АКЦИОНЕРНОЕ ОБЩЕСТВО

«ЦЕНТР ОТКРЫТЫХ СИСТЕМ
И ВЫСОКИХ ТЕХНОЛОГИЙ»

Программный комплекс ситуационного анализа (ядро операционного центра) COSOC

ОПИСАНИЕ

Москва, 2018

Содержание

Определения, обозначения и сокращения

API — (от англ. Application Programming Interface) — программный интерфейс приложения — набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением для использования во внешних программных продуктах

CAP — (от англ. Common Alerting Protocol) - протокол общего оповещения - стандарт OASIS, утвержденный FEMA (Federal Emergency Management Agency, определяющий формат xml-сообщения о событиях и угрозах

CSV — (CSV от англ. Comma-Separated Values — значения, разделённые запятыми) — текстовый формат, предназначенный для представления табличных данных

Dynamic HTML — набор средств, которые позволяют создавать более интерактивные Web-страницы без увеличения загрузки сервера

GUI — (от англ. Graphical User Interface) - графический интерфейс пользователя, разновидность пользовательского интерфейса, в котором элементы интерфейса (меню, кнопки, значки, списки и т. п.) исполнены в виде графических изображений

HTML — Язык гипертекстовой разметки документов (от англ. Hypertext Markup Language – “язык гипертекстовой разметки”)

HTTP — Протокол прикладного уровня для передачи данных, используемый в Web (от англ. HyperText Transfer Protocol - «протокол передачи гипертекста»)

IP-адрес — Уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP

JavaScript — Прототипноориентированный сценарный язык программирования. Наиболее широкое применение находит в браузерах как язык сценариев для придания интерактивности веб-страницам

JPEG (JPG) — JPEG - один из популярных графических форматов, применяемый для хранения фотоизображений и подобных им

изображений. Файлы, содержащие данные JPEG, обычно имеют расширения .jpg, .jfif, .jpe или .jpeg.

KPI (или КПЭ) — (от англ. Key Performance Indicator) - ключевой показатель эффективности

PDF — Portable Document Format (PDF) — межплатформенный формат электронных документов, разработанный фирмой Adobe Systems

PHP — Скриптовый язык общего назначения, интенсивно применяемый для разработки веб-приложений.

PNG — Растровый формат хранения графической информации, использующий сжатие без потерь качества

АИС — Автоматизированная информационная система

АС — Автоматизированная система

Интернет — Информационно-коммуникационная сеть Интернет

ИТ — Информационные технологии, информационно-технологический

МЭДО — межведомственный электронный документооборот

НСИ — Нормативно – справочная информация

Открытые данные — Информация, размещаемая ее обладателями в сети «Интернет» в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования

ПО — Программное обеспечение

СМЭВ — Система межведомственного электронного взаимодействия

ФОИВ — Федеральный орган исполнительной власти

Реферат

Программное решение ситуационного анализа COSOC предназначено для информационно-аналитической поддержки процессов управления состоянием объектов/территорий, выполняемых в повседневном режиме или в условиях чрезвычайных/кризисных ситуаций, в том числе:

1) анализ и оценка ситуаций на основе информации о событиях и угрозах, поступающей из различных источников;

2) поддержка принятия решений на основе распознавания типовых ситуаций.

Основной вариант использования COSOC: подсистема обработки поступающих сообщений в стандартизованном формате в составе интеллектуальных операционных (ситуационных) центров различного уровня, работающая автономно или в интеграции с аналогичными решениями.

1 Назначение и общие принципы построения программного продукта

1.1 Назначение программного комплекса

Программный комплекс COSOC предназначен для обеспечения информационно-аналитической поддержки процессов сбора, хранения и обработки сообщений о событиях и угрозах, поступающих в структурированном виде от внешних источников информации.

Предметом автоматизации COSOC являются деловые процессы, в том числе процессы информационного взаимодействия внутреннего и внешнего характера.

