

КОМПЛЕКСНАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТА УПРАВЛЕНИЯ НА ОСНОВЕ СИТУАЦИОННОГО ЦЕНТРА¹

Симанков Владимир Сергеевич

Д.т.н., профессор, Кубанский государственный
технологический университет, г. Краснодар
vs@simankov.ru

Величко Александра Александровна

Аспирант, Кубанский государственный
технологический университет, г. Краснодар
aleksandravelichko@mail.ru

INTEGRATED SECURITY SYSTEM OF THE MANAGEMENT FACILITY BASED ON THE SITUATION CENTER

**V. Simankov
A. Velichko**

Summary. The structural analysis of the integrated security system within the hierarchical structure of the intellectual situational center is carried out. A structural and functional model of the lower-level object management system is proposed. The tasks of complex security system maintenance are considered.

Keywords: Integrated security system, management object, hierarchy, intelligent situational center.

Аннотация. Проведен структурный анализ комплексной системы обеспечения безопасности в рамках иерархической структуры интеллектуального ситуационного центра. Предложена структурно-функциональная модель системы управления объектом нижнего уровня. Рассмотрены задачи комплексного обеспечения системы безопасности.

Ключевые слова: комплексная система обеспечения безопасности, объект управления, иерархия, интеллектуальный ситуационный центр.

В настоящее время, большинство объектов управления представляют собой сложные организационно-технические системы. В рамках этого такими системами необходимо управлять в реальном режиме времени с целью избегания критических ситуаций, обеспечения безопасности объекта управления. Наиболее подходящей системой для контроля и управления в таком случае представляется ситуационный центр.

Ситуационный центр — представляет собой интеллектуальный комплекс программных и технических средств сбора, анализа и отображения информации в удобном для принятия ответственных решений виде. В настоящее время накоплен достаточный опыт по использованию ситуационных центров в различных областях деятельности[1].

В рамках любого отраслевого взаимодействия объекты управления представляют собой иерархическую систему. Каждый последующий уровень характеризуется усложнением системы взаимодействия между иерархиями. Пример иерархической системы взаимодействия объектов управления, ситуационных центров и входящих в состав ситуационного центра комплексных систем обеспечения безопасности представлена рисунке 1.

Иерархическая система ситуационных центров реализует возможность создания и функционирования комплексной безопасности объектов управления. В свою очередь ситуационный центр представляет собой сложную иерархическую организационно-техническую систему (критическая информационная инфраструктура), нуждающаяся в обеспечении комплекс-

¹ Исследование выполнено при финансовой поддержке РФФИ и администрации Краснодарского края в рамках научного проекта № 20–47–235003 «Разработка теоретических основ и алгоритмов функционирования адаптивных иерархических систем управления с использованием методов искусственного интеллекта на основе ситуационных центров»

