ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН ЗАО «Интегра-С» с участием ЗАО «Волгаспецремстрой», ООО «Интегра-Т», ООО «ИНТЕГРА-М», ФГУП «НИЦ охрана» МВД РФ

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии» по согласованию с ТК 71 «Гражданская оборона, предупреждение и ликвидация чрезвычайных ситуаций», ТК 234 «Системы охранной сигнализации и противокриминальной защиты»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 26 февраля 2016 г. № 81-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Январь 2019 г.

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2016, 2019

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины и определения 3
4 Сокращения 6
5 Основные положения интеграции систем мониторинга и обеспечения безопасности распределенных объектов предприятий и территорий 7
5.1 Назначение 7
5.2 Сферы применения 7
5.3 Режимы мониторинга и управления объектами 8
5.4 Варианты реализации алгоритмов управления 8
5.5 Интерфейс взаимодействия 8
5.6 Требования к операционной системе 8
5.7 Требования к организационно-техническим решениям 9
5.8 Семантические связи основных понятий 9
5.9 Открытость архитектуры 10
5.10 Интеграция и масштабирование проектных решений 11
5.11 Инструменты доступа к оборудованию и ресурсам 11
5.12 Полицентричность архитектуры ИИСМиОБП 11
6 Требования к анализу архитектуры предприятий и его связей 12
6.1 Исследование предприятий при создании ИИСМиОБП 12
6.2 Модель безопасности предприятия 15
7 Архитектура и типология интегрированных интеллектуальных систем мониторинга распределенных объектов предприятий и территорий 18
7.1 Функциональные элементы архитектуры 18
7.2 Средства проектной компоновки 18
7.3 Основные уровни архитектурного решения 18
7.4 Функциональная архитектура распределенной ИИСМиОБП 18
8 Общие технические требования к программно-аппаратным технологическим платформам интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия 19
8.1 Структура комплексов 19
8.2 Безопасность информационных ресурсов 20
8.3 Требования к построению сетей передачи данных 20
8.4 Требования к показателям качества 21
8.5 Требования к надежности 22
8.6 Требования безопасности 22
9 Требования к функциональным компонентам и типовым проектным решениям интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятий 23
9.1 Системы и средства основных функциональных компонентов 23
9.2 Общие технические требования к ИИСМиОБП 23
9.3 Требования по модернизации программного обеспечения и удаленному доступу к нему 24
9.4 Функциональные возможности выходных контроллеров и силовых реле 24
10 Требования к организации распределенной сети региональных ситуационных и информационно-аналитических центров мониторинга состояния целостности объектов и безопасности территорий 24

10.1 Организационные вопросы создания 25
10.2 Требования к обработке событий в распределенных интегрированных системах мониторинга состояния объектов 26
11 Требования к защите информационных ресурсов предприятий и правам доступа пользователей интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия 26
11.1 Общие требования 26
11.2 Идентификация сообщений 27
11.3 Требования к непрерывности цикла защиты информационных ресурсов 27
11.4 Классификация уровня защищенности 27
11.5 Способы защиты информационных ресурсов 27
11.6 Средства разграничения доступа 28
11.7 Инструменты управления и поддержки эксплуатации программно-аппаратной платформы интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия 28
11.8 Топология построения 28
11.9 Требования к межсетевым экранам 29
11.10 Аутентификация удаленных пользователей 29
11.11 Уровень защищенности системы разграничения доступа к информационным ресурсам 30
Приложение А (справочное) Стадии и этапы жизненного цикла интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия 31
Приложение Б (рекомендуемое) Функциональные компоненты архитектуры интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия 33
Приложение В (рекомендуемое) Форма описания структуры базового профиля интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия 34
Приложение Г (рекомендуемое) Типовая архитектура ситуационного центра 38

Введение

Настоящий стандарт разработан с целью расширения группы национальных стандартов по нормализации требований при создании интегрированных интеллектуальных систем мониторинга и обеспечения безопасности предприятий (далее — ИИСМиОБП), их распределенных объектов и территорий, формализации общих требований к проектированию ИИСМиОБП и оснащению предприятий средствами информационно-коммуникационных технологий (далее — ИКТ) общего назначения, оборудованием и программными средствами для решения прикладных задач оценки состояния целостности и безопасности объектов, процессов и ресурсов предприятий, организации взаимодействия служб восстановления целостности и ликвидации последствий аварийных и критических ситуаций на объектах предприятий и смежных территориях с учетом других информационных источников, отражающих современные направления развития систем безопасности промышленных и социальных объектов, расширения области применения, а также приведения в соответствие с действующей нормативной базой. Применение настоящего стандарта взаимосвязано со стандартами:

ГОСТ Р 22.1.01—95 «Безопасность в чрезвычайных ситуациях. Мониторинг и прогнозирование. Основные положения»;

ГОСТ Р 22.1.12—2005 «Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Общие требования»;

ГОСТ Р 22.1.31—2013 «Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений требования к порядку создания и эксплуатации»;

ГОСТ Р 34.10—2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

ГОСТ Р 12.1.019—2009 «Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты»,

а также с международными и национальными стандартами по вопросам информационной безопасности.

На рынке реализации ИКТ — решений в ИИСМиОБП России участники создают локальные интегрированные интеллектуальные системы безопасности (ИИСБ), которые из-за взаимных разногласий и несогласованности в принципах своего построения невозможно объединить с целью создания единой системы безопасности объектов и территорий государства. Федеральный закон от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности», статья 11 «Информационное обеспечение в области транспортной безопасности», а также распоряжение Правительства РФ от 17 декабря 2010 г. № 2299-р «О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения (2011—2015 годы)» подтверждают факт необходимости создания такой информационно-технической системы, которая обеспечит комплексную защиту жителей России и государственно важных объектов и территорий.

Для обеспечения безопасности людей, юридических лиц, их имущества доступ к информации и ее передача в единой системе безопасности государства посредством использования электронной подписи, позволяет работникам правоохранительных органов и другим уполномоченным компетентным лицам использовать в своей работе защищенную надлежащим образом базу идентифицированных данных системы безопасности вне зависимости от того, оборудование какого производителя и чье программное обеспечение используется в качестве структурных элементов в системе безопасности, кто ее проектировал, производил монтаж и настройку. В связи с этим возникла острая необходимость в создании стандартов, обуславливающих единство требований, которые должны предъявляться к вновь проектируемым или подлежащим реконструкции ИИСБ.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. СИСТЕМЫ БЕЗОПАСНОСТИ КОМПЛЕКСНЫЕ И ИНТЕГРИРОВАННЫЕ

Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий

Information technologies. Comprehensive and integrated security systems. Standart requirements for the architecture, hardware and software intelligent monitoring systems to ensure the safety of enterprises and territories

Дата введения — 2017—01—01

1 Область применения

Настоящий стандарт определяет назначение и устанавливает общие технические требования к архитектуре, составу компонентов и функциям интегрированных интеллектуальных систем мониторинга и обеспечения безопасности распределенных объектов предприятий (ИИСМиОБП) и территорий стратегических и социально-значимых объектов в регионах Российской Федерации. Определяет общие требования к проектированию данных систем и оснащению предприятий средствами информационно-коммуникационных технологий (ИКТ) общего назначения, оборудованием и программным средствам для решения прикладных задач оценки состояния целостности и безопасности объектов, процессов и ресурсов предприятий, организации взаимодействия служб восстановления целостности и ликвидации последствий аварийных и критических ситуаций на объектах предприятий и смежных территориях.

Положения настоящего стандарта распространяются на следующие объекты стандартизации:

03.220.20 Дорожный транспорт;
03.220.30 Рельсовый транспорт;
03.220.40 Водный транспорт;
03.220.50 Воздушный транспорт;
03.220.99 Виды транспорта прочие;
13.020.30 Оценка воздействия на окружающую среду;
13.200 Борьба с несчастными случаями и катастрофами;
13.220.01 Защита от пожаров;
13.280 Защита от радиационного излучения;
13.310 Защита от преступлений;
13.320 Системы аварийной сигнализации и оповещения;
33.020 Телекоммуникации в целом;
33.040 Телекоммуникационные системы;
33.050 Телекоммуникационная оконечная аппаратура;
33.060.30 Радиорелейные и стационарные спутниковые системы связи;
33.070 Подвижные службы;
33.080 Цифровая сеть связи с интеграцией служб (ISDN);
33.200 Телемеханика. Телеметрия;
35.020 Информационные технологии (ИТ) в целом;
35.040 Наборы знаков и кодирование информации;
35.080 Программное обеспечение;
35.100. Взаимосвязь открытых систем;
35.110 Организация сети;
35.140 Компьютерная графика;

Издание официальное

35.160 Микропроцессорные системы;
35.180 Информационно-технологические терминалы и другие периферийные устройства;
35.200 Интерфейсы и межсоединительные устройства;
35.220.01 Запоминающие устройства;
35.240 Применение информационных технологий;
47 Судостроение и морские сооружения;
49.140 Космические системы и операции;
93.080.30 Дорожное оборудование и установки;
93.100 Сооружение железных дорог;
93.120 Сооружение аэропортов;
93.160 Сооружение гидротехнических объектов;
95.020 Военная техника. Военные вопросы. Вооружение.

Требования настоящего стандарта предназначены для использования федеральными и региональными органами исполнительной власти субъектов Российской Федерации и местного самоуправления, научно-исследовательскими, проектными, строительными и монтажными организациями, осуществляющими проектирование, строительство, монтаж, эксплуатацию, техническое обслуживание и сопровождение средств ИИСМиОБП на объектах инженерной, транспортной и социальной инфраструктуры предприятий и регионов, таких как:

- национальные электросети;
- магистральные линии связи;
- объекты телерадиовещания;
- опасные производственные объекты;
- магистральные железнодорожные сети;
- магистральные трубопроводы;
- нефтегазоперерабатывающие производства;
- энергогенерирующие объекты мощностью более 50 МВт;
- национальные почтовые сети;
- международные аэропорты;
- морские порты международного значения;
- аэронавигационные системы управления воздушным движением;
- системы и устройства, регулирующие и гарантирующие безопасность судоходства;
- объекты атомной энергетики;
- объекты космической отрасли;
- водохозяйственные сооружения;
- автомобильные дороги федерального значения и др., а также при организации и планировании мероприятий по привлечению сил и средств для предупреждения и ликвидации аварийных и чрезвычайных ситуаций в регионах различного характера.

Отдельные положения стандарта следует использовать органам технического регулирования и аккредитованными в установленном порядке организациям (предприятиям), осуществляющим оценку и сертификацию оборудования и программных средств на соответствие национальным и международным стандартам.

На основе положений настоящего стандарта следует разрабатывать, региональные и отраслевые нормативные документы и профили средств ИИСМиОБП, учитывающие региональные особенности и отраслевую специфику объектов, процессов и ресурсов предприятий.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 27.002 Надежность в технике. Основные понятия. Термины и определения*

ГОСТ 34.003 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

ГОСТ 34.601 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

---

* Действует ГОСТ 27.002—2015 «Надежность в технике. Термины и определения».

ГОСТ 34.602 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Техническое задание на создание автоматизированной системы

ГОСТ 34.603 Информационная технология. Виды испытаний автоматизированных систем

ГОСТ 28147 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

ГОСТ Р 1.0 Стандартизация в Российской Федерации. Основные положения

ГОСТ Р 22.1.01 Безопасность в чрезвычайных ситуациях. Мониторинг и прогнозирование. Основные положения

ГОСТ Р 34.10 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.11 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ Р 50739 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ Р 50922 Защита информации. Основные термины и определения.

ГОСТ Р 51275 Защита информации. Объекты информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 55062 Информационные технологии. Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения

ГОСТ Р 57193 Системная и программная инженерия. Процессы жизненного цикла систем

ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств

ГОСТ Р ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО 15704 Промышленные автоматизированные системы. Требования к стандартным архитектурам и методологиям предприятия

ГОСТ Р ИСО/МЭК 29361 Информационная технология. Интероперабельность сетевых услуг. Базовый профиль WS-1. Версия 1.1

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **активные элементы:** Органы принятия решений (человек-оператор, коллектив лиц и технические устройства), работа которых поддерживается специальными методическими и программными средствами (идентификация сигналов датчиков, алгоритмы обработки данных, сценарии действий в конкретных ситуациях и процедуры согласования и принятия решений в типовых ситуациях).

3.2 **архитектура предприятия:** Упорядоченная совокупность организационно-правовых оснований деятельности, организационных структур управления, объектов инженерной, производственной и социальной инфраструктуры предприятия, определяющая целостность предприятия и условия его функционирования в окружающей среде.

3.3 **архитектура систем безопасности:** Составная часть архитектуры предприятия, обеспечивающая функционирование предприятия и его целостность, а также его защиту от разного рода негативных воздействий, определяющая состав организационно-правового, методического, технического и программного обеспечения систем мониторинга состояния объектов, требования к функциям служб

безопасности, специального оборудования и электронных коммуникаций, процедурам подготовки информации для принятия решений по нейтрализации инцидентов-угроз безопасности и минимизации рисков и ущерба в основной деятельности предприятия.

3.4 **безопасность:** Условия, при которых процессы и ресурсы предприятия не подвержены внешним и внутренним негативным воздействиям.

3.5 **геоинформационная система:** Информационная система, оперирующая пространственными данными.

3.6 **жизненный цикл:** Период создания и использования системы, охватывающий различные состояния, начиная с момента возникновения необходимости в такой системе и заканчивая моментом выхода системы из употребления и ее ликвидации.

Примечание — Включает в себя по ГОСТ Р 57193 стадии: замысла, разработки, производства, применения, поддержки применения, прекращения применения и списания. Каждая стадия разделяется на ряд этапов и предусматривает составление документации, отражающей результаты работ.

3.7 **защищенность объекта:** Совокупность свойств объекта (состояние организационно-технических мероприятий и инжерно-технических средств защиты материальных и информационных ресурсов предприятия), характеризующая возможности функционирования объекта при воздействии на них внутренних и внешних негативных воздействий различной природы (включая защиту от ошибок операторов, неправомочного доступа на объекты и территорию предприятия, использование ресурсов, природных явлений и террористических актов и др.).

3.8 **информационно-коммуникационные технологии общего назначения:** Совокупность методов, процессов и программно-технических средств, интегрированных с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах неопределенного круга пользователей.

3.9 **информационно-коммуникационные технологии специального назначения:** Совокупность методов, процессов и программно-технических средств, интегрированных с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах определенного узкого круга пользователей.

3.10 **инвариантность архитектуры:** Свойство архитектуры сохранять свою структуру и связи при определенных изменениях обстоятельств и параметров внешней среды.

3.11 **интеллектуальная система:** Сложная система, способная воспринимать, сравнивать, преобразовывать, создавать и хранить внутри себя модели определенных объектов.

3.12 **интегрированная система:** Совокупность двух взаимоувязанных систем или более, в которой функционирование одной из них зависит от результатов функционирования другой(их) так, что эту совокупность можно рассматривать как единую систему.

