УДК 004.9

# ОПЫТ ИНТЕГРАЦИИ И ПРОБЛЕМЫ СТАНДАРТИЗАЦИИ РАСПРЕДЕЛЕННОЙ (ПОЛИЦЕНТРИЧЕСКОЙ) СЕТИ СИТУАЦИОННЫХ И ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ ЦЕНТРОВ МОНИТОРИНГА СОСТОЯНИЯ СТРАСТЕГИЧЕСКИХ И СОЦИАЛЬНО ЗНАЧИМЫХ ОБЪЕКТОВ И ТЕРРИТОРИЙ

**[1]Куделькин В.А.**

*[1] Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет информационных технологий, радиотехники и электроники» (МИРЭА), Москва, Россия (119454 Россия, г. Москва, проспект Вернадского, 78), e-mail: dtghmflysq@gmail.com*

**Рассматривается опыт разработок интегрированных интеллектуальных систем мониторинга и обеспечения безопасности стратегических и социально-значимых объектов и территорий. Предлагается открытая архитектура распределенной (полицентирической) сети ситуационных и информационно-аналитических центров, интерфейсы, протоколы и процедуры межведомственного взаимодействия. Обсуждаются проблемы организационно-методического обеспечения разработок и стандартизации технологических платформ в сфере комплексной безопасности технических объектов и систем.**

Ключевые слова: мониторинг, распределенные системы, интеграция, архитектура систем, информационные технологии, ситуационный центр, безопасность, технологическая платформа, стандартизация.

# EXPERIENCE OF INTEGRATION AND PROBLEMS OF STANDARDIZATION OF DISTRIBUTED (POLYCENTRIC) NETWORK SITUATIONAL AND INFORMATIONAL-ANALYTICAL CENTERS OF MONITORING OF THE STATE OF STRATEGIC AND SOCIALLY IMPORTANT OBJECTS AND AREAS

**[1]Kudelkin V.A.**

*[1] Federal State Educational Institution of Higher Education «Moscow State University of Information Technologies, Radio Engineering and Electronics»(MIREA),Moscow, Russia (119454 Russia, Moscow, Vernadskogo avenu, 78), e-mail: dtghmflysq@gmail.com*

**The experience of the development of integrated intelligent monitoring systems and security strategic and socially important objects and areas. Proposed open architecture distributed (polycentricism) network situational and informational-analytical centers, interfaces, protocols and procedures of interagency cooperation. Discusses the problems of organizational and methodological support of the development and standardization of technology platforms in the field of integrated safety of technical objects and systems.**

Key words: monitoring, distributed systems, integration, system architecture, information technology, situation center, security, technological platform, standardization.

Анализ реального состояния систем безопасности стратегических объектов государства, промышленных объектов, Городов и социальной сферы, результативности и эффективности их применения в критических ситуациях показывает ряд существенных недостатков и проблем системного обоснования проектов систем. Требуется ряд существенных мер на федеральном и региональном уровне по правовому и организационно-методическому обеспечению, координации и консолидированному ресурсообеспечению проектов

безопасности. Особая роль при разработке таких систем отводится вопросам унификации и стандартизации системной архитектуры, оборудования и программного обеспечения. Анализ опыта отечественных и зарубежных разработок распределенных организационно-технических систем управления объектами, процессами и ресурсами инфраструктуры Городов, транспорта, энергетики, промышленных предприятий, и др. показывает актуальность задач обеспечения защиты информационных и иных ресурсов от различного рода негативных и внешних воздействий..