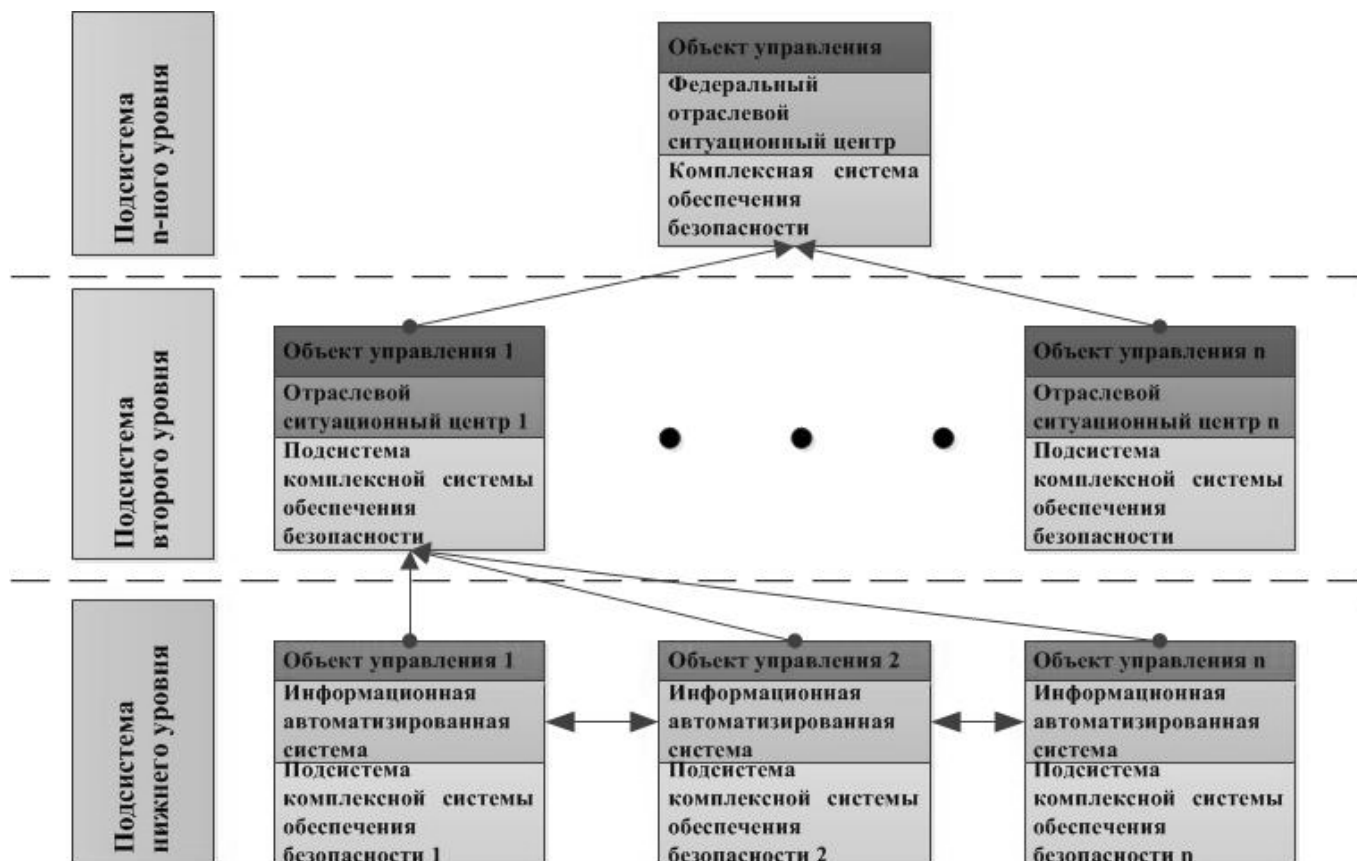


Рис. 1. Система обеспечения комплексной безопасности объекта управления на основе иерархической системы ситуационных центров

ной безопасности. В статье рассматривается иерархия структура обеспечения безопасности объекта управления на низком уровне.

Структура ситуационного центра отраслевого регионального уровня приведена в работе [3] и на рисунке 2.

Комплексная система обеспечения безопасности представляет собой часть подсистемы ситуационного центра. Организация функционирования комплексной системы обеспечения безопасности (КСОБ) строится на активном включении в ее работу информационных систем без нарушения работоспособности систем и их быстродействия. Комплексная система обеспечения безопасности объекта управления нижнего уровня – интегрированная платформа для быстрого обнаружения и реагирования на угрозы с автоматическим сбором и интеллектуальным анализом данных. Такая платформа постоянно наблюдает за безопасностью системы и не только оповещает о нарушениях и подозрительных событиях, но и создает и формирует модель событий. КСОБ поддерживает процессы мониторинга, прогнозирования, планирования и принятия решений

с точки зрения информационной и комплексной безопасности на всех этапах функционирования ситуационного центра.[2]

Комплексная система безопасности — это объединение в едином информационном поле отраслевых, государственных и муниципальных систем и их элементов (правового, нормативного, административного, организационного, технического, инженерного, материального, финансового, и иного характера), направленных на повышение защищенности и устойчивости функционирования объектов и территорий в зоне их влияния при угрозе и возникновения чрезвычайных ситуаций, в том числе вызванных террористическими акциями, а также наличие органов управления, сил и средств, обеспечивающих функционирование комплексной системы безопасности.

