Практическое занятие №7

2 часа

Тема: Сравнительный анализ стандартов в области аудита информационной безопасности.
Цель практического занятия: Получение практических навыков по анализу стандартов, выявлению достоинств и недостатков рассматриваемых стандартов.

Задание №1.

Провести сравнительный анализ стандартов в области аудита информационной безопасности.

Отчет по практическому занятию должен быть выполнен согласно утвержденным на кафедре требованиям и содержать:

1. Тема ПЗ.
2. Цель ПЗ.
3. Частную модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
4. Профиль защиты персональных данных в ИСПДн.
5. Инструкцию ответственного за обеспечение безопасности ПДн.
6. Выводы по заданию.
7. Заключение.
8. Список использованной литературы.

Методический материал к практическому занятию (Приложение 1).

Приложение 1.

Методический материал

2.2 Обзор методик проведения аудита ИБ

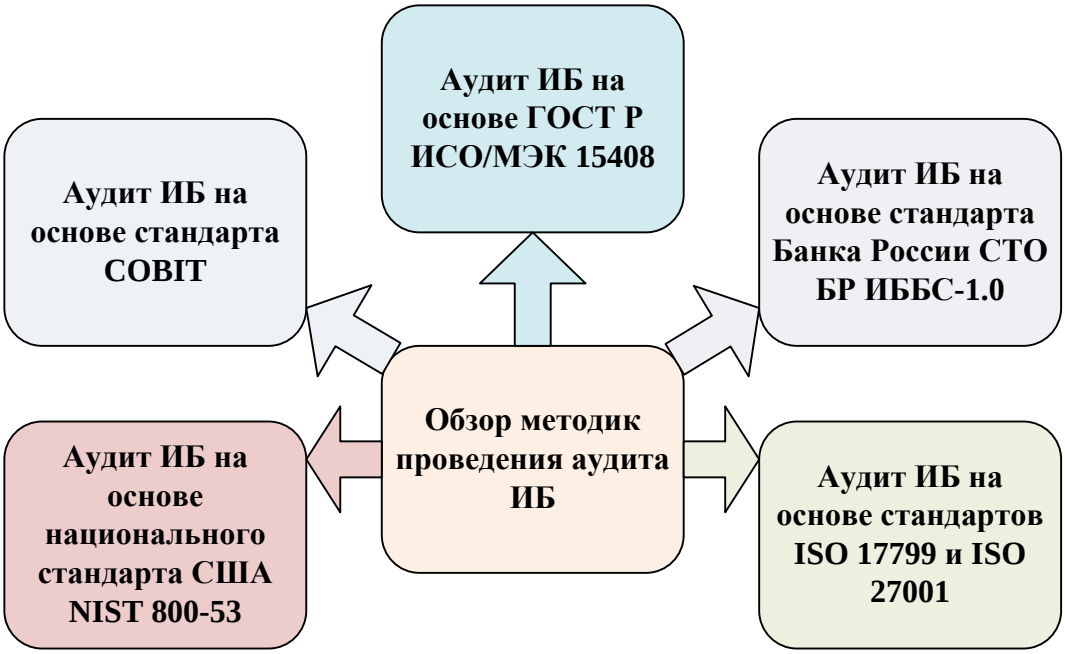

Рисунок 2.1 - Обзор методик проведения аудита ИБ

2.3 Методика проведения аудита на основе ГОСТ Р ИСО/МЭК 15408 и международных стандартов

2.3.1 Организация и терминология требований

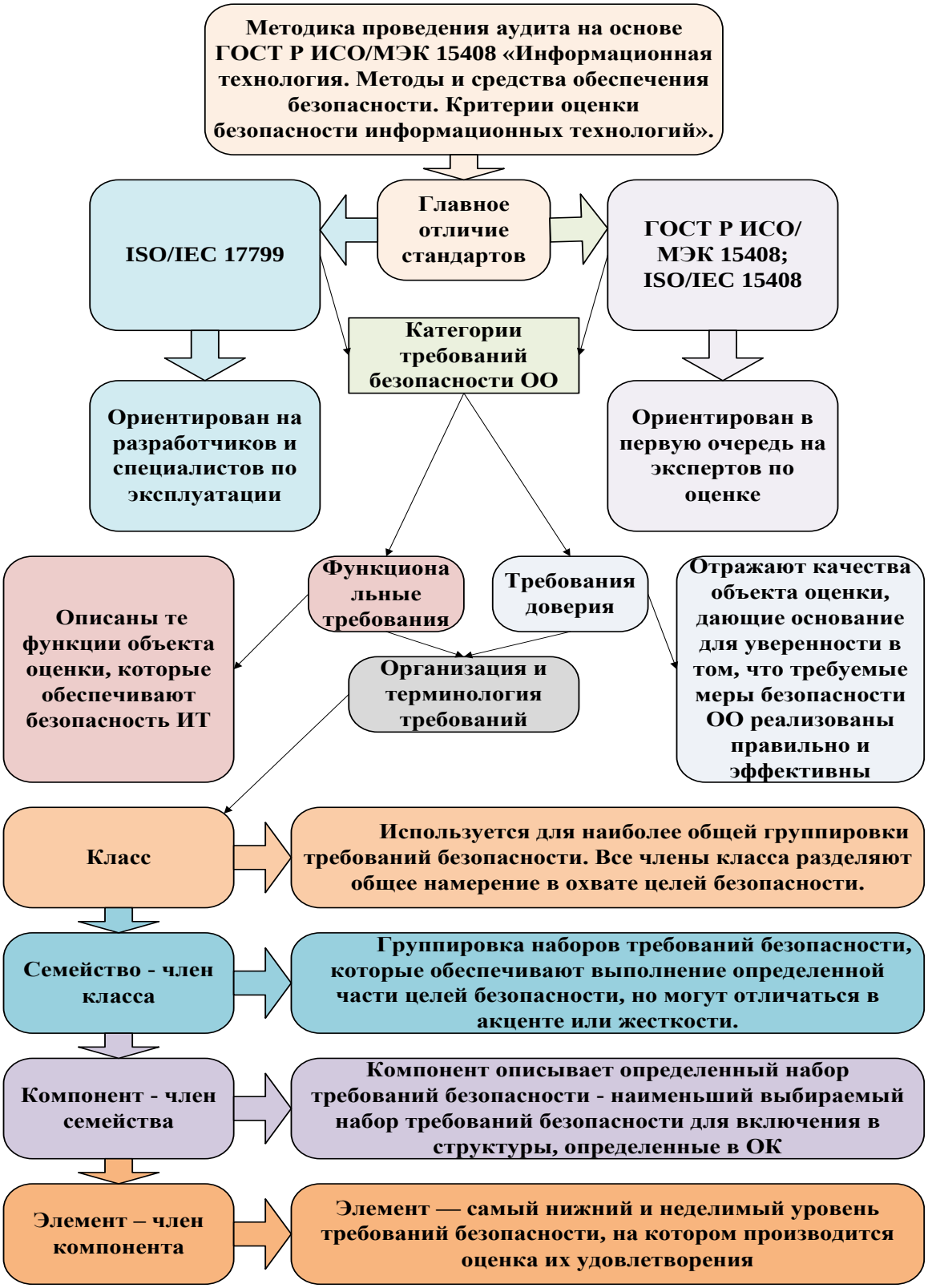

Рисунок 2.2 - Организация и терминология требований

2.3.2 Понятия, используемые при проведении аудита

Рисунок 2.3 – Понятия, используемые в методике при проведении аудита

2.3.3 Общая модель оценки на основе ГОСТ Р ИСО/МЭК 15408

В соответствии с ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», РД — Безопасность информационных технологий — Общая методология оценки безопасности информационных технологий, ФСТЭК России, 2005). оценка проводится не на соответствие универсальным требованиям руководящих документов ФСТЭК России или разработанным разработчиком техническим условиям, а на соответствие так называемым заданиям по безопасности, содержащим как исходные предпосылки (угрозы безопасности, предположения, политику безопасности организации), так и собственно требования безопасности, выполняемые объектом оценки, и его функциональные возможности. Задание по безопасности создается разработчиком продукта или системы ИТ, как правило, в соответствии с выбранным профилем защиты, содержащим необходимый объем требований для данного типа изделий ИТ

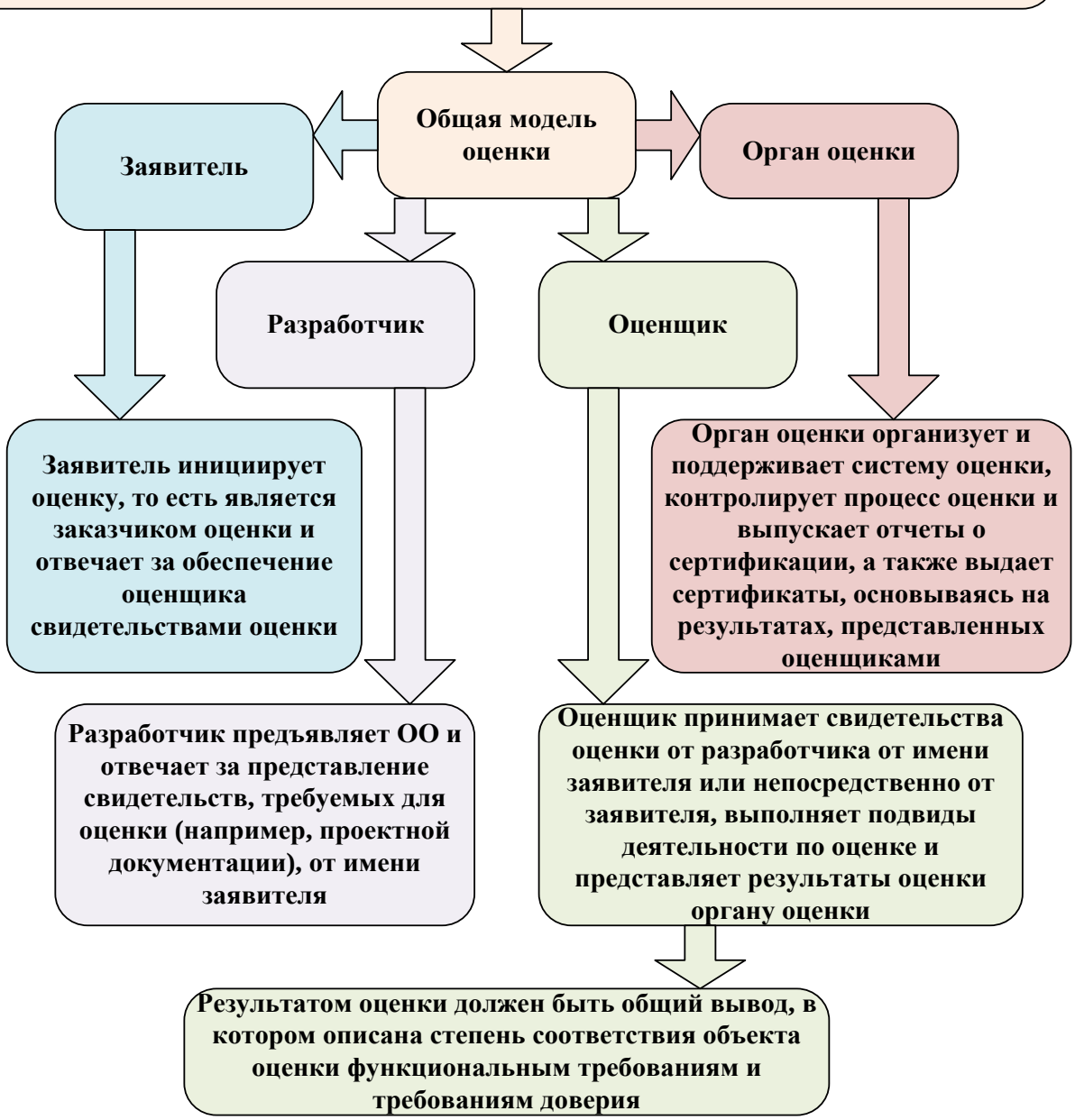

Рисунок 2.4 - Общая модель оценки на основе ГОСТ Р ИСО/МЭК 15408

2.3.4 Категории безопасности международных стандартов (стандарт ISO/IEC 17799 и стандарт ISO/IEC 27001)

Рисунок 2.5 - Категории безопасности международных стандартов (стандарт ISO/IEC 17799 и стандарт ISO/IEC 27001)

2.3.4.1 Порядок оценки соответствия требованиям стандартов ISO/IEC 17799 и ISO/IEC 27001

Рисунок 2.5 - Порядок оценки соответствия требованиям стандартов ISO/IEC 17799 и ISO/IEC 27001

2.3.5 Структура стандарта BSI/IT Baseline Protection Manual

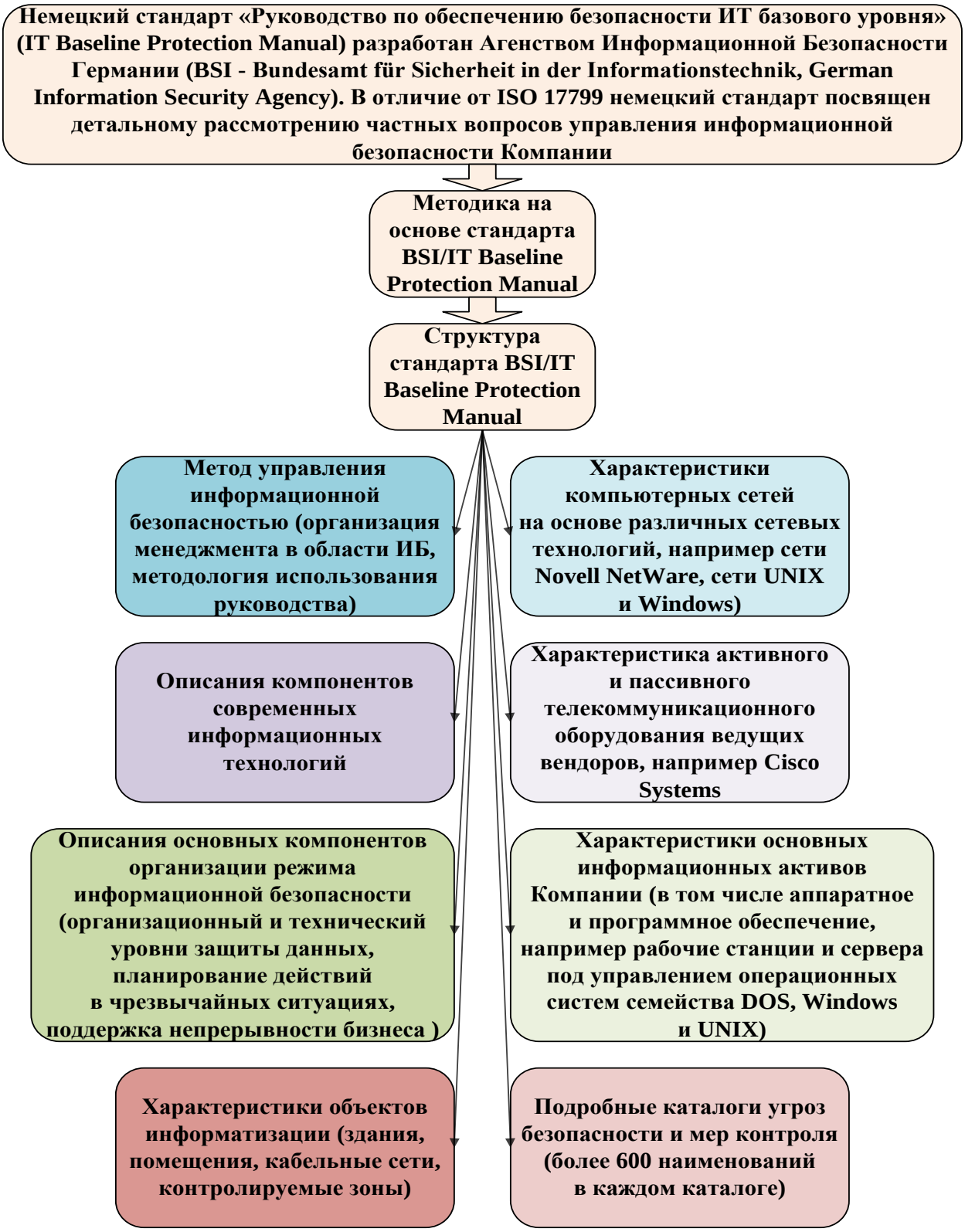

Рисунок 2.6 - Структура стандарта BSI/IT Baseline Protection Manual

2.3.5.1 Содержание стандарта BSI/IT Baseline Protection Manual и методика оценки

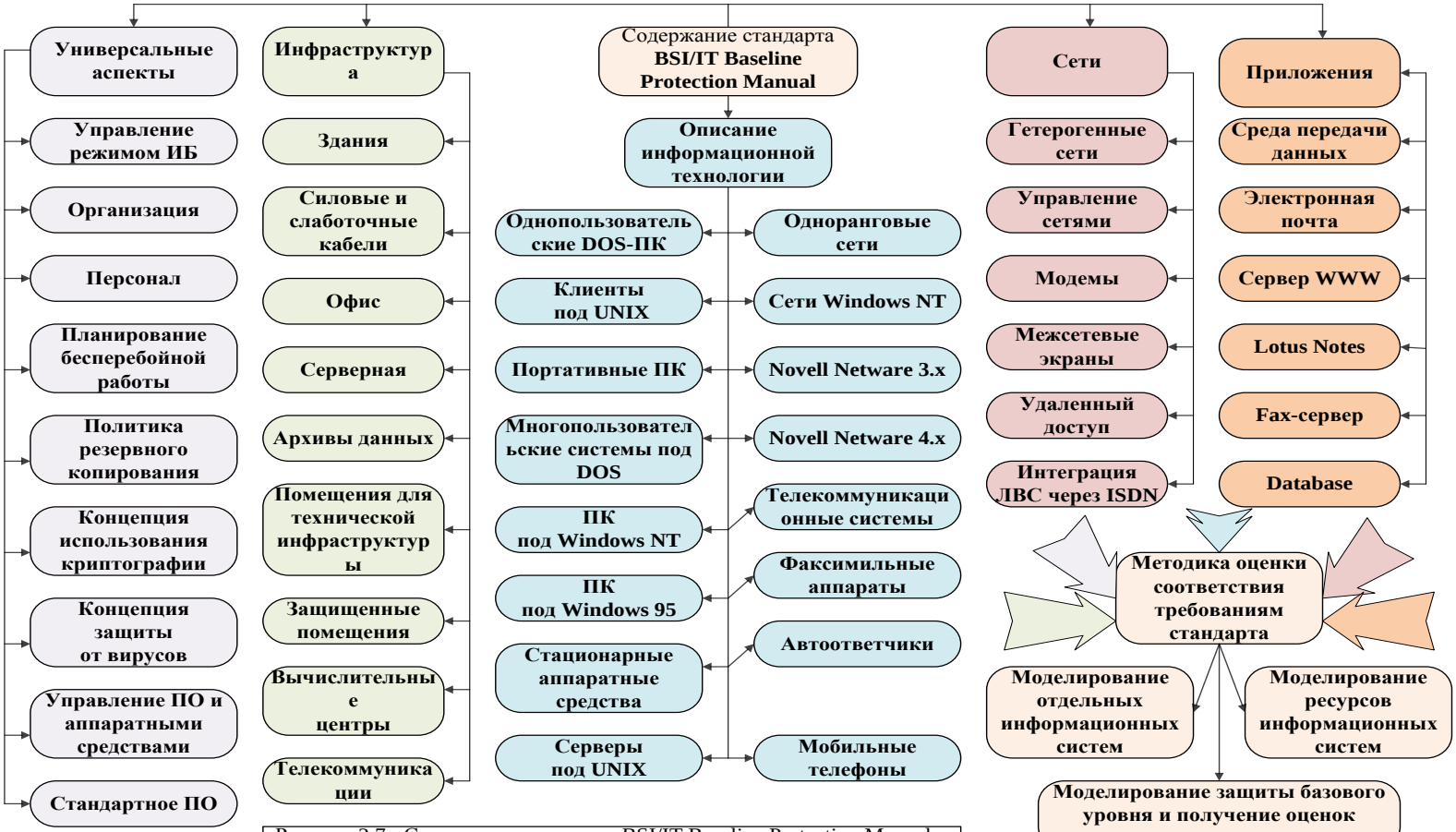

Рисунок 2.7 - Содержание стандарта BSI/IT Baseline Protection Manual и методика оценки

2.3.6 Показатели методики оценки соответствия информационной безопасности в организациях банковской сферы РФ