Можно утверждать, что к настоящему времени развитие ИКТ и индустрии безопасности обеспечивают технические возможности практически полного «тотального» контроля всех объектов и субъектов безопасности на разных уровнях управления. Однако при создании систем безопасности предприятий, муниципальных образований, регионов и государства, помимо технических, организационных и финансовых аспектов, необходимо решение общезначимых проблем законности, соблюдения правовых, психологических и морально-этических аспектов создания и эксплуатации таких систем. Поэтому на передний план выступают задачи мотивации и формирования целевого назначения, корректной постановки задачи и обоснованного выбора средств обеспечения безопасности конкретных объектов с учетом состояния уровня уязвимости/защищенности объектов, интенсивности и объемов негативных внутренних и внешних воздействий, оценки их влияния на устойчивость, целостность, безопасность и результативность. Анализ состояния ИКТ и тенденций развития индустрии безопасности показывает актуальность решения задач построения в России распределенной (полицентрической) сети ситуационных и информационно-аналитических центров (РСИАЦ), работающих по единым правилам и стандартам на функциональную архитектуру систем, компоненты, интерфейсы, согласованным регламентам и процедурам взаимодействия, протоколам обмена данными в системах принятия решений на разных уровнях управления.

Разработка организационно–правовых механизмов, методических и инструментальных средств РСИАЦ направлена на снятие неопределенности в деятельности организаций и предприятий, минимизацию совокупных затрат на создание и эксплуатацию систем безопасности и, главное, на минимизацию ущербов в деятельности стратегических объектов инфраструктуры (энергетика, транспорт, строительство, оборона и др.) и социальных значимых объектов в регионах (коммунальное хозяйство здравоохранение, общественная безопасность, экология и др.).

Концепции и основные целевые задачи создания РСИАЦ определены в работах /1-5 / Среди них особо выделяются:

• системное описание объектов, процессов и ресурсов предприятий и корректная постановки задач мониторинга состояния их целостности в аварийных и критических ситуациях;

• упорядочение организационно - правовых, экономических и технических механизмов разработок и эксплуатации систем безопасности предприятий и минимизации рисков реализации проектов;

• разработка функционально-полной архитектуры систем безопасности объектов, процессов и ресурсов с повышенными рисками и угрозами безопасности, их «встраивание» в действующие системы управления объектами;

• обеспечение необходимой координации разработок и консолидированного ресурсообеспечения проектов РСИАЦ на основе принятых стандартов и соглашений о взаимодействии.

В качестве примера на рис. 1. приведена обобщенная структура взаимодействия объектов и субъектов мониторинга «Безопасного города»


Рис.1. Структура взаимодействия субъектов и объектов РИАСЦ города

Средства РСИАЦ должны обеспечивать саморегулируемые информационные обмены между предприятиями в различных сферах экономики, содержать средства мониторинга событий - инцидентов угроз безопасности на разных уровнях управления объектами, средства аналитической обработки данных и принятия решений по восстановлению целостности объектов. унифицированные процедуры актуализации и хранения данных, предоставлять

инструменты для оценки и согласования необходимых ресурсов для восстановления целостности объектов в аварийных и критических ситуациях.

В настоящее время в России накоплен определенный опыт разработок программно-аппаратных технологических платформ систем безопасности, среди которых следует отметить следующие:

программно-аппаратная платформа систем физической защиты объектов «Индигирка» (ООО «Сигма - интегрированные системы»);

- радиочастотные системы охранно-пожарной сигнализации «АРГУС-СПЕКТР);
- интегрированные интеллектуальные системы мониторинга и обеспечения безопасности распределенных объектов предприятий и территорий «ИИСМиБП» ( ЗАО «Интегра-С»);

- системы интеллектуального видеонаблюдения «Интеллект» (ITV);
- Комплексная Автоматизированная Информационная Система безопасности ( ЗАО «Технокерт»);
- «Ароганит-Мегаполис» (группа компаний Insystem);
- системы оповещения ОКСИОН, НАБАТ (МЧС) и др.