1.2 Общие принципы работы программного комплекса

Программное обеспечение ситуационного анализа создано в соответствии с следующими базовыми принципами:

1) вся информация собирается в виде сообщений об угрозах и событиях в соответствии с требованиями Common Alerting Protocol (стандарт OASIS, утвержденный FEMA (Federal Emergency Management Agency) V1.2);

2) вся информация собирается и обрабатывается в едином центре, и предоставляется через API во внешние интегрированные системы и/или на АРМ сотрудников ситуационных центров и руководителей, которые осуществляют мониторинг ситуации и принятие решений по управлению силами и средствами, иных управленческих решений оперативного и стратегического уровня;

3) источниками информации могут служить сообщения граждан, сообщения автоматизированных систем мониторинга (метеостанции, системы контроля периметра, интеллектуальные видеокамеры, системы экологического контроля и т.д.), ЕДДС и иные диспетчерские службы, внешние по отношению к программному комплексу автоматизированные системы, такие как: система-112, "Безопасный город", АИС департаментов и муниципальных предприятий, и т.д.;

4) деятельность по управлению объектом (городом, регионом) разбивается на набор типов и подтипов деятельности, причем в рамках каждого подтипа деятельности формируется несколько моделей деятельности;

5) в рамках каждой модели деятельности может формироваться набор метрик и ключевых показателей, образующих иерархию;

6) программный комплекс обеспечивает мониторинг и прогнозирование ситуации, основываясь на моделях деятельности и метриках, вычисляемых на основании информации, содержащейся в поступающих сообщениях;

7) интеграция с внешними системами реализуется путем создания специализированных шлюзов.

2 Основные подходы к построению решения

Программный комплекс ситуационного анализа COSOC предназначен для использования в составе систем информационно-аналитической поддержки процессов управления состоянием объектов/территорий, выполняемых в повседневном режиме или в условиях чрезвычайных/кризисных ситуаций, в том числе:

1) анализ и оценка ситуаций на основе информации о событиях и угрозах, поступающей из различных источников;

2) поддержка принятия решений на основе распознавания типовых ситуаций.

Основной вариант использования COSOC – модуль обработки сообщений в стандартизованном формате Common Alerting Protocol в составе операционных (ситуационных) центров различного уровня, работающий автономно или в интеграции с аналогичными решениями (например, АПК "Безопасный город").

Правила и алгоритмы обработки входящих сообщений, формулы расчета метрик и ключевых показателей, методы распознавания типовых ситуаций, прогнозные модели разрабатываются в составе моделей для каждой предметной области (вида деятельности) и описываются в COSOC наборами xml-файлов.

COSOC строится на основе сервис-ориентированной архитектуры. В случае необходимости тесной интеграции с другими АИС или источниками данных, для которых формат CAP использовать нецелесообразно, COSOC может поставляться в коплекте с Интеграционной Платформой (не входит в базовую поставку).

Информация о событиях и угрозах поступает от внешних источников (субъектов или объектов) в формате Common Alerting Protocol (CAP, Протокол Общего Оповещения). CAP – это xml-формат, поддерживаемый Организацией по развитию стандартов структурированной информации (ОРССИ), а также определенный в Рекомендации МСЭ-Т X.1303.

Детальное описание формата CAP сообщения приведено в Приложении №1 к Руководству администратора COSOC "Методические ре-

комендации по использованию Common Alerting Protocol для передачи информации о событиях и угрозах в программном комплексе ситуационного анализа COSOC".

В качестве источников информации могут выступать:

— мобильные устройства, позволяющие гражданам сообщать о событиях и угрозах (при условии установки на них специальных приложений, преобразующих сообщения в формат CAP);

— стационарные устройства типа «тревожная кнопка»;

— обслуживаемые и необслуживаемые системы сенсоров (транспортных, метеорологических, экологических и т.п.);

— системы интеллектуального видеонаблюдения;

— дежурные диспетчерские службы;

— внешние системы, передающие информацию по каналам межведомственного взаимодействия (включая международные);

— средства массовой информации, телеграфные агентства;

— публичные сервисы.

