DOI 10.37882/2223–2966.2021.07.27

МЕТОДОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПОДСИСТЕМЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В СОСТАВЕ ИНТЕЛЛЕКТУАЛЬНОГО СИТУАЦИОННОГО ЦЕНТРА[1]

METHODOLOGICAL SUPPORT OF THE INTEGRATED SECURITY SUBSYSTEM AS PART OF THE INTELLIGENT SITUATIONAL CENTER

V. Simankov
A. Vlasenko
A. Cherkasov

Summary. The article examines an integrated security system as a subsystem of an intelligent situational center. The paper reflects the methodological principles of organizing the security of the control object based on the intelligent procedures of the situation center.

Keywords: situational center, integrated security subsystem, intellectualization, control.

Симанков Владимир Сергеевич
Д.т.н., профессор, Кубанский государственный технологический университет (г. Краснодар)
vs@simankov.ru
Власенко Александра Владимировна
К.т.н., Кубанский государственный технологический университет (г. Краснодар)
alex_vlasenko@list.ru
Черкасов Александр Николаевич
К.т.н., доцент, Кубанский государственный технологический университет (г. Краснодар)
cherk@mail.ru

Аннотация. В статье рассматривается комплексная система безопасности как подсистема интеллектуального ситуационного центра. В работе отражены методологические принципы организации безопасности объекта управления на основе интеллектуальных процедур ситуационного центра.

Ключевые слова: ситуационный центр, подсистема комплексной безопасности, интеллектуализация, управление.

В настоящее время в мире происходит ускоренная разработка высокотехнологичных платформ и внедрение новых технологических решений на основе искусственного интеллекта. На первый план выходит оперативность решения в различных ситуациях и реализация новых стратегий с учетом совокупности различных факторов. В таком случае, необходимым инструментом управления становятся интеллектуальные ситуационные центры, без которых сегодня невозможно управлять ни одним сложным объектом: регионом, отраслью экономики, холдингом или отдельно взятым предприятием [2],[3].

Современные ситуационные центры должны представлять собой единую «онлайн-платформу», обеспечивающую немедленное реагирование на возникающие инциденты, организующая и координируюшая процессы мониторинга, анализа и оперативного разрешения штатных и нештатных ситуаций. Кроме того, к наиболее распространенным функциям согласно [4] необходимо отнести следующие:

- мониторинг социально-экономического, политического и общественного состояния объекта управления с прогнозированием развития ситуации на основе анализа поступающей информации;
- моделирование последствий управленческих решений, на базе использования информационно-аналитических систем;
- экспертная оценка принимаемых решений и их оптимизация;
- управление в кризисной ситуации;
- организация санкционированного доступа к информационным ресурсам СЦ и других государственных информационных систем;
- разработка и внедрение перспективных информационных технологий в исполнительных органах государственной власти (ИОГВ);

[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»

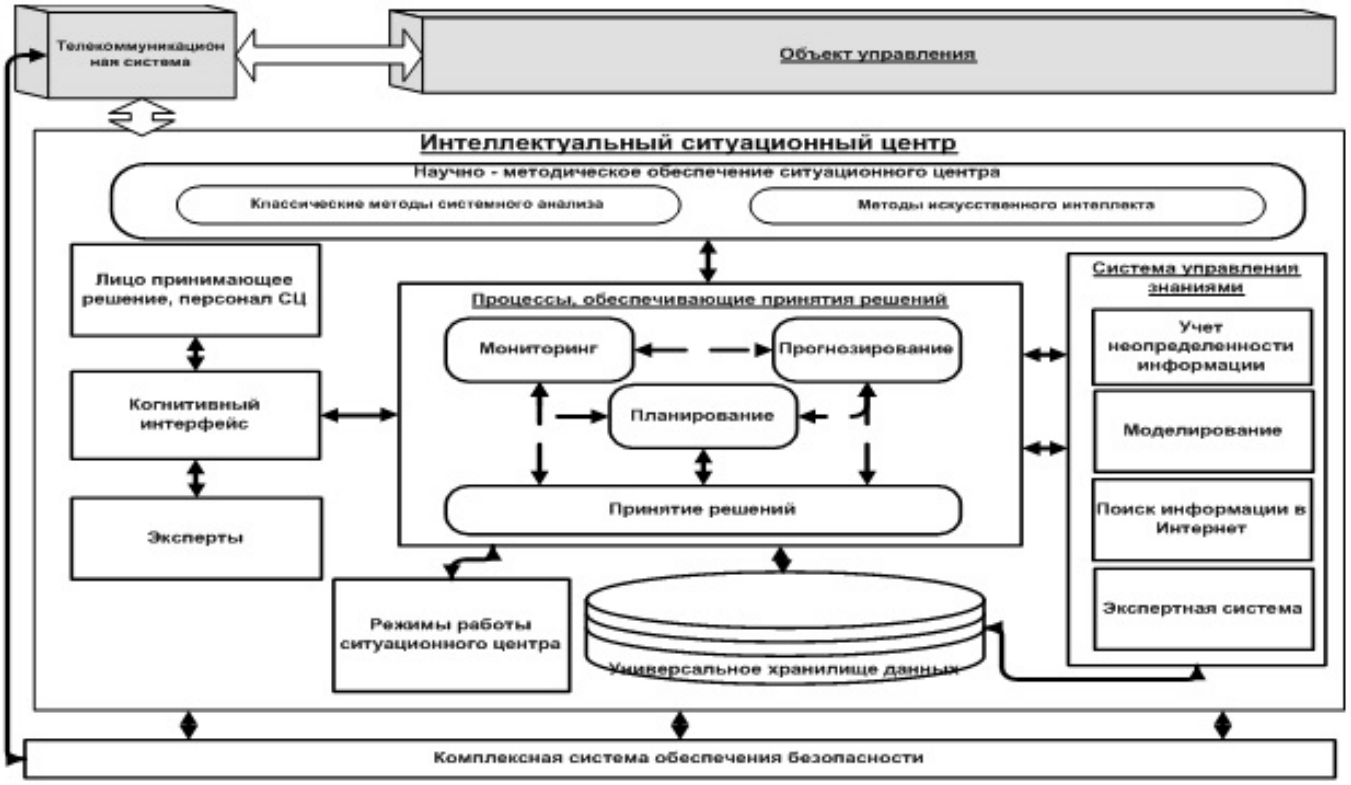

Рис. 1. Обобщенная структурно-функциональная схема ситуационного центра

- обеспечение комплексной безопасности субъекта и объекта управления.

Одним из основных технологических достоинств ситуационного центра становится адаптация и стандартизация: использование на местах единых требований к организации и технологическим решениям СЦ. Это приведет в дальнейшем к созданию системы распределенных ситуационных центров, сокращению времени на рассмотрение ситуаций за счёт использования типовых программных платформ [2]. Обобщенная структурно-функциональная схема ситуационного центра представлена на рисунке 1.

Использование интегрированной платформы обеспечит информационно-аналитическую поддержку деятельности любого объекта и субъекта управления [7]. В различных режимах работы ведется постоянный мониторинг, анализ, прогнозирование, планирования и поддержки принятия решений по вопросам функционирования технического, технологического, социального или другого типа объекта.

Основные функциональные характеристики систем, объектов и субъектов процесса принятия решений в ситуационном центре позволяют рассмотреть комплексный подход к реализации интеллектуальной системы ситуационного центра, где основной системой представляется система поддержки принятия решений. Использование такого подхода позволяет обеспечивать возможность рассмотрения и решения максимального количества задач, уменьшение времени анализа и подготовки информации для решения, используя интеллектуальный подход к извлечению и использованию разнородных знаний [5], [6]. Структурно-функциональная схема интеллектуальной системы ситуационного центра приведена на рисунке 2.

В качестве платформы для построения интеллектуальной системы ситуационного центра целесообразно применять интегрированные программные средства, способные обеспечить решение различного рода задач на основе разнородных источников информации с учетом полной неопределенности.

Реализация интеллектуальной системы ситуационного центра в рамках приведенной схемы, дает возможность максимально расширять количество и круг задач, при условии программной модернизации, накопления необходимой экспертной информации, эффективного использования математического аппарата и наполнения универсального хранилища данных [8].

Отдельная роль в эффективном функционировании интеллектуального ситуационного центра (ИСЦ)

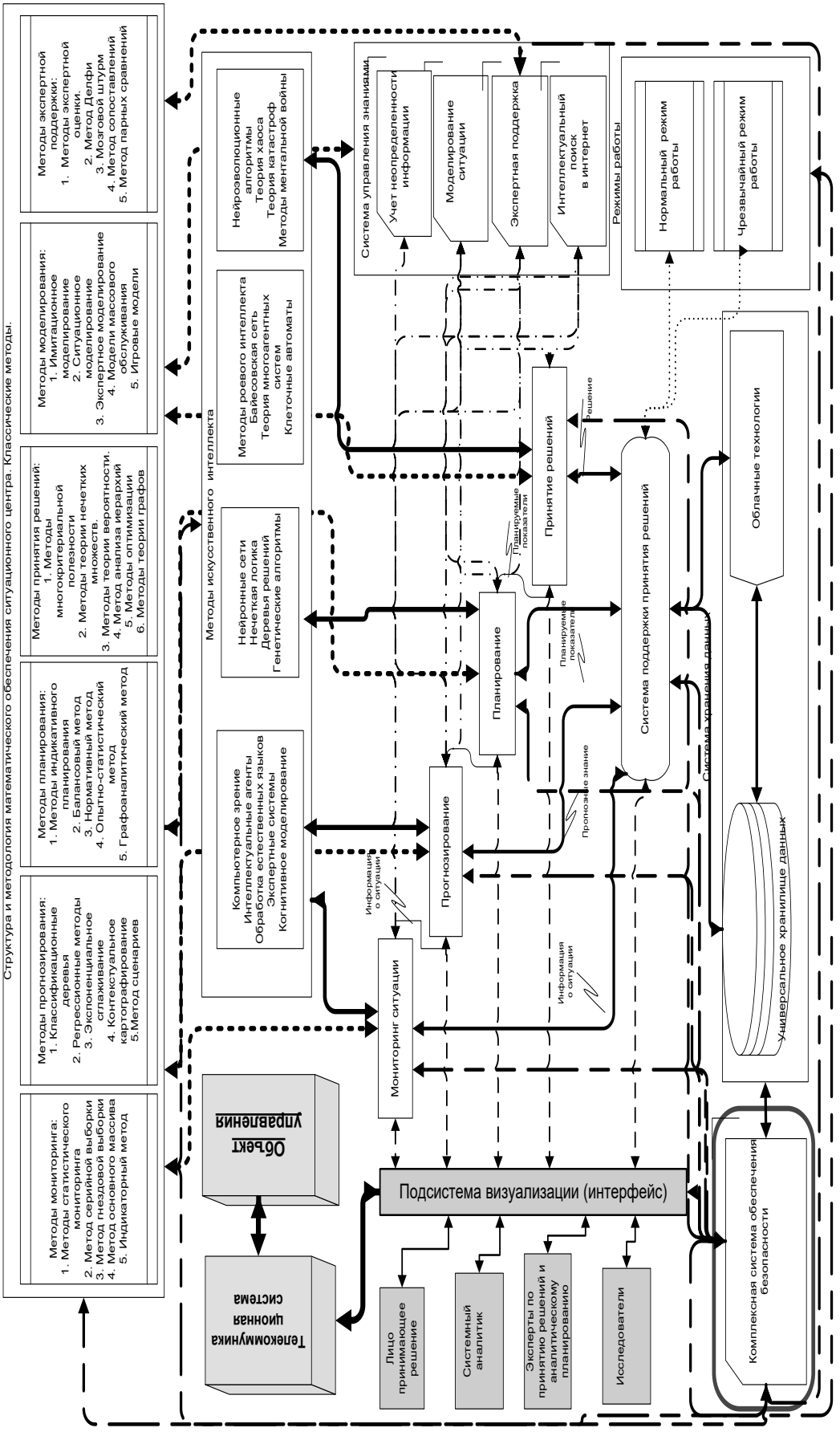

Рис. 2. Структурно-функциональная схема интеллектуального ситуационного центра

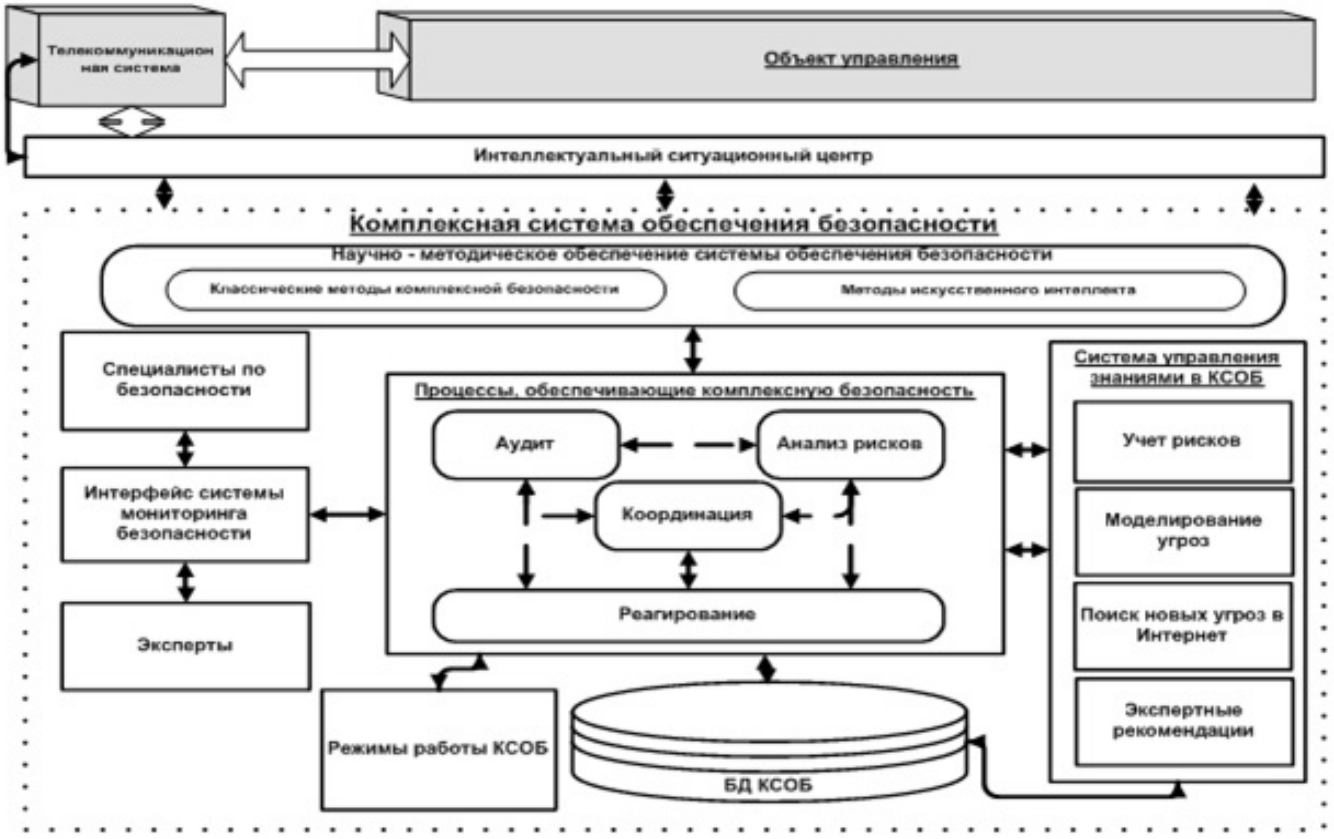

Рис. 3. Обобщенная структурно-функциональная схема комплексной подсистемы обеспечения безопасности

отводится подсистеме обеспечения комплексной безопасности (КСОБ). Перечень основных задач, которые должны решаться КСОБ определяются по результатам анализа возможных угроз, уязвимостей, организационных и методических требований к безопасности как ситуационного центра, так и объекта, которым он управляет.

Подсистема обеспечения безопасности является должна ориентироваться на применении существующих методов управления и адаптации в отношении вопросов информационной безопасности. Проведенные исследования показывают, что большинство систем управления строятся на основе регламентированных и устоявшихся моделях адаптации систем управления безопасностью [10]. Использование интегрированной КСОБ, как подсистемы ситуационного центра, является актуальной и позволит охватить решение большого спектра задач по мониторингу, обработке и контролю разнородной информации о степени защиты объекта управления. Эффективная работа различных подсистем, в рамках такой комплексной подсистемы обеспечения безопасности позволит обеспечить выполнение большего количества задач с минимальным привлечением ресурсов.

Обобщенная структурно-функциональная схема комплексной системы обеспечения безопасности приведена на рисунке 3.

Авторами статьи предложена перспективная методология создания и функционирования интегрированной комплексной подсистемы обеспечения безопасности, позволяющей обеспечить одновременно безопасность и ситуационного центра, и объекта управления. Разработанная структурно-функциональная схема приведена на рисунке 4.

Основная цель подсистемы КСОБ — реализация функций контроля, координации, аудит рисков и реагирования на инциденты. Данные процессы обеспечивают функционирование системы безопасности в следующих режимах: противодействие, пресечение, предотвращение, предупреждение. Выбор режима регламентируется степенью неопределенности полученной информации об объекте или субъекте управления (степень угрозы, тяжесть инцидента, масштаб уязвимости и т.д.). [9]

В общем виде авторами определены следующие задачи КСОБ, функционирующей в рамках ИИСЦ, выпол-

няемые как для субъекта управления (ИИСЦ), так и для объекта управления в целом (организация, предприятие, отрасль и т.д.):

1. Аудит и контроль безопасности — системный процесс получения объективных качественных и количественных оценок о текущем состоянии субъекта и объекта управления в соответствии с определёнными критериями и показателями безопасности;
2. Координация обеспечения безопасности заключается в планировании и реализации совместной деятельности различных подсистем КСОБ;
3. Анализ рисков — это процесс, основной задачей которого является своевременное обнаружение, оценка и прогнозирование рисков вероятности появления угроз различного характера;
4. Реагирование на инциденты это обнаружение и прекращение атаки или утечки данных из инфраструктуры субъекта и объекта управления, устранения последствий.

С целью организации и реализации той или иной модели защиты, предусмотрена методологическая составляющая, в которой реализованы отдельные модели, которые помогут оперативно развернуть систему безопасности в зависимости от задачи и условий работы. Учет такого важного параметра исходной информации, как ее неопределенность позволит осуществить выбор подходящих математических методов анализа данных и искусственного интеллекта для адаптации КСОБ к изменяемым условиям и различным предметным областям.

Для обеспечения методологической составляющей комплексной подсистемы обеспечения безопасности привлекается традиционный аппарат, который регламентируется профильными организациями (ФСТЭК, ФСБ, ФСО и т.д.), а также методы и алгоритмы искусственного интеллекта: генетические алгоритмы, нейронные сети, компьютерное зрение и т.д. Выбор необходимых методов по обеспечения защиты субъекта и объекта управления проводится на основе математического и интеллектуального аппарата, обеспечивающего функционирование ситуационного центра.

С целью определения будущих угроз безопасности, реализация (возникновение) которых возможна в рамках функционирования подсистем субъекта и объекта управления необходимо постоянное накопление знаний по вопросам обеспечения безопасности. Приобретение новых знаний в области безопасности осуществляется при помощи модулей, функционирующих в рамках ситуационного центра по следующим направлениям:

- поиск информации в сети интернет на основе новых способов релевантной информации;
- различные способы моделирования систем защиты;
- учет рисков — как степени неопределенности информации, которая обрабатывается КСОБ и ИИСЦ для выбора необходимых методов и способов защиты;
- экспертные рекомендации организаций ведущих регламентацию деятельности систем безопасности.

Комплексная подсистема обеспечения безопасности функционирует в следующих режимах, которые определяются в зависимости от тяжести инцидента и степени угрозы:

- упреждение — обеспечение безопасности направленное на выявление возможных угроз, а также на разработку эффективных мер предупреждения посягательств на объекты и субъекты управления;
- предотвращение — снижение угроз безопасности путем снижения рисков, обусловленных несколькими видами и/или источниками опасности;
- пресечение или локализация угроз — это действия, направленные на устранение действующей угрозы и конкретных преступных действий;
- противодействие — методы и способы, направленные на устранение последствий реализации угроз.

Переход в один из режимов осуществляется в зависимости от степени тяжести и неопределенности информации об инциденте. Комплексная система обеспечения безопасности сигнализирует ситуационного центру о необходимости перехода в один из режимов.

Наиболее важная роль в КСОБ отводится подсистеме мониторинга и управления безопасностью. К основным функциям подсистемы стоит отнести: обеспечение бесперебойной работы, реагирование на инциденты, управление функциями всех подсистем КСОБ, обеспечение взаимодействия программной среды и персонала через визуальный интерфейс.

Она является основой для контроля подсистем, обеспечивающих функционирование комплексной подсистемы безопасности: подсистема хранения данных комплексной безопасности, подсистема сетевого управления, подсистема защиты он несанкционированного доступа, подсистема контроля доступа территории; подсистема юридического и нормативного обеспечения, подсистема технических средств защиты,

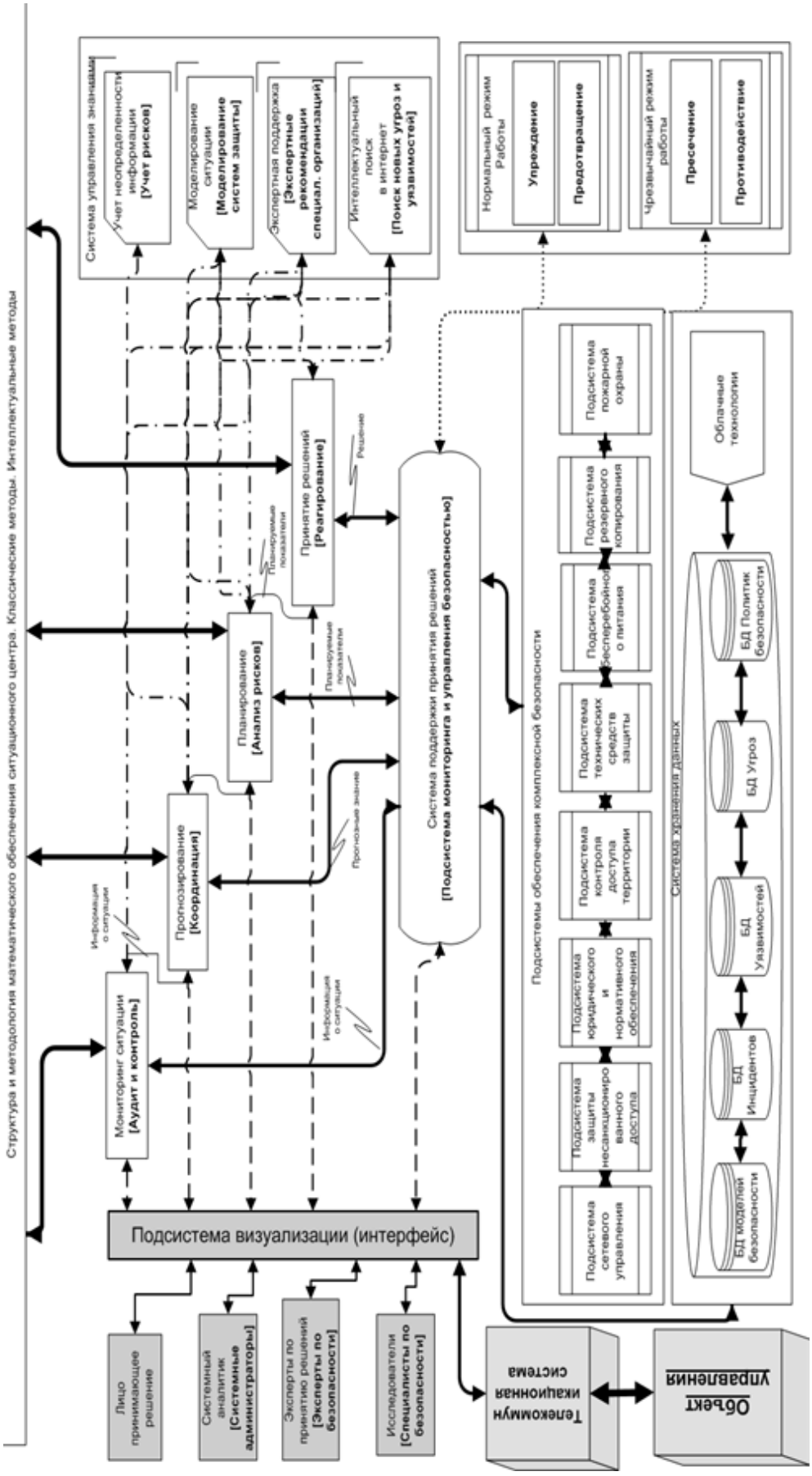

Рис. 4. Структурно-функциональная схема комплексной подсистемы обеспечения безопасности ситуационного центра

подсистема резервного копирования, подсистема бесперебойного питания.

Подсистема хранения данных КБ является частью универсального хранилища данных ситуационного центра. Данная подсистема содержит основные базы данных, в которых хранится информация об инцидентах, моделях и политиках безопасности, типы угроз и уязвимостей.

Организация функционирования комплексной подсистемой обеспечения безопасности (КСОБ) строится на активном включении ее работу информационных систем без нарушения работоспособности систем и их быстродействия. КСОБ — интегрированная платформа для быстрого обнаружения и реагирования на угрозы с автоматическим сбором и интеллектуальным анализом данных. Такая платформа постоянно наблюдает за безопасностью субъекта и объекта управления, и не только оповещает о и нарушениях и подозрительных событиях, но 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.

