

# НЕОБХОДИМОСТЬ СТАНДАРТИЗАЦИИ РАЗРАБОТОК РАСПРЕДЕЛЕННЫХ ИНТЕГРИРОВАННЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ И РЕГИОНОВ

Куделькин В.А., Денисов В.Ф.

*Подкомитет ПК125 «Взаимосвязь оборудования для информационных технологий» Национального технического комитета по стандартизации ТК 22 «Информационные технологии»*

---

**Рассматриваются проблемы стандартизации распределенных интегрированных систем обеспечения комплексной безопасности предприятий и регионов.**

---

Ключевые слова: предприятия, архитектура систем, комплексная безопасность

## NECESSITY STANDARDIZATION OF DEVELOPMENT OF DISTRIBUTED INTEGRATED SYSTEMS OF ENSURING COMPREHENSIVE SAFETY OF ENTERPRISES AND REGIONS

Kudelkin V.A., Denisov V.F.

*Subcommittee PK125 "Interconnection of information technology equipment" of the National Technical Committee for Standardization TC 22 "Information Technology"*

---

**We consider the problems of standardization of integrated systems of complex safety of enterprises and regions.**

---

Keywords: enterprise, system architecture, integrated security

Распределенные интегрированные системы комплексной безопасности (безопасности предприятий и регионов (РИИСКБП) разрабатываются для объектов транспорта, энергетики, промышленности, коммунальных служб и других стратегических и социально-значимых объектов и территорий.

Основные проблемы создания РИИСКБП связаны с исходной неопределенностью оценок состояния объектов управления, многообразием внутренних и внешних негативных воздействий, приводящих к нарушению целостности объектов и безопасности человека, рискам в деятельности предприятий.

Функциональные компоненты РИИСКБП обычно основаны на различных «отраслевых» концепциях обеспечения безопасности отдельных объектов, используют различные методы описания объектов, процессов и ресурсов информационных систем, реализуются на различных программно-аппаратных платформах с применением оборудования и программных средств информационно-коммуникационных технологий от различных производителей. При этом естественно, возникает проблема обоснования рациональной архитектуры конкретных систем - «проблема интероперабельности» [1].

Обеспечение интероперабельности основано на методологии открытых систем и предусматривает решение задач стандартизации системной архитектуры и функциональных элементов организационно-методического, нормативного, технического и программного обеспечения, интерфейсов и протоколов обмена данными в локальных и глобальных сетях электронного взаимодействия предприятий.

Опыт разработок РИИСКБП [2,3] показывает актуальность создания в регионах России полицентрической сети отраслевых и межведомственных ситуационных центров корпоративных предприятий, муниципальных образований и регионов, работающих по единым стандартам, определяющим типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий [4], а также порядок применения типовых проектных решений, протоколов обмена данными, требования к испытаниям, сертификации оборудования на соответствие принятым национальным и международным стандартам. Особая роль отводится вопросам обоснования и применения методов информационного моделирования для обоснования архитектуры обеспечения организационной, семантической и технической интероперабельности, совместимости оборудования и программных средств от различных производителей, организации технического обслуживания и

сопровождения систем.

Развитие полицентрической сети ИИСКБП в регионах требует упорядочения применения геопространственных данных (картография, цифровые трехмерные модели объектов и местности, мониторинг природных явлений и техногенных катастроф) в таких областях, как городской транспорт, энергетика, коммунальное хозяйство, общественная безопасность, сельское хозяйство. В ряде отраслевых и региональных ситуационных центрах используются различные конструктивные 3-D модели зданий, сооружений и территорий, интерфейсы, форматы и протоколы обмена геопространственными данными, что не в полной мере обеспечивает решение задач согласованного управления объектами в аварийных и критических ситуациях. Актуальным направлением развития РИСКБПиТ является применение унифицированных программно-аппаратных технологических платформ интеграции оборудования и программного обеспечения ИКТ общего и специального назначения от различных производителей, операционных систем с открытыми кодами, открытых спецификаций требований к комплексам прикладных задач обработки данных на рабочих местах операторов и аналитиков служб эксплуатации и безопасности, мобильных приложений для удаленных пользователей - потребителей информационных ресурсов предприятий

Опыт разработок ИСКБП [2, 3] показывает актуальность выбора рациональной архитектуры обеспечения безопасности предприятий и территорий [5], а также порядок применения типовых проектных решений, протоколов обмена данными, требования к испытаниям, сертификации оборудования на соответствие принятым национальным и международным стандартам.