Информация из CAP-сообщений извлекается в соответствии с регламентами обмена, при необходимости группируется, после чего проводится ее обработка по алгоритмам и методикам, специально разрабатываемым для различных видов дейтельности на трех иерархических уровнях, в соответствии с компонентной бизнес-моделью (Component Business Model):

1) уровня непосредственного реагирования на событие;
2) уровня принятия тактических решений по ситуациям;
3) уровня принятия стратегических решений.

Поступающая информация обрабатывается по процедурам и алгоритмам, характерным для каждого уровня принятия решений.

Разработка синтаксиса и семантики соответствующих полей CAP-сообщений (языка взаимодействия) выполняется на подготовительном этапе и основывается на онтологическом анализе процедур информационного взаимодействия между объектами инфраструктуры и COSOC.

На первом уровне проводится анализ событий, фактов, угроз из поступающих CAP-сообщений и, в случае необходимости, предлагаются определённые сценарии реагирования оперативного характера.

На втором уровне проводится анализ сложившейся/складывающейся ситуации на основе вычисления ключевых показателей (KPI) по поступающим CAP-сообщениям за определённый промежуток времени и, в случае выявления необходимости, принимаются соответствующие тактические решения.

На третьем уровне проводится анализ совокупности взаимосвязанных ситуаций на основе вычисления агрегированных показателей, в том числе аналитическими методами, строятся прогнозы и предлагаются стратегические решения.

Кроме расчета ключевых показателей, в COSOC заложена возможность распознавания типовых ситуаций, что обеспечивает поддержку принятия решений по управлению кризисными ситуациями. В случае выявления типовой тактической ситуации COSOC может выдавать команду в смежные системы на выполнение предусмотренных регламентами Планов реагирования.

ПРИМЕЧАНИЕ: Модули (программы) расчёта ключевых показателей и выявления тактических ситуаций не входят в базовый комплект поставки и разрабатываются по техническому заданию для конкретного объекта управления в соответствии с моделью деятельности.

В качестве источников получения информации также могут использоваться видеокамеры: в формате CAP имеется возможность передавать как моментальные снимки с видеокамер, находящихся в зоне события, так и подключаться к видеокамерам для воспроизведения видеопотока в пользовательском интерфейсе.

Программное обеспечение пользовательского интерфейса не входит в базовую поставку ПК COSOC. Пользовательский интерфейс поставляется отдельно или разрабатывается под конкретные нужды заказчика. Пользовательский интерфейс может быть реализован на основе портальных технологий, что позволяет интегрировать на рабочем месте

пользователя системы как данные о событиях, так и широкий набор аналитических программ или специально разработанных приложений.

В COSOC заложена функция формирования выборки записей ранее поступивших CAP-сообщений с целью их повторного "воспроизведения" (путем подачи на вход COSOC) с откорректированными, при необходимости, параметрами, а также временным сдвигом. Такой режим позволяет:

— во-первых, проводить детальный анализ происшествий в отложенном режиме;

— во-вторых, проводить учения личного состава ситуационного центра на базе реальных событий.

Для обеспечения расчетов метрик и ключевых показателей, алгоритмов и методик работы, вместе с COSOC дополнительно могут поставляться инструменты формирования следующих видов информационного обеспечения:

1. Справочника CAP-сообщений, включающего описание типов и кодов сообщений, перечень внешних источников, привязанных к данным типам сообщений.

2. Справочника внешних источников сообщений, включающего описание типов источников, а также параметров протоколов обмена с ними, включая методы построения запросов к ним и характеристики формируемых запросов.

3. Классификатора KPI, описывающего, по сути, модель предметной области, и включающего, в том числе, алгоритмы расчета KPI и пороговые значения.