Представленные выше авторами статьи возможности организации и функционирования комплексной системы обеспечения безопасности, апробированы на практике и позволяют сделать следующие выводы:

1. Фундаментальные исследования в области системного анализа позволили систематизировать основные функции интеллектуальных ситуационных центров и разработать единый методологический подход к их построению вне зависимости от степени, сложности и неопределенности инцидентов. Применение единого методологического подхода позволяет осуществить разработку методик, моделей и программных комплексов для эффективного решения задач и управления ими в любой области.
2. Единый методологический подход к разработке информационно-аналитических систем в рамках ИСЦ базируется на интеллектуализации методов, способов и алгоритмов управления приоритетными задачами и инцидентами в целях оперативного доступа к необходимым данным и немедленного реагирования на решение приоритетных задач. Данная методология позволяет синтезировать интеллектуальные системы различного класса в рамках ситуационного центра с учетом неполноту и неточности данных о реальном поведении объекта управления.
3. Разработанная комплексная подсистема обеспечения безопасности рассматривается как сложная система в составе интеллектуального ситуационного центра, обеспечивающая совокупность функций защиты субъекта (ситуационного центра) и объекта управления. Структура подсистемы позволяет интегрировать ее в состав ситуационного центр без потери функционала и возможностей управления объекта различного назначения.
4. Предложенные фундаментальные положения дают возможность интегрировать и систематизировать функционирование информационно-аналитических систем в рамках единого интеллектуального пространства и построения иерархии распределенных ситуационных центров развития. Это позволит построить эффективную систему управления объектами, обеспечить возможность интеграции данных и разнородных информационных систем.

ЛИТЕРАТУРА

1. Симанков В.С. Автоматизация системных исследований: монография. Краснодар, КубГТУ, 2002. — 376 с.
2. Зацаринный А.А., Ильин Н.И., Райков А.Н. и др. Ситуационные центры развития как интеграторы государственного управления в саморазвивающихся полисубъектных средах: монография. М: ООО «Когитоцентр», 2019. — 252 с.
3. Н.И. Ильин, Н.Н. Демидов, Е.В. Новикова Ситуационные центры: опыт, состояние, тенденции развития. Монография. — Москва: Медиа Пресс, 2011. — 334.
4. Авдеева З.К., Барышников П.Ю., Журенков Д.А., Зацаринный А.А., Ильин Н.И., Колин К.К., Лепский В.Е., Малинецкий Г.Г., Райков А.Н., Савельев А.М., Сильвестров С.Н., Славин Б.Б., Славин А.Б. Стратегическое целеполагание в ситуационных центрах развития. М.: Когито-Центр, 2018. — 320 с.
5. Авдеева З.К., Райков А.Н., Лепский В.Е., Ильин Н.И., Зацаринный А.А., Бауэр В.П., Сильвестров С.Н., Колин К.К., Малинецкий Г.Г., Славин Б.Б., Журенков Д.А., Савельев А.М. Социогуманитарные аспекты ситуационных центров развития. М.: Когито-Центр, 2017. — 416 с.
6. Райков А.Н. Ловушки безопасности на пути развития сильного искусственного интеллекта / Материалы 27-й Международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС'2019, Москва). М.: ИПУ РАН, 2019. С. 53–58.
7. Симанков В.С., Черкасов А.Н. Структура и методология функционирования интеллектуальной системы ситуационного центра. // Глобальный научный потенциал. 2015. № 12 (57). С. 32–37.

8. Симанков В.С., Черкасов А.Н. Теоретические основы анализа и синтеза системы распределенных ситуационных центров с учетом факторов защищенности информации. // Глобальный научный потенциал. 2016. № 12 (69). С. 136–139.
9. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности.— Москва: Академия, 2017.— 335 с.
10. Шелупанов А.А. Актуальные направления развития методов и средств защиты. Доклады ТУСУР, 2017. № 20 (3). С. 11–24.

© Симанков Владимир Сергеевич (vs@simankov.ru),
Власенко Александра Владимировна (alex_vlasenko@list.ru), Черкасов Александр Николаевич (cherk@mail.ru).
Журнал «Современная наука: актуальные проблемы теории и практики»

г. Краснодар