра принимается на основе координирующих сигналов и оценки степени ситуационной осведомленности [6] всех участников процесса управления безопасностью.

Под ситуационной осведомленностью субъекта управления в СЦ понимается информация о проблемной ситуации, ориентируясь на которую при наличии необходимых у него ресурсов субъект получает возможность корректировать свое поведение и стратегию деятельности, координировать действия других участников процесса управления и тем самым влиять на функционирование объекта управления. Сеть большая, много решающих центров и всем требуется предоставить информацию, точно соответствующую ситуации. В связи с этим интероперабельность средств информационной поддержки СЦ во много определяет уровень ситуационной осведомленности на этапах выработки, реализации и контроля исполнения управленческих решений в условиях критических ситуаций.

Анализ проблем интероперабельности. Постановка задачи

Для региональных СЦ характерны следующие проблемы: ограниченная функциональность и изолированность используемых средств контроля и аналитической обработки возрастающего объема разноплановой информации о влиянии различных факторов на состояние региональных систем для управления рисками критических инфраструктур, а также необходимость координации взаимодействия пространственно-распределенных СЦ и обеспечения свойств гибкой масштабируемости и интероперабельности информационных систем СЦ. Решению этих проблем во многом препятствует смешение сфер интересов различных ведомств и организаций, участвующих в процессах управления региональным развитием через систему СЦ. Как правило, формат представления данных и регламент информационного обмена определяются локальными целями и функциональностью отдельных субъектов управления, а объем информации, необходимой для принятия решений, определяется исходя из требований к полноте знаний о критической ситуации, о состоянии функционирования объекта управления и о параметрах внешней среды. Перечисленные аспекты затрудняют совместное использование ресурсов для оценки ситуации и увеличивают время на коллективную выработку и согласование управленческих решений в критической обстановке.

Проблемы обеспечения интероперабельности информационных систем СЦ согласно эталонной модели интероперабельности [1] следует рассматривать на трех уровнях взаимодействия элементов этих систем – технологическом, семантическом и организационном (рис. 1), а также учитывать структуру взаимосвязей между ними.

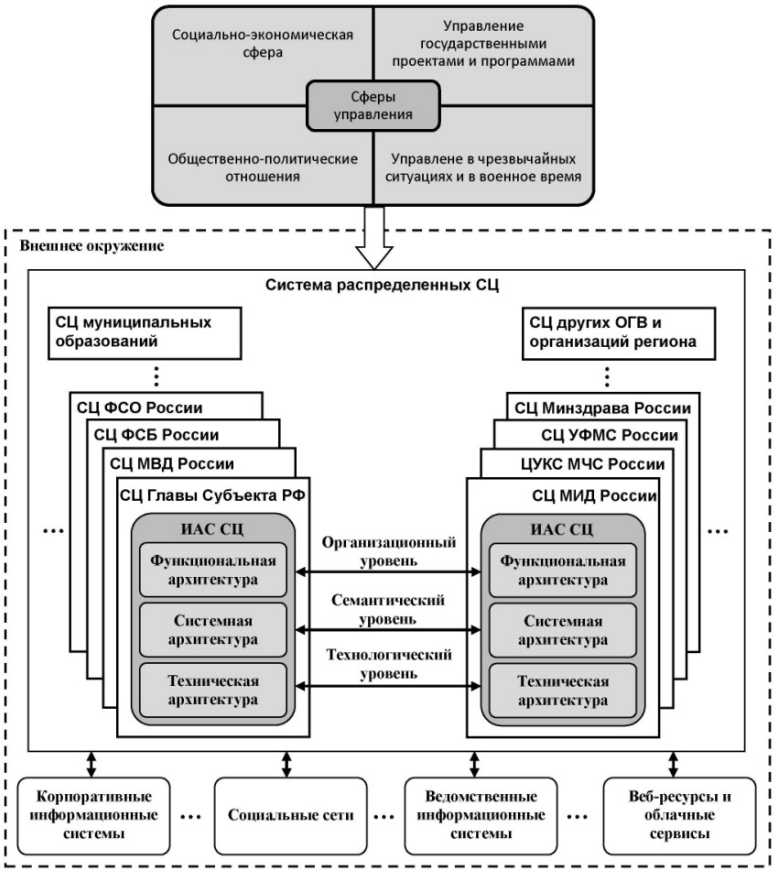

Рис. 1. Модель интероперабельности информационных систем СЦ:
ИАС – информационно-аналитическая система; ОГВ – органы государственной власти

Разнородность и территориальная распределенность субъектов управления безопасностью региона обусловливает технологическую и семантическую неоднородность сетецентрической среды региональной безопасности. Для информационной поддержки СЦ управления региональной безопасностью характерна высокая степень не только технологической (использование различных форматов хранения, представления и обмена данными, разных СУБД и структур баз данных и т.д.),

но и семантической разнородности информационных ресурсов (использование профильными ведомствами собственных тезаурусов и регламентов, синонимия в именовании информационных объектов, использование различных оценочных шкал, и т.п.). Вместе с тем к работе в СЦ управления региональной безопасностью привлекаются специалисты/эксперты из разных предметных областей, использующие различную терминологическую базу и отличные ментальные модели одних и тех же понятий и процессов. Источником технологической неоднородности информационных ресурсов является организационная разнородность субъектов управления безопасностью, которые, как правило, к моменту начала совместной деятельности уже имеют и используют собственные, отличные по архитектуре и технологиям, информационные инфраструктуры. Эти особенности препятствуют развитию современной системы СЦ и созданию единой виртуальной среды для сетецентрического управления региональной безопасностью.