Основными задачами КСОБ объекта управления на основе ситуационного центра представляются следующие:

- ♦ выполнение основных функций защищаемым объектом как в нормальных, так и в чрезвычайных ситуациях (ЧС);

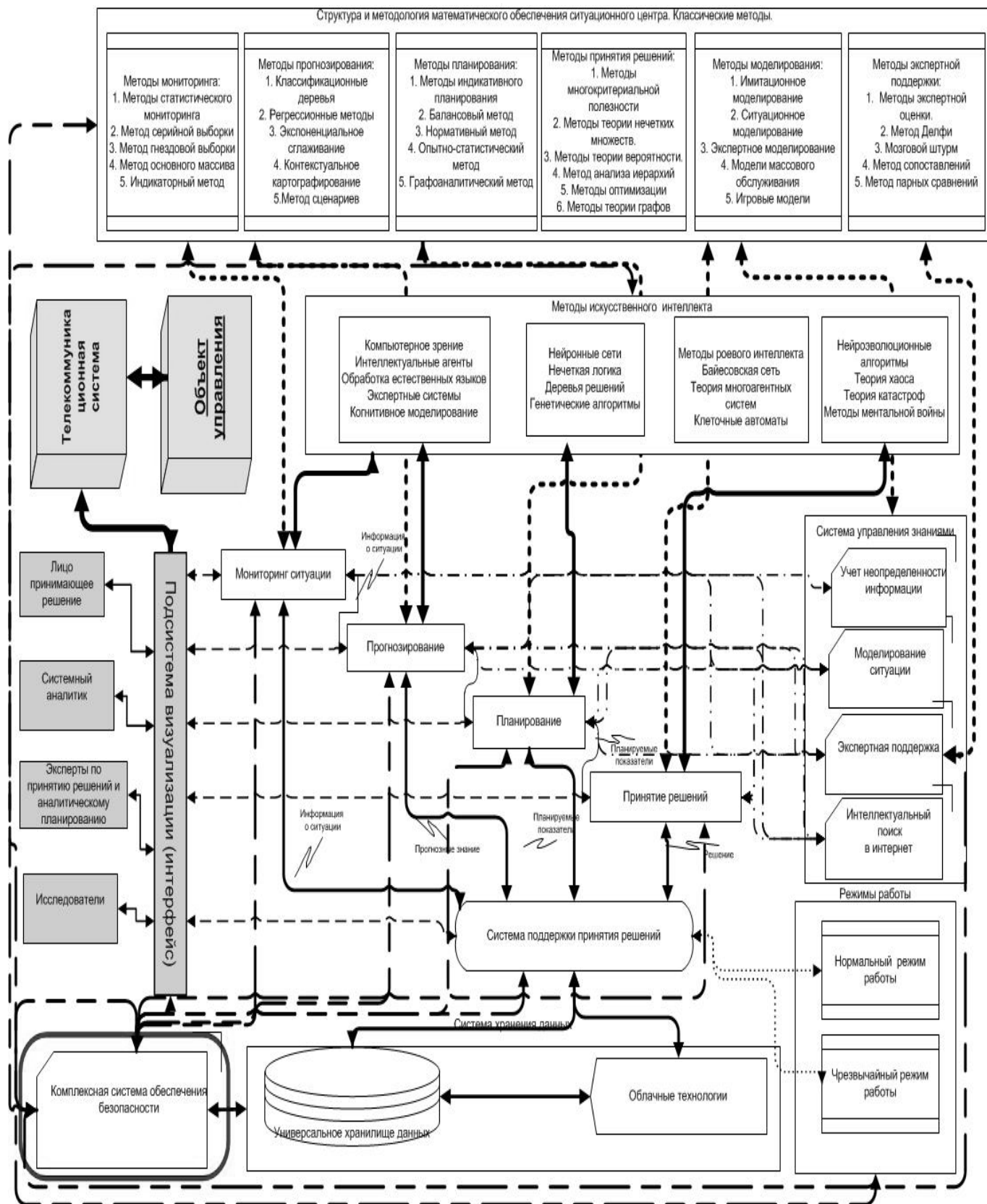


Рис. 2. Структурно-функциональная схема интеллектуального ситуационного центра[3]