4. Кодификатора типовых тактических ситуаций, содержащего:

— перечень типовых тактических ситуаций,

— перечень значений KPI, одиночных и групповых CAP-сообщений, по которым может распознаваться ситуация,

— перечень запросов дополнительной информации из внешних источников (или вводимых вручную), а также формализованные критерии оценки всей совокупности параметров.

2.1 Функции программного комплекса

Программный комплекс COSOC обеспечивает выполнение следующих функций:

— прием и фиксация сообщений от субъектов (различные ДДС, коммунальные службы, граждане и т.д.) и объектов (SCADA-систем, видеокамер, и т.п.) в централизованном или децентрализованном хранилище;

— создание списков записей сообщений о событиях для последующего их воспроизведения с целью детального разбора ситуаций или проведения учений;

— ведение учета угроз, происшествий, инцидентов, событий;

— выборка ранее записанных сообщений через API;

— обработка сообщений по заранее настроенным алгоритмам и правилам (не входит в базовую поставку);

— расчет и отображение ключевых показателей, описывающих текущую ситуацию по направлениям деятельности объекта мониторинга (не входит в базовую поставку);

— распознавание и оценка сложившейся ситуации на основании полученных сообщений (не входит в базовую поставку).

Форматы информационных полей входящих сообщений, правила и алгоритмы обработки сообщений, формулы расчета ключевых показателей, методы распознавания типовых ситуаций, прогнозные модели-разрабатываются в составе моделей каждой предметной области (вида деятельности), описываемых в COSOC наборами xml-файлов.

3 Методологические основы решения

3.1 Модель деятельности

Под моделью деятельности следует понимать совокупность информации, правил и алгоритмов, описывающих автономный функционал, относящийся к некоторому типу и подтипу деятельности. Модель – основной элемент в декомпозиции деятельности, соответствующий виду деятельности, и содержащий:

— описание типов сообщений - полный перечень типов сообщений о событиях и угрозах и параметры для каждого типа события;

— описание сил и средств - типы сил и средств, участвующих в плановых работах по ликвидации ЧС в рамках данной модели, планы реагирования на события, угрозы и типовые ситуации в рамках данной модели;

— описание показателей, задающих интегральную оценку данного вида деятельности - множество ключевых показателей и метрик, включая правила их расчета.

На рисуноке 3.1 приведен пример модели «Состояние дорожного покрытия».

Примеры типов сообщений для этой модели:

1) «Яма на проезжей части»
2) «Повышенная колейность на проезжей части»

В рамках модели также могут перечисляются и описываются свойства объектов критической инфраструктуры. При необходимости в рамках модели также описываются планы информирования и оповещения муниципальных органов и населения при ЧС.

Для создания моделей разработан специальный *редактор моделей* COSOC-Editor - простой и интуитивно понятный инструмент для аналитиков - разработчиков моделей. Редактор моделей поставляется отдельно. На рисунке 3.2 изображен общий интерфейс редактора моделей деятельности.

