Информзащита
Системный интегратор

Оценка эффективности SOC

Андрей Тамойкин
Начальник отдела систем мониторинга

Security Operation Center (SOC)

Выявление и реагирование на угрозы и атаки ИБ

SIEM/SOC

25
заказчиков на контроле

24x7x365

5 мин
регистрация инцидентов ИБ в собственном SD

360
инцидентов ИБ ежемесячно

15 минут
время реакции

99,5%
выполнение SLA

5000
ежедневных транзакций

7
различных вендоров SIEM

15+
реализованных проектов внедрения SIEM

SOC +

Комплексный подход, направленный на улучшение состояния информационной безопасности

Эффективность SOC

- Эффективно ли SOC противостоит возникающим угрозам
- Достаточно ли используемых ресурсов
- Эффективно ли используются эти ресурсы
- На какие аспекты SOC следует обратить внимание
- Есть ли динамика в достижении целей

Существующие методики оценки эффективности SOC

Hewlett Packard Enterprise

CISCO

RSA SECURITY™

IBM

Security Operation Maturity Model (SOMM) HPE

Сфокусирована на 4 категориях, которые разбиты на подкатегории

Business	People	Process	Technology
Mission	General	General	Architecture
Accountability	Training	Operational Process	Data Collection
Sponsorship	Certifications	Analytical Process	Monitoring
Relationship	Experience	Business Process	Correlation
Deliverables	Skill Assessments	Technology Process	General
Vendor Engagement	Career Path		
Facilities	Leadership		

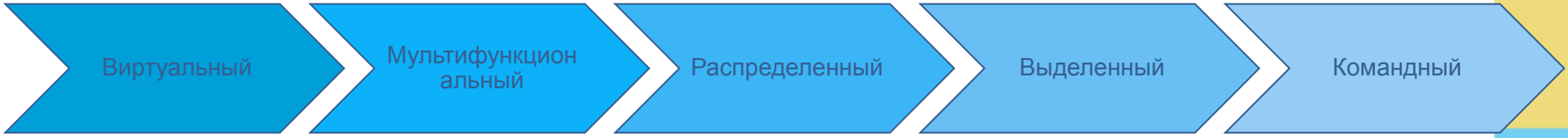
Результатом является оценка SOC по модели зрелости (0-5) – AVG всех категорий

- Категории оцениваются независимо друг от друга
- Технологии привязаны к решению класса SIEM
- Не учитывает локальную специфику: 382-П, СТО БР, ГосСОПКА и т.д.

Наш подход к оценке эффективности SOC

Security Operation Center (SOC) – **совокупность** технологий, процессов и людей

5 моделей SOC (GARTNER)



Основные функции любого SOC

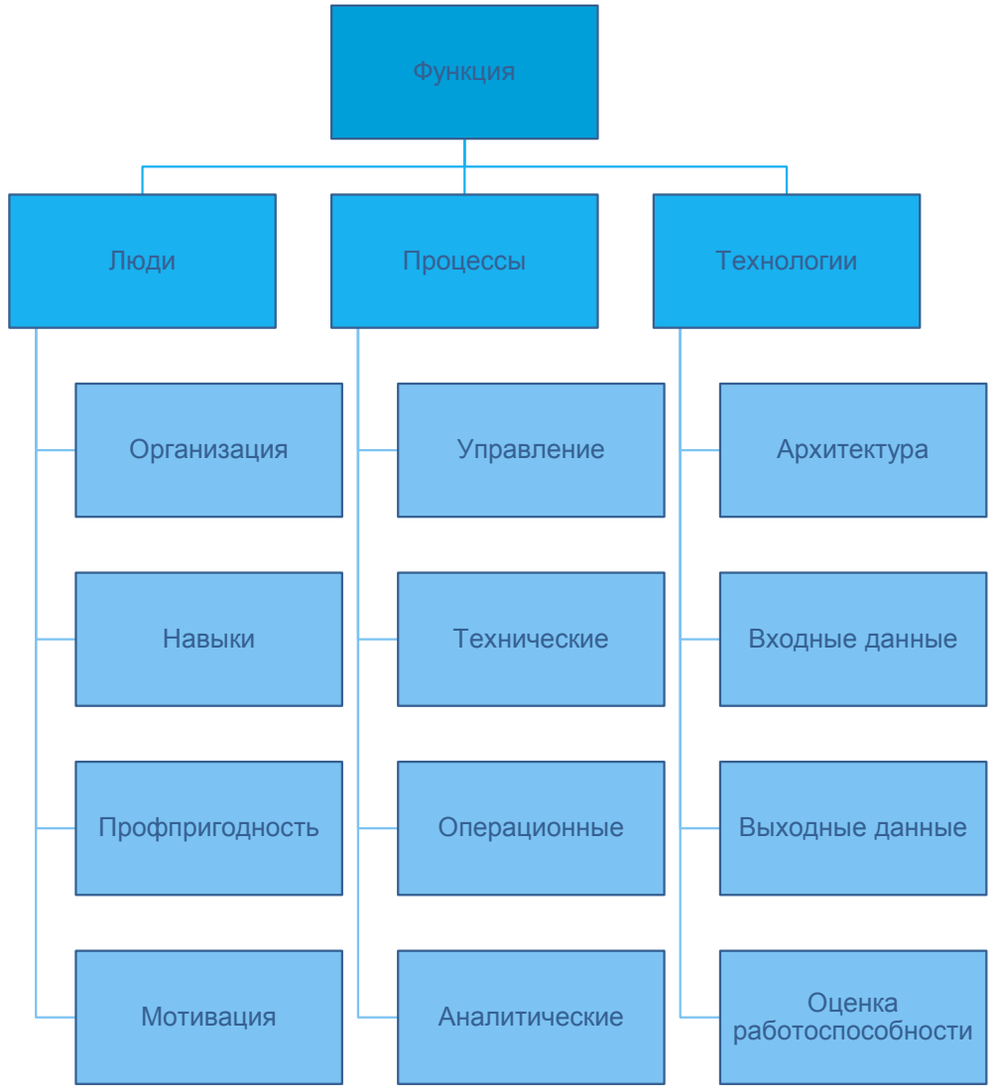
- Мониторинг безопасности
- Управление угрозами и уязвимостями
- Реагирование на инциденты ИБ
- Контроль соответствия стандартам
- Управление СЗИ и техническое обслуживание
- Обучение мерам безопасности

Эффективность SOC – формирование результирующей оценки, составленной по **каждой** из функций SOC с учетом технологий, процессов и людей

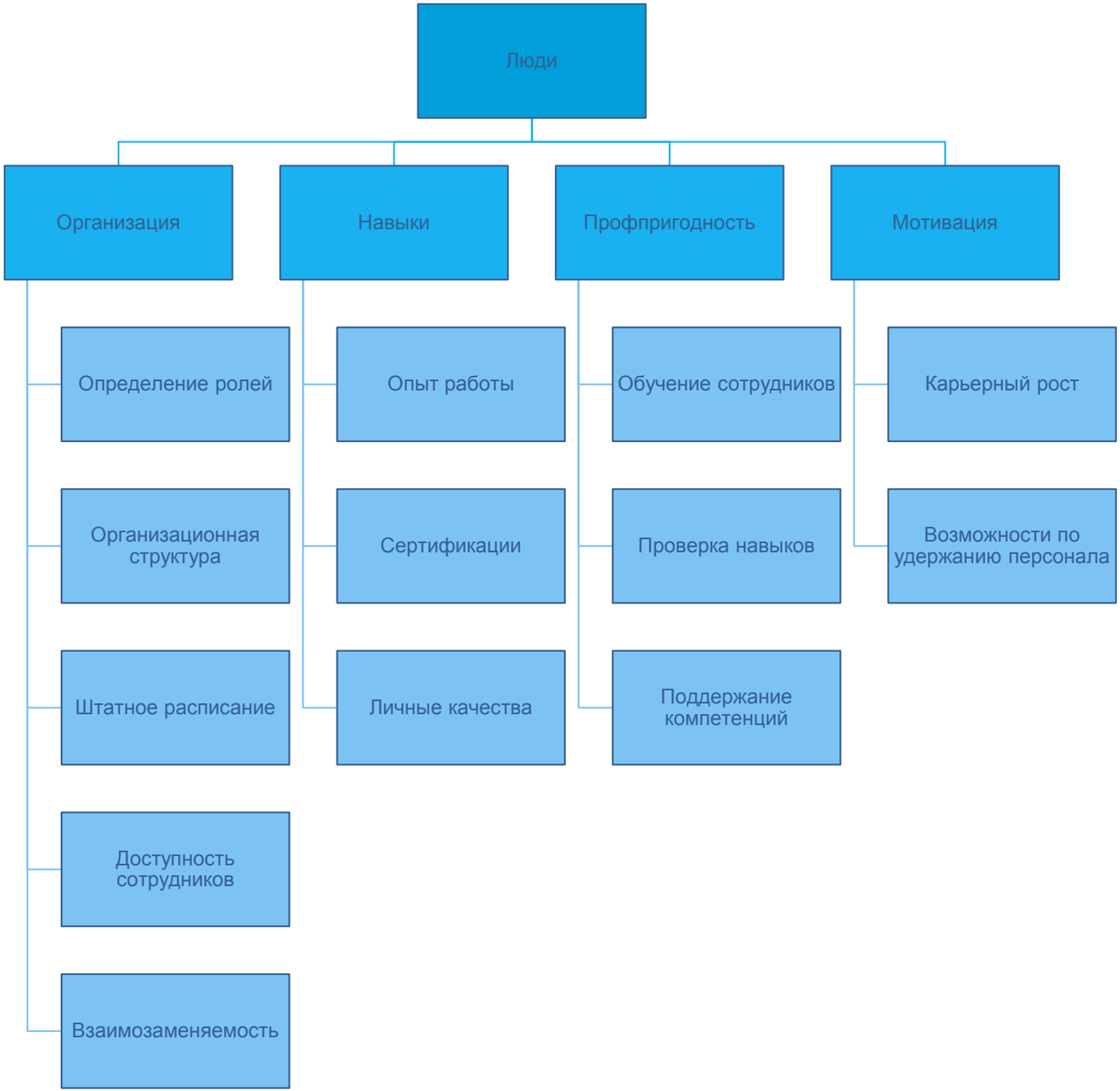
Адаптированная методология SOMM

Каждая функция оценивается по трем составляющим

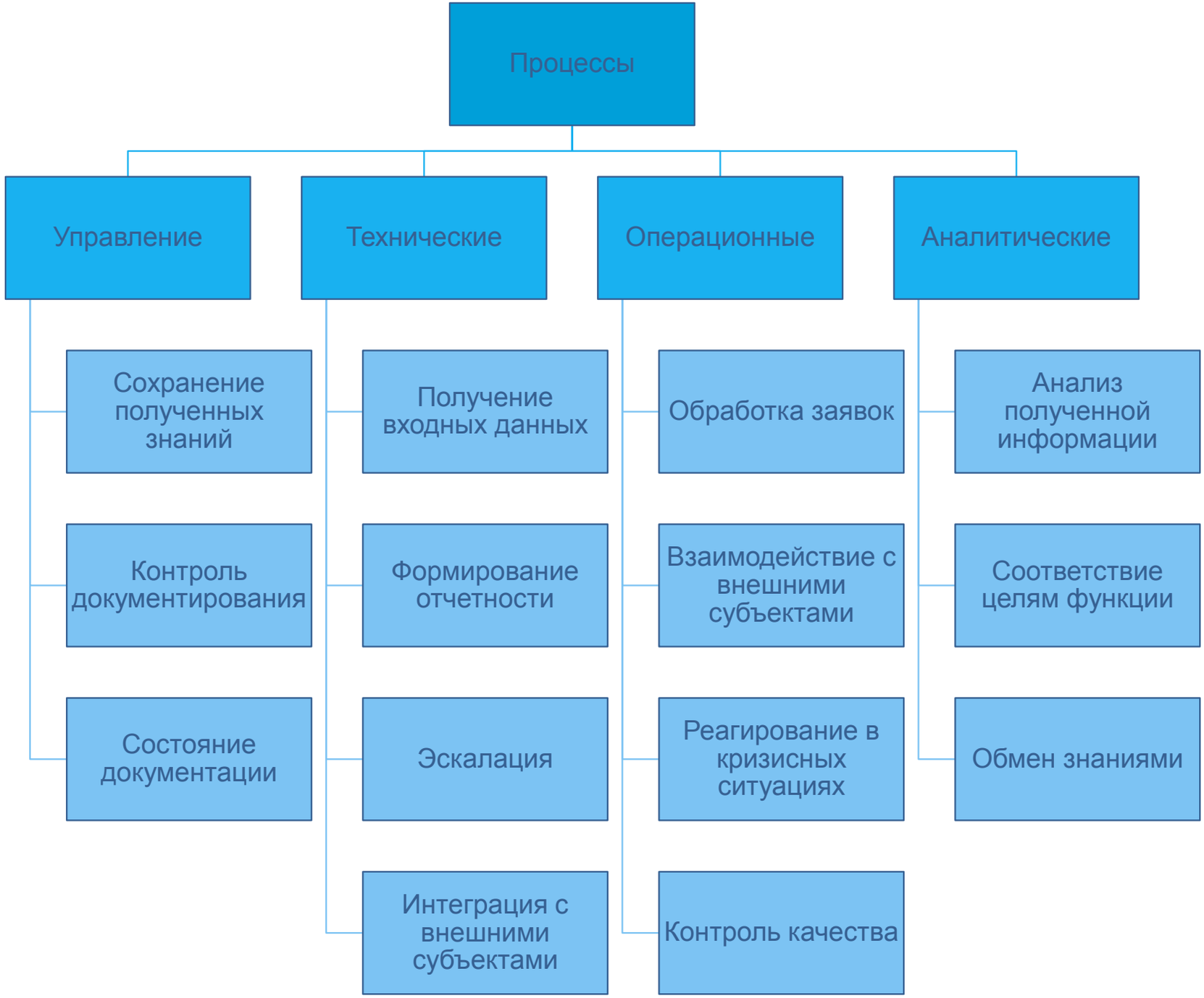
Каждая составляющая оценивается по собственным критериям



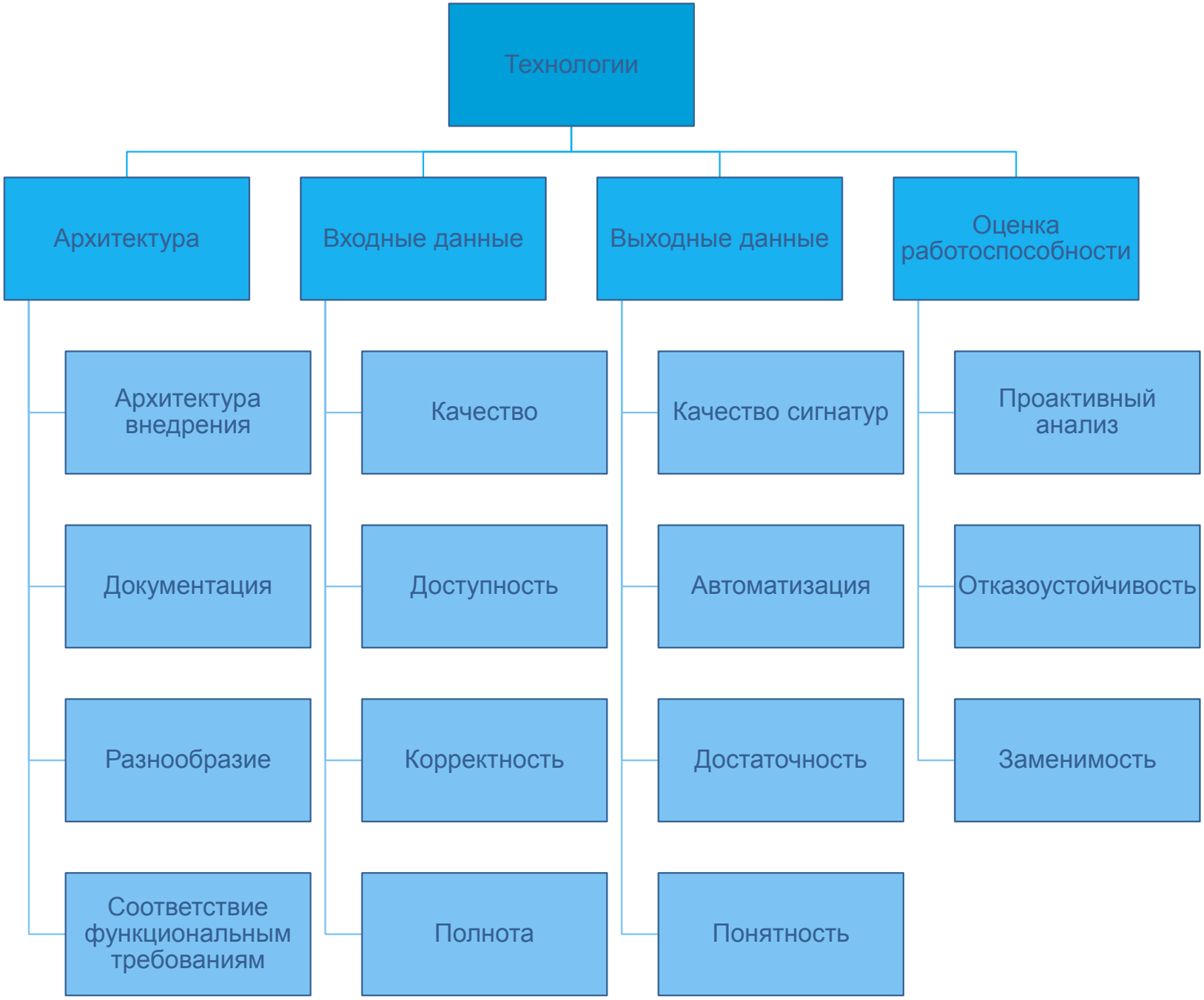
Адаптированная методология SOMM. Люди



Адаптированная методология SOMM. Процессы



Адаптированная методология SOMM. Технологии



Использование методики оценки эффективности

Отчет по результатам измерения

Отчёт

Измерение эффективности

- Содержит сводные данные по общей эффективности SOC и каждому компоненту
- Подробное описание каждой составляющей измерения и компоненты по выполненным проверкам и «сухим» результатам

Входные данные

- Отчет об измерениях
- Цели SOC
- Критичная инфраструктура

Действия

- Анализ отчета в контексте целей SOC
- Выделение потенциальных последствий
- Определение проблем, нуждающихся во внимании

Результат

- Отчет со списком проблем и потенциальных последствий
- Рекомендации по устранению проблем

Результаты:

- Отчет по измерению эффективности, содержащий «сухие» данные по текущему состоянию SOC
- Аналитический отчет с подробным описанием SOC и всех его функций, содержащий анализ измеренных показателей выявленные проблемы и потенциальные последствия
- Рекомендации по дальнейшему повышению эффективности SOC

Что дальше?

Дополнительные услуги, по результатам оценки эффективности:

- Подготовка подробного плана по развитию и повышению эффективности SOC
- Реализация (готовый проект) этапов плана развития и повышения функциональности SOC
- Периодическая оценка эффективности SOC
- Запуск новых сервисов SOC
- Построение SOC, эффективность которого отвечает требованиям Заказчика, с нуля
- Выбор MSSP провайдера услуг SOC

Информзащита
Системный интегратор

Спасибо.
Вопросы?

+7 (495) 980 23 45
a.tamoykin@infosec.ru