3.13 **инцидент (событие):** Зафиксированный любыми доступными средствами факт нарушения целостности и безопасности объекта или посягательство на несанкционированный доступ на объекты предприятия (здания, сооружения, территорию) к материальным и информационным ресурсам и их несанкционированное использование.

Примечание — Каждое событие определяется датой и временем наступления, источником угроз (сообщения), уровнем угрозы и возможными последствиями.

3.14 **источник угроз (сообщение об инцидентах):** Внутренний или внешний субъект деятельности предприятия или материальный носитель информации о событиях (фактах), приводящих к рискам в деятельности предприятия, возможному нарушению целостности и безопасности объектов, процессов и ресурсов, а также имиджу предприятия.

Примечание — Источниками угроз также являются некорректные записи в проектной документации, соглашениях о сотрудничестве, договорах на поставку оборудования и оказание услуг, публикации в СМИ, неправомочные действия персонала, контрагентов, а также неустановленных лиц и организаций.

3.15 **криптография:** Наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации, а также прикладная инженерно-техническая дисциплина, которая занимается разработкой, анализом и обоснованием стойкости криптографических средств защиты информации от угроз со стороны противника, обеспечивая конфиденциальность, целостность, неотслеживаемость.

3.16 **критически важный объект:** Наиболее важный, определяющий, узловой объект системы, от нормального функционирования которого зависит работоспособность всей системы.

3.17 **кроссплатформенная реализация:** Использование программного обеспечения, работающего более чем на одной аппаратной платформе и/или операционной системе.

3.18 **модель безопасности:** Упорядоченная совокупность организационной структуры предприятия, материальных и информационных потоков (документов, сообщений, сигналов), алгоритмов идентификации и измерения характеристик состояния целостности и безопасности объектов мониторинга в текущей или прогнозной ситуации.

3.19 **мониторинг:** Систематический сбор и обработка информации по процессам и объектам внимания для оценки их состояния и прогнозов развития с целью принятия решения.

3.20 **надежность автоматизированной системы:** Комплексное свойство автоматизированной системы сохранять во времени в установленных пределах значения всех параметров, характеризующих способность данной системы выполнять свои функции в заданных режимах и условиях эксплуатации.

3.21 **объекты мониторинга:** Процессы и ресурсы предприятия, объекты инженерной инфраструктуры предприятия, включающие в себя значимые для него территорию, акваторию водных бассейнов, атмосферу и свойства окружающей среды, состояние которых может изменяться из-за внутренних и внешних негативных воздействий с возникновением угроз нарушения нормального функционирования предприятия, целостности объектов, безопасности персонала, населения и нанесения ущерба окружающей среде.

3.22 **открытая архитектура:** Архитектура компьютера, периферийного устройства, программного обеспечения или системы в целом, на которые опубликованы спецификации, что позволяет другим производителям разрабатывать дополнительные устройства к системам с такой архитектурой.

3.23 **открытое программное обеспечение:** Программное обеспечение с открытым исходным кодом, который доступен для просмотра, изучения и изменения, что позволяет пользователю принять участие в доработке самой открытой программы.

3.24 **открытые протоколы:** Находящиеся в свободном доступе сетевые протоколы передачи данных.

3.25 **показатель состояния объекта комплексный:** Интегральная оценка целостности, функциональной полноты и уровня безопасности объектов, процессов и ресурсов предприятия.

3.26 **предприятие:** Антропогенная реально действующая система, включающая в себя и обеспечивающая взаимодействие людских, материальных, финансовых и природных ресурсов, предпринимающая востребованные обществом действия, работающая во взаимосвязи с другими подобными системами и населением.

3.27 **прикладная задача:** Цель, намеченная для решения проблемной ситуации для заданного ограниченного множества объектов управления определенной отрасли путем реализации одной или нескольких функций автоматизированной системы.

Примечание — Задачи характеризуются входными данными, выполняемыми функциями, внешними возмущениями и ограничениями, выходными целевыми результатами и показателями качества решения.

3.28 **полицентрическая сеть:** Сеть, имеющая два ведущих административных (управляющих) центра и более без явного преобладания лидерства одного над другим.

3.29 **программно-аппаратная платформа:** Совокупность оборудования вычислительных комплексов, средств связи операционных систем и программных средств общего назначения, на базе которых создаются автоматизированные системы для реализации прикладных задач сбора, обработки данных и управления объектами в одной или нескольких сферах деятельности предприятия.

3.30 **распределенная сеть:** Группа размещенных на большом расстоянии друг от друга компьютеров, в том числе как отдельных, так и их локальных сетей, соединенных в единую систему линиями проводной (кабельной) и/или волновой связи.

3.31 **режим 24/7/365:** Непрерывный режим работы без перерывов круглосуточно полную неделю в течение всего календарного года.

3.32 **риск:** Возможность возникновения неблагоприятной ситуации или неудачного исхода от какого-либо вида действия или бездействия.

3.33 **сеть передачи данных:** Совокупность оконечных устройств (терминалов) связи, объединенных каналами передачи данных и коммутирующими устройствами (узлами сети), обеспечивающими обмен сообщениями между всеми оконечными устройствами.

3.34 **система безопасности:** Комбинация людских, материальных и финансовых ресурсов, используемая компетентными службами предприятия в сложившихся условиях, границах функциональных возможностей имеющегося обеспечения и направленная на обнаружение источников внешних и внутренних негативных воздействий на процессы и ресурсы предприятия, на ликвидацию указанных источников, нейтрализацию негативного воздействия или на устранение его последствий.

3.35 **ситуационный центр:** Стационарный или мобильный инженерно-технический комплекс, оснащенный необходимыми телекоммуникационными системами для сбора и обработки информации о состоянии объектов мониторинга, предназначенный для обеспечения оперативного и соответствующего реагирования на угрозу возникновения или возникновение тревожных или чрезвычайных ситуаций, эффективного взаимодействия привлекаемых сил и управленческой деятельности и принятия компетентных решений.

3.36 **ситуация:** Субъективная оценка состояния реального или виртуального ограниченного пространства в течение фиксированного промежутка времени.

3.37 **стратегические и социально-значимые объекты:** Объекты мониторинга, существенно влияющие на нормальное существование, развитие общества и на обеспечение его безопасности.

3.38 **субъекты систем безопасности:** Элементы структуры управления предприятием, внешних контрагентов, предприятий, органов технического регулирования, а также отдельные юридические и физические лица, прямо или косвенно влияющие на состояние объектов мониторинга и/или заинтересованные в использовании результатов мониторинга для реализации своих провозглашенных и скрытых (латентных) целей и задач.

3.39 **характеристики безопасности объекта:** Качественные и количественные нормализованные показатели состояния проектируемых или реально существующих объектов мониторинга, зафиксированные на определенный момент времени с учетом конкретной фактической или предполагаемой ситуации.

3.40 **электронная цифровая подпись:** Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

АС — автоматизированная система;

АИС — автоматизированная информационная система;

ГИСБ — геоинформационная система безопасности;

ИИСМиОБП — интегрированная интеллектуальная система мониторинга и обеспечения безопасности предприятия;

НТД — нормативно-техническая документация;

НСД — несанкционированный доступ на территорию, в здания, отдельные помещения и на сооружения предприятия, к системам хранения материальных и информационных ресурсов предприятия и прав на их использование;

ПАП — программно-аппаратная платформа;

ПТК — программно-технический комплекс;

ПМК — программно-методический комплекс;

ПЛК — программируемый логический контроллер;

ПС — программные средства многократного применения, отчуждаемые от разработчика и являющиеся предметом отдельной поставки для включения в состав программного обеспечения АС и автоматизированного оборудования;

ПО — программное обеспечение автоматизированных систем и оборудования;

ИКТ — информационно-коммуникационные технологии;

ТПР — типовое проектное решение;

РИАСЦ — региональный информационно-аналитический ситуационный центр;

РИСМО — распределенные интегрированные системы мониторинга состояния объектов;

СБ — система безопасности;

СРД — система разграничения доступа к информационным ресурсам;

СКЗИ — средства контроля и защиты информации;

СГОД — сервер группового сбора обработки и хранения данных;

РМП — рабочее место пользователя системы;

НИР — научно-исследовательские работы;

ЛПР — лица, принимающие решение.

5 Основные положения интеграции систем мониторинга и обеспечения безопасности распределенных объектов предприятий и территорий

5.1 Назначение

Интегрированные интеллектуальные системы мониторинга и безопасности предприятий предназначены для обеспечения непрерывного мониторинга территориально распределенных объектов и территорий (интеллектуальное видеонаблюдение уязвимых элементов, обнаружение опасных веществ, контроль транспортной и инженерной инфраструктуры, систем обеспечения жизнедеятельности, метрологической и экологической обстановки), например, опасный объект, муниципальное образование, субъект, регион и территория Российской Федерации.

Интегрированные интеллектуальные системы мониторинга и обеспечения безопасности распределенных объектов предприятий и территорий рассматривают как автоматизированные информационные системы обеспечения основной деятельности предприятия. Целевое назначение ИИСМиОБП — сбор и обработка информации для решения задач оценки текущего состояния показателей целостности и безопасности инфраструктуры предприятия, окружающей среды, продукции, процессов и ресурсов предприятия в условиях воздействия на них внутренних и внешних негативных факторов, разработка мероприятий и организационно-технических решений по предупреждению и восстановлению целостности объектов в условиях аварийных и критических ситуаций.

ИИСМиОБП базируются на применении ИКТ общего назначения и специализированных инженерно-технических средств защиты объектов, процессов и ресурсов предприятий и специализируются на реализации следующего:

- выполняют функции сбора и упорядочения данных о состоянии стационарных и движущихся объектов от разнообразных пассивных и дистанционно управляемых источников информации, распределенных по объектам предприятия и территории региона;
- обеспечивают идентификацию событий и анализ состояния объектов, подготовку решений и рекомендаций по управлению объектами в аварийных и критических ситуациях;
- решают прикладные задачи расчета текущих показателей состояния целостности и безопасности объектов мониторинга, оценки рисков в деятельности предприятия и его отдельных проектов;
- решают задачи планирования и распределения ресурсов, необходимых для поддержания целостности объектов инфраструктуры предприятия, защиты материальных и информационных ресурсов предприятия, реализации мероприятий по восстановлению целостности объектов в сложившейся ситуации.

5.2 Сферы применения

Основными сферами применения ИИСМиОБП являются стратегические и социально-значимые объекты инфраструктуры регионов (транспорт, энергообеспечение, производство, коммунальное хозяйство, экология, общественная безопасность и др.).

Непосредственное управление объектами мониторинга, соблюдение регламентов и норм безопасности осуществляются их владельцами и персоналом основных служб предприятия, а в аварийных и критических ситуациях — внутренними и внешними службами безопасности (охрана, противопожарная служба, органы МЧС, МВД и др.).

5.3 Режимы мониторинга и управления объектами

Мониторинг и управление объектами осуществляются при помощи стандартных средств сетевого управления (Web, SSH, Telnet, консольный порт, а также SNMP), SMS-сообщений и e-mail в следующих режимах:

- ручной мониторинг — пользователь регулярно подключается к устройству регистрации и/или специализированному серверу и проверяет состояние входных сигналов;
- регулярный мониторинг по расписанию — сервер системы регулярно в соответствии с заданным расписанием проверяет состояние информационных служб и объектовых контроллеров и при достижении минимально или максимально допустимых значений пороговых и других величин запускает соответствующие сценарии обработки (формирование и рассылка классифицированных сообщений по корреспондирующим службам принятия решений и реагирования, активация технических средств и исполнительных устройств автоматизированного реагирования);
- мониторинг событий, формируемых интеллектуальными сенсорами и их сетями, объектовым оборудованием и информационными системами и доставляемыми на сервер системами в асинхронном режиме, где события обрабатываются в соответствии с их приоритетом и значимостью;
- проактивный мониторинг, формирующий прогнозы по рискам на основе всех доступных потоков данных и их аналитики, баз знаний и лучших практик с целью предотвращения вероятных критических событий.

5.4 Варианты реализации алгоритмов управления

Для реализации алгоритмов управления событиями допускается использовать:

- встроенный механизм конфигурации по принципу «событие — реакция»;
- встроенная командная оболочка обработки событий (Linux (ash) и ее язык скриптов);
- утилиты для вызова команд основной командной оболочки NSG Linux;
- любой другой скриптовый язык или язык программирования, позволяющий компилировать или импортировать дополнительное программное обеспечение на платформу NSG Linux в виде двоичных файлов.

5.5 Интерфейс взаимодействия

Сбор информации от датчиков и управление технологическим оборудованием на объектах должны базироваться на более простых и гибких технических вариантах построения системы, включая распределение датчиков и контроллеров в пределах технологической площадки, совместное использование продуктов различных производителей.

Примечание — Например, для этого может быть использован открытый интерфейс по стандарту RS 232 и низкоскоростная шина.

5.6 Требования к операционной системе

Оборудование специализированных серверов и коммутаторов потоков данных, устанавливаемых на объектах предприятия, должны работать под управлением операционных систем с открытыми исходными кодами и обеспечивать возможность контроля:

- срабатывания дискретных датчиков, подключенных ко входам локальных серверов обработки данных и управляемых коммутаторов, подключаемых к асинхронным портам через внешние адаптеры типа RS-232/1-Wire;
- нажатия программируемых кнопок на устройствах управления серверами и коммутаторах NSG;
- заданных пороговых значений на входах аналого-цифровых преобразователей (АЦП), контролируемых параметров на других специализированных датчиках;
- отсутствия ожидаемых событий о состоянии объектов мониторинга, формируемых по расписанию с заданным периодом опроса интеллектуальных датчиков состояния.

В исключительных случаях в условиях повышенной секретности допускается применение специализированного ПО отечественной разработки ограниченного применения с закрытыми исходными кодами.

5.7 Требования к организационно-техническим решениям

5.7.1 Организационно-технические решения по оснащению предприятий средствами ИКТ общего назначения и специальными средствами ИИСМиОБП должны учитывать возможности и необходимость интеграции систем и содержать инструменты для проектной компоновки, сборки и испытаний «индивидуальных» систем для конкретных применений с использованием ТПР и оборудования ИКТ промышленного производства, прошедших тестирование на функционирование и совместимость в производственных условиях предприятия — интегратора, поставщика систем.

5.7.2 Разработка концептуальных, функциональных, информационных и математических моделей безопасности предприятия должна выполняться на уровне предприятия в целом, основных структурных подразделений и ключевых продуктов, процессов и ресурсов предприятия для всех потенциально возможных источников и инцидентов — угроз нарушения целостности объектов и безопасности деятельности предприятия.

5.7.3 Функционально комплекс обеспечения безопасности предприятия должен обеспечивать работу всех служб и систем безопасности в замкнутом контуре управления процессами (услугами систем безопасности) для каждого объекта мониторинга с учетом интенсивности и объемов входных — выходных потоков данных между элементами систем.