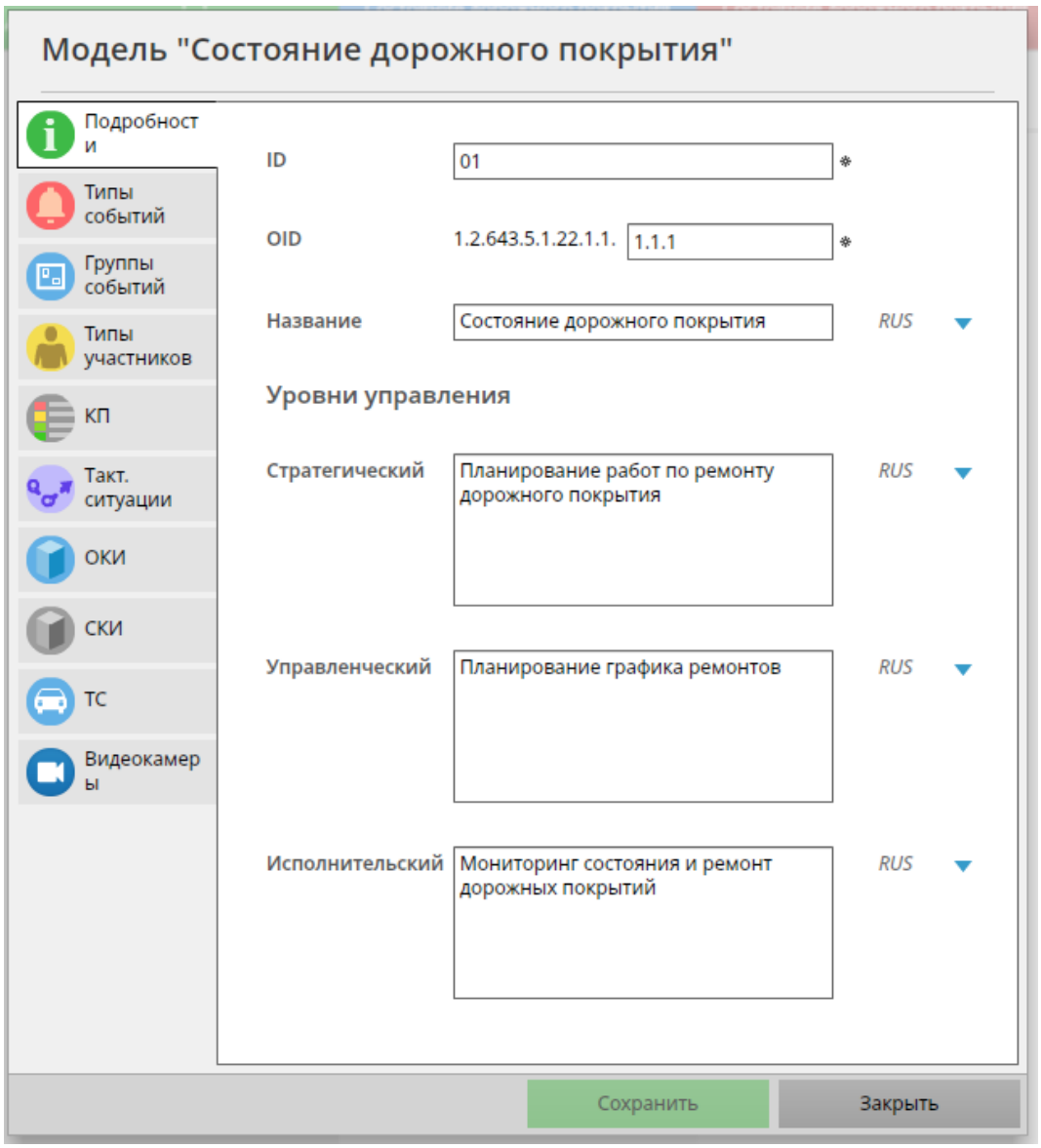

Рисунок 3.1 — Редактирование модели

При создании на основе COSOC систем, предназначенных только для мониторинга, планы реагирования на события, угрозы и типовые ситуации, типы сил и средств, участвующих в плановых работах и ликвидации ЧС в рамках модели могут не задаваться.

3.2 Компонентная модель

Для того, чтобы решать задачи по наиболее эффективной обработке событий, относящихся к различным сферам деятельности, в COSOC предусмотрена возможность осуществить декомпозицию всех наблюдаемых видов деятельности по тематическому признаку. Так, например:

— **Тип деятельности:** Безопасные и Качественные Дороги
— **Подтип деятельности:** Состояние дорожного покрытия
— **Вид деятельности:** Уборка и эксплуатация дорог

Трехуровневая структура иерархии типов и видов деятельности, наложенная на многоуровневую модель управления (стратегическое, оперативное, тактическое) образует т.н. **компонентную модель**, широко используемую для декомпозиции и описания бизнес-процессов а сложных организационных структурах.

