6. Гизатуллин З.М. Анализ воздействия высоковольтных линий электропередачи на функционирование цифровых элементов печатных плат // Технологии электромагнитной совместимости. – 2006. – № 3. – С. 3.

7. Гизатуллин З.М., Гизатуллин Р.М. Экспериментальные исследования помехоустойчивости персонального компьютера при импульсном разряде статического электричества // Вестник Казанского государственного технического университета им. А.Н. Туполева . – 2011. – №3. – С. 78-83.

8. Гизатуллин З.М. Электромагнитная совместимость электронно-вычислительных средств при воздействии электростатического разряда // Известия высших учебных заведений. Проблемы энергетики. – 2009. - №1-2. – С. 104-112.

В.Ф. Денисов

АРХИТЕКТУРА И ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОЙ (ПОЛИЦЕНТРИЧЕСКОЙ) СЕТИ СИТУАЦИОННЫХ ЦЕНТРОВ

(Консорциум «Интегра-С», АНО «Группа ИТ-стандарт»)

Интегрированные интеллектуальные системы мониторинга и обеспечения безопасности предприятий (ИИСМиБП) разрабатываются на ряде объектов транспорта, энергетики, промышленности, коммунальных служб, экология, общественная безопасность и др.). Такие системы:

1. **базируются** на применении информационно-коммуникационных технологий (ИКТ) общего назначения и специализированных средств защиты объектов, процессов и ресурсов предприятий;
2. в**ыполняют функции** сбора и упорядочения данных о состоянии целостности и безопасности стационарных и движущихся объектов;
3. **обеспечивают** идентификацию событий, анализ реального состояния объектов, подготовку решений и рекомендаций по управлению объектами в аварийных и критических ситуациях;
4. **решают задачи** планирования и распределения ресурсов, необходимых для поддержания целостности, защиты объектов от разного рода негативных воздействий;
5. **осуществляют координацию** мероприятий по восстановлению целостности объектов и ликвидации последствий аварийных и критических ситуаций;
6. **поддерживают эксплуатацию** и техническое обслуживание средств ИКТ и оперативного взаимодействия объектов со службами безопасности регионов (МВД, МЧС и др.).

Анализ состояния разработок ИИСМиБП [1-3] показывает актуальность решения задач создания в России полицентрической сети ситуационных и информационно-аналитических центров (РСИАЦ), работающих по единым стандартам на функциональную архитектуру систем, компоненты ИКТ, интерфейсы

и протоколы обмена данными, регламентам взаимодействия служб по ликвидации аварийных и критических ситуаций на разных уровнях управления.

В состав полицентрической сети РСИАЦ входят региональные, муниципальные и отраслевые ситуационные и информационно-аналитические центры, которые обладают определенными компетенциями и ресурсами, реализуют основные функции ИИСМиБП в заданной сфере деятельности, взаимодействуют с органами государственной власти и местного самоуправления, владельцами знаний и технологий, учебными центрами, общественными профессиональными организациями, финансовыми институтами и др.).

Основные проблемы создания функционально-полных РСИАЦ связаны с исходной неопределенностью состояния объектов, вероятностно-статистическими характеристиками процессов, а также мотивами владельцев объектов, разработчиков систем, провайдеров сетей и других участников проектов, несогласованностью организационно-правовой базы и ведомственная разобщенность проектов.

Следует отметить, что разработка РСИАЦ сдерживается практическим отсутствием конструктивных 3-Д моделей зданий и сооружений, неполнотой, несогласованностью и не своевременной актуализацией геопространственных данных в организациях инфраструктуры регионального развития и ситуационных центрах, осуществляющих мониторинг состояния закрепленных за ними объектов.

Функциональные компоненты РСИАЦ обычно реализуются на разных программно-аппаратных технологических платформах. При этом, естественно, возникает проблема обеспечения их взаимодействия - «проблема интероперабельности» [2]. Эта проблема должна решаться с использованием региональных и отраслевых профилей РСИАЦ [1], учитывающих особенности объектов (оргструктуры, технологии, математические модели процессов, характерстики потенциальных угроз целостности и безопасности объектов, состояние «наследуемых» ИКТ, средств инженерно-технической защиты объектов и территорий, рисков в деятельности предприятий.

Особая роль при разработке РСИАЦ отводится вопросам унификации и стандартизации системной архитектуры, унификации компонент, интерфейсов и протоколов обмена данными, обеспечения организационной, семантической и технической интероперабельности, совместимости оборудования и программных средств от различных производителей.

Средства РСИАЦ должны **обеспечивать** саморегулируемые информационные обмены между узлами, **содержать** унифицированные процедуры формирования и актуализации геопространственных данных о состоянии объектов, концептуальные модели, средства аналитической обработки данных и принятия решений по восстановлению целостности объектов **предоставлять** инструменты интеграции и согласования необходимых ресурсов управления объектами.

Технологии проектирования РСИАЦ определяются в соответствии с основными положениям ГОСТ Р/ИСО12207-2006 «Системная инженерия. Стадии

жизненного цикла систем" и предусматривают выполнение следующих основных работ:

- обследование объектов, разработка концептуальных, математических и информационных моделей деятельности по закрепленным сферам ответственности ситуационного центра;
- разработка соглашений о взаимодействии узлов РСИАЦ;
- выбор архитектуры и прикладных средств обработки данных;
- проектирование (приобретение) оборудования и программных средств;
- тестирование компонент на совместимость, комплексирование, организация системных испытаний;
- подготовка объектов к внедрению, разработка моделей технического обслуживания.

В состав типовых проектов оснащения ситуационных центров включаются:

- системы связи и защищенных коммуникаций с удаленными объектами мониторинга;
- средства идентификации пользователей, определения их прав, полномочий и защиты информационных ресурсов в, т.ч., с применением средств «электронной подписи»;
- системы отображения данных о состоянии объектов с применением динамических трехмерных 3D-моделей зданий и сооружений с привязкой к географическим координатам местности;
- системы хранения данных (включая тексты, коды, аудио, видео и др.) и
- информационно-поисковые системы по запросам пользователей;
- системы моделирования, оценки ситуаций и принятия решений, оценки необходимых ресурсов для восстановления целостности объектов;
- системы адресного оповещения служб безопасности и восстановления целостности объектов в аварийных и критических ситуациях.

Пример функциональной архитектуры типового ситуационного цента как узла РИАСЦ приведен на рис.1.

Учитывая инфраструктурный характер РСИАЦ особое внимание необходимо уделять механизмам самоорганизации и координации работ заказчиков, исполнителей, поставщиков компонент, консолидированной разработке проектов и организационно -технических мероприятий по их реализации, в. т.ч., основанных на развитии сервис -ориентрованной архитектуры и услуг ситуационных центров.

Разработка организационно-правового и нормативно-методического обеспечения РСИАЦ, методических и инструментальных средств РСИАЦ [5] направлена на снятие неопределенности в деятельности предприятий минимизацию совокупных затрат на создание и эксплуатацию средств РСИАЦ и, главное, на минимизацию ущербов в деятельности стратегических объектов инфраструктуры региона и предприятий (энергетика, транспорт, строительство, оборона и др.) и социальных значимых объектов в регионах (коммунальное хозяйство здравоохранение, общественная безопасность, экология и др.).

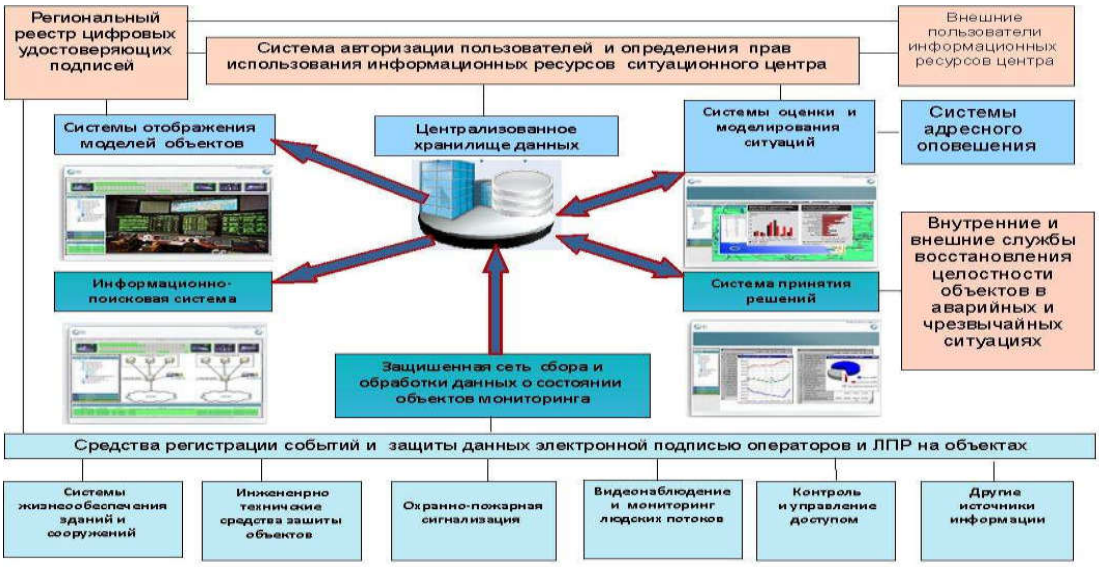

Рис.1. Функциональная архитектура типового ситуационного центра

Актуальными являются вопросы применения в узлах РСИАЦ унифицированных программно-аппаратных технологических платформ и прикладных систем ИИСМиБП под управлением открытых операционных систем с открытыми кодами, открытых спецификаций требований к комплексам прикладных задач на рабочих местах операторов и аналитиков служб безопасности, мобильным приложениям удаленных пользователей - потребителей информационных ресурсов РСИАЦ.

Ситуационные центры могут создаваться на разных уровнях управления объектами региона и быть ориентированы на решение прикладных задач в сферах своей деятельности. Однако важно обеспечить их межведомственное взаимодействие со смежными центрами РСИАЦ и органами принятия решений

Реализация проектов РИАСЦ требует особого внимания к решению задач гармонизации ИТ-стандартов и стандартов в прикладных сферах деятельности предприятий, таких как строительство, системы охранной сигнализации и антикриминальной защиты, технологии производства продукции, транспортных систем, энергетики, охраны окружающей среды и др., а также со стандартами в сфере регионального развития, консолидированного ресурсообеспечения и управления проектами.

Разрабатываемые типовые проектные решения РСИАЦ позволяют существенно сократить сроки проектирования, обеспечить снижение совокупной стоимости владения средствами ИИСМиБП на объектах, затрат на эксплуатацию, техническое обслуживание и сопровождение.

Литература

1. 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, СНЦ РАН, 2009- 199с., илл.

2. ГОСТ Р 55062-2012 «Системы промышленной автоматизации и их интеграция. Интероперабельнсть . Основные положения.

3. 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.

4. 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.

5. 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.

6. ISO/IEC DIS 18384-3 Distributed Application Platforms and Services (DAPS)-Reference Architecture for Service Oriented Architecture(SOA). Part 3:Service Oriented Architecture Ontology (draft international standard)

Е.Г. Загузина

ПОСТРОЕНИЕ ФУНКЦИИ РАБОТОСПОСОБНОСТИ ПРИ ОЦЕНКЕ «ЖИВУЧЕСТИ» СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

(Санкт-Петербургский государственный экономический университет)

В условиях информационной экономики одним из актуальных вопросов является сохранение информационной безопасности государства. Информационная безопасность является основной составляющей национальной безопасности. Условием информационной безопасности является наличие системы защиты информации (СЗИ), представляющей собой в широком смысле сложно структурированную систему, работа которой направлена на защиту критической инфраструктуры государства. В более узком смысле СЗИ представляет собой комплекс организационных и технических мер, направленных на обеспечение информационной безопасности. Главным объектом защиты являются данные, которые обрабатываются в автоматизированной системе управления (АСУ) и задействованы при выполнении бизнес-процессов.

Как любая другая система, СЗИ должна обладать основными свойствами системы, обеспечивающими работу системы в целом и ее элементов. Одна из форм свойства устойчивости (способности противостоять разрушающим систему воздействиям) является свойство «живучесть», которое определяется работоспособностью системы. Термин «живучесть» заимствован из терминологии биологических систем.

Живучесть СЗИ представляет собой способность системы сохранять и восстанавливать выполнение основных функций в заданном объеме и на протяжении заданного времени в случае изменения структуры системы и/или алгоритмов и