5.7.4 Распределение функций между активными элементами ИИСМиОБП и органами принятия решений по управлению объектами в аварийных и критических ситуациях определяется сложностью и характеристиками объектов мониторинга, организационно-техническими регламентами предприятия, стандартами организации и должно быть отражено в документированных соглашениях о взаимодействии и в технологических инструкциях для исполнителей.

5.8 Семантические связи основных понятий

Организацию разработок и принятие решений о создании или модификации ИИСМиОБП следует выполнять на основе системного описания объектов, процессов и ресурсов конкретных предприятий, предпроектной оценки характеристик внутренних и внешних негативных воздействий и рисков в деятельности предприятия. Формирование целевого назначения ИИСМиОБП должно быть основано на разграничении понятий «Объекты мониторинга», «Модель безопасности» и «Объекты проектирования» и определении семантических отношений между ними для конкретных сфер деятельности предприятия. На рисунке 1 приведен пример определения семантических связей между основными понятиями в области проектирования АС, которые можно использовать для обоснования архитектуры ИИСМиОБП и способов ее реализации, формирования требований к базовым компонентам и технологиям их реализации.

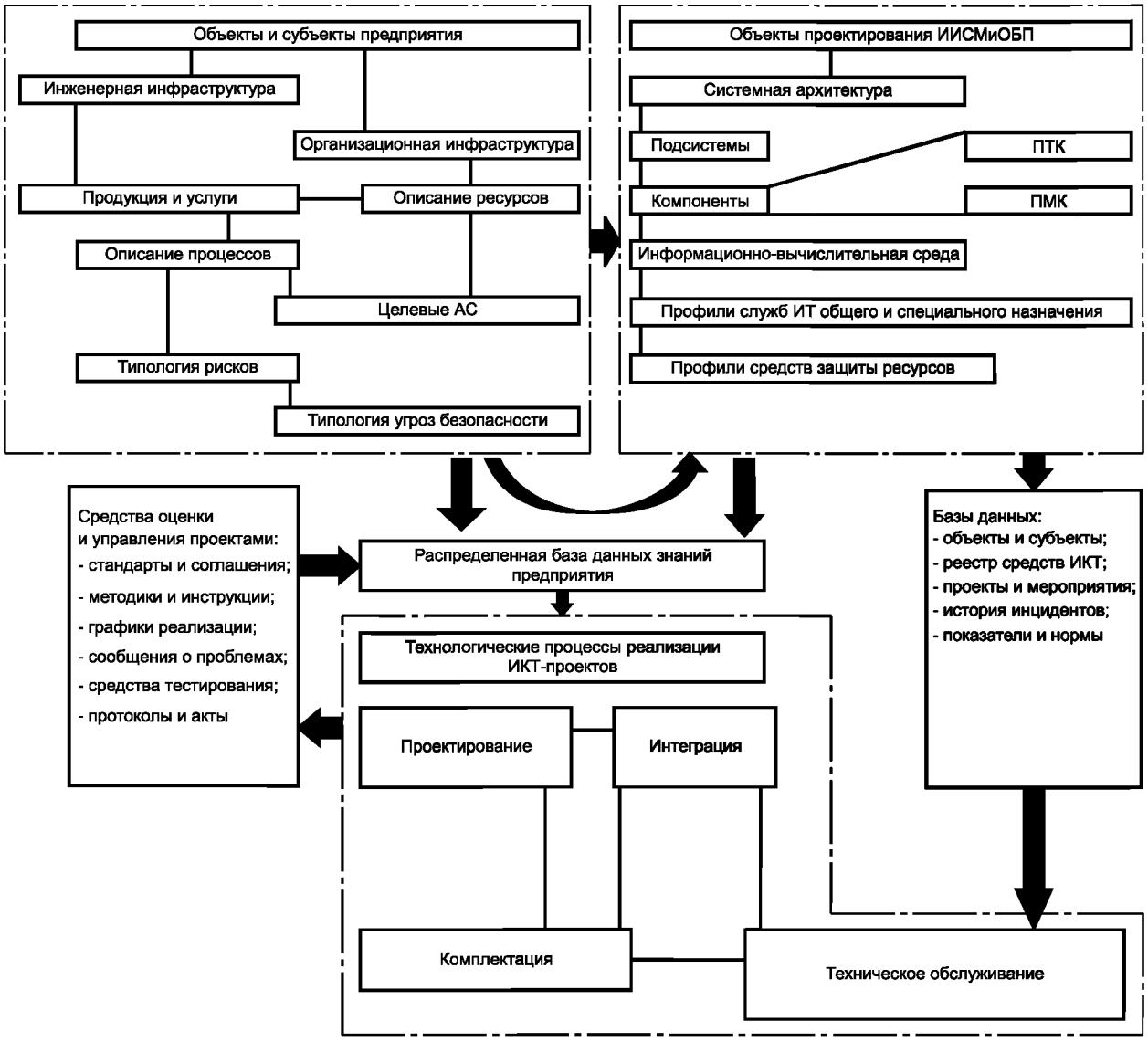


Рисунок 1 — Семантические связи основных понятий ИИСМиОБП

5.9 Открытость архитектуры

5.9.1 Архитектура ИИСМиОБП должна быть открытой и содержать компоненты организационного, методического, технического и программного обеспечения, унифицированные системные интерфейсы и открытые протоколы взаимодействия элементов системы и внешнего окружения.

5.9.2 Комплекс моделей организации взаимодействия ИИСМиОБП со смежными автоматизированными системами предприятия, инфраструктуры региона, муниципальными и региональными службами безопасности должен удовлетворять требованиям организационной, семантической и технической интероперабельности в соответствии с основными положениями ГОСТ Р 55062 и ГОСТ Р ИСО/МЭК 29361.

5.9.3 При проектировании региональных и муниципальных ИИСМиОБП должны быть предусмотрены организационно-технические мероприятия и соглашения по использованию оборудования, установленного на объектах для мониторинга состояния смежных объектов и территорий (например, применение обзорных систем видеонаблюдения на территории муниципальных образований, передача сообщений об инцидентах угроз безопасности в службы восстановления целостности и ликвидации аварийных и чрезвычайных ситуаций, анализ транспортных потоков и др.).

5.9.4 ИИСМиОБП стратегических и социально-значимых объектов и территорий должны быть реализованы на основе унифицированных программно-аппаратных технологических платформ ИИСМиОБП и типовых проектных решений (ТПР), обеспечивающих:

- инвариантность архитектуры ИИСМиОБП относительно сферы деятельности предприятия;
- функционирование ПАП под управлением операционных систем с открытыми кодами;
- возможности наращивания функций и доработки ТПР для решения конкретных прикладных задач заказчика методами проектной компоновки и сборки индивидуальных систем из унифицированного ряда оборудования и программных средств ИКТ общего и специального назначения;
- кроссплатформенную реализацию прикладных компонентов и мобильных приложений, т. е. возможность их функционирования на различных ПАП;
- возможность импорта картографических данных из общедоступных обменных форматов;
- отображение объектов на 2D- и 3D-плане местности в многоуровневом 3D-изображении самого объекта с размещением всех систем безопасности и контроля с привязкой к географическим координатам;
- объединение всех подсистем безопасности в единую геоинформационную систему, представляющую собой ситуационный анализ территорий и объектов на многослойных 3D-картах с возможностью отображения инцидентов во времени;
- доступ уполномоченных лиц к разрешенной для них информации с использованием защищенной электронной подписи по любым каналам связи, в том числе общедоступным (Интернет), с использованием механизмов шифрования;
- достоверность и идентификацию передаваемых данных применением электронной подписи отправителя.

5.10 Интеграция и масштабирование проектных решений

5.10.1 Интеграция и масштабирование проектных решений ИИСМиОБП для предприятий различного уровня сложности мониторинга на основе применения базовых ПАП ИИСМиОБП может осуществляться двумя основными способами:

- «вертикальная» интеграция — объединение на основе базовой ПАП различных типов прикладных функциональных компонентов (жизнеобеспечение зданий, энергоснабжение, охранная сигнализация, пожарная сигнализация, контроль доступа, видеонаблюдение и др.), входящих в линейку продукции разработчика платформы ИИСМиОБП;
- «горизонтальная» интеграция — объединение на базовой ПАП оборудования и программных средств разных производителей в рамках одной системы.

5.10.2 Решения по интеграции систем безопасности должны обеспечивать распределенную обработку информации по узлам принятия решений и профессионально-ориентированный доступ пользователей-операторов, осуществляющих управление закрепленными за ними объектами мониторинга, аналитиков служб безопасности, лиц, принимающих решения при возникновении аварийных и критических ситуаций, и внешних пользователей — потребителей информационных ресурсов.

5.11 Инструменты доступа к оборудованию и ресурсам

Работа пользователей ИИСМиОБП должна поддерживаться специализированными инструментальными средствами доступа к оборудованию ИИСМиОБП, информационным ресурсам (базам данных мониторинга) и прикладным программам сбора, обработки, отображения и принятия решений по закрепленным за ними ролям, функциям, компетенциям и сферам ответственности.

5.12 Полицентричность архитектуры ИИСМиОБП

5.12.1 При проектировании ИИСМиОБП отраслей (корпораций), муниципальных образований и регионов должно быть предусмотрено создание распределенной (полицентрической) сети специализированных ситуационных и информационно-аналитических центров принятия решений.

5.12.2 Ситуационные и информационно-аналитические центры предприятий и муниципальных образований и регионов должны быть разработаны на основе базовых программно-аппаратных технологических платформ и отраслевых типовых проектных решений ИИСМиОБП, быть оснащены специализированными комплексами прикладных задач обработки данных и принятия решений в соответствии с направлениями их деятельности, а также должны поддерживаться соглашениями о взаимодействии с предприятиями владельцами объектов, смежными центрами и другими внешними пользователями — потребителями информационных ресурсов и результатов мониторинга.

6 Требования к анализу архитектуры предприятий и его связей

6.1 Исследование предприятий при создании ИИСМиОБП

6.1.1 Решения по созданию ИИСМиОБП должны быть основаны на предпроектном анализе архитектуры предприятия и его связей с внешним окружением в условиях исходной неопределенности характеристик внутренних и внешних негативных воздействий.

6.1.2 Исходными данными для проектных исследований и обоснования архитектуры ИИСМиОБП являются следующие качественные характеристики:

- информация об отнесении предприятия к критически важным объектам инфраструктуры региона и наличии объектов мониторинга с повышенными требованиями к их защищенности;
- общие сведения о предприятии [организационная структура, размещение подразделений, общая численность работающих на объекте (максимальная численность, число работающих в дневное и ночное время), режим работы объекта, наличие вокруг объекта других предприятий, населенных пунктов, жилых зданий и иных объектов массового скопления людей, размещение объекта по отношению к транспортным коммуникациям, сведения об опасных веществах и материалах, используемых на объекте];
- возможные условия возникновения и развития аварийных и чрезвычайных ситуаций с опасными социально-экономическими последствиями;
- масштабы возможных социально-экономических последствий инцидентов — угроз нарушения целостности и безопасности предприятия, в том числе в результате совершения актов незаконного вмешательства, техногенных аварий и катастроф и возможных террористических актов;
- ситуационные планы и схемы объекта, планы и экспликации отдельных зданий и сооружений и их частей, инженерные коммуникации, план мероприятий по локализации и ликвидации последствий аварий на объекте, проектная документация на объект, декларация промышленной безопасности объекта, документация на технологические процессы, используемые на объекте.

Количественными характеристиками одного или нескольких свойств, определяющих показатель надежности системы в соответствии с ГОСТ 27.002, являются вероятностные показатели безотказности, ремонтопригодности и долговечности.

Показателями безотказности являются:

- вероятность безотказной работы — вероятность того, что в пределах заданной наработки отказ системы не произойдет;
- вероятность отказа — обратная величина, вероятность того, что в пределах заданной наработки отказ системы произойдет;
- средняя наработка до отказа — математическое ожидание наработки системы до первого отказа (для невосстанавливаемых систем);
- средняя наработка на отказ — отношение наработки восстанавливаемой системы к математическому ожиданию числа ее отказов в пределах этой наработки;
- интенсивность отказов — условная плотность вероятности возникновения отказа невосстанавливаемой системы, определяемая для рассматриваемого момента времени при условии, что до этого момента отказ не произошел;
- параметр потока отказов — отношение среднего числа отказов для восстанавливаемой системы за произвольно малую ее наработку к значению этой наработки.

Показателями ремонтопригодности являются:

- вероятность восстановления работоспособного состояния — вероятность того, что время восстановления работоспособного состояния не превысит заданного;
- среднее время восстановления работоспособного состояния — математическое ожидание времени восстановления работоспособного состояния системы.

Показателями долговечности являются:

- средний ресурс — математическое ожидание наработки системы в течение срока службы;
- комплексные показатели надежности, например коэффициент безопасности $К_б$, — вероятность того, что система будет в работоспособном или защитном состоянии в произвольный момент времени, кроме планируемых периодов, в течение которых применение системы по назначению не предусматривается.

Наряду с вероятностными показателями надежности при формировании исходных данных необходимо определить или рассчитать ряд детерминированных показателей, таких как:

а) интенсивность, длительность и график проводимых на объектах работ;

б) финансовые расходы и трудозатраты на обеспечение безопасности;

в) количество и тяжесть имевших место происшествий.

Детерминированные показатели обычно выражаются физическими величинами или отношением этих величин, например: безопасность многоканальной резервированной аппаратуры может оцениваться числом каналов, отказы которых приводят к опасным ситуациям, срок службы определяется календарной продолжительностью эксплуатации системы или ее возобновления после ремонта до наступления предельного состояния.

Пример номенклатуры качественных и количественных показателей и характеризуемые ими свойства ИИСМиОБП приведены в таблице 1.