Компонентная модель состоит из типов, подтипов деятельности, видов деятельности (моделей) и уровней управления. Каждому подтипу и уровню соответствует множество моделей. Множество моделей, относящихся к одному виду деятельности, но к различным уровням управления, в совокупности образуют вид деятельности.

Пример компонентной модели приведен на рисунке 3.3

3.3 Распознавание тактических ситуаций

Тактическая ситуация – событие, для которого система на основе анализа предлагает конкретный план действий. Возможность распознавания тактических ситуаций заложена в COSOC, однако реализуется только в случае создания соответствующей модели, Задача распознавания тактических ситуаций в предлагаемом решении может решаться различными способами.

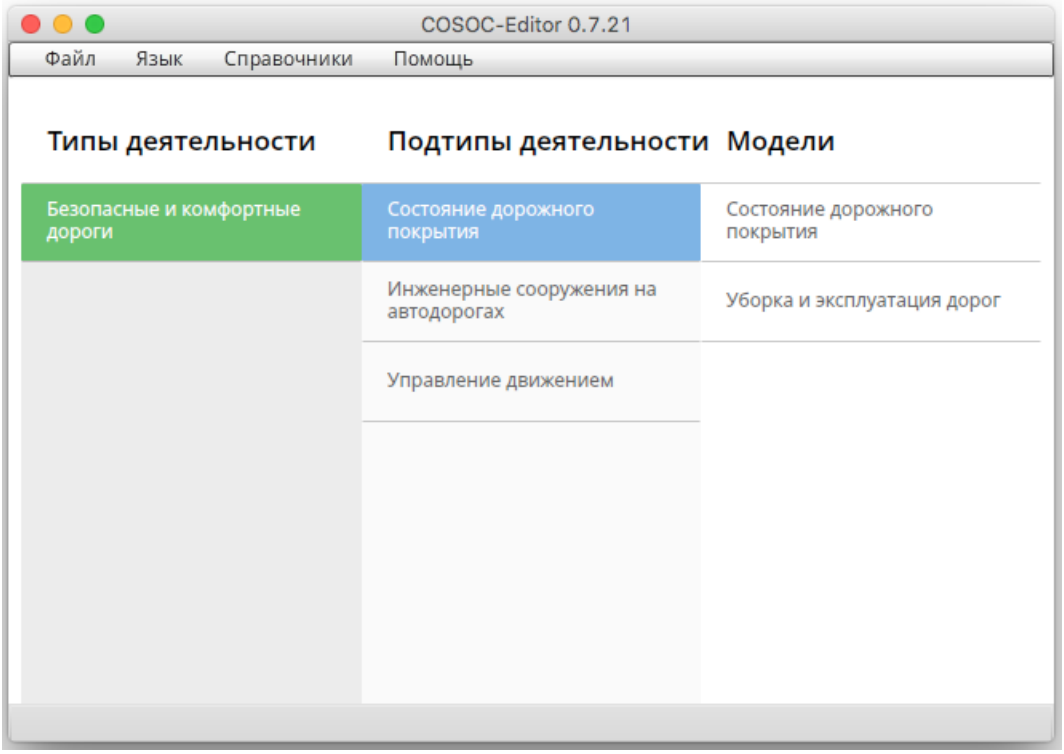

Рисунок 3.2 — Пример графического представления типа деятельности в редакторе моделей

	Лесное хозяйство	Транспорт	Медицина
Стратегия	Лесные пожары Свалки мусора	Дорожная сеть Ремонт инфраструктуры	Готовность эпидемслужбы Количество койко - мест
Планирование	Лесные пожары Свалки мусора	Светофоры Дорожное покрытие	Планирование экипажей скорой Планирование нагрузки на ЛПУ
Реагирование	Лесные пожары Свалки мусора	ДТП Светофоры	Эпидем. ситуация Медицина катастроф

Рисунок 3.3 — Пример компонентной модели

В простейшем случае тактическую ситуацию может порождать обособленное событие. При этом условием является некоторая заданная комбинация параметров CAP-сообщения. Этот вид распознавания реализуется штатной функциональностью COSOC, необходимо только задать соответствующие параметры описания событий в модели деятельности.