- ◆ раннее обнаружение угроз и фактов их реализации или подготовки к реализации;
- ◆ своевременное информирование руководства организации об угрозах или фактах их реализации для принятия адекватных мер и исключения перехода ситуации в критическую;
- ◆ снижение риска нанесения ущерба объекту, персоналу и информации обрабатываемой на объекте при возникновении ЧС;
- ◆ организация спасения персонала, ценного имущества и информации при возникновении ЧС.

В состав комплексная система обеспечения безопасности объекта управления нижнего уровня могут быть включены следующие подсистемы:

- ◆ Подсистема автоматической пожарной сигнализации;
- ◆ Подсистема оповещения и управления эвакуацией;
- ◆ Подсистема автоматического пожаротушения;
- ◆ Подсистема автоматической охранной сигнализации;
- ◆ Подсистема видеонаблюдения;
- ◆ Подсистема контроля загазованности;
- ◆ Подсистема контроля и управления доступом;
- ◆ Подсистема сетевого управления;
- ◆ Подсистема защиты несанкционированного доступа;
- ◆ Подсистема юридического и нормативного обеспечения;
- ◆ Подсистема технических средств защиты;
- ◆ Подсистема бесперебойного питания;
- ◆ Подсистема резервного копирования. [6]

Комплексная система обеспечения безопасности обеспечивает «безопасные условия» функционирования организации и должна защищать от всех видов угроз, которые могут возникнуть. Именно поэтому она содержит большое количество подсистем, объединенных по своему функциональному назначению.

Структура КСОБ

При разработке КСОБ (СКОБ) в её состав включают следующие виды обеспечения: информационное, техническое, программное, математическое, алгоритмическое, методическое, правовое и организационное.

Основными задачами данных компонентов являются:

- ◆ охрана как всего объекта, так и отдельных зон;
- ◆ проведение профилактических и компенсационных мероприятий по различным видам предполагаемых угроз;
- ◆ осуществление функций управления СКОБ;

- ◆ эксплуатация инженерно-технических систем.
- ◆ исключение или снижение вероятности реализации отдельных видов угроз;
- ◆ поддержание устойчивого функционирования СКОБ в штатных и нештатных ситуациях;
- ◆ подготовка персонала объекта к действиям в условиях возникновения или реализации чрезвычайных ситуаций;
- ◆ обеспечение готовности всех служб безопасности к противодействию различным видам угроз;
- ◆ обеспечение безопасной эвакуации людей и материальных ценностей при реализации различных угроз.

Для СКОБ в общем случае сохраняются этапы жизненного цикла, характерного для типовой АС. Среди них основными являются следующие этапы:

1. Создание (совершенствование) СКОБ.
2. Разработка и поддержание в рабочем состоянии объектовой документации по вопросам комплексного обеспечения безопасности.
3. Подбор и подготовка персонала.
4. Эксплуатация комплекса инженерно-технических средств СКОБ.
5. Внутренний аудит и мониторинг состояния комплексного обеспечения безопасности объекта.