Таблица 1 — Номенклатура показателей ИИСМиОБП

Наименование показателя качества	Обозначение показателя качества	Наименование характеризуемого свойства
Показатели назначения Показатели функциональные и технической эффективности		
Модульность и функциональная взаимосвязь систем на программном уровне: количество систем	—	Интеграционный параметр
Модульность и функциональная взаимосвязь систем на аппаратном уровне: количество систем	—	Интеграционный параметр
Конфигурационная вариантность: количество вариантов	—	Степень автономности
Конструктивные показатели		
Время хранения отчетов и архивов, сут	—	Эксплуатационный параметр
Длина участка, оснащенного инженерными сооружениями обеспечения безопасности, м	—	Эксплуатационный параметр
Число рубежей охраны, шт.	—	Эксплуатационный параметр
Число центров сбора и обработки информации, шт.	—	Эксплуатационный параметр
Число рабочих мест операторов системы, шт.	—	Эксплуатационный параметр
Площадь обзора камерами телевизионного наблюдения, кв.м	—	Эксплуатационный параметр
Целевая задача телевизионного наблюдения: идентификация, распознавание, обнаружение, мониторинг	—	Эксплуатационный параметр
Интеллектуальный анализ видеоизображения: да/нет	—	Эксплуатационный параметр
Длина участка, оснащенного техническими средствами охранной сигнализации, м	—	Эксплуатационный параметр
Площадь помещений, оснащенных техническими средствами охранной сигнализации, $м^2$	—	Эксплуатационный параметр
Число тревожных извещателей, шт.	—	Эксплуатационный параметр
Площадь помещений, оснащенных техническими средствами контроля и управления доступом, $м^2$	—	Эксплуатационный параметр
Площадь участка, оснащенного системой громкоговорящего оповещения, $м^2$	—	Эксплуатационный параметр

Окончание таблицы 1

Наименование показателя качества	Обозначение показателя качества	Наименование характеризуемого свойства
Категория надежности системы электроснабжения	—	Безотказность
Наличие системы мониторинга исправности элементов ИИСМиОБП, да/нет	—	Ремонтопригодность
Показатели надежности		
Средняя наработка до отказа для аппаратуры многократного применения, ч	$\Delta t_{отк1}$	Безотказность
Наработка до первого отказа (для аппаратуры однократного применения), ч	$\Delta t_{отк2}$	Безотказность
Средний ресурс, лет	$T_р$	Долговечность
Среднее время восстановления работоспособного состояния, мин	$\Delta t_в$	Ремонтопригодность
Среднее время восстановления до заданного значения показателя качества, мин	$T_в$	Сохраняемость
Среднее время безотказного хранения, ч	$T_{хр}$	Сохраняемость
Показатели устойчивости, стойкости к воздействию внешних негативных факторов		
Рабочий диапазон температур окружающей среды, °С	Δt	Устойчивость к температурным воздействиям
Рабочий диапазон относительной влажности воздуха, %	ΔV	Устойчивость к климатическим воздействиям
Показатели транспортабельности		
Показатель воздействия транспортной тряски и вибрации (с ускорением и при частоте ударов), %	—	Прочность при транспортировании в упакованном виде
Габаритные размеры, мм	d×l×h	Приспособленность к транспортированию и эксплуатации
Масса, г	m	Приспособленность к транспортированию и эксплуатации
Допустимые виды транспортирования изделия	—	—
Показатели стандартизации и унификации		
Коэффициент применяемости, %	$K_{пр}$	—
Коэффициент повторяемости, %	$K_п$	—
Показатели безопасности		
Электрическая прочность изоляции кабельных трасс, кВ	—	—
Электрическое сопротивление изоляции кабельных трасс, Ом	—	—

6.1.3 Обследование объектов предприятия осуществляют в соответствии с методиками, учитывающими особенности продукции и инфраструктуры предприятия.

По результатам обследования определяют (уточняют):

- состав объектов, процессов и ресурсов предприятия, подлежащих защите от негативных воздействий;

- описания объектов мониторинга и субъектов обеспечения их безопасности;
- значения заданных норм и показателей безопасности объекта;
- характеристики внутренних и внешних событий и возмущений — угроз безопасности;
- органы принятия решений в аварийных и критических ситуациях по закрепленным за ними объектам инженерной инфраструктуры предприятия, продукции, процессов, ресурсов, документации и др.;
- наличие соглашений о взаимодействии с внешними органами власти и местного самоуправления, организациями региональных служб безопасности;
- схемы информационных потоков и размещение узлов принятия решений на территории и в помещениях предприятия и смежных предприятий, включая расположенные в других регионах России и других государствах;
- характеристики доступных ресурсов (персонал, спецоборудование, программные средства, НТД, типовые решения по обеспечению безопасности объектов, источники и формы их приобретения).

6.1.4 По результатам обследования определяют:

- исходные постановки задач создания (модификации и развития) системы безопасности предприятия;
- концептуальные модели обеспечения безопасности объектов предприятия, организационные регламенты и процедуры принятия решений;
- общие функциональные требования к системе безопасности и ее архитектуре;
- требования к компонентам организационного, информационного, технического и программного обеспечения систем безопасности;
- требования к представлению данных о состоянии объектов мониторинга на устройствах отображения общего назначения и рабочих местах удаленных пользователей и их привязке к и координатам местности;
- исходные материалы для разработки и использования конструктивных 3D-моделей зданий и сооружений инженерной инфраструктуры предприятия, геоинформационных систем общего и специального назначения;
- рекомендации по выбору проектных решений по организации межведомственного взаимодействия.

6.1.5 На этапе НИР следует разрабатывать или на этапе проектирования использовать типовые модели безопасности предприятия. Модель безопасности предприятия должна быть положена в основу концепции создания (развития) ИИСМиОБП и отвечать на вопросы, что будет, если изменится какой-либо элемент архитектуры предприятия, его инженерной, производственной и социальной инфраструктуры, характеристики внешних воздействий, какие факторы необходимо учитывать при постановке задач обеспечения безопасности и выборе средств их реализации.

6.2 Модель безопасности предприятия

6.2.1 При разработке моделей безопасности предприятия должны быть определены основные требования к организационно-методическому и информационному обеспечению систем безопасности, включая:

- характеристики объектов мониторинга и внешней среды;
- показатели оценки социально-экономического состояния региона и факторы, оказывающие влияние на целостность и требуемый уровень защищенности объектов, процессов и ресурсов предприятия от негативных воздействий;
- технические регламенты и нормы безопасности объектов инфраструктуры предприятия и прилегающих территорий;
- концептуальные и математические модели оценки рисков и обоснование выбора средств защиты ресурсов от негативных воздействий;
- состояние наследуемых информационных систем предприятий и рынка средств ИКТ и специализированного оборудования систем защиты ресурсов предприятия;
- регламенты обмена данными, форматы сообщений и протоколы передачи данных в локальных (LAN), региональных (MAN) и глобальных (WAN) сетях с интеграцией служб частного пользования;
- методы статистической обработки данных и формы запросов на представление отчетов по результатам мониторинга внешним потребителям.

6.2.2 Требования к функциональным, информационным, математическим и процедурным моделям АС мониторинга состояния объектов предприятия, наряду с условиями и требованиями ГОСТ Р 22.1.01, должны включать в себя:

- определение и идентификацию инцидентов угроз целостности и безопасности объектов;
- определение частных и комплексных (интегральных) показателей состояния целостности и безопасности объектов мониторинга, функциональных зависимостей и корреляционных связей между ними, включая определение минимального необходимого набора контролируемых параметров, выбора частоты опроса датчиков (сенсоров) и источников сообщений, рациональных настроек средств коммутации потоков данных и других настроек систем контроля параметров объектов и средств внутренних и внешних коммуникаций;
- требования к документообороту служб безопасности, контролю исполнения решений и показателям эффективности использования ресурсов (оборудование, персонал, энергия, деньги);
- оценку текущей ситуации по интегральным (комплексным) показателям и прогноз последствий ее развития;
- методы обоснования принятия решений по нейтрализации угроз и планированию ресурсов для обеспечения безопасности объектов и восстановления их целостности в аварийных и критических ситуациях;
- выбор способов отображения результатов мониторинга и адресного оповещения ЛПР для активизации сил и средств служб безопасности предприятий и регионов;
- методы хранения и статистической обработки данных об истории инцидентов и эффективности действий эксплуатационного персонала объектов и служб обеспечения безопасности.

6.2.3 При разработке моделей безопасности предприятия необходимо учитывать его взаимодействие:

- с системой жизнеобеспечения распределенных объектов предприятия и региона;
- региональными службами обеспечения безопасности и антитеррористической защищенности объектов транспорта, энергетики, промышленных предприятий, экологии;
- органами технического регулирования, оценки соответствия и надзора;
- службами восстановления целостности объектов предприятий и ликвидации последствий аварийных и чрезвычайных ситуаций;
- органами государственной власти и местного самоуправления.

6.2.4 Структура комплекса моделей безопасности обобщенного предприятия приведена на рисунке 2.

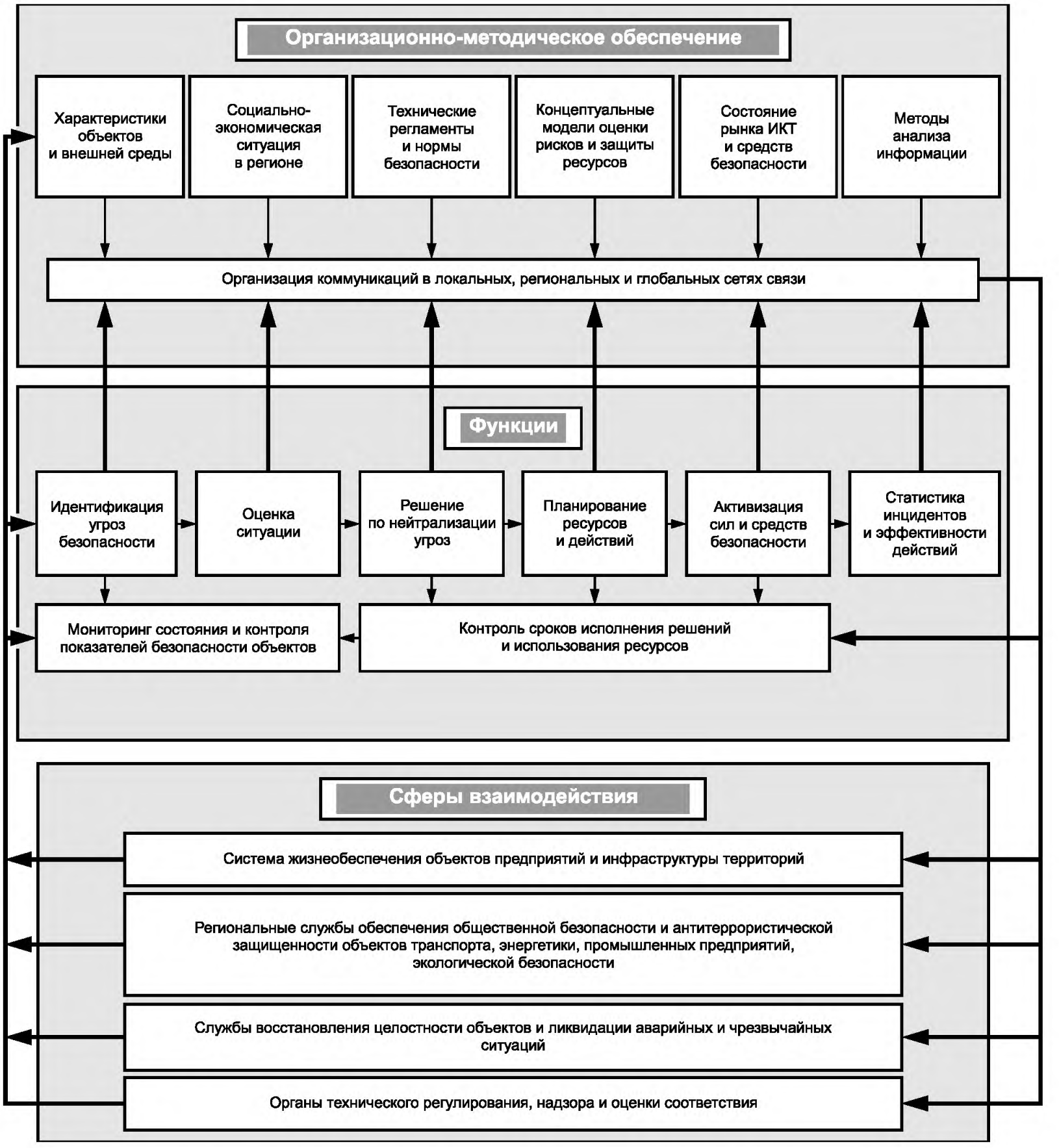


Рисунок 2 — Пример функциональной модели безопасности предприятия

6.2.5 При разработке моделей безопасности предприятия необходимо обеспечивать их функциональную полноту для обеспечения мониторинга.

7 Архитектура и типология интегрированных интеллектуальных систем мониторинга распределенных объектов предприятий и территорий

7.1 Функциональные элементы архитектуры

Архитектура ИИСМиОБП определяет состав функциональных элементов организационного, методического, информационного, технического и программного обеспечения и связей с ними и должна включать в свое содержание роли людей, описание процессов (функции и поведение) и представление всех вспомогательных технологий на протяжении всего жизненного цикла предприятия по ГОСТ Р ИСО 15704.

7.2 Средства проектной компоновки

Средства проектной компоновки ИИСМиОБП должны обеспечивать реализацию функций настройки и масштабирование на условия применения в различных предметных сферах деятельности предприятий, таких как:

- оценка проектной, технологической и организационно-распорядительной документации на наличие в текстах сведений, содержащих коммерческую и государственную тайну, недопустимых или некорректных определений терминов и понятий, числовых значений характеристик объектов и других ошибок в текстах, приводящих к рискам и возможным потерям ресурсов, включая имидж и доверие потребителей;
- мониторинг состояния оборудования ИКТ, специализированных средств инженерно-технической защиты объектов и информационно-вычислительных сетей предприятия;
- мониторинг инженерных систем жизнеобеспечения зданий и сооружений и оценка факторов, угрожающих безопасности инфраструктуры предприятия (пожарная безопасность, энергообеспечение, погодные условия, техногенные катастрофы др.);
- охрана территории предприятия и контроль несанкционированного доступа на объекты предприятия;
- контроль документации на поставку комплектующих и материалов при приемке, несанкционированного (нецелевого) использования материальных ресурсов предприятия;
- защита информационных ресурсов и интеллектуальной собственности предприятия;
- безопасность труда и обеспечение здоровья персонала.

7.3 Основные уровни архитектурного решения

Архитектурные решения ИИСМиОБП при их построении должны располагаться на следующих четырех уровнях.

7.3.1 Уровень формирования базовых программно-аппаратных технологических платформ среды функционирования ИИСМиОБП и функционально-полного комплекса оборудования и программных средств для решения прикладных задач мониторинга состояния объектов в предметных сферах деятельности предприятий.

Примечание — Решения этого уровня должны учитывать действующие нормативно-правовые требования в сфере безопасности и содержать правовые, организационно-экономические и технические механизмы разработки интегрированных систем безопасности и постановки на производство новых средств ИКТ общего и специальных средств защиты ресурсов предприятий преимущественно российского производства.

7.3.2 Уровень системного проектирования ИИСМиОБП и их «встраивания» в действующие и перспективные организационно-технические системы управления предприятия.

7.3.3 Уровень проектирования и интеграции информационных систем межведомственного взаимодействия распределенной полицентрической сети региональных ситуационных и информационно-аналитических центров мониторинга стратегических и социально-значимых объектов регионов и территорий.

7.3.4 Прикладной уровень эксплуатации ИИСМиОБП и обеспечения взаимодействия служб безопасности в процессах текущей деятельности предприятий.

