ТЕХНОЛОГИИ И СТАНДАРТЫ РАСПРЕДЕЛЕННОЙ (ПОЛИЦЕНТРИЧЕСКОЙ) СЕТИ СИТУАЦИОННЫХ И ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ ЦЕНТРОВ В РЕГИОНАХ РОССИИ

[1]Денисов В.Ф., [1]Куделькин В.А.

[1]ЗАО «Интегра-С», 443084, Самарская обл., Самара, ул. Стара Загора, 96А, e-mail: zaovolga@integra-s.com

Рассматриваются современные концепции, организационно-технические модели и технологии распределенной сети ситуационных и информационно - аналитических центров обеспечения комплексной безопасности стратегических и социально-значимых объектов и территорий государства. Предлагается открытая архитектура сети, системные требования к компонентам, интерфейсам и протоколам межведомственного взаимодействия. Особое внимание уделяется вопросам интеграции, стандартизации и обеспечения организационной, семантической и технической интероперабельности прикладных систем обработки данных.

Ключевые слова: безопасность, ситуационный центр, открытые системы, интерфейсы, протоколы связи, типовые проектные решения, стандартизация

TECHNOLOGY AND STANDARDS DISTRIBUTION (POLYCENTRIC) NETWORK SITUATIONAL AND ANALYTICAL CENTERS IN THE REGION OF RUSSIA

[1]Denisov V.F., [1]KudelkinV.A.

[1] "Integra-S", 443084, Samara region., Samara, st. Stara Zagora, 96A, e-mail: zaovolga@integra-s.com

We consider the current concept, organizational and technical models and distributed network technology and situational information - think tanks provide a comprehensive security policy and socially important facilities and areas of the state. It is proposed to open network architecture, system requirements to components, interfaces and protocols interagency cooperation. Particular attention is paid to the integration, standardization and organizational, semantic and technical interoperability of the application data processing systems.

Keywords: security, situation center, open systems, interfaces, communication protocols, standard design solutions, standardization

Интегрированные системы комплексной безопасности и предприятий (ИСКБП) разрабатываются для объектов транспорта, энергетики, промышленности, коммунальных служб и других стратегических и социально-значимых объектов и территорий. Такие системы в**ыполняют функции** сбора и упорядочения данных о состоянии целостности и безопасности стационарных и движущихся объектов, **обеспечивают** идентификацию событий, анализ реального состояния объектов, подготовку решений и рекомендаций по управлению объектами в аварийных и критических ситуациях; **решают задачи** планирования и распределения ресурсов, необходимых для поддержания целостности, защиты объектов от разного рода негативных воздействий, **осуществляют координацию** мероприятий по восстановлению целостности объектов и ликвидации последствий аварийных и критических ситуаций; **поддерживают эксплуатацию** и техническое обслуживание средств ИКТ и оперативного взаимодействия объектов со службами безопасности регионов (МВД, МЧС и др.).

Анализ состояния разработок ИСКБП [1-3] показывает актуальность решения задач построения в России распределенной (полицентрической) сети ситуационных и информационно-аналитических центров (РСИАЦ), работающих по единым стандартам на архитектуру систем, компоненты ИКТ, интерфейсы и протоколы обмена данными, согласованным регламентам взаимодействия служб по ликвидации аварийных и критических ситуаций на разных уровнях управления.

Разработана базовая модель деятельности ситуационных центров предприятий (рис.1), которая определяет требования к организационно-методическому обеспечению, общие процессы и функции подразделений, сферы взаимодействия с внешним окружением, а также требования к методам принятия решений и взаимодействия участников проектов.

Базовая модель носит универсальный характер и обладает свойствами инвариантности относительно применяемых методов и средств для конкретных сфер применения. В зависимости от характеристик объектов мониторинга необходима разработка индивидуальной концепции и системного проекта обеспечения комплексной безопасности на основе системного анализа защищенности и уязвимости стратегических (оборона, энергетика, транспорт) и социально-значимых объектов (строительство, ЖКХ, образование, здравоохранение и др.) региона.

В состав РСИАЦ входят региональные, муниципальные и отраслевые ситуационные и информационно-аналитические центры, которые обладают определенными компетенциями и ресурсами, реализуют функции мониторинга и анализа состояния объектов 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.).

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.