Еще одним обстоятельством, затрудняющим интеграционные процессы при построении виртуальной сетецентрической среды СЦ управления региональной безопасностью, является существование класса так называемых «унаследованных систем» – невзаимосвязанных гетерогенных информационных систем управления безопасностью. К ним относятся различного рода ведомственные и корпоративные информационные системы, информационно-аналитические системы СЦ, отдельные веб-сервисы и Интернет-ресурсы и т.д. Эти системы оперируют большим объемом разноплановой информации о различных аспектах региональной безопасности, объектах, процессах и событиях безопасности, инцидентах. При интеграции «унаследованных систем» в сетецентрическую среду технологическая разнородность ресурсов выражается в различных форматах хранения данных, различных технологиях создания ресурсов и, как следствие, различных способах организации пользовательской работы с ними. Семантическая разнородность заключается в использовании в рамках ресурсов различных семантических моделей, определяющих смысл содержащегося в них контента. В результате внешне (синтаксически) одни и те же понятия могут иметь различную смысловую нагрузку и, наоборот, одно понятие может обозначаться формально различными синтаксическими конструкциями, что затрудняет возможность унификации приемов оперирования информацией, содержащихся в данных ресурсах. Организационная разнородность подразумевает различную принадлежность и целеполагание при использовании информационных ресурсов, что порождает специфические проблемы регулирования доступа к информации. Все это требует обеспечения интероперабельности интегрируемых в рамках сетецентрической виртуальной среды региональной безопасности компонентов СЦ, ресурсов и сервисов для повышения эффективности систем поддержки принятия решений в этой сфере.

С учетом того, что ситуационная осведомленность лиц, принимающих решения, в сетецентрической системе управления формируется на основе восприятия элементов в окружающей среде, понимания ситуации и прогноза будущего состояния объекта управления, а также взаимного информационного обмена, на каждом уровне модели интероперабельности необходимо обеспечить:

1) использование общих протоколов, интерфейсов и форматов хранения, представления и обмена данными, единых технических регламентов совместного применения программно-аппаратных средств получения, обработки и анализа информации в рамках взаимодействия, стандартов обеспечения информационной безопасности – на уровне технологической интероперабельности;

2) способность взаимодействующих информационных систем СЦ однозначно понимать и корректно интерпретировать смысловые и содержательные аспекты полученной в процессе сбора и коммуникации информации о ситуации, проводить ее верификацию и комбинирование с другой уже имеющейся информацией в ходе совместной обработки, учет влияния человеческого фактора (психологических и культурных особенностей пользователей при работе с разными типами человеко-машинных интерфейсов) в рамках информационного обмена – на уровне семантической интероперабельности;

3) согласование параметров локальных целевых функций всех участников информационного обмена (субъектов управления) с общей глобальной целью взаимодействия региональных СЦ в зависимости от режима функционирования СЦ и ситуации в регионе, использование единых административных регламентов (договоров, соглашений и других нормативно-правовых документов), определяющих правила и обязанности субъектов и объектов информационного взаимодействия – на уровне организационной интероперабельности.

Таким образом, на основании вышесказанного можно заключить, что для достижения интероперабельности информационных систем СЦ на всех уровнях сетецентрического управления региональной безопасностью применение только согласованных наборов стандартов информационно-

коммуникационных технологий представляется необходимым, но недостаточным условием. Для получения ощутимого комплексного эффекта интероперабельность должна обеспечиваться на более высоких уровнях – семантическом и административном, связанных с восприятием, осмыслением и использованием информации в организационных контурах принятия решений. Разработка формальных процедур и средств обеспечения семантической и организационной интероперабельности в процессе координации информационного взаимодействия в сетецентрических системах управления является сложной задачей. Эта проблема еще до конца не решена, несмотря на ее острую актуальность для различных приложений.

При разработке средств обеспечения интероперабельности компонентов информационных систем СЦ в сетецентрической среде управления региональной безопасностью важную роль играет анализ архитектурных особенностей построения этих систем. Проектирование архитектуры осуществляется в трех взаимосвязанных измерениях – функциональном, системном и техническом, отражающих различные аспекты функционирования и взаимодействия информационных систем СЦ. Этим обеспечивается целостность и единообразие в формализации представления всех элементов, процессов и системы в целом.

Функциональная архитектура определяет объекты системы, их роль и функции в системе, задачи и порядок их информационного взаимодействия, эффект от коммуникации на разных уровнях системы.

Системная архитектура определяет средства информационной поддержки, необходимые для достижения цели функционирования, форматы представления данных, информационные модели и процессы обработки информации, связи между ресурсами системы.

Техническая архитектура определяет состав коммуникационной инфраструктуры системы – каналы связи, спецификации используемых технических средств обеспечения внутриуровневого и межуровневого взаимодействия между элементами системы, совокупность стандартов, протоколов и интерфейсов информационного взаимодействия систем, технические регламенты и рекомендации по эксплуатации отдельных элементов и подсистем внутри единой системы и при взаимодействии с другими системами внешнего окружения.

При решении комплекса проблем интеграции «унаследованных систем» в единую виртуальную сетецентрическую среду необходимо сопоставлять основные параметры интероперабельности, заложенные в перечисленные типы архитектур, на начальной стадии проектирования информационных систем СЦ. К этим параметрам относятся: технико-экономические параметры, определяющие общие требования к информационно-технологической архитектуре системы и позволяющие оценить степень соответствия ее эксплуатационных возможностей и целей функционирования; внутренние и внешние параметры системы, определяющие релевантность передаваемых и обрабатываемых данных используемым программно-аппаратным средствам обработки и анализа информации и позволяющие установить зависимость эффективности информационного взаимодействия между компонентами системы от конкретных технологий их реализации, используемых протоколов или других технических решений; параметры сетевого взаимодействия, определяющие способ реализации информационного взаимодействия и степень соответствия системной архитектуры принятым стандартам и уровню развития технической архитектуры.