В более сложных случаях для распознавания ситуаций могут использоваться математические методы, такие например, как Байесовская сеть оценки гипотез, машинное обучение, формальные методы (например, ALLOY, или аналогичные формальные языки описания совокупности признаков, задающих тактическую ситуацию). Этот вид распонавания не входит в стандартную поставку COSOC.

4 Анализ и аналитика

Анализ поступающих и накопленных данных в системе делится на 2 вида:

— ”on-line” анализ информации в поступающих сообщениях в процессе их приёма и обработки системой (практически в реальном масштабе времени); такой анализ, как правило, затрагивает некоторое ограниченное количество недавно полученных сообщений (например, за текущие сутки), и используется, в основном, для расчёта текущих значений метрик и KPI и выявления признаков тактических ситуаций;

— последующий анализ (пост-анализ) информации, содержащейся в записанных в базу данных сообщениях, который может проводиться в любой момент, не обязательно привязынный к текущим событиям, и который, как правило, затрагивает большое количество сообщений за определённый промежуток времени (например, неделю или месяц).

Основным инструментом анализа в системе является on-line анализ, т.е. формирование и поддержание в актуальном состоянии базы данных ключевых показателей и метрик, сгруппированных по моделям, подтипам и типам деятельности. На рисунке 4.1 приведен пример изображения окна матрицы ключевых показателей верхнего уровня.

ОТОБРАЖЕНИЕ	РАСШИФРОВКА
1	2
Нормальное состояние	Все метрики и показатели находятся в допустимых пределах (Повседневный режим)
Внимание	Некоторые метрики и показатели имеют значения, требующие реагирования (Режим угрозы)
Чрезвычайная ситуация	Ситуация не является нормальной и требует немедленного реагирования (Режим ЧС)
Проведение учений	Ситуация требует немедленного анализа и возможно создания оперативного штаба (Режим учений)

Рисунок 4.1 — Окно отображения матрицы показателей верхнего уровня

4.1 Анализ структурированных данных

Основной штатной системой анализа COSOC является on-line аналитика поступающих формализованных сообщений, осуществляемая модулями вычисления метрик и показателей на основе формализованных типовых моделей. Результаты вычисления могут быть представлены в виде раскрашенной компонентной модели. Типовым цветовым набором, используемым для описания состояния видов деятельности являются четыре цвета, приведенных в таблице.

Нормальное состояние. Все метрики и показатели находятся в допустимых пределах (Повседневный режим)

Внимание. Некоторые метрики и показатели имеют значения, требующие реагирования (Режим угрозы)

Чрезвычайная ситуация. Ситуация не является нормальной и требует немедленного реагирования (Режим ЧС)

Проведение учений. Ситуация требует немедленного анализа и возможно создания оперативного штаба (Режим учений)

4.2 Анализ многомерных данных и статистический анализ

Средства анализа многомерных данных относятся ко второму виду аналитики (**пост-анализу**, см. п. 3.4) и не входят в комплект поставки COSOC. При необходимости по требованию заказчика такие средства подключаются через API, и для этой цели могут быть использованы различные, как свободно распространяемые, так и коммерческе продукты, наиболее адекватные решаемым задачам. В случае необходимости, для ускорения доступа к данным и удобства обработки может потребоваться добавление в систему специальных хранилищ данных, формируемых для использования аналитическими приложениями из массива оперативных данных.

Частным случаем является анализ данных в геопространственной привязке, который может выполняться средствами, встроенными ГИС-

систему, наличие которой в составе ПО ситуационных центров является обязательным.

В качестве средства анализа может быть выбран язык R, который достаточно прост, позволяет работать с большими объемами данных и не требует лицензионных отчислений.