В состав базовой архитектуры ИСКБП и территорий включаются:

- комплексы прикладных программ обработки данных и принятия решений;
- системы хранения «больших» данных о состоянии объектов;
- системы отображения 3-D моделей объектов и территорий;
- системы организации доступа пользователей к геоинформационным базам данных градообразующих объектов и территорий региона.
- программно-аппаратная технологическая платформа интеграции прикладных систем;
- системные интерфейсы и протоколы обмена данными, интерфейсы пользователей прикладных программ;
- программно-технические комплексы (ПТК) проектной компоновки конфигурации программно-аппаратной платформы, интерфейсов и протоколов обмена данными для конкретных потребителей;
- программно-методические комплексы (ПМК) организации распределенных служб и сервисов средств эксплуатации и технического обслуживания.

Ключевым элементом РИСКБП являются ситуационные и информационно-аналитические центры (узлы распределенной полицентрической сети служб мониторинга состояния объектов, обеспечения безопасности и восстановлении целостности объектов в аварийных и критических ситуациях. Пример функциональной архитектуры типового ситуационного приведен на рис. 1.

Наиболее перспективными при построении РИИСКБП являются инновационные подходы, включающие актуализацию задач гармонизации стандартов на архитектуру, оборудование и технологии РСИАЦ со стандартами в прикладных сферах, таких как строительство, энергетика, транспорт, охрана и антикриминальная защита объектов, охрана окружающей среды, информационная безопасность и др.

В основе этих подходов - необходимость сотрудничества участников проектов, соглашения о координации и консолидированном ресурсообеспечении проектов РСИАЦ на основе развития механизмов государственно-частного партнерства.

#### Список литературы

1. ГОСТР 55062-2012. Информационные технологии. Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения.
2. Куделькин В.А., Денисов В.Ф. Архитектура интегрированных распределенных систем мониторинга и обеспечения безопасности организационно-технических систем и территорий.//Мониторинг. Наука и безопасность», 2013, №4 (12), с. 64-79.
3. Куделькин В.А., Денисов В.Ф. Организационно-методическое обеспечение и стандартизация интегрированных систем мониторинга и обеспечения безопасности стратегических и социально значимых объектов и территорий государства// Журн. Интеграл, № 1 (74), 2014 г, с.50-52.
4. Денисов В.Ф., Куделькин В.А. Архитектура и профили автоматизированных систем обеспечения

деятельности предприятий инфраструктуры инновационного развития региона./ Труды второй международной конф. "Стандартизация информационных технологий и интероперабельность"(СИТОП-2008)- М.: ОИТ и ВС РАН, ФАИТ и др., с. 42-48.

ГОСТ Р 56875-2016. Информационные технологии. Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий.



Рис.1. Функциональная архитектура типового ситуационного центра

#### References

1. GOST R 55062-2012. Information Technology. Industrial automation systems and integration. Interoperability. The main provisions.
2. Kudelkin V.A., Denisov V.F. Architecture of integrated distributed monitoring systems and safety technical-organizational systems and territories // monitoring. Science and Security ", 2013, №4 (12), p. 64-79.
3. Kudelkin V.A., Denisov V.F. Organizational and methodological support and standardization of integrated systems for monitoring and ensuring the security of strategic and social facilities and areas of the state // Journal. The integral, number 1 (74), 2014, s.50-52.
4. 4. Denisov V.F., Kudelkin V.A. Architecture and profiles of the automated systems of enterprises providing innovative infrastructure development in the region. / Proceedings of the Second International Conf. "Standardizing Information Technology and Interoperability" (SITOP 2008) - М.: ICU and Sun RAS, FAIT, etc., with.. 42-48.
5. GOST R 56875-2016. Information Technology. Security systems complex and integrated. Typical requirements for the architecture and technology of intelligent monitoring systems for security enterprises and territories.