Создание (совершенствование) СКОБ, предполагает выполнение следующих мероприятий:

- ◆ организация или участие в разработке исходно-разрешительной документации в области обеспечения безопасности;
- ◆ проведение анализа уязвимости объекта самостоятельно или с привлечением специализированных организаций;
- ◆ определение перечня угроз и модели нарушителя;
- ◆ установление категории объекта и соответствующего состава СКОБ;
- ◆ выделение зон доступа;
- ◆ определение критериев приемки проектных решений и оборудования СКОБ;
- ◆ разработка ТЗ на СКОБ в целом и при необходимости частных ТЗ на составные части;
- ◆ определение состава возможных исполнителей-разработчиков, имеющих необходимые разрешительные документы на проведение подобных работ;
- ◆ сопровождение разработки проектной документации;
- ◆ проверка (экспертиза), в том числе с привлечением сторонних экспертов, принятых (предложенных) проектных решений несоответствие требованиям исходной документации и ТЗ в целом;

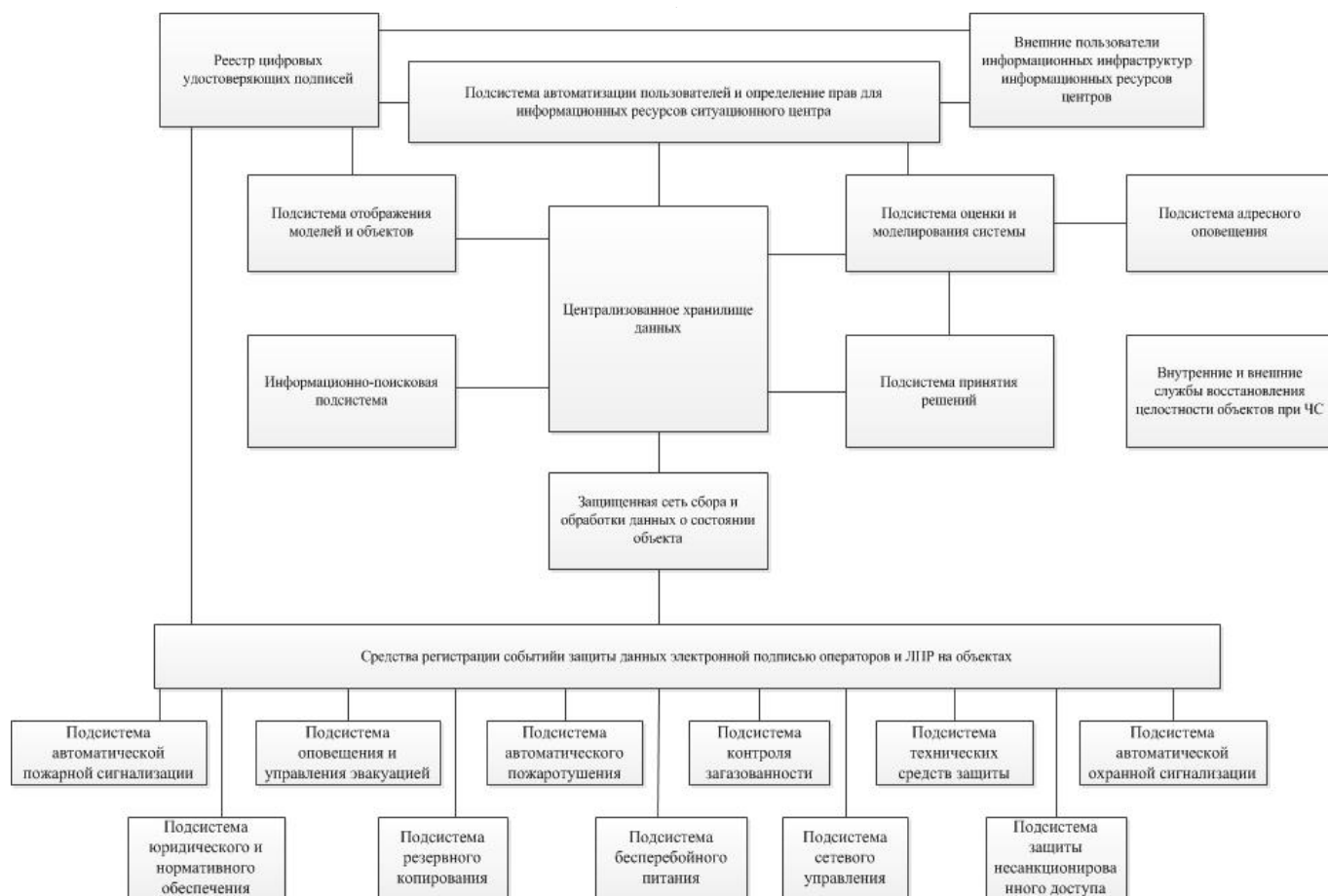


Рис. 3. Типовая архитектура системы управления объектом нижнего уровня с подсистемой комплексного обеспечения безопасности