Нормативно-правовое обеспечение интероперабельности

К настоящему времени разработан ряд руководящих документов и методических рекомендаций по обеспечению интероперабельности в сетецентрических информационных системах как гражданского, так и военного назначения. Эти документы призваны стандартизировать модели и процессы интероперабельности и регламентируют механизмы их реализации в сетецентрических системах управления. Среди этих документов наибольшее внимание заслуживают следующие:

– Концепции по построению архитектуры Министерства обороны США – DODAF (DOD Architecture Framework);

– Концепция функционального объединения на основе сетецентрической среды NCE JFC (Net-Centric Environment Joint Functional Concept);

– Концепция оперативного интегрального объединения на основе сетецентрической среды NCOE JFC (Net-Centric Operational Environment Joint Integrating Concept);

– Стратегия построения сетецентрических объединений сил и средств в интересах Министерства обороны США (Department of Defense Net-Centric Services Strategy for a Net-Centric, Service Oriented DoD Enterprise);

– Стратегия перехода организаций Министерства обороны США к сетецентрической архитектуре (Department of Defense Enterprise Architecture Transition Strategy);

– Европейская концепция интероперабельности – EIF (European Interoperability Framework);

– Стандарты и профили интероперабельности НАТО – NISP (NATO Interoperability Standards and Profiles);

– Руководство по объединенной совместной интеграции и развитию систем – JCIDS (Joint Capability Integration and Development System);

– Концепция интероперабельности объединенных систем «Net Ready».

Вместе с тем международный консорциум NCOIC (Network-Centric Operations Industry Consortium) разработал ряд дополнительных методических рекомендаций в области интероперабельности систем сетецентрического управления:

– Рекомендации по обеспечению интероперабельности при проектировании организационно-технических систем NIF (NCOIC Interoperability Framework);

– «Основы сетецентрических систем» (Core Net-centric Principles);

– «Функциональные шаблоны для сетецентрических систем» (Operational Net-centric Patterns);

– «Средства анализа сетецентрических систем» NCAT (Network-Centric Analysis Tool);

– Белая книга по обеспечению информационной безопасности в сетецентрических системах (NCOIC White Paper on the Cybersecurity Landscape);

– Рекомендации по обеспечению интероперабельности в сложных сетецентрических системах с учетом аспектов управления, техники, экономики и культуры (NCOIC QuadTrangle).

Адаптация зарубежного опыта проектирования и разработки сетецентрических систем управления к российской специфике позволила также системно взглянуть на проблему интероперабельности и выработать концептуальные положения по ее решению в современных условиях. Эти положения легли в основу отечественных стандартов интероперабельности, среди которых следует отметить следующие:

– ГОСТ Р 55062-2012. Информационные технологии (ИТ). Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения (2014 г.);

– ГОСТ Р 11354-1-2012. Усовершенствованные автоматизированные технологии и их применение. Требования к установлению интероперабельности процессов промышленных предприятий. Часть 1. Основа интероперабельности предприятий (2014 г.).

Разработка нормативно-технической базы для регулирования различных вопросов интеграции и обеспечения интероперабельности сетецентрических информационно-управляющих систем является отдельной самостоятельной задачей, сложность решения которой упирается в многоаспектность и несовершенность правового поля при позиционировании и использовании виртуальных сетецентрических систем как инструмента государственного управления.

Методы и подходы решения проблем интероперабельности

На сегодняшний день известно множество методов и технологий обеспечения различных аспектов интероперабельности распределенных систем. Однако эти средства применяются изолированно друг от друга и не увязаны в целостную методологическую систему. Все множество известных подходов к решению проблем интероперабельности на технологическом, концептуальном и организационном уровнях можно условно разделить на следующие категории [7]:

1) восходящий подход (подход «снизу – вверх»), который ориентирован, в первую очередь, на решение проблем технологической интероперабельности информационных систем путем использования общих стандартов и технологий передачи, хранения, представления и обработки информации на всех уровнях интеграции этих систем;

2) нисходящий подход (подход «сверху – вниз»), который сосредоточен на декомпозиции решения проблем интероперабельности с точки зрения архитектуры системы в целом, а затем с точки зрения отдельных подсистем и процессов вплоть до атомарных элементов;

3) общесистемный подход, основанный на анализе внутренних коммуникаций между компонентами внутри интегрированной системы и ориентированный на решение проблем интероперабельности путем формирования единой среды информационного взаимодействия между ними;

4) интерактивный подход, учитывающий характер сопряжения и взаимодействия различных систем между собой и внешней средой и ориентированный на достижение интероперабельности тех систем и их компонентов, уже имеющих различную технологическую реализацию и использующих отличные стандарты передачи, хранения, представления и обработки информации.

5) процессный подход, сосредоточенный на решении проблем интероперабельности с учетом идентификации, анализа и оптимизации полной группы технологических, организационных и организационно-технических факторов, запускающих на протяжении жизненного цикла систем различные процессы, влияющие на функционирование систем в целом и на изменение свойства их интероперабельности.

Выбор того или другого подхода зависит от функциональной разрозненности информационных систем, принципов их построения и технической реализации отдельных компонентов и других факторов.

Опираясь на идеологию перечисленных подходов и тот факт, что они зачастую применяются в комбинации для преодоления проблем интероперабельности, по мнению автора, эффективное решение задач интеграции технологически и семантически неоднородных совместно используемых информационно-вычислительных ресурсов СЦ в задачах информационной поддержки управления региональной безопасностью достигается на основе применения агентных технологий, программного обеспечения промежуточного слоя и онтологий. В исследовании [4] показано, что мультиагентные технологии [8] являются эффективным средством реализации сетецентрической системы СЦ управления региональной безопасностью. Это обусловливается тремя ключевыми факторами: высокой динамичностью структуры виртуальной среды взаимодействия субъектов управления, необходимостью координации децентрализованного принятия решений, а также учета человеческого фактора и организационных особенностей в процессе управления. Сетевые семантические модели представления знаний, в частности, онтологии [9] и концептуальное моделирование предметной области [10] являются эффективным средством описания и анализа семантики разнородных информационных ресурсов и сервисов. Решение проблемы семантической интероперабельности ресурсов СЦ основано на согласовании семантики через интеграцию онтологий ресурсов. Для интеграции онтологий используется дескриптивный подход [11], т.е. связывание онтологий посредством общего тезауруса, который является расширяемым. Этим обеспечивается возможность интеграции в виртуальную сетецентрическую среду новых ресурсов и компонентов без существенной перенастройки всей системы. Главная проблема интеграции онтологий – установление смысловой эквивалентности их концептов и разрешение возникающих семантических конфликтов. Для автоматизированной оценки степени смыслового соответствия пары концептов сравниваются их имена, структурное положение в онтологии и наборы необходимых и достаточных атрибутов.