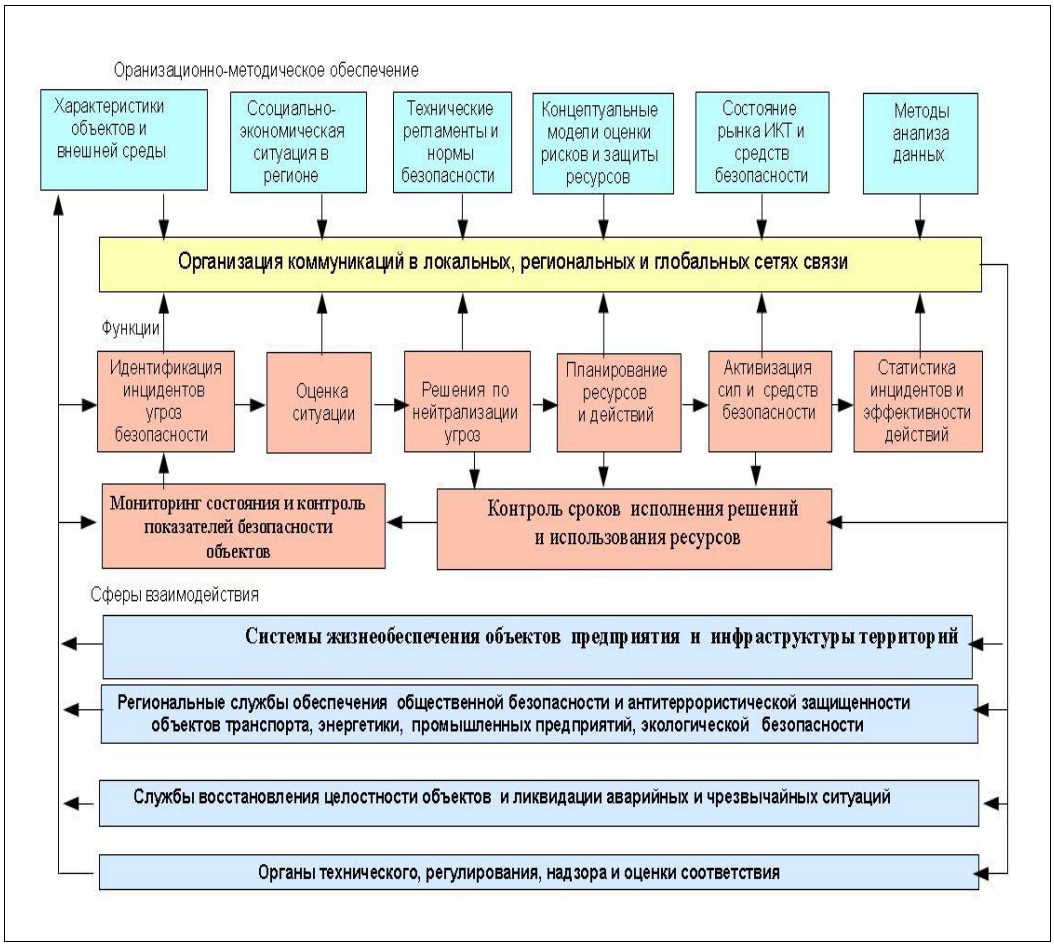

Рис.1. Обобщенная модель деятельности ситуационного центра

Функциональные компоненты РСИАЦ обычно реализуются на разных программно-аппаратных технологических платформах. При этом, естественно, возникает проблема обеспечения их взаимодействия - «проблема интероперабельности» [4]. Эта проблема должна решаться с использованием региональных и отраслевых профилей РСИАЦ, учитывающих особенности объектов (оргструктуры, технологии, математические модели процессов, характеристики 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, компонент, интерфейсов и протоколов обмена данными в системах муж ведомственного взаимодействия служб безопасности на разных уровнях управления объектами и территориями, согласовании действий в аварийных и критических ситуациях , организационной, семантической и

технической непрезентабельности, совместимости оборудования и программных средств от различных производителей, а также решению задач технического обслуживания и сопровождения систем .

Выбор моделей рациональной архитектуры РСИАЦ зависит от сложности объектов, геополитического положения региона, интенсивности и характеристиках потенциально опасных негативных воздействий на объекты, и оценки их влияния на состояние безопасности и показатели технико-экономического и социального развития региона и отдельных предприятий.