- ◆ анализ полноты и качества исполнения проектной документации;
- ◆ организация подготовки и обучения персонала, задействованного в реализации обеспечения безопасности, его аттестация на готовность самостоятельно эксплуатировать оборудование;
- ◆ контроль выполнения строительно-монтажных работ по системам, применяемым для обеспечения безопасности;
- ◆ участие в составлении программы и методики испытаний оборудования и всей системы в целом;
- ◆ участие соответствующего персонала СКОБ в проведении предварительных испытаний смонтированного оборудования;
- ◆ организация опытной эксплуатации, выявление несоответствия ТЗ, возможных ошибок, сбоев и т.п.;
- ◆ организация доработок технической составляющей СКОБ;
- ◆ участие соответствующего персонала СКОБ в приемных испытаниях.

Внутренний аудит и мониторинг выполняются следующие работы:

- ◆ анализ уязвимости объекта и оценка эффективности его СКОБ;
- ◆ корректировка при необходимости перечня угроз и модели нарушителя с учетом изменения обстановки как на самом объекте, так и в его окружении;
- ◆ сбор, анализ и обобщение всей информации о нештатных ситуациях в СКОБ, а также в процессе эксплуатации объекта;
- ◆ проведение анализа порядка и хода выполнения предписаний надзорных и контролирующих органов;
- ◆ подготовка предложений по совершенствованию СКОБ.[7]

В настоящее время существуют модели КСОБ нижней ступени иерархии, приведем некоторые из них:

1. КСОБ «I TRIUM» [8] — платформа «глубокой» интеграции средств обеспечения безопасности с поддержкой максимума их функциональных возможностей. Платформа I TRIUM решает глав-

ные задачи, стоящие при создании ИСБ — преодоление несовместимости (интеграция) различных технических средств и систем и достижение целевых характеристик функциональности, быстродействия, надёжности, удобства использования, эксплуатации и обслуживания системы.

2. КСОБ «ПожСтройРегион» [9]. КСОБ реализуется на программно-аппаратной платформе и поддерживает программные средства и протоколы ведущих мировых производителей.
3. СКОБ ОХРАНМОНТАЖ-ЮГ[10] устанавливает оборудование, сигнализирующее о незаконном проникновении, задымлении, подтоплении, загазованности. Наши клиенты могут выбрать следующие способы сигнализации:
 - ◆ автономный — оповещает о возникновении нештатной ситуации звуком сирены.
 - ◆ gsm — сигнал поступает на телефон владельца имущества. Владелец принимает решение о вызове соответствующих служб в зависимости от того, какой датчик сработал.
 - ◆ пультовый — сигнал по проводной или беспроводной линии связи поступает на пульт диспетчера охранной организации.
4. КСОБ «Легис». Специфика охранных систем интегрированного типа заключается в сочетании сразу нескольких комплексов технических средств безопасности, предназначенных для реализации различных целей. Хотя стоимость такого способа обеспечения охраны объекта сравнительно выше, чем аналогичный показатель любой другой охранной системы, фактически, именно этот формат является самым эффективным в отношении экономии. Дело в том, что системы безопасности КСБ одновременно выполняют различные функции, замещая сразу несколько отдельных комплексов. При этом многие технические средства, используемые в них, применяются только в одном экземпляре.

На основе проведенного анализа создана структура КСОБ на основе ситуационного центра. Типовая архи-

тектура комплексная система обеспечения безопасности объекта управления нижнего уровня ситуационного центра представлена на рисунке 3.