7.4 Функциональная архитектура распределенной ИИСМиОБП

Современные мультисервисные распределенные корпоративные (сети) системы обработки данных, в том числе и в ИИСМиОБП, представляют собой совокупность высокоскоростного сетевого обору-

дования, поддерживающего приоритезацию трафика, а также большого числа всевозможных прикладных платформ и сервисов реального времени (IP-телефонии и видеоконференцсвязи), реализующих IT-фундамент бизнес-процессов и средств общения.

7.4.1 В состав функциональной архитектуры ИИСМиОБП включают совокупность ПТК и ПМК, каждый из которых рассматривают как отдельный продукт, который может иметь своих потребителей и различные модификации, учитывающие особенности их применения на конкретных предприятиях.

7.4.2 Функциональные компоненты архитектуры ИИСМиОБП (см. приложение Б) должны быть представлены как законченные продукты, являющиеся предметом отдельной поставки, прошедшие все испытания на предприятии-изготовителе и содержать необходимые средства настройки для применения в условиях предприятия разработчика ИИСМиОБП. На их базе при необходимости реализуются системы мониторинга однотипных объектов в ситуационных центрах отраслей, регионов, муниципальных образований на разных ИКТ-платформах с использованием оборудования и программного обеспечения различных изготовителей и интегрироваться с действующими автоматизированными информационными системами предприятий. Необходимые связи между компонентами определяются унифицированной системой интерфейсов взаимодействия между элементами и поддерживаются средствами интеграции различных компонентов и модулей с их тестированием на совместимость и работоспособность в конкретных условиях.

В зависимости от сложности объектов мониторинга в составе ИИСМиОБП используют как простейшие системы контроля отдельных параметров, так и сложные иерархические комплексы средств оценки комплексного (интегрального) состояния объектов.

7.4.3 Рациональная архитектура ИИСМиОБП для конкретных объектов должна обеспечивать:

- адекватную минимизацию состава контролируемых параметров и показателей состояния объектов мониторинга;
- использование алгоритмов обработки данных и логики принятия решений;
- определение и закрепление узлов принятия решений и распределение сфер их ответственности в зависимости от ситуации на объекте;
- оптимальную минимизацию информационных потоков и загрузки каналов связи;
- адекватное и своевременное отображение данных мониторинга и оповещение лиц, принимающих решения по управлению объектами.

7.4.4 Средства обнаружения событий — инцидентов угроз безопасности должны обеспечивать обработку потока данных от различных источников и решать следующие функциональные задачи:

- определение регламента обслуживания потока данных (сигналов датчиков, сообщений, документов);
- регистрацию события и определение источника сообщения о событии;
- выделение признаков угроз из потока отдельных сообщений;
- идентификацию типа угрозы и определение возможных последствий развития события;
- инициализацию действий лиц, принимающих решения в системах безопасности предприятия;
- упорядочение потока событий, ведение архива истории событий.

8 Общие технические требования к программно-аппаратным технологическим платформам интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия

8.1 Структура комплексов

Автоматизированные комплексы средств ИИСМиОБП для реализации прикладных задач сбора, обработки данных мониторинга состояния и управления объектами предприятия следует создавать на основе базовых ПАП ИКТ общего назначения (вычислительных комплексов, средств связи и поддерживающих их операционных систем и инструментальных средств), реализованных на основе принципов создания открытых систем с целью упрощения интеграции с другими системами. Геоинформационная система безопасности должна содержать открытые программные интерфейсы для интеграции с источниками информации и внешними информационными системами и соответствовать следующим требованиям.

8.1.1 В состав основного оборудования базовой ПАП ИИСМиОБП, устанавливаемой на объектах предприятия, в соответствии с решаемыми задачами и требуемым уровнем информационной безопасности должны быть включены:

- устройства сбора информации с первичных датчиков (сенсоров) состояния объектов мониторинга;
- локальная вычислительная сеть предприятия;
- регистраторы различного вида сообщений, аудио- и видеоданных, включая стационарные и подвижные;
- локальные серверы сбора, хранения и обработки данных о состоянии заданной группы объектов мониторинга;
- контроллеры управления устройствами систем жизнеобеспечения зданий и сооружений, контроля доступа в здания и сооружения и на территорию предприятия, видеонаблюдения, индикации и отображения состояния объектов, мониторинга групповых и индивидуальных рабочих мест пользователей;
- средства коммутации потоков данных (управляемые и неуправляемые);
- средства администрирования СБ с установленным программным обеспечением процесса администрирования СБ и системы разграничения доступа к оборудованию и информационным ресурсам системы;
- сервер хранения данных, оборудованный устройствами хранения и доступа к базам данных информационных ресурсов службы безопасности предприятия с достаточными емкостью памяти, производительностью, длительностью времени хранения архивов данных (истории событий) и обработки запросов пользователей на поиск и представление данных для принятия решений; имеющий достаточный объем памяти для длительного хранения данных мониторинга СБ предприятия, и производительность, обеспечивающую требуемую скорость обработки запросов пользователей;
- рабочие места операторов системы, обеспечивающие работу в локальной компьютерной сети предприятия с заданным уровнем доступа к оборудованию ИИСМиОБП и средствам коллективного (группового) отображения информации;
- удаленные рабочие места внешних зарегистрированных пользователей системы, оборудованные стационарными или мобильными ИТ устройствами, имеющими доступ в локальные и корпоративные сети и оснащенные приложениями для доступа к информационным ресурсам ИИСМиОБП.

8.1.2 В состав базового отраслевого или регионального (муниципального) профиля ИИСМиОБП рекомендуется включать компоненты, указанные в форме описания структуры базового профиля ИИСМиОБП, согласно приложению В.

8.1.3 Состав, число и характеристики средств ИИСМиОБП для конкретных объектов определяют по результатам оценки уровня защищенности объектов предприятия и технико-экономического обоснования проекта оснащения объектов предприятия средствами ИКТ общего и специального назначения.

8.2 Безопасность информационных ресурсов

Безопасность информационных ресурсов ИИСМиОБП, РСИАЦ определяется состоянием защищенности ИРП от различных угроз и в итоге — способностью обеспечить конкретному зарегистрированному пользователю доступность, целостность и конфиденциальность требуемой информации в системе в соответствии с его функциями, компетентностью и уровнем доступа к разделам распределенной базы данных ИРП.

8.3 Требования к построению сетей передачи данных

Базовое программное обеспечение систем связи должно быть ориентировано, в первую очередь, на соблюдение требований соответствующих международных и национальных стандартов.

Ключевым компонентом, связывающим узлы сети передачи данных, является вид используемой связи, которая обеспечивает передачу трафика между узлами. Для организации передачи данных между узлами рекомендуется использовать следующие виды каналов и способов связи:

- выделенные линии связи — оптические или медные кабели и радиочастотные каналы, соединяющие узлы сети заказчика;
- выделенные каналы данных — каналы данных, предоставляемые оператором связи поверх своей сети передачи данных, например ATM (PVC), E1/E3/STM-1, Ethernet VLAN; соединение на базе «группового» доступа, например IP VPN, обмен данными по технологии VPLS (служба виртуальной

частной локальной сети), с эмуляцией распределенной локальной вычислительной сети поверх сети оператора;

- глобальную сеть Интернет.

Применяемые при построении сети передачи данных принципы шифрации и распределения трафика, использования межсетевых экранов, проведения работ со средствами вычислительной техники должны соответствовать требованиям российского законодательства и руководящих документов Государственной технической комиссии при Президенте Российской Федерации и Федеральной службы по техническому и экспортному контролю.

8.4 Требования к показателям качества

8.4.1 Формируемые требования к качеству ИИСМиОБП должны быть направлены на достижение целевых показателей назначения систем при ограничениях на допустимые затраты и приемлемый уровень безопасности НИР. Степень реализации целей функционирования ИИСМиОБП определяют в зависимости от совокупности объективных и субъективных факторов, воздействующих на процессы принятия решений о их создании (модификации и/или реконструкции и обновлении). Классификация данных факторов — по ГОСТ Р 51275.

В состав требований к качеству ИИСМиОБП в целом и отдельных ПТК и ПМК должны быть включены следующие:

- к надежности, своевременности и доступности представления информации для различных категорий персонала эксплуатационных служб и внешних пользователей;
- полноте и достоверности используемой информации на момент принятия решений или за заданный период;
- защищенности систем хранения информационных ресурсов от НСД и конфиденциальности информации;
- составу, функциям персонала служб эксплуатации ИИСМиОБП и оценке их компетенции;
- снижению вероятности ошибочных действий должностных лиц и защищенности объектов от опасных программно-технических воздействий.

8.4.2 Для обеспечения требуемого качества ИИСМиОБП должен осуществляться сбор количественной и качественной информации о необходимых и достаточных параметрах и характеристиках действий должностных лиц в системе. Понятие ошибки должно быть определено в эксплуатационной документации для каждой конкретной задачи информационной системы в зависимости от целевого назначения информации. Понятие безошибочности действий должно регламентироваться на уровне требований эксплуатационной документации, в том числе инструкций должностных лиц.

8.4.3 Показатели качества, определяющие уровни целостности критически важных объектов мониторинга предприятия, должны устанавливаться в техническом задании (ТЗ), оцениваться и уточняться при проектировании, а также контролироваться в режиме реального времени с периодом опроса в зависимости от интенсивности входных потоков данных.

Рекомендуемая номенклатура показателей качества ИИСМиОБП и базовых функциональных компонентов приведена в таблице 2.

Таблица 2 — Рекомендуемая типовая номенклатура показателей качества функциональных компонентов

Характеристика качества функционирования компонентов	Основной показатель качества функционирования компонентов ИИСМиОБП, для которых должны быть заданы допустимые значения
Надежность представления информации о состоянии объектов мониторинга, предоставляемой по регламенту или запросу пользователя	Средняя наработка объекта на отказ или сбой $T_{нар}$. Среднее время восстановления объекта после отказа оборудования, человека-оператора или сбоя программного обеспечения $T_{вос}$. Коэффициент готовности объекта $K_г$. Вероятность надежного представления выходной информации $P_{над}$ в течение заданного периода функционирования $T_{зад}$. Вероятность надежного выполнения технологических операций $P_{над}$ в течение заданного периода функционирования ИС $T_{зад}$

Окончание таблицы 2

Характеристика качества функционирования компонентов	Основной показатель качества функционирования компонентов ИИСМиОБП, для которых должны быть заданы допустимые значения
Своевременность представления информации о состоянии объектов мониторинга или выполнении задаваемых технологических операций	Среднее время реакции системы при обработке запроса и/или доведении информации $T_{полн}$ или вероятность своевременной обработки информации $P_{св}$ за заданное время $T_{зад}$. Среднее время выполнения технологической операции $T_{полн}$ или вероятность выполнения технологической операции $P_{св}$ за заданное время $T_{зад}$
Полнота используемой информации о состоянии объектов	Вероятность обеспечения полноты оперативного отражения новых реально существующих объектов и явлений предметной области $P_{полн}$
Актуальность используемой информации	Вероятность сохранения актуальности информации на момент ее использования $P_{акт}$
Корректность обработки информации	Вероятность $P_{корр}$ получения корректных результатов обработки информации за заданное время $T_{зад}$
Конфиденциальность информации	Вероятность сохранения конфиденциальности информации $P_{конф}$ в течение заданного периода конфиденциальности $T_{конф}$
Безошибочность действий персонала и должностных лиц	Вероятность безошибочных действий должностных лиц $P_{чел}$ в течение заданного периода функционирования $T_{зад}$
Защищенность от опасных программно-технических воздействий	Вероятность отсутствия опасного воздействия $P_{возд}$ в течение заданного периода функционирования ИС $T_{зад}$
Защищенность от НСД	Вероятность сохранения защищенности от НСД информационных и программных ресурсов — $P_{НСД}$

8.4.4 Методы, порядок и правила оценки и контроля качества функционирования АИС должны устанавливаться по согласованию между заказчиком и разработчиком (поставщиком) в зависимости от специфики создаваемой (поставляемой) системы с учетом специфики системы и принятых у заказчика норм, правил и требований.

Для оценки и контроля показателей качества функционирования АИС рекомендуется использовать типовые методики, которыми должны располагать разработчики, заказчики систем, органы по сертификации и испытательные лаборатории. Типовые методики должны быть адаптированы с учетом специфики системы, методов оценки результатов натурных испытаний и требований ГОСТ 34.603.

8.5 Требования к надежности

Надежность ИИСМиОБП должна быть обеспечена на основе специальных технологических решений, обеспечивающих отказоустойчивость наиболее ответственного оборудования ИИСМиОБП. Срок службы ИИСМиОБП должен быть не менее 7 лет с учетом замены неисправных и выработавших свой ресурс компонентов. Гарантийный срок на работы по оснащению, на установленное оборудование и использованные материалы должен быть не менее 12 мес.

Среднее время наработки на отказ оборудования ИИСМиОБП — не менее 10000 ч.

8.6 Требования безопасности

8.6.1 Устройства ИИСМиОБП, устанавливаемые на объектах предприятий, не должны оказывать вредного воздействия на персонал предприятия и других людей, имеющих доступ на территорию объекта.

8.6.2 Устанавливаемое на объектах предприятий оборудование должно соответствовать требованиям электробезопасности и иметь устройство заземления в соответствии с ПУЭ Правилами устройства электроустановок*.

---

* Правила устройства электроустановок (ПУЭ). Изд. 7-е (утверждены приказом Минэнерго России от 8 июля 2002 г. № 204).

8.6.3 Оборудование ИИСМиОБП и используемые расходные материалы для эксплуатации должны соответствовать требованиям действующих нормативных документов по охране труда, а также требованиям по электро- и пожарной безопасности.

9 Требования к функциональным компонентам и типовым проектным решениям интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятий

9.1 Системы и средства основных функциональных компонентов

В общем случае в состав основных функциональных компонентов ИИСМиОБП должны входить следующие системы и средства:

- локальные системы сбора данных о состоянии объектов, оперативной обработки информации и управления исполнительными механизмами (датчики и преобразователи сигналов систем жизнеобеспечения, видеокамеры, коммутаторы и регистраторы, средства контроля доступа, охранной и пожарной сигнализация и оповещения др.), которые с помощью цифрового видеонаблюдения должны осуществлять отображение, детализацию различной степени, а при необходимости добавлять или накладывать видеоизображение на объекты в трехмерном пространстве с привязкой их к географическим координатам;
- средства автоматизированного проектирования 3D-моделей зданий и сооружений, подготовки планов объектов и размещения оборудования на объектах для отображения объекта и всех его систем безопасности и контроля на многослойных 3D-картах, объединяя их в единую геоинформационную систему, позволяющую проводить ситуационный анализ объектов и территорий с возможностью отображения во времени (4D);
- средства комплектации оборудования, оценки совместимости интерфейсов, интеграции, инсталляции, тестирования и настройки на условия конкретных объектов;
- средства организации коммуникаций и видеоконференц-связи;
- средства идентификации пользователей, контроля доступа в корпоративные сети с ноутбуков, КПК, сотовых телефонов и др.;
- средства хранения информации (события, тексты, видеоизображения, голос, и др.) о состоянии объектов;
- средства ведения геоинформационных баз данных общего и специального назначения;
- средства идентификации внутренних и внешних событий — инцидентов угроз безопасности и оценки рисков нарушения целостности объектов, процессов и ресурсов предприятия;
- средства ведения реестров оборудования и ресурсов распределенных служб технического обслуживания территориально распределенных объектов;
- средства информационной поддержки оперативного взаимодействия эксплуатационного персонала объектов с внешними пользователями и спецслужбами регионов (МВД, МЧС и др.), включая соглашения о взаимодействии, организационные и электронные регламенты, стандарты и форматы обмена данными в локальных и глобальных сетях ЭВМ.