На базе этих разработок формируются типовые проектные решения (ТПР), ориентированные для применения в отдельных ведомствах (РЖД, РОСНЕФТЬ, МВД, МЧС, РОСАТОМ, РОСМОРРЕЧФЛОТ, РОСАВТОДОРи др.). Вместе с тем следует отметить, что применение ИИСМиБП в ведомственных и региональных ситуационных центрах сдерживается практическим отсутствием унифицированных архитектурных моделей зданий и обустройства Территорий, неполнотой, не своевременной актуализацией и несогласованностью информационных баз данных о состоянии объектов мониторинга, неотработанностью регламентов, протоколов и форматов обмена данными для принятия решений в аварийных и критических ситуациях.

Развитие интеграционных процессов в сфере ИКТ и индустрии безопасности выдвигает повышенные требования к организационной, семантической и технической интероперабельности автоматизированных систем предприятий /7-9/. Решение этих задач базируется на развитии стандартов на архитектуру, функциональные компоненты и интерфейсы ИИСМиБП /4,5 /. Открытая архитектура ИИСМиБП определяет функционально-полный состав программно-технических (ПТК) и программно-методических комплексов (ПМК) с унифицированными связями между ними. Открытые спецификации требований к функциональным компонентам ИИСМиБП, унифицированные интерфейсы и протоколы связи между компонентами распределенных систем позволяют проектным путем осуществлять выбор средств ИКТ общего назначения и специализированных средств

индустрии безопасности, а также организовать компоновку индивидуальных систем в соответствии с требованиями конкретных заказчиков.

Функциональная архитектура компонент РСИАЦ, положенная в основу проекта ГОСТ Р «Архитектура интегрированных интеллектуальных систем мониторинга распределенных объектов предприятий и территорий. Общие технические требования к оборудованию и программным средствам» / 5 / приведена на рис.2.