На основе существующих комплексных систем обеспечения безопасности можно сделать вывод о архитектуре КСОБ объекта управления нижнего уровня.

В данной статье рассмотрена иерархическая структура КСОБ и определена система обеспечения безопасности нижнего уровня. Приведенная схема позволяет обеспечивать вышестоящие уровни информацией об объекте управления в любой момент времени.

ВЫВОДЫ

1. Проведен структурно-функциональный анализ комплексных систем обеспечения безопасности в рамках иерархической структуры интеллектуальных ситуационных центров, определяющий интеграцию КСОБ для решения задач безопасности разноуровневых объектов управления. В тоже время интеллектуальный ситуационный центр реализует безопасность не только объектов управления, но и обеспечивает собственную безопасность, как критического объекта управления, определяющую стабильность функционирования ИСЦ.
2. Предложена структурно-функциональная модель системы управления объектом нижнего уровня с подсистемой комплексного обеспечения безопасности. В рамках модели продемонстрирована интеграция подсистемы КСОБ в единую платформу, охватывающие полный перечень аспектов управления и безопасности объекта.
3. Рассмотренные задачи комплексной системы обеспечения безопасности позволяют без потери функционала и возможностей управления объектом низкого уровня интегрировать и систематизировать функционирование подсистем в рамках единой КСОБ объекта.

ЛИТЕРАТУРА

1. Simankov V.S., Cherkasov A.N., Buchatskiy P.Y., Teploukhov S.V., Buchatskaya V.V. Synthesis of a decision support system based on an situational center. В сборнике: Proceedings of 2020 23rd International Conference on Soft Computing and Measurements, SCM 2020. 23. 2020. С. 182–185.
2. <https://searchinform.ru/services/outsource-ib/zaschita-informatsii/kompleksnaya/>
3. Симанков В.С., Власенко А.В., Черкасов А.Н. Методологическое обеспечение подсистемы обеспечения комплексной безопасности в составе интеллектуального ситуационного центра // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. — 2021. - № 07. - С. 107–114 DOI 10.37882/2223–2966.2021.07.27
4. Ворона, В.А. Комплексные (интегрированные) системы обеспечения безопасности / — Вып. 7. — Москва: Горячая линия — Телеком, 2018. — 160 с. (Серия «Обеспечение безопасности объектов») — ISBN978–5–9912–0238–1.
5. Симанков В.С., Черкасов А.Н. Анализ и синтез системы поддержки принятия решений на основе интеллектуальных систем ситуационного центра. Наука и бизнес: пути развития. 2014. № 12 (42). С. 93–98.

6. ГОСТ Р 56875–2016 Информационные технологии. Системы безопасности комплексные и интегрированные с. 46
7. Минин П.Е., Конев В.Н., Сычев Н.В., Крымов А.С., Савчук А.В., Андрияков Д.А. Анализ существующих автоматизированных систем управления технологическим процессом // Спецтехника и связь. 2014. № 1. URL: <https://cyberleninka.ru/article/n/analiz-suschestvuyuschih-avtomatizirovannyh-sistem-upravleniya-tehnologicheskim-protssom>.
8. ИТРИУМ ITRIUM (лицензии), Лицензия Web-мониторинг для мониторинга и управления КСОБ ITRIUM в Красноярске [электронный ресурс] <https://store.softline.ru/itrium/itrium-l-web-monitoring-184380/> (дата обращения 10.09.2021)
9. Проектирование и монтаж систем пожаротушения [электронный ресурс] <https://sl-npb.ru/> (дата обращения 10.09.2021)
10. Комплексные системы охраны и безопасности [электронный ресурс] <https://ksb-krd.ru/> (дата обращения 10.09.2021)

© Симанков Владимир Сергеевич (vs@simankov.ru), Величко Александра Александровна (aleksandravelichko@mail.ru).

Журнал «Современная наука: актуальные проблемы теории и практики»



г. Краснодар