При постановке задач и обосновании рациональной архитектуры РСИАЦ необходимо :

- определение и упорядочение объектов и субъектов безопасности, понятийного аппарата в конкретных отраслевых сферах деятельности;
- оценка организационно - правовых и технических оснований для создания систем безопасности (по критериям минимизации рисков в деятельности предприятий, соблюдения принятых технических регламентов и норм безопасности);
- разработка функционально - полного комплекса средств информационно-коммуникационных технологий (ИКТ) и инженерно-технических средств защиты объектов и организации их производства на Российских предприятиях;
- разработка технологий проектирования и интеграции систем безопасности на основе применения апробированных типовых проектных решений и «встраивание» систем безопасности в действующие организационно-технические системы управления объектами;
- формирование требований к функциям и компетентности персонала по проектированию, эксплуатации, техническому обслуживанию и сопровождению систем.

Актуальными являются вопросы применения в РСИАЦ унифицированных программно-аппаратных технологических платформ ИКТ под управлением открытых операционных систем с открытыми кодами, унифицированных интерфейсов внешним оборудованием и комплексами прикладных задач обработки данных на рабочих местах операторов и аналитиков служб безопасности, мобильных приложений для удаленных пользователей – потребителей информационных ресурсов РСИАЦ.

В России действует ряд стандартов на географические информационные системы (ГИС) общего назначения для решения задач картографии, дистанционного зондирования земли, мониторинга природных явлений и техногенных катастроф, ликвидации аварийных и чрезвычайных ситуациях. Однако их использование в таких областях, как городской транспорт, энергетика, коммунальное хозяйство, общественная безопасность, социальное развитие, сельское хозяйство, природопользование носит ограниченный характер, используют различные форматы и протоколы обмена данными и, не в полной мере, обеспечивают решение задач актуализации геопространственных данных и их обмена со смежными структурами. В связи со стратегическим значением проблематики создания РСИАЦ весьма актуальным является формирования национальной технологической платформы комплексной безопасности и ГИС-технологий, технического регулирования формирования и использования геопростанственных данных Российской Федерации (ФГИС высокого уровня).

В СОСТАВ ТЕХНОЛОГИЙ РСИАЦ ВКЛЮЧАЮТСЯ МЕТОДИЧЕСКИЕ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА [5-7] **:**

- обследования объектов для разработки концептуальных, математических и информационных моделей по закрепленным сферам деятельности ситуационного (аналитического) центра;
- анализа информационных протоков данных и разработки соглашений о взаимодействии узлов РСИАЦ;
- проектирования архитектуры и прикладных средств обработки данных в узлах РСИАЦ (ситуационных центров регионов и предприятий , объектах мониторинга, провайдерах сетей ЭВМ, аналитиков служб безопасности, восстановления целостности объектов и ликвидации последствий аварийных и чрезвычайных ситуаций;
- идентификации пользователей, определения их прав, полномочий и защиты информационных ресурсов в, т.ч., с применением средств «электронной подписи»;
- средства регистрации и отображения данных о состоянии объектов с применением виртуальных трехмерных 3D-моделей зданий и сооружений, движущихся объектов с привязкой к географическим координатам местности;
- хранения данных об истории событий и принятых мерах
- защиты информационных ресурсов предприятий;
- оценки ситуаций, моделирования и принятия решений, потребностей в ресурсов для восстановления целостности объектов;
- средства связи с внешним окружением в региональных и глобальных сетях электронных коммуникаций, в частности, со службами безопасности и восстановления целостности объектов в аварийных и критических ситуациях.

Пример типовой функциональной архитектуры ситуационного центра приведен на рис.2.

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, а также со стандартами в сфере управления проектами, их координации и консолидированного ресурсообеспечения на основе государственно-частного партнерства.