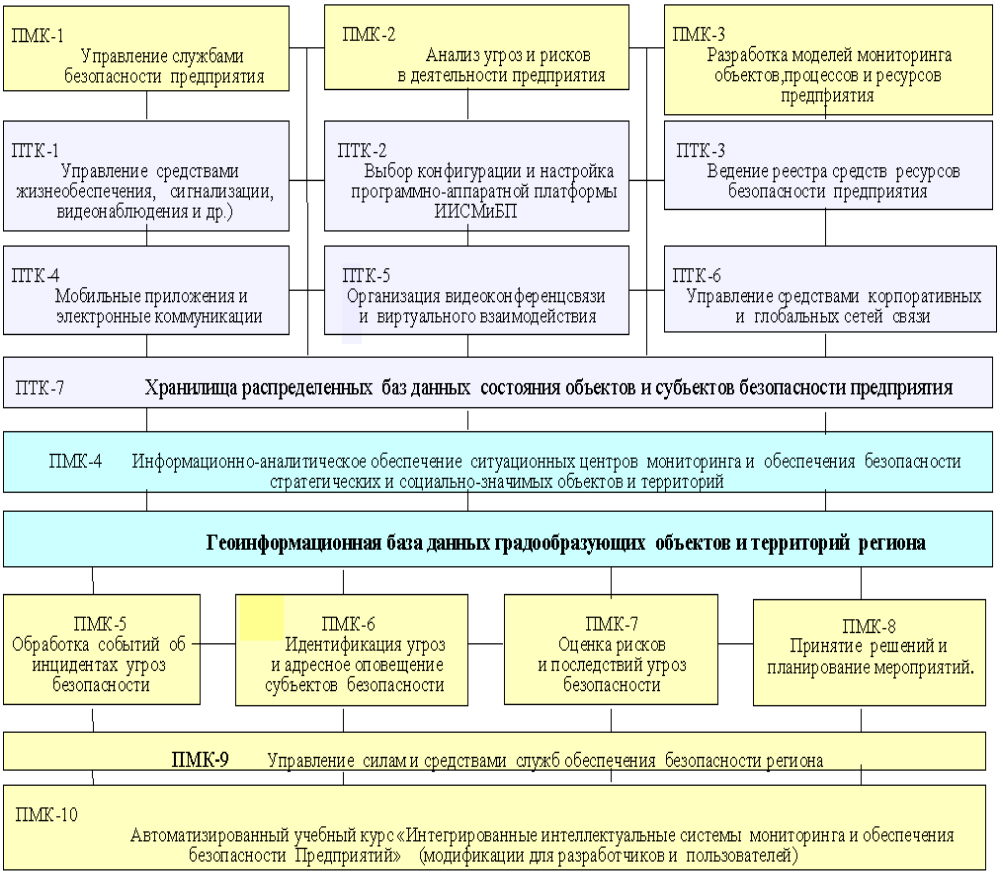


Рис.2. Функциональная архитектура прикладных компонент РИАСЦ.

Функциональные компоненты ИИСМиБП и РСИАЦ могут быть предметом отдельной поставки как комплектующие "индивидуальных" систем мониторинга объектов в ситуационных центрах предприятий, отраслей, муниципальных образований и регионов.

Применение общих технических требований к компонентам, стандартизация интерфейсов является основой интеграции систем и позволяет применять в конкретных проектах сертифицированное оборудование и программное обеспечение ИКТ от различных производителей, прошедшие испытания на совместимость и соответствие национальными и международными стандартам. Это позволяет существенно снизить зависимость предприятий заказчиков от технических решений поставщиков и недобросовестной конкуренции на рынке, стимулировать разработчиков компонент на повышение качества продуктов,

упорядочить процедуры организации конкурсов, тендеров, и закупок для комплектации, технического обслуживания и сопровождения систем.

В состав конкретных проектов ИИСМиБП и РСИАЦ включаются средства:

- контроля систем жизнеобеспечения зданий и сооружений;
- противопожарной защиты и сигнализации, оповещения персонала и служб безопасности;
- контроля доступа на территорию, здания и помещения;
- контроля состояния технологического оборудования с повышенными требованиями к безопасности персонала и окружающей среды;
- разработки концептуальных, математических и информационных моделей мониторинга объектов, процессов и ресурсов предприятия;
- автоматизированной подготовки 3D-моделей зданий, сооружений и территории объектов;
- организации видеоконференцсвязи;
- видеонаблюдения и идентификации статических и движущихся объектов;
- обработки событий о инцидентах - угроз безопасности и их наглядного отображения в динамике на 3- Д моделях и картах -схемах территорий;
- хранения данных о состоянии объектов, истории событий, принятых решениях и действий;

1. идентификации пользователей, определения их прав, полномочий и защиты информационных ресурсов предприятиия;
2. проектной компоновки конфигурации средств ИИСМиБП и настройки на условия функционирования для конкретных объектов

Особая роль в РСИАЦ отводится применению геоинформационных систем и привязке объектов мониторинга к координатам местности, решению задач информационно-аналитического обеспечения и обработки данных для принятия решений по управлению объектами, планирования ресурсов и организации взаимодействия сил и средств подразделений безопасности в аварийных и критических ситуациях, ликвидации их последствий и восстановления целостности объектов.

Актуальным являются вопросы применения в РСИАЦ основных концепций создания базовых программно-аппаратных технологических платформ и модификаций прикладных ПТК и ПМК по направлению «Комплексная безопасность промышленности и энергетики». В таблице 1. приведены предложения по перспективным направлениям НИОКР и стандартам пилотных проектов создания РСИАЦ.