Практика показывает, что сетецентрические системы управления должны строиться только на принципах слабой связанности между компонентами. Технологическую основу слабосвязанных архитектур составляет программное обеспечение промежуточного слоя MOM (message-oriented middleware). Наиболее популярной современной разновидностью MOM являются веб-сервисы – программные системы, идентифицируемые строкой URL (Uniform Resource Locator), чьи общедоступные интерфейсы определяются на языках XML, JSON или YAML. Описание этих программных систем может быть найдено другими системами, которые могут взаимодействовать с ними согласно этому описанию посредством сообщений. На основе технологии веб-сервисов реализуются как системы с распределенной обработкой данных, так и с распределенным доступом и хранением информации. В последнем случае обеспечивается возможность децентрализованного администрирования серверных элементов информационной системы, что позволяет решать проблему организационной интероперабельности компонентов сетецентрических информационно-управляющих систем при совместном использовании и интеграции в них функционально разнородных элементов.

Архитектура сетецентрической виртуальной среды управления региональной безопасностью должна поддерживать использование в ее рамках унаследованных систем. Для этого необходимо организовать унифицированный доступ к информационным ресурсам и сервисам, используемым для решения задач управления, как к единому целому. Логическая интеграция этих ресурсов, с одной стороны, обеспечивает пользователя свободным доступом к семантически разнородным данным, хранящимся на различных технологически и организационно разнородных информационных серверах, а также прозрачный доступ к пространственно распределенным данным при реализации процедур автоматизированной обработки и анализа информации. При этом стоит отметить, что в условиях организационной разнородности субъектов управления и требований свободной расширя-

емости сетецентрической среды подход к логической интеграции ресурсов и сервисов на базе единого централизованного сервера или выделенной интегрирующей системы не применим.

Требования к функциональности и эксплуатационным характеристикам подобной виртуальной сетецентрической среды обусловливаются особенностями процессов управления региональной безопасностью. Эти требования приведены в табл. 1.

Таблица 1

Требования к функциональности и архитектуре
информационной среды региональной безопасности (ИС РБ)

Особенности системы управления региональной безопасностью	**Требования к архитектуре и функциональности ИС РБ**
Распределенность информационных ресурсов и субъектов безопасности	Распределенное хранение, аналитическая обработка и доступ к информации
Технологическая, семантическая, организационная неоднородность информационных ресурсов и сервисов	Логическая интеграция ресурсов, поддержка интероперабельности разнородных программных компонентов
Организационная разнородность субъектов безопасности, наличие смешенных горизонтально-вертикальных связей, децентрализованное принятие решений	Сетецентрическая структура, координация децентрализованного управления, кооперативность участников информационных процессов, целостность
Динамичность состава участников и параметров процессов управления безопасностью в кризисных ситуациях, в том числе ресурсов, объектов и угроз безопасности	Расширяемость, адаптивность, способность к самоорганизации, мультипредметность, возможность для свободного подключения узлов и сервисов
Симметричный характер взаимодействия и долговременный характер информационных интересов субъектов управления безопасностью	Сервис-ориентированная архитектура; про-активность, мобильность, персонализация компонентов; мультиагентная реализация; потенциал к саморазвитию

Исходя из табл. 1 и в соответствии с современными технологиями разработки распределенных систем с обозначенными характеристиками, виртуальная сетецентрическая среда управления региональной безопасностью имеет гибридную одноранговую сервис-ориентированную архитектуру, общий вид которой показан на рис. 2.

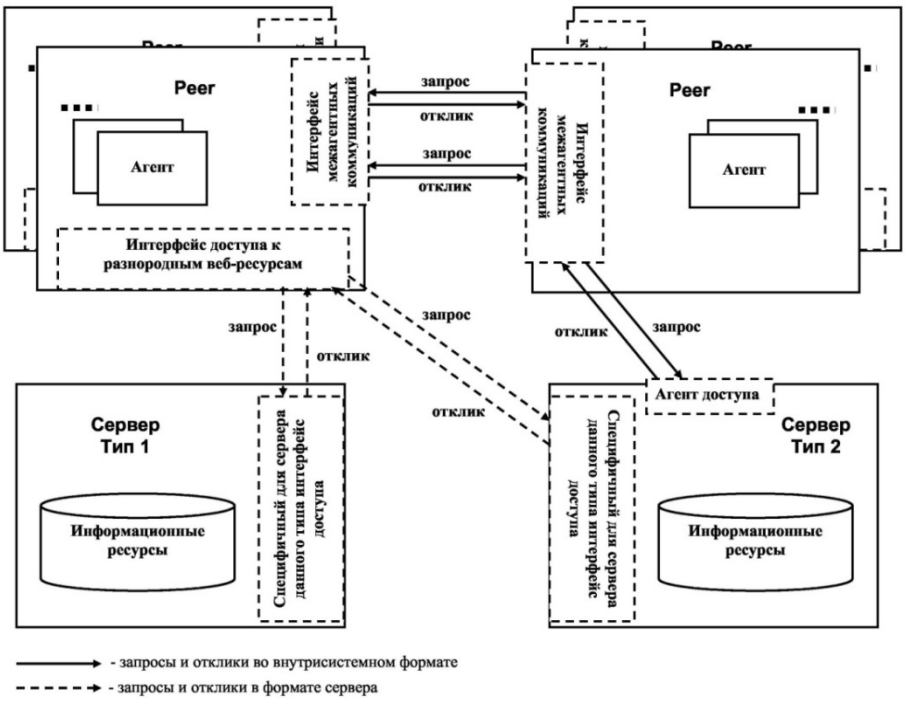

Рис. 2. Обобщенная архитектура распределенной информационной среды региональной безопасности на базе агентных и P2P-технологий