Конкретный состав и функции компонентов ИИСМиОБП формируют с учетом назначения системы мониторинга предприятий и территорий по критериям «эффективность — безопасность — стоимость».

9.2 Общие технические требования к ИИСМиОБП

9.2.1 В состав общих технических требований к ИИСМиОБП должны входить:

- требования к структуре и функциям системы;
- требования к компонентам и видам обеспечения (организационно-методическое, информационное, математическое, техническое, программное);
- требования к надежности;
- требования безопасности;
- требования к эргономике;
- требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы;
- требования к составу численности и квалификации персонала разработчиков и пользователей системы;

- требования к защите информационных ресурсов от несанкционированного доступа;
- требования к патентной чистоте;
- требования по стандартизации и унификации;
- дополнительные требования, учитывающие специфические особенности предприятия.

9.2.2 Функциональные компоненты должны быть ориентированы на применение в проектах ИИСМиОБП типовых проектных решений:

- организационно-методическое обеспечение систем;
- архитектура функциональных компонентов;
- унифицированные интерфейсы;
- унифицированные шкафы контроля и управления.

9.3 Требования по модернизации программного обеспечения и удаленному доступу к нему

9.3.1 Для всех устройств должна быть предусмотрена возможность модернизации ПО.

9.3.2 Для устройств распределенной сети должна быть обеспечена возможность удаленного доступа к ПО СБ, а также к управлению оборудованием по сети с поддержкой интерфейса RS-485, аксессуаров на базе USB и низкоскоростной технологической шины 1-Wire.

9.3.3 Силовые контроллеры электрических цепей (до 220В/16А) должны обеспечивать удаленное управление питанием оборудования и рестарт при возникновении отказов оборудования, сбоев в ПО, а также инициализацию запросов на выполнение ответственных операций по восстановлению работоспособности и замене программного обеспечения на управляемом оборудовании.

9.3.4 Интерфейсные модули и внешние аксессуары для удаленного управления контроллерами управления оборудованием, специализированными локальными серверами, маршрутизаторам и коммутаторами предназначены для непосредственного мониторинга и управления физическими параметрами (такими как токи, факт замыкания или размыкания электрической цепи, напряжения, температуры и т. п.) и должны обеспечивать контроль:

- срабатывания пожарных, охранных и других датчиков состояния систем жизнеобеспечения, концевых выключателей и других двоичных датчиков любого рода;
- наличия напряжения питания (в двоичном виде — «да/нет»);
- напряжения на резервных аккумуляторных батареях (в аналоговом виде);
- температуры окружающей среды и отдельных электронных устройств на объектах в местах установки оборудования;
- состояния сигнальных «сухих контактов» на телекоммуникационном оборудовании.

9.4 Функциональные возможности выходных контроллеров и силовых реле

Выходные контроллеры и силовые реле должны обеспечивать управление электрическими цепями любого типа и назначения, как слаботочными, так и силовыми, в том числе:

- включать сигнальные табло, сирены, блокировать двери и т. п.;
- перезагружать проблемное оборудование, расположенное в непосредственной близости от устройства NSG, путем замыкания его цепей RESET или POWER;
- принудительно перезагружать проблемное оборудование путем прерывания его цепи электропитания;
- последовательно включать оборудование в телекоммуникационных узлах с заданными задержками, избегая перегрузок питания при общем единовременном старте;
- управлять системами резервного электропитания;
- управлять системами отопления и кондиционирования шкафов.

10 Требования к организации распределенной сети региональных ситуационных и информационно-аналитических центров мониторинга состояния целостности объектов и безопасности территорий

Особая роль при разработке технологий создания РИСМО отводится формированию моделей обработки событий и процедур принятия решений в ситуационных центрах предприятий. Деятельность современных предприятий во многом определяется состоянием инфраструктур территорий, использованием ресурсов землепользования, энергоснабжения, транспорта, коммунальных служб города и другими процессами взаимодействия с внешним окружением и взаимовлиянием на состояние безо-

пасности инженерной и социальной инфраструктуры региона, экологической, промышленной и общественной и иных видов безопасности. Пример обобщенной схемы взаимодействия ИИСМиОБП в регионе приведен на рисунке 3.

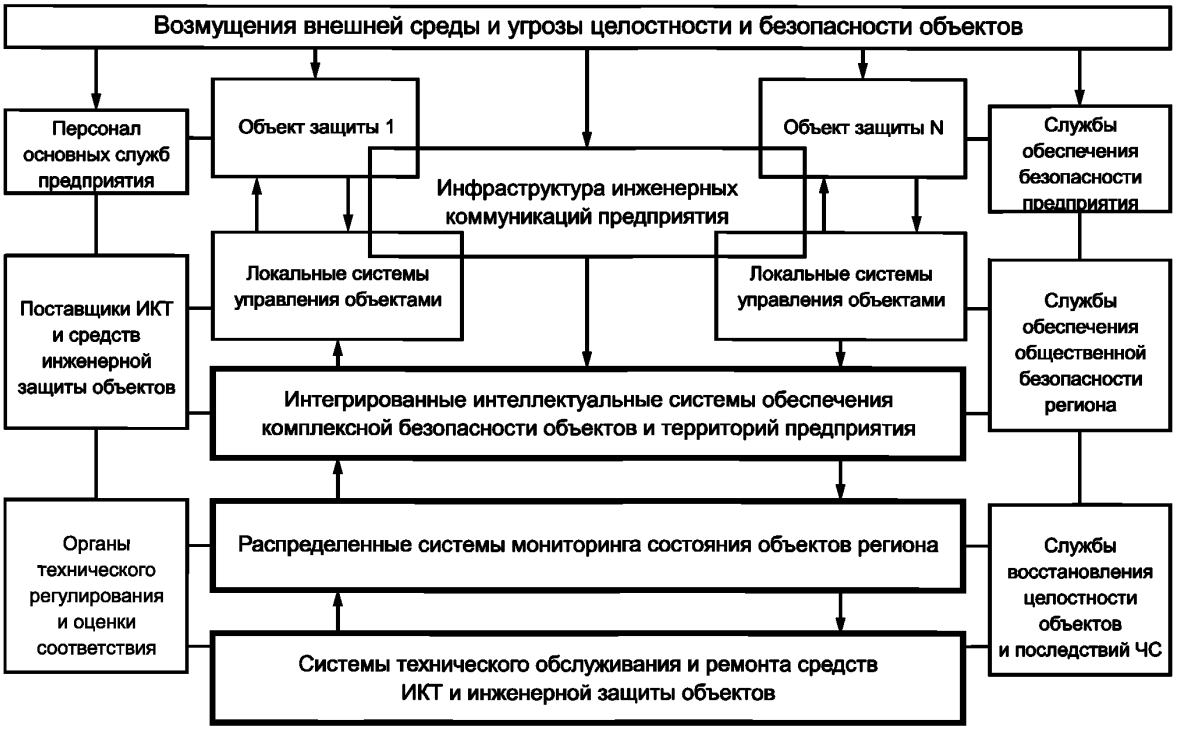


Рисунок 3 — Обобщенная схема взаимодействия ИИСМиОБП региона

В инфраструктуре регионов (городов и муниципальных образований) выделяются ряд специализированных организаций, ориентированных на решение задач мониторинга состояния безопасности закрепленных за ними группы объектов, в которых создаются соответствующие ситуационные и информационно-аналитические центры по отдельным направлениям (энергетика, транспорт, общественная безопасность, экология, ликвидация аварийных и чрезвычайных ситуаций и др.).

10.1 Организационные вопросы создания

10.1.1 Организация работ по созданию ИИСМиОБП должна включать в себя типовую схему проведения работ на стадиях жизненного цикла ИИСМиОБП (см. приложение А), соответствовать требованиям ГОСТ 34.601 и содержать необходимый и достаточный набор методических и инструментальных средств проектной компоновки заказных «индивидуальных» систем по открытым спецификациям требований для конкретных заказчиков, а также средства документирования проектов и правил взаимодействия участников проектов.

10.1.2 При организации сетевого взаимодействия участники сетевого обмена должны согласовать и принять соглашения по уровням и типам электрических сигналов, критическим размерам сообщений, методам контроля достоверности. Соглашения должны быть приняты по всем уровням взаимодействия, начиная от самого низкого — передача битов информации, и заканчивая самым высоким, реализующим обслуживание пользователей сети. Межведомственный обмен данными для подготовки и принятия решений по мероприятиям обеспечения безопасности стратегических и социальнозначимых объектов и территорий должен выполняться по согласованным регламентам, протоколам и форматам обмена данными в распределенной полицентрической сети ситуационных и информационно-аналитических центров Российской Федерации.

10.1.3 Организационно-технические решения по выбору среды реализации, оборудования ИКТ общего назначения в ситуационных центрах предприятий, муниципальных образований и регионов должны обеспечивать взаимодействие всех необходимых и достаточных подразделений и служб эксплуатации объектов мониторинга и восстановления целостности объектов в аварийных и критических ситуациях.

10.1.4 Отдельные ситуационные центры могут специализироваться на решении задач оценки состояния безопасности персонала и населения, общественной безопасности, экологической безопасности, радиационной и химической защиты, энергетики, транспорта, промышленных производств и технологий, коммунального хозяйства и др.

10.2 Требования к обработке событий в распределенных интегрированных системах мониторинга состояния объектов

Событие должно быть представлено как зафиксированное на определенный момент времени состояние входящего, в общем случае, случайного нестационарного потока данных. Основными задачами обработки такого потока для обнаружения и нейтрализации негативных событий и минимизации ущербов в деятельности предприятия и его ключевых процессов являются:

- регистрация события и определение источника сообщения о событии;
- выделение признаков угроз из потока;
- идентификация типа угроз и возможных последствий развития события и инициируемых им действий;
- обнаружение источников угроз с одной стороны и элементов принятия решений (в общем случае лиц, принимающих решения, или интеллектуальных устройств) в системах управления предприятия разного уровня;
- определение регламента обслуживания соответствующего потока данных (сообщений, сигналов, документов);
- упорядочение потока событий и организация эффективного накопления потока событий (ведение архива истории событий);
- оперативная обработка поступающей информации в соответствии с заранее определенными правилами обработки и принятия решений;
- вторичная обработка массивов разнородных событий и корреляционных связей между ними (поиск взаимосвязанных событий, объектов и субъектов для принятия дополнительных мер, планирования мероприятий и других действий);
- принятие решений и формирование необходимых адресных сообщений для их исполнения.

11 Требования к защите информационных ресурсов предприятий и правам доступа пользователей интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия

11.1 Общие требования

11.1.1 Архитектура ИИСМиОБП должна предусматривать наличие ПТК, обеспечивающего необходимый уровень защиты и сохранности информационных ресурсов предприятия в условиях сбоев и отказов программно-аппаратных средств, включая сбой в системе электропитания. Указанный ПТК ИИСМиОБП должен обеспечивать корректное восстановление работы ИИСМиОБП после сбоев без потери данных.

11.1.2 В целях обеспечения сохранности информационных ресурсов ИИСМиОБП должно быть в обязательном порядке предусмотрено наличие функции резервного копирования данных.

11.1.3 Требования к допустимым значениям показателей функционирования и к основным характеристикам АС (надежность, быстродействие, возможность изменения конфигурации) должны соблюдаться при использовании программно-технических средств защиты.

11.1.4 ИИСМиОБП должна обеспечивать контроль эффективности средств защиты от НСД, который может быть либо периодическим, либо инициироваться по мере необходимости пользователем или контролирующими органами.

11.1.5 Средства защиты информационных ресурсов предприятий и информационно-аналитических и ситуационных центров должны включать в себя организационно-распорядительные меры, средства физической и электронной защиты по ГОСТ Р 50739, ГОСТ Р 50922, ГОСТ Р 51275 в зависимости от места расположения объекта, конкретных условий и особенностей объектов мониторинга, режима безопасности, действующего внутри объекта, наличия инженерно-технических средств физической защиты накопителей данных.

11.2 Идентификация сообщений

Сообщения о состоянии объектов мониторинга с повышенным уровнем угроз безопасности (зоны ограниченного доступа в здания, сооружения, на территорию и информационные ресурсы предприятия и т. п.) должны содержать средства автоматической цифровой электронной подписи, сертифицированные уполномоченными органами и структурами России.

11.3 Требования к непрерывности цикла защиты информационных ресурсов

Защита информационных ресурсов АС должна быть обеспечена на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

11.4 Классификация уровня защищенности

Для классификации объектов мониторинга по уровню защищенности информационных ресурсов объекта должны быть использованы следующие характеристики:

- информационные, определяющие ценность информации, ее объем и степень конфиденциальности, а также возможные последствия неправильного функционирования из-за искажения (потери) информации;
- организационные, определяющие полномочия пользователей;
- технологические, определяющие условия обработки информации, например способ обработки (автономный, мультипрограммный и т. д.), время циркуляции (транзит, хранение и т. д.), вид АС (автономная, сеть, стационарная, подвижная и т. д.).

11.5 Способы защиты информационных ресурсов

Обеспечение защиты информационных ресурсов ИИСМиОБП осуществляется:

- СРД пользователей к оборудованию, информационным ресурсам и программным средствам обработки данных, отображения и принятия решений;
- реализацией правил разграничения доступа к устройствам создания твердых копий с документации;
- изоляцией программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управлением потоками данных в целях предотвращения записи данных на носители несоответствующего грифа.

Основными требованиями к СКЗИ при этом являются следующие:

- выполнение целевых функций;
- удобство и простота обслуживания;
- оптимальная производительность;
- высокая надежность в режиме работы 24/7/365;
- невысокая совокупная стоимость эксплуатации в течение всего жизненного цикла;
- соответствие требованиям регулирующих органов (сертификаты соответствия);
- шифрование по ГОСТ 28147 (256 битов).

Сценариями использования СКЗИ являются следующие:

- межсетевые взаимодействия;
- защищенный доступ удаленных и мобильных пользователей;
- защита беспроводных сетей связи;
- защита мультисервисных сетей (включая IP-телефонию и видеоконференц-связь);
- разграничение доступа к информации в локальных сетях, а также любые комбинации вышеперечисленных сценариев.