Таблица 1. Направления НИОКР и стандартизации проектов РСИАЦ

| Перспективные направления НИОКР и стандартизации РСИАЦ | Основное содержание и результаты |
|---|---|
| Предпроектные исследования (обследование), оценка уязвимости/защищенности объектов и формирование требований к средствам инженерно-технической защиты объектов | Описание объектов и субъектов безопасности предприятий;<br>Показатели уязвимости / защищенности объектов |
| Методика оценки организационной, семантической и технической интероперабельности ИИСМиБП и РИАСЦ | Типология и архитектура ИИСМиБП;<br>Показатели интероперабельности;<br>Экспертные и аналитические методы оценки показателей |
| Унификация приборных интерфейсов датчиков состояния средств инженерно-технической защиты объектов | Решения по интеллектуальным средствами сбора, хранения, обработки и передачи данных в локальных и глобальных сетях |
| Требования к программно-аппаратным технологическим платформам и комплексам прикладных задач мониторинга состояния объектов | Архитектура программно - аппаратных платформ<br>Операционные системы с открытыми кодами<br>Требования к и системным интерфейсам «Объект-Сенсоры-ЭВМ-Человек-Коммуникации»<br>Средства разработки приложений |
| Типовые проектные решения и отраслевые профили ИИСМиБП | Типология и порядок разработки ТПР;<br>Требования к качеству и совместимости компонент,<br>Методы испытаний и сертификации ТПР;<br>Порядок ведения реестров ТПР |

Реализация проектов РИАСЦ требует особого внимания к гармонизациии ИТ-стандартов и стандартов в прикладных сферах деятельности предприятий (строительство, системы охранной сигнализации и антикриминальной защиты, технологии производства наукоемкой продукции, транспорт, энергетика, охрана окружающей среды) , а также со стандартами в сфере регионального развития управления проектами. .

Практическое значение организационно-методического и правового обеспечения разработок и стандартизации компонентов РИАСЦ в России сегодня остро востребовано, а в связи с решениями о вступлении в ВТО, реализации Соглашений о международном сотрудничестве со странами Таможенного союза, БРИКС, международными организациями по

стандартизации ИСО/МЭК, СЕН/СЕНЕЛЕК и др. будет еще более востребованным и потребует гармонизации с международными стандартами, в том числе для обеспечения конкуретоспособности отечественной продукции на рынке ИКТ и индустрии средств безопасности.

Список литературы


1. Денисов В. Ф. Куделькин В. А. Архитектура интегрированных интеллектуальных систем обеспечения комплексной безопасности государства//Труды третьей всероссийской конф. «Стандартизация информационных технологий и интероперабельность» (СИТОП - 2009). - М.: ОИТ и ВС РАН, ФАИТ, 2009. С. 61–66.
2. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем. М.: Изд. «Вооружение. Политика. Конверсия», 2008г.-404 с.
3. Прохоров С.А., Федосеев А.А., Денисов В.Ф., Иващенко А.В. Методы и средства проектирования профилей интегрированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения. // Самара, СамНЦ РАН, 2009- 199с..
4. Куделькин В.А., Денисов В.Ф. Модели и инструментальные средства мониторинга состояния комплексной безопасности стратегических объектов и территорий.// журнал «Мониторинг. Наука и безопасность.» - М., 2012, №2 (6),с. 16-24.
5. Куделькин В.А., Денисов В.Ф. Архитектура интегрированных распределенных систем мониторинга и обеспечения безопасности организационно-технических систем и территорий// журнал «Мониторинг. Наука и безопасность.» - М., 2012, №4 (12),с. 64- 79.
6. Габричидзе Т.Г. Основы комплексной системы безопасности критически важных (потенциально опасных) объектов муниципального и регионального уровня. - Самара
: Изд-во СамНЦ РАН , 2012 .-392 с.
7. Куделькин В.А., Денисов В.Ф. Организационно-методическое обеспечение и стандартизация стратегических и социально-значимых объектов и территорий. // журнал «Интеграл.», №1(74),2014 г., с.50-52
8. ГОСТ Р 55062-2012 «Системы промышленной автоматизации и их интеграция. Интероперабельность». Основные положения.
9. ISO/IEC JTC1/SC7/WG4 N597 2012-01-15. Software and systems engineering – Reference model for product line engineering and management.
10. Р50.1.041-2002 «Информационные технологии. Проектирование профилей среды открытой системы».