Основная функциональность сетецентрической системы управления реализуется узлами одноранговой сети (на рис. 2 – Peer), выполняющими также роль агентной платформы. Взаимодействие между агентами, функционирующими на узлах сети, симметрично: каждый из них может быть как 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 сетецентрической среды СЦ существующие системы информационной поддержки управления региональной 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 узла (Peer) 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 решения проблем технологической интероперабельности неоднородных ресурсов на стороне информационных серверов СЦ используются программные адаптеры ресурсов (рис. 3), так называемые коннекторы. Адаптеры связывают интерфейсы прикладного программирования компонентов разнородных систем и обеспечивают согласование разных технологий хранения и представления данных на этапе их взаимодействия за счет реализации специфичных для каждого конкретного ресурса механизмов доступа и извлечения данных. Такие адаптеры и их функции определяются стандартом архитектуры для соединения серверов приложений JCA (Java EE Connector Architecture). Адаптеры ресурсов реализуют в том числе и алгоритм взаимодействия одноранговых узлов, основанный на спецификации JXTA (Juxtapose), имеющей статус стандарта де-факто. Применение REST-интерфейсов и стандартных протоколов обеспечивает возможность для привлечения к созданию программных адаптеров сторонних разработчиков.

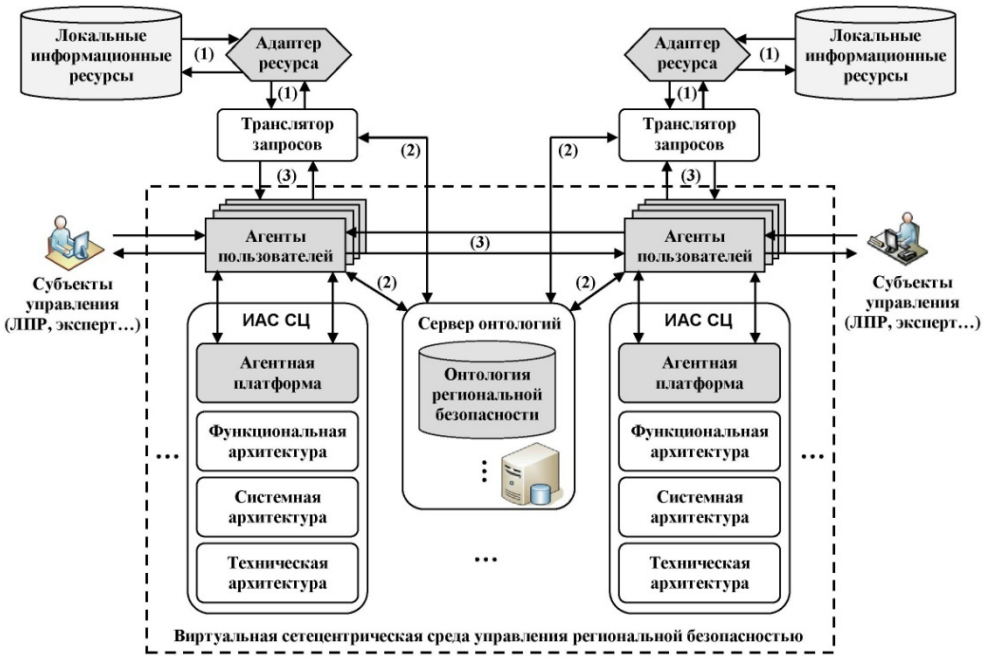

Рис. 3. Общая схема решения проблем интероперабельности ИАС СЦ региона на базе мультиагентного подхода и онтологий: ИАС – информационно-аналитическая система; ЛПР – лицо, принимающее решение; *1* – запросы и результаты в локальных терминах; *2* – согласование семантики локального и общесистемного представления; *3* – запросы и результаты в общесистемных терминах

Интерфейсные модули узлов системы, реализуемые на основе технологии веб-сервисов, описываются на языке WSDL, а в качестве коммуникационного протокола используется SOAP.

Для комплексного решения задач обеспечения семантической интероперабельности информационных систем СЦ региона разработана интегрированная онтологическая модель жизненного цикла угроз региональной безопасности [4] (позиционирована на рис. 3). Модель представляет собой разновидность неоднородной семантической сети. Отличительной особенностью данной модели является то, что в ней совмещаются формализованные модели предметной области «региональная безопасность» и исполнительной среды информационно-аналитической поддержки решения задач в этой предметной области. Модель обеспечивает как формальную основу для имитационного моделирования и автоматизации процессов управления региональной безопасностью, так и согласованное информационное взаимодействие ситуационных центров региона за счет автоматизированной обработки, унификации и интеграции семантически разнородных данных на стратегическом, тактическом и оперативном уровнях управления безопасностью. Это позволяет сформировать единое информационное поле ситуационной осведомленности для лиц, принимающих решения, в сетецентрической системе управления региональной безопасностью.

Программная реализация модели выполнена в виде прикладной онтологии региональной безопасности. Онтология создана средствами языка онтологического моделирования OWL (*Web Ontology Language*) в инструментальной среде разработки онтологий Protégé. Созданная онтология содержит семь уровней таксономии и включает в себя более 500 классов, более 150 атрибутов, более 100 иерархических, ассоциативных и функциональных ограничений. Онтология имеет высокую степень детализации, что обеспечивает достаточную полноту концептуального описания объектов и задач обеспечения безопасности и связанных с ними информационных процессов. Так как агенты реализованы на платформе JADE, то для формирования моделей знаний агентов и обеспечения возможности агентов работы с разработанной онтологией использована специальная библиотека AgentOWL.

Для формирования интероперабельной сетецентрической среды ситуационного управления региональной безопасностью предлагается использовать средства мультиагентной виртуализации в составе систем поддержки принятия решений СЦ региона. К этим средствам относятся мультиагентная исполнительная среда (система агентов и веб-сервисов) и семантическое пространство знаний (комплекс онтологических моделей предметных областей, для которых предназначены агенты, и сеть информационных ресурсов). Эти средства позволяют решать проблемы технологической и семантической интероперабельности на базе использования единых стандартов разработки мультиагентных систем и технологий Семантического Веба. Средства виртуализации и структурная схема, отражающая отличительные особенности подхода к построению интероперабельной сетецентрической среды управления на базе автономных программных агентов от известных технологий, приведены на рис. 4. При таком подходе единая информационная среда для взаимодействия СЦ региона формируется в виде сети виртуальных центров управления для каждой области региональной безопасности. Преимущества виртуальных центров ситуационного управления по сравнению с традиционными СЦ представлены в табл. 2. Технически виртуальные центры управления реализуются как гибридные облачные сервисы с применением архитектуры IaaS (Infrastructure as a service – модель обслуживания по принципу инфраструктура как сервис) [12].

Интеграция предлагаемых решений с известными разработками в области обеспечения интероперабельности информационных систем позволит усилить эффект от совместного использования инструментов СЦ для различных задач ситуационного управления безопасностью, а также разрешить ряд противоречий, возникающих на практике при взаимодействии СЦ в условиях региональных кризисных ситуаций. Так, особое внимание заслуживает исследование [13], в котором подробно рассматривается российский и зарубежный опыт решения проблем интероперабельности разнородных сетецентрических информационно-управляющих систем на основе разработанной в Институте радиоэлектроники им. В. А. Котельникова РАН модели интероперабельности в соответствии с ГОСТ Р 55062–2012 и совместного использования американских моделей LISI (Levels of Information Systems Interoperability – модель уровней интероперабельности информационных систем), SCOPE (Systems, Capabilities, Operations, Programs, and Enterprises model for interoperability assessment – модель оценки интероперабельности систем, возможностей, действий, программ и организаций) и концепции DODAF, а также предлагаются варианты сопряжения и адаптации этих моделей для оте-

чественных сетецентрических систем управления с учетом специфики их приложения. Представленные в работе результаты и критический анализ моделей интероперабельности сетецентрических систем [14–17] позволяют говорить о возможности комплексного решения проблем обеспечения интероперабельности информационных систем региональных СЦ в ближайшей перспективе.

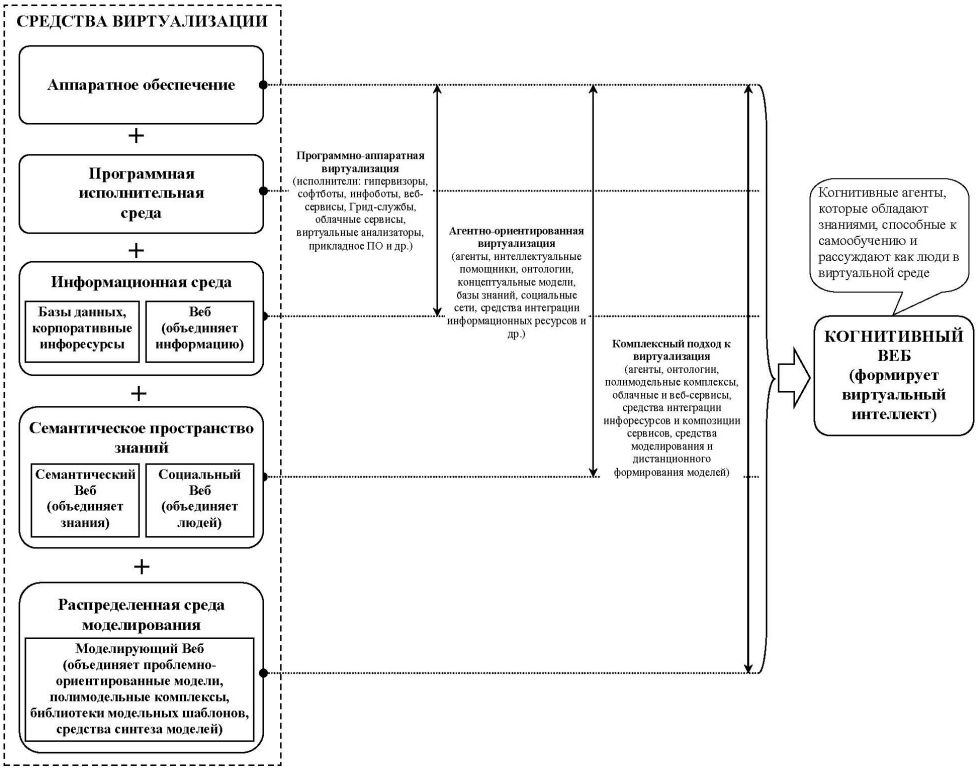

Рис. 4. Средства построения сетецентрической среды управления безопасностью региона на базе подхода мультиагентной виртуализации

Таблица 2

Преимущества виртуальных центров управления по сравнению с традиционными СЦ

Традиционный СЦ	**Виртуальный центр управления**
1	2
Физическая локальность, изолированность системы управления, централизация всех ресурсов в одной точке	Децентрализация субъектов управления и средств информационной поддержки, распределенный доступ к ресурсам и сервисам единой виртуальной среды
Сложность оперативного перераспределения ресурсов, сил и средств реагирования, а также формирования экспертных групп и координационных комиссий «под задачу» в условиях изменения кризисных ситуаций	Оперативная перенастройка и реконфигурация структуры и состава участников процессов обеспечения безопасности в динамических условиях обстановки, независимость локализации ситуации/объекта управления от средств мониторинга и контроля
Высокие затраты на приобретение специального оборудования, техническое сопровождение, аренду и охрану помещений	Относительно низкая стоимость развертывания/аренды облачной инфраструктуры, предоставляющей программно-аппаратные средства и специализированные сервисы субъектам управления СЦ
Централизованное администрирование и локальная настройка программно-аппаратных средств и коммуникационной инфраструктуры СЦ	Распределенное администрирование и гибкая настройка компонентов системы через общесистемный облачный интерфейс, предоставляющий унифицированный доступ к системе

Окончание табл. 2

1	2
Необходимость обеспечения конфиденциальности и контроля технических регламентов работы всех компонентов СЦ как в стабильных, так и в критических ситуациях	Информационная безопасность и защищенность компонентов СЦ обеспечивается ограниченным набором программно-технических средств администрирования и контроля доступа к ресурсам СЦ, а также надежными протоколами сетевого взаимодействия
Необходимость физического присутствия субъектов управления на территории СЦ в условиях возникновения кризисных ситуаций, временные затраты на формирование рабочих групп и комиссий под проблемную ситуацию	Оперативное согласование локальных планов и действий субъектов управления СЦ посредством переговорного процесса между их агентами в автономном режиме и алгоритмов динамического формирования проблемно-ориентированных коалиций агентов «под задачу»
Функционально фиксированный пользовательский интерфейс, зависящий от профиля деятельности и индивидуальных особенностей работы разнотипных субъектов управления СЦ	Интеллектуальный пользовательский интерфейс с возможностью автоматизированной когнитивной настройки под конкретную категорию пользователя СЦ в зависимости от входных данных о ситуации и его ситуационной осведомленности
Ограниченные возможности интеграции с другими СЦ, длительное согласование организационных и технических регламентов взаимодействия при подключении дублирующих или сторонних СЦ	Механизмы гибкой интеграции с другими СЦ в независимости от их архитектуры и уровней технической реализации, свободное подключение к сети новых СЦ и их компонентов
Относительная нормативно-техническая поддержка процесса эксплуатации СЦ на разных уровнях государственного управления	Несовершенность нормативно-правовой базы для внедрения виртуальных СЦ в систему государственного управления

Заключение

Рост сложности управления социально-экономическими системами в условиях высокой неопределенности и множественных рисков, с одной стороны, а также необходимость автоматизации и интеллектуализации средств управления этими системами в условиях перехода к цифровой экономике – с другой, обусловливают повышение требований к современной сетецентрической системе СЦ, ориентированных на информационно-аналитическую поддержку принятия стратегических и оперативных управленческих решений на всех уровнях государственного и регионального управления. Вместе с тем проблему обостряет необходимость оперативной адаптации различных средств информационно-аналитической поддержки и обеспечения возможности их совместного использования в рамках существующей системы СЦ. Окончательное решение этой задачи пока еще не получено, и поэтому проблема обеспечения интероперабельности информационных систем региональных СЦ для нужд государственного управления и обеспечения безопасности является перспективной научно-технической задачей. Это связано сегодня с современными тенденциями в области интеграции проблемно-ориентированных информационных систем двойного назначения, а также с развитием и применением систем сетецентрического управления для различных актуальных приложений в социально-экономической сфере.

Несмотря на то, что интеграция «унаследованных» информационных систем СЦ в единую виртуальную сетецентрическую среду сопряжена с определенными трудностями, в работе предложены возможные пути решения проблемы обеспечения технологической, семантической и организационной интероперабельности компонентов этих систем. Улучшение этих решений может быть предметом будущих исследований и разработок. При этом для преодоления ограничивающих факторов интероперабельности технического характера с целью широкого использования всего функционала сетецентрической системы СЦ целесообразно придерживаться единых подходов, основанных на отечественных и зарубежных методиках и открытых стандартах ИКТ, регламентирующих обеспечение функциональной совместимости компонентов сетецентрических информационно-управляющих систем с учетом формирования профилей интероперабельности на уровне протоколов, интерфейсов и процессов в этих системах.

Результаты исследования будут использованы при реализации основных направлений государственной политики РФ в Арктике на период до 2035 г. в части разработки методов и средств поддержки принятия решений для информационно-аналитического обеспечения региональных ситуационных центров в Мурманской области.

Дальнейшие исследования направлены на совершенствование многоуровневой системы управления региональной безопасностью в части разработки новых технологий динамического конфигурирования сетецентрической среды управления безопасностью региона на концептуальном, виртуальном и организационном уровнях на базе современных стандартов интероперабельности и интеграции систем.

Работа выполнена при поддержке Министерства науки и высшего образования РФ (тема НИР № 0226-2019-0035) и Российского фонда фундаментальных исследований (проект 18-29-03022-мк).

Библиографический список

1. ГОСТ Р 55062-2012. Информационные технологии. Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения. – Москва : Стандартинформ, 2014. – 12 с.
2. Технология открытых систем / под ред. А. Я. Олейникова. – Москва : Янус-К, 2004. – 288 с.
3. Net-Centric Environment Joint Functional Concept. – Washington : Department of Defense Washington DC, 2005. – 76 p.
4. *Маслобоев, А. В.* Информационное измерение региональной безопасности в Арктике / А. В. Маслобоев, В. А. Путилов. – Апатиты : КНЦ РАН, 2016. – 222 с.
5. *Маслобоев, А. В.* Модель и технология поддержки принятия решений в условиях сетецентрического управления региональной безопасностью / А. В. Маслобоев // Надежность и качество сложных систем. – 2019. – № 2 (26). – С. 43–59.
6. *Endsley, M. R.* Final Reflections: Situation Awareness Models and Measures / M. R. Endsley // Journal of Cognitive Engineering and Decision Making. – 2015. – Vol. 9, № 1. – P. 101–111.
7. Systems, Capabilities, Operations, Programs, and Enterprises (SCOPE) Model for Interoperability Assessment. Version 1.0. – NCOIC, 2008. – 154 p.
8. *Wooldridge, M.* An Introduction to MultiAgent Systems. Second Edition / M. Wooldridge. – John Wiley & Sons, 2009. – 484 p.
9. *Олейник, А. Г.* Разработка онтологии интегрированного пространства знаний / А. Г. Олейник, П. А. Ломов // Онтология проектирования. – 2016. – Т. 6, № 4 (22). – С. 465–474.
10. *Кузьмин, И. А.* Распределенная обработка информации в научных исследованиях / И. А. Кузьмин, В. А. Путилов, В. В. Фильчаков. – Ленинград : Наука, 1991. – 304 с.
11. *Ломов, П. А.* Интеграция онтологий с использованием тезауруса для осуществления семантического поиска / П. А. Ломов, М. Г. Шишаев // Информационные технологии и вычислительные системы. – 2009. – № 3. – С. 49–59.
12. *Сухорослов, О. В.* Интеграция вычислительных приложений и распределенных ресурсов на базе облачной программной платформы / О. В. Сухорослов // Программные системы: теория и приложения. – 2014. – Т. 5, № 4 (22). – С. 171–182.
13. *Макаренко, С. И.* Модели интероперабельности информационных систем / С. И. Макаренко, А. Я. Олейников, Т. Е. Черницкая // Системы управления, связи и безопасности. – 2019. – № 4. – С. 215–245.
14. *Франгулова, Е. В.* Классификация подходов к интеграции и интероперабельности информационных систем / Е. В. Франгулова // Вестник Астраханского государственного технического университета. Сер.: Управление, вычислительная техника и информатика. – 2010. – № 2. – С. 176–180.
15. *Куприянов, А. А.* Сетецентрические военные действия и вопросы интероперабельности автоматизированных систем / А. А. Куприянов // Автоматизация процессов управления. – 2011. – № 3. – С. 82–97.
16. *Зацаринный, А. А.* Интероперабельность консолидируемых организационных систем / А. А. Зацаринный, С. В. Козлов, А. П. Шабанов // Проблемы управления. – 2017. – № 6. – С. 43–49.
17. *Акаткин, Ю. М.* Цифровая трансформация государственного управления: датацентричность и семантическая интероперабельность / Ю. М. Акаткин, Е. Д. Ясиновская. – Москва : ЛЕНАНД, 2019. – 724 с.

References

1. GOST R 55062-2012. *Informatsionnye tekhnologii. Sistemy promyshlennoy avtomatizatsii i ikh integratsiya. Interoperabel'nost'. Osnovnye polozheniya* [GOST R 55062-2012. Information technology.

Industrial automation systems and their integration. Interoperability. Fundamentals]. Moscow: Standartinform, 2014, 12 p. [In Russian]
2. *Tekhnologiya otkrytykh sistem* [Open systems technology]. Ed. A. Ya. Oleynikov. Moscow: Yanus-K, 2004, 288 p. [In Russian]
3. *Net-Centric Environment Joint Functional Concept*. Washington: Department of Defense Washington DC, 2005, 76 p.
4. Masloboev A. V., Putilov V. A. *Informatsionnoe izmerenie regional'noy bezopasnosti v Arktike* [Information dimension of regional security in the Arctic]. Apatity: KNTs RAN, 2016, 222 p. [In Russian]
5. Masloboev A. V. *Nadezhnost' i kachestvo slozhnykh system* [Reliability and quality of complex systems]. 2019, no. 2 (26), pp. 43–59. [In Russian]
6. Endsley M. R. *Journal of Cognitive Engineering and Decision Making*. 2015, vol. 9, no. 1, pp. 101–111.
7. *Systems, Capabilities, Operations, Programs, and Enterprises (SCOPE) Model for Interoperability Assessment. Version 1.0*. NCOIC, 2008, 154 p.
8. Wooldridge M. *An Introduction to MultiAgent Systems. Second Edition*. John Wiley & Sons, 2009, 484 p.
9. Oleynik A. G., Lomov P. A. *Ontologiya proektirovaniya* [Design ontology]. 2016, vol. 6, no. 4 (22), pp. 465–474. [In Russian]
10. Kuz'min I. A., Putilov V. A., Fil'chakov V. V. *Raspredelennaya obrabotka informatsii v nauchnykh issledovaniyakh* [Distributed information processing in scientific research]. Leningrad: Nauka, 1991, 304 p. [In Russian]
11. Lomov P. A., Shishaev M. G. *Informatsionnye tekhnologii i vychislitel'nye sistemy* [Information technologies and computer systems]. 2009, no. 3, pp. 49–59. [In Russian]
12. Sukhoroslov O. V. *Programmnye sistemy: teoriya i prilozheniya* [Software systems: theory and applications]. 2014, vol. 5, no. 4 (22), pp. 171–182. [In Russian]
13. Makarenko S. I., Oleynikov A. Ya., Chernitskaya T. E. *Sistemy upravleniya, svyazi i bezopasnosti* [Management, communication and security systems]. 2019, no. 4, pp. 215–245. [In Russian]
14. Frangulova E. V. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Ser.: Upravlenie, vychislitel'naya tekhnika i informatika* [Bulletin of the Astrakhan state technical University. Ser.: Management, computer engineering and Informatics]. 2010, no. 2, pp. 176–180. [In Russian]
15. Kupriyanov A. A. *Avtomatizatsiya protsessov upravleniya* [Automation of management processes]. 2011, no. 3, pp. 82–97. [In Russian]
16. Zatsarinnyy A. A., Kozlov S. V., Shabanov A. P. *Problemy upravleniya* [Management problem]. 2017, no. 6, pp. 43–49. [In Russian]
17. Akatkin Yu. M., Yasinovskaya E. D. *Tsifrovaya transformatsiya gosudarstvennogo upravleniya: datatsentrichnost' i semanticheskaya interoperabel'nost'* [Digital transformation of public administration: data-centricity and semantic interoperability]. Moscow: LENAND, 2019, 724 p. [In Russian]

Маслобоев Андрей Владимирович
доктор технических наук, доцент,
ведущий научный сотрудник,
Институт информатики и математического моделирования,
Кольский научный центр
Российской академии наук
(Россия, Мурманская обл.,
г. Апатиты, ул. Ферсмана, 14)
E-mail: masloboev@iimm.ru

Masloboev Andrey Vladimirovich
doctor of technical sciences, associate professor,
leading research,
Institute for Informatics and Mathematical Modeling,
Kola Science Centre of the Russian Academy
of Sciences
(14 Fersmana street, Apatity,
Murmansk region, Russia)

Образец цитирования:
Маслобоев, А. В. Средства поддержки интероперабельности сетецентрических систем управления региональной безопасностью / А. В. Маслобоев // Надежность и качество сложных систем. – 2020. – № 1 (29). – С. 91–105. – DOI 10.21685/2307-4205-2020-1-11.