11.6 Средства разграничения доступа

11.6.1 СРД пользователей к материальным и информационным ресурсам предприятия должны обеспечивать:

- двухфакторную идентификацию и опознание (аутентификацию) зарегистрированных пользователей и при необходимости определение привязки к месту его нахождения;
- регистрацию действий пользователей по несанкционированному доступу к оборудованию и информационным ресурсам предприятия и их использованию;
- исключение и включение новых пользователей и объектов доступа, а также изменение полномочий пользователей;
- реакцию на попытки НСД, например сигнализацию, блокировку, восстановление после НСД;
- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищенными данными;
- контроль целостности баз данных информационных ресурсов и СРД.

11.6.2 Способы реализации СРД зависят от конкретных особенностей объектов мониторинга предприятия. Допускается применять следующие способы защиты и любые их сочетания:

- СРД, локализованные в программно-техническом комплексе (ядро защиты);
- СРД на уровне операционных систем, систéм управлéния бáзами дáнных или прикладных программ;
- СРД в средствах реализации сетевых взаимодействий или на уровне приложений;
- использование криптографических преобразований или методов непосредственного контроля доступа;
- распределенные СРД;
- программная и (или) техническая реализация СРД;
- организация доступа уполномоченного лица к разрешенной информации, защищенный электронной подписью.

11.6.3 СРД и средства защиты информационных ресурсов предприятия должны обеспечивать конфиденциальность и целостность получаемой информации с учетом назначения, важности и специфики объектов мониторинга.

Примерами отдельных решений могут быть следующие:

- конфиденциальность и целостность передаваемой по сети информации путем криптографической обработки каждого сетевого пакета с помощью криптографических алгоритмов;
- аутентификация отдельного пользователя и реализация индивидуальных политик доступа к заданным компьютерам, прикладным программам обработки данных и к разделам баз данных;
- вход в защищенную сеть только для владельца легитимного криптоключа;
- выполнение требований стандартов безопасности IKE/IPsec с применением российских алгоритмов криптографического преобразования по ГОСТ 28147, ГОСТ Р 34.10 и ГОСТ Р 34.11.

11.7 Инструменты управления и поддержки эксплуатации программно-аппаратной платформы интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия

Инструменты управления и поддержки эксплуатации ПАП ИИСМиОБП должны включать в себя средства реализации политики безопасности VPN клиентов и шлюзов, осуществлять управление этими устройствами, включая настройки сетевых интерфейсов, системы протоколирования, обеспечивать возможность плановой замены сертификатов без прерывания цикла эксплуатации и связи, удаленного обновления программного обеспечения.

11.8 Топология построения

Шлюзы безопасности должны обеспечивать построение любых топологических схем («звезда», «дерево», «полносвязная сеть»). При необходимости реализуют схемы с повышенной надежностью, обеспечиваемой как за счет резервирования шлюзов, так и за счет использования альтернативных маршрутов сети. Пример такой схемы изображен на рисунке 4.

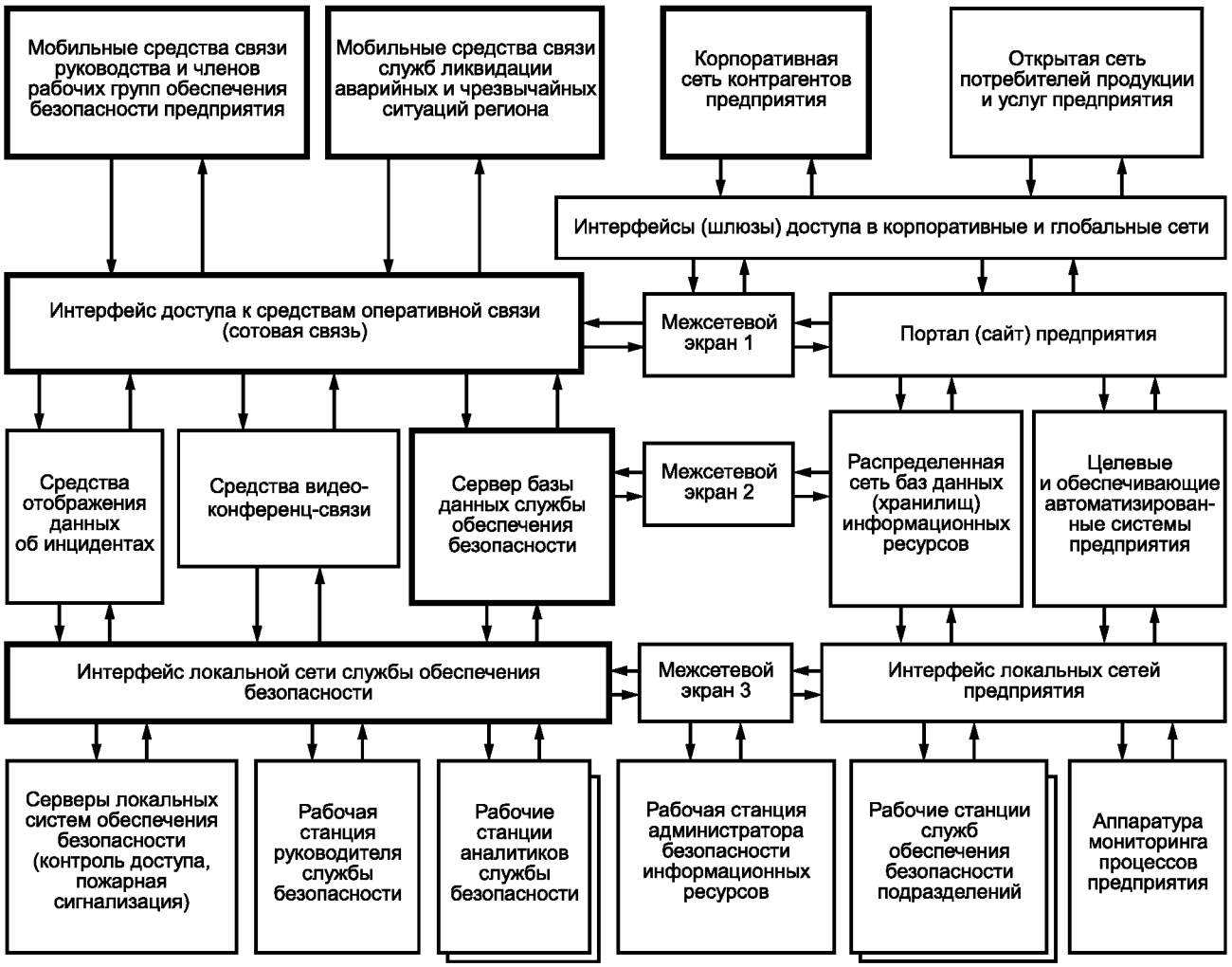


Рисунок 4 — Схема реализации ИИСМиОБП с использованием шлюзов безопасности и межсетевых экранов

11.9 Требования к межсетевым экранам

При включении межсетевых экранов в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее межсетевого экрана, не должен понижаться. Межсетевые экраны должны быть сертифицированы как СКЗИ классов защищенности, соответствующих требованиям Федеральной службы по техническому и экспортному контролю России к обеспечению защиты информации в автоматизированных системах и ГОСТ Р ИСО/МЭК 15408-1.

11.10 Аутентификация удаленных пользователей

Для удаленных пользователей применяются различные механизмы аутентификации, например индивидуальный предустановленный ключ, пароль, электронная подпись. Для построения на стратегически и социально значимых объектах доверенного сеанса связи и обеспечения безопасности коммуникаций в рамках доверенного доступа к выделенному конфиденциальному ресурсу должна обеспечиваться целостность программной среды терминала, изоляция вычислительного процесса клиента, строгая двухфакторная аутентификация, изоляция сетевой среды удаленного пользователя, конфиденциальность и целостность передаваемых данных.

11.11 Уровень защищенности системы разграничения доступа к информационным ресурсам

Требования к уровню защищенности СРД должны быть тщательно документированы. В состав документации включают руководство пользователя по использованию и руководство по управлению средствами защиты, а также, при необходимости, другие эксплуатационные, удостоверяющие и разрешительные документы службы безопасности.

Приложение А
(справочное)

Стадии и этапы жизненного цикла интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия

Стадии и основные этапы жизненного цикла ИИСМиОБП выбирают в соответствии с рекомендациями ГОСТ Р ИСО/МЭК 12207. Основные цели каждой стадии и состав возможных технических решений для обоснования и проектирования профиля конкретной системы обеспечения безопасности предприятия приведены в таблице А.1

Таблица А.1 — Стадии жизненного цикла и основные технические решения ИИСМиОБП

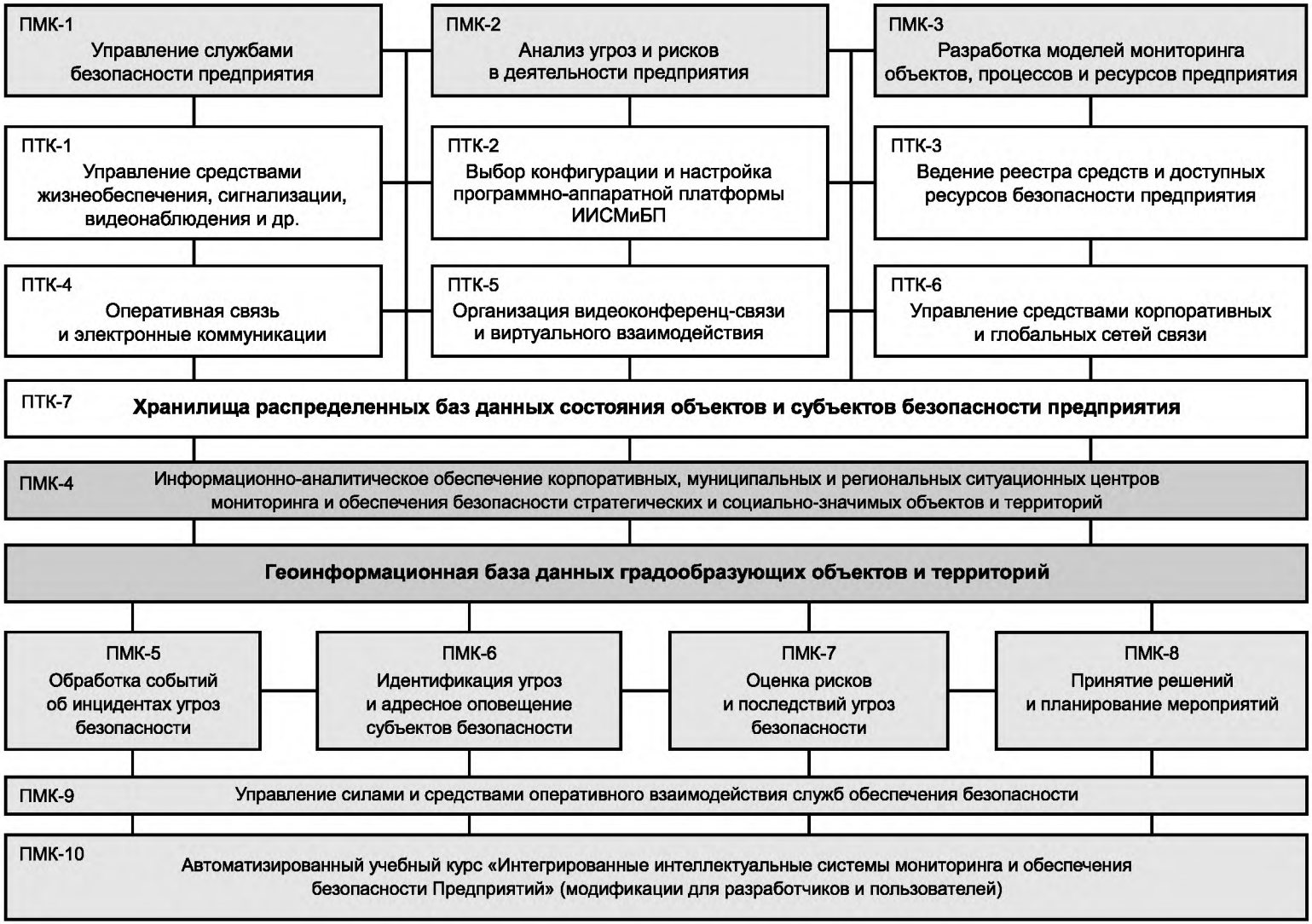
Стадия жизненного цикла ИИСМиОБП	Целевые установки стадии	Диапазон решений
Концепция	Определить состав объектов и угроз безопасности предприятия. Определить состав показателей целостности и защищенности ключевых объектов и субъектов предприятия. Сформулировать концепцию обеспечения безопасности ключевых процессов. Определить функциональную архитектуру. Предложить приемлемые проектные решения. Определить состав пользователей и персонала служб обеспечения безопасности, распределение их компетенции, функций, прав и ответственности. Разработать спецификации требований к подсистемам и базовым ПТК ИКТ. Определить принципы координации деятельности рабочих групп исполнителей и ресурсообеспечения общесистемного и частных проектов обеспечения безопасности предприятия	Локальные системы мониторинга и безопасности ключевых объектов и процессов предприятия. Интегрированные системы обеспечения комплексной безопасности предприятия
Разработка соглашений, регламентов и внутренних стандартов деятельности предприятия по обеспечению безопасности	Уточнить системные требования к средствам обеспечения безопасности. Определить общие регламенты взаимодействия служб обеспечения безопасности предприятия, основных подразделений — владельцев потенциально опасных объектов и процессов предприятия, их внутренних и внешних контрагентов. Разработать документооборот служб обеспечения безопасности	Соглашения на основе законодательства Российской Федерации. Корпоративные соглашения. Регламенты, процедуры и форматы обмена данными. Протоколы передачи данных
Проектирование (приобретение) средств обеспечения безопасности	Выполнить анализ процессов и средств обеспечения безопасности ключевых процессов предприятия. Разработать функциональные и математические модели процессов обеспечения безопасности. Подготовить варианты проектных решений по выбору средств организационного, методического, технического и программного обеспечения. Выполнить анализ технических предложений и провести их тестирование на совместимость с эксплуатируемыми (наследуемыми) целевыми автоматизированными системами предприятия.	Разработка (закупка) локальных систем. Актуализация и применение условий действующих стандартов и типовых проектных решений средств безопасности. Применение отраслевых (корпоративных) требований. Системная интеграция

Окончание таблицы А.1

Стадия жизненного цикла ИИСМиОБП	Целевые установки стадии	Диапазон решений
	Сформировать перечень (реестр) средств обеспечения безопасности, рекомендуемых для применения в проекте. Организовать проектирование (закупку) средств обеспечения безопасности. Выполнить работы по комплексированию и инсталляции средств ИИСМиОБП на рабочих местах служб обеспечения безопасности	
Эксплуатация	Разработать модели технического обслуживания средств обеспечения безопасности предприятия. Определить требования к знаниям, навыкам и умениям персонала служб безопасности и эксплуатации технического и программного обеспечения. Провести обучение и аттестацию персонала. Обеспечить выделение необходимых ресурсов для эксплуатации системы. Эксплуатировать систему с целью удовлетворения потребностей пользователей целевых и обеспечивающих автоматизированную систему предприятия в сервисах безопасности.	Требования и условия технического обслуживания локальных (автономных) систем обеспечения безопасности ключевых процессов и объектов предприятия. Централизованный мониторинг состояния объектов службой безопасности. Централизованный мониторинг состояния безопасности информационных ресурсов предприятия
Сопровождение	Организовать службу мониторинга и сопровождения средств безопасности предприятия. Разработать регламенты взаимодействия и типовые сценарии анализа инцидентов — угроз безопасности. Анализировать изменения в архитектуре предприятия, продукции, процессах и технологиях и их влияние на состояние безопасности для модификации систем и эксплуатации. Обеспечить выделение необходимых ресурсов для длительного функционирование системы с учетом возможной модификации или замены отдельных компонентов по мере их морального или физического износа	Сопровождение средств безопасности силами специализированных служб предприятия. Сопровождение компонентов силами разработчиков и поставщиков оборудования и программного обеспечения. Сопровождение силами специализированных организаций
Завершение (ликвидация)	Анализировать работу средств ИИСМиОБП на объектах предприятия. Вести учет и прогнозирование технического и морального старения компонентов, планировать своевременную замену, выделения ресурсов для восстановления целостности системы. Хранение или утилизация средств ИИСМиОБП	Замена отказавших и морально устаревших компонентов, списание и уничтожение объектов. Реализация компонентов на рынке. Организация и осуществление хранения средств и компонентов ИИСМиОБП

Приложение Б
(рекомендуемое)

Функциональные компоненты архитектуры интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия



Приложение В
(рекомендуемое)

Форма описания структуры базового профиля интегрированной интеллектуальной системы мониторинга и обеспечения безопасности предприятия

Основные типы базовых моделей, рекомендуемых для описания при разработке ИИСМиОБП, приведены в таблице В.1.