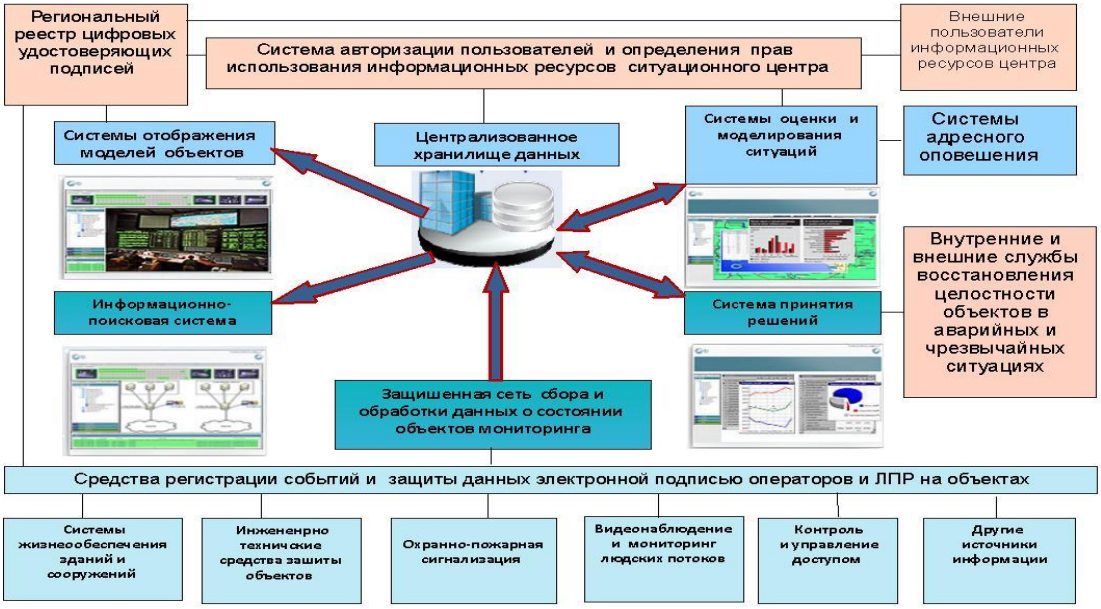

Рис.2. Типовая структура комплекса средств ситуационного центра

В этой связи в Программу национальной стандартизации предлагается включить комплекс нормативно-методических материалов и стандартов на компоненты ИСКБП и технологии проектирования РСИАЦ:

– предпроектные исследования (обследование), оценка уязвимости/защищенности объектов на стадиях жизненного цикла целевых автоматизированных систем предприятий;

– формирование требований к архитектуре РСИАЦ, средствам инженерно-технической защиты объектов, процессов и ресурсов предприятий и ситуационных центров;

– методы оценки организационной, семантической и технической интероперабельности типовых компонент ИСКБП;

– системные требования и методы испытаний программно-аппаратных технологических платформ, комплексов прикладных задач и мобильных приложений;

– организация и ведение реестров типовых проектных решений и отраслевых профилей ИСКБП. .

Типовые проектные решения ИСКБП и стандарты на компоненты, интерфейсы и протоколы межведомственного взаимодействия РСИАЦ позволят существенно сократить затраты и сроки проектирования, интеграции оборудования и программного обеспечения систем от различных производителей (это не исключает возможности конкуренции между ними за лучшее соотношение "цена - качество" типового компонента) обеспечения интероперабельности и должного взаимодействия лиц (и интеллектуальных устройств) принимающих решения на разных уровнях управления в зависимости от ситуации на объектах.

Список литературы

1. .Васильев В.А., Денисов В.Ф. Стратегии развития и концепция создания сети электронного взаимодействия предприятий./Стандарты в проектах современных информационных систем. //сборник трудов IV Всерос. практ. конф. - М.: Фостас, изд-во «Открытые системы», 2004 г.с.64-66.

2. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем формационных систем / - М.: Изд-во ВПК, 2008. - 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, СНЦ РАН, 2009- 199с., илл.

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

5. 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.

6. 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.

7. 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.

Reference

1. Vasilev V.A., Denisov V.F. Development Strategy and the concept of e-business interaction network. / Standards in projects of modern information systems. // Collection of works of IV All-Russia. Pract. Conf. - M .: FOSTAS, publishing house "Open Systems", 2004 g.s.64-66.
2. Kostogryzov A.I., Stepanov P.V. Innovative quality management and risk management in the life cycle of systems, information systems / - M .: Publishing House of the MIC, 2008. - 404 p.
3. Prokhorov S.A., Fedoseyev A.A., Denisov V.F., Ivashchenko A.V. Methods and tools for the design of integrated systems of profiles of complex safety of high-tech engineering companies. // Samara, SSC of RAS, 2009- 199s., Fig.
4. GOST R 55062-2012 "Industrial automation systems and integration. Interoperabelnst. The main provisions. "
5. Kudelkin V.A., Denisov V.F. Models and tools for monitoring the status of complex safety of strategic facilities and territories .// magazine "Monitor. Science and security. "-M., 2012, №2 (6), p. 16-24.
6. Kudelkin V.A., Denisov V.F. Architecture of integrated distributed monitoring and safety systems, organizational-technical systems and territories .// Research, Science and Security ", 2013, №4 (12), p. 64-79.
7. 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 // Zh. The integral, number 1 (74), 2014, s.50-52.