Таблица В.1 — Структура базового профиля ИИСМиОБП

Тип	Наименование базовой модели	Формат описания
1	Функциональные модели деятельности подразделений предприятия — владельца объекта	Для каждой службы предприятия указываются объекты, процессы и ресурсы, подлежащие защите
1.1	Подразделения административного управления	Описание функций (текст). Организационная структура. Схема (диаграмма) взаимодействия. Список объектов, процессов и ресурсов, подлежащих защите от негативных воздействий. Диаграмма процессов
1.2	Научные и проектные подразделения	Описание объектов деятельности. Диаграмма потоков данных. Список объектов, процессов и ресурсов, подлежащих защите от негативных воздействий
1.3	Производственные подразделения	Список объектов, процессов и ресурсов, подлежащих защите от негативных воздействий. Список контролируемых параметров производственных подразделений
1.4	Подразделения инженерной инфраструктуры предприятия	Список объектов, процессов и ресурсов, подлежащих защите от негативных воздействий. Планы размещения оборудования. Конструктивные 3D-модели зданий и сооружений
1.5	Подразделения информационной службы предприятия	Реестр информационных ресурсов предприятий. Реестр оборудования и программного обеспечения АС систем предприятия
1.6	Подразделения безопасности	—
1.7	Подразделения служб	—
1.8	Подразделения филиалов и представительств предприятия в других регионах	—
2	Информационные модели документооборота (диаграммы потоков данных)	Схема документооборота предприятия. Матрица применяемости документов в подразделениях. Маршруты, диаграммы потоков данных
3	Законодательное и нормативное обеспечение задач обеспечения безопасности продукции, процессов и ресурсов предприятия	Список НТД. Таблицы применяемости. Регламентированные (нормированные) значения показателей

Продолжение таблицы В.1

Тип	Наименование базовой модели	Формат описания
4	Информационно-логические модели баз данных	Схема базы данных логическая
4.1	Общего назначения	Справочник метаданных распределенной базы данных предприятия. Схема базы данных. Список зарегистрированных пользователей. Права доступа модель защиты от НСД и использования информационных ресурсов
4.2	Локальных баз данных о характеристиках объектов и показателях безопасности продукции, процессов и ресурсов предприятия	Схема базы данных физическая. Типовые формы ввода данных, запросы пользователей информационных ресурсов. Форматы выходных отчетов
4.3	База данных (реестр) средств защиты и обеспечения безопасности ресурсов предприятия	Схема базы данных физическая. Типовые формы ввода данных, запросы пользователей информационных ресурсов. Форматы выходных отчетов
4.4	Модели выбора информационной среды пользователей (тип ОС, СУБД и др.)	Обоснование выбора (текст). Математическая модель (расчетные формулы) оценки производительности, объемов памяти, времени отклика. Таблица сравнительных характеристик вариантов ТПР
4.5	Модели организации доступа к данным по инцидентам угроз безопасности и истории принятых мер	Список пользователей. Права доступа к данным. Приоритеты обслуживания. Модель защиты данных. Статистика использования
5	Интерфейсы, соглашения по обмену данными в ИИСМиБП	—
5.1	Организационные регламенты	Список соглашений и принятых регламентов взаимодействия участников проектов (текст). Диаграмма внешних связей. Семантическая модель предметной области
5.2	Технические (аппаратные)	Описание интерфейса оборудования и устройств связи (текст). Схема функциональная. Схема принципиальная. Инструкция по настройке
5.3	Программные	Описание интерфейса (текст). Схема алгоритма
5.4	Протоколы передачи данных	Описание протокола (текст). Описание программного модуля передачи данных (открытый код на языке программирования)
6	Базовые модели деятельности (организационные регламенты)	—
6.1	Руководителей и ведущих специалистов предприятия (совета безопасности предприятия)	Таблица (матрица) распределения функций и зон ответственности по закрепленным направлениям деятельности подразделений предприятия

Продолжение таблицы В.1

Тип	Наименование базовой модели	Формат описания
6.2	Аналитиков по отдельным направлениям обеспечения безопасности продукции, процессов и ресурсов предприятия	Описание функций поста и зон ответственности (текст). Список (таблица) контролируемых показателей состояния объектов мониторинга. Запросы на поиск информации в базе данных (текст на языке предметной области проекта). Модель представления и отображения данных на рабочем месте аналитика. Таблицы решений. Деревья решений. Статистическая (вероятностная) модель оценки возмущающих воздействий на объект мониторинга. Математическая модель (расчетная формула) оценки комплексного состояния объекта. Сценарии действий в аварийных и критических ситуациях
6.3	Персонала по текущей оперативной работе	Технологические инструкции по действиям в аварийных и критических ситуациях
6.4	Администраторов локальных баз данных информационных ресурсов подразделений предприятия	Реестр объектов информационных ресурсов. Реестр оборудования инженерно-технических средств защиты. Реестр (таблица) пользователей и прав их доступа к информационным ресурсам предприятия
6.5	Администраторов баз данных общего назначения	
6.6	Администраторов корпоративных сетей ЭВМ	
6.7	Администраторов почтовых служб	Списки пользователей. Модель доступа и защиты отправлений, модель защиты от спама
6.8	Технического персонала по обслуживанию средств и электронных коммуникаций	Реестр оборудования ИИСМиОБП, установленного на объектах обслуживания. График технического обслуживания. Показатели технического обслуживания. Расчетные формулы оценки затрат на техническое обслуживание и ремонт
7	Расчетно-аналитические модели для решения прикладных задач обработки данных и принятия решений по инцидентам угроз безопасности в региональных (отраслевых) целевых АС предприятия	—
7.1	Ввод, идентификация и предварительная обработка данных о состоянии объектов и субъектов безопасности предприятия	Описание входного потока данных. Схема алгоритма обработки сообщений, формы ввода данных оператором. Запросы на поиск данных
7.2	Упорядочение данных, группировки и оценка текущих и прогнозных показателей безопасности предприятия	Схема алгоритма обработки сообщений. Классификация потоков. Модель приоритетного обслуживания сообщений
7.3	Модели оценки рисков. Расчет нормативных (приемлемых) уровней рисков обеспечения заданных конструктивно-технологических характеристик объектов, процессов и ресурсов предприятия	Математическая модель оценки риска. Расчетные формулы нормативных (приемлемых) уровней риска

Окончание таблицы В.1

Тип	Наименование базовой модели	Формат описания
7.4	Модели статистического оценивания и прогноза показателей безопасности. Экспертная оценка ситуаций и подготовка альтернатив принятия решений по мероприятиям (проектам) обеспечения безопасности	Математическая модель, расчетные формулы. Статистика. Экспертная оценка ситуаций и подготовка альтернатив принятия решений
7.5	Модели анализа влияния показателей безопасности на ключевые технико-экономические показатели деятельности предприятия (муниципального образования, региона)	Семантическая модель предметной области. Математическая модель, расчетные формулы. Статистика
7.6	Балансовые модели распределения средств и услуг безопасности по подразделениям предприятия. Модели согласования ресурсов на проекты, оборудование и услуги подразделений безопасности	Таблица (матрица) распределения ресурсов. Функциональная математическая модель оценки потребности в ресурсе. Статистика использования ресурсов. Математическая модель многокритериального анализа альтернатив принятия решений
7.7	Модели планирования операций и согласования решений проблемно-ситуационных задач управления по нейтрализации внутренних и внешних угроз безопасности и минимизации ущербов в деятельности предприятия (региона)	Сетевая модель планирования. График Ганта. Сценарии развития событий, анализ временных рядов Таблицы решений. Деревья решений. Математическая модель оптимизации. Расчетные формулы
7.8	Технико-экономические расчеты по программам, проектам и мероприятиям обеспечения безопасности	Описание проектов и мероприятий по обеспечению безопасности. Математические модели влияния показателей безопасности на показатели деятельности предприятия. Расчетные формулы оценки потребности в ресурсах на проекты
8	Проектные модели оптимизации структуры комплекса средств обеспечения безопасности	Описание архитектуры и ТПР (текст). Схема функциональная ИИСМиОБП. Схема потоков данных. Описание системных характеристик оборудования и программного обеспечения альтернативных вариантов проектных решений. Математические модели оценки надежности, пропускной способности и производительности. Имитационная модель функционирования. Расчетные формулы
9	Модели технического обслуживания и сопровождения средств безопасности в подразделениях	Математические модели. Расчетные формулы
10	Модели формирования требований к функциям и компетентности эксплуатационного персонала, оценки деятельности должностных лиц	Описание функций поста (текст). Схема (диаграмма) рабочего процесса. Модель оперативных действий. Показатели качества. Показатели результативности. Показатели надежности операторской деятельности

Приложение Г
(рекомендуемое)

Типовая архитектура ситуационного центра

Типовая структура ситуационного центра приведена на рисунке Г.1.

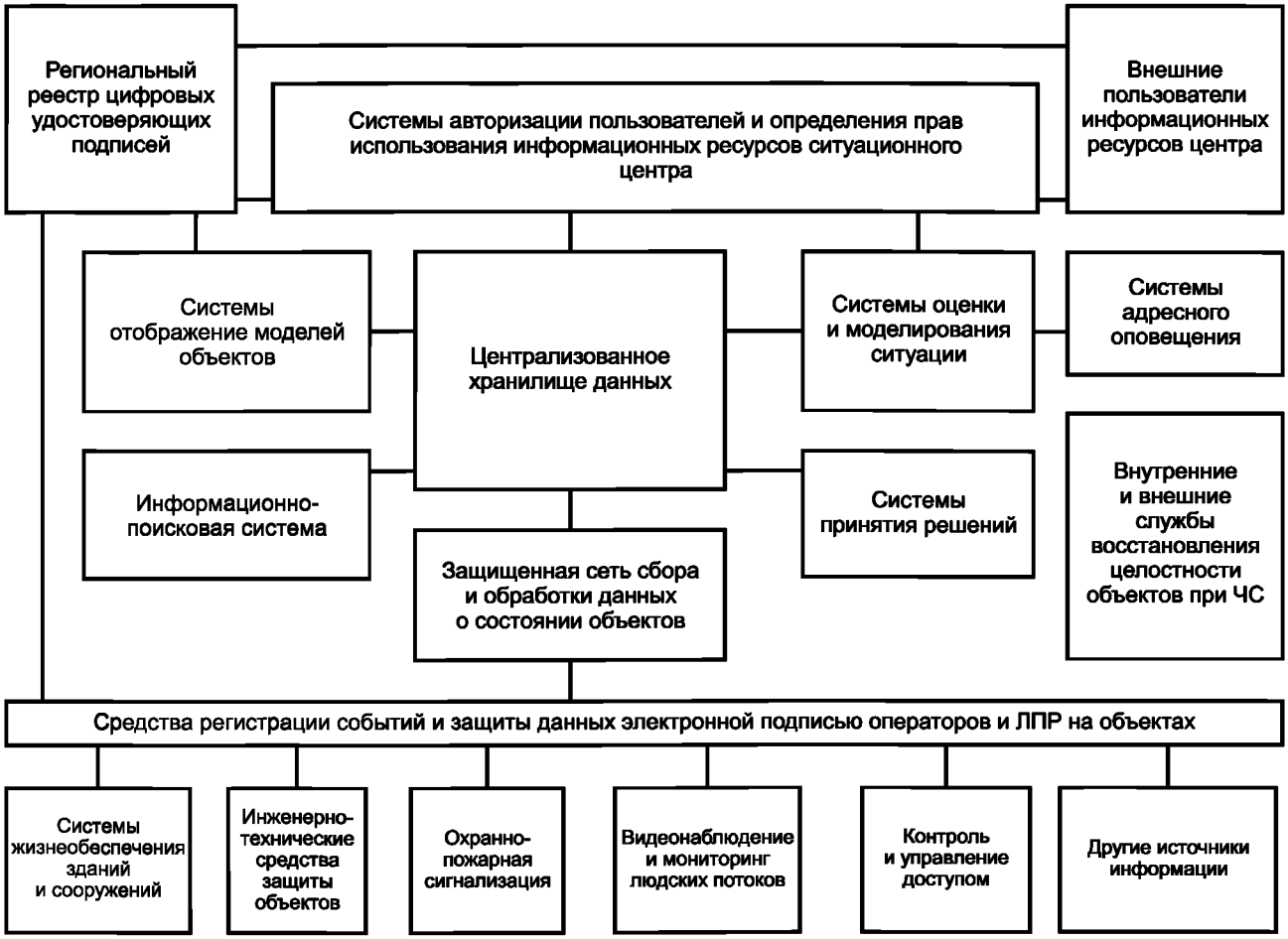


Рисунок Г.1 — Типовая структура ситуационного центра

УДК 658.382.3:006.354

ОКС 35.100
35.200

Ключевые слова: архитектура систем, интеграция, интеллектуальные системы, общественная безопасность, мониторинг, общие технические требования, программные средства, ситуационный центр, открытые коды, полицентричность, интероперабельность

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *С.В. Смирнова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 16.01.2019. Подписано в печать 30.01.2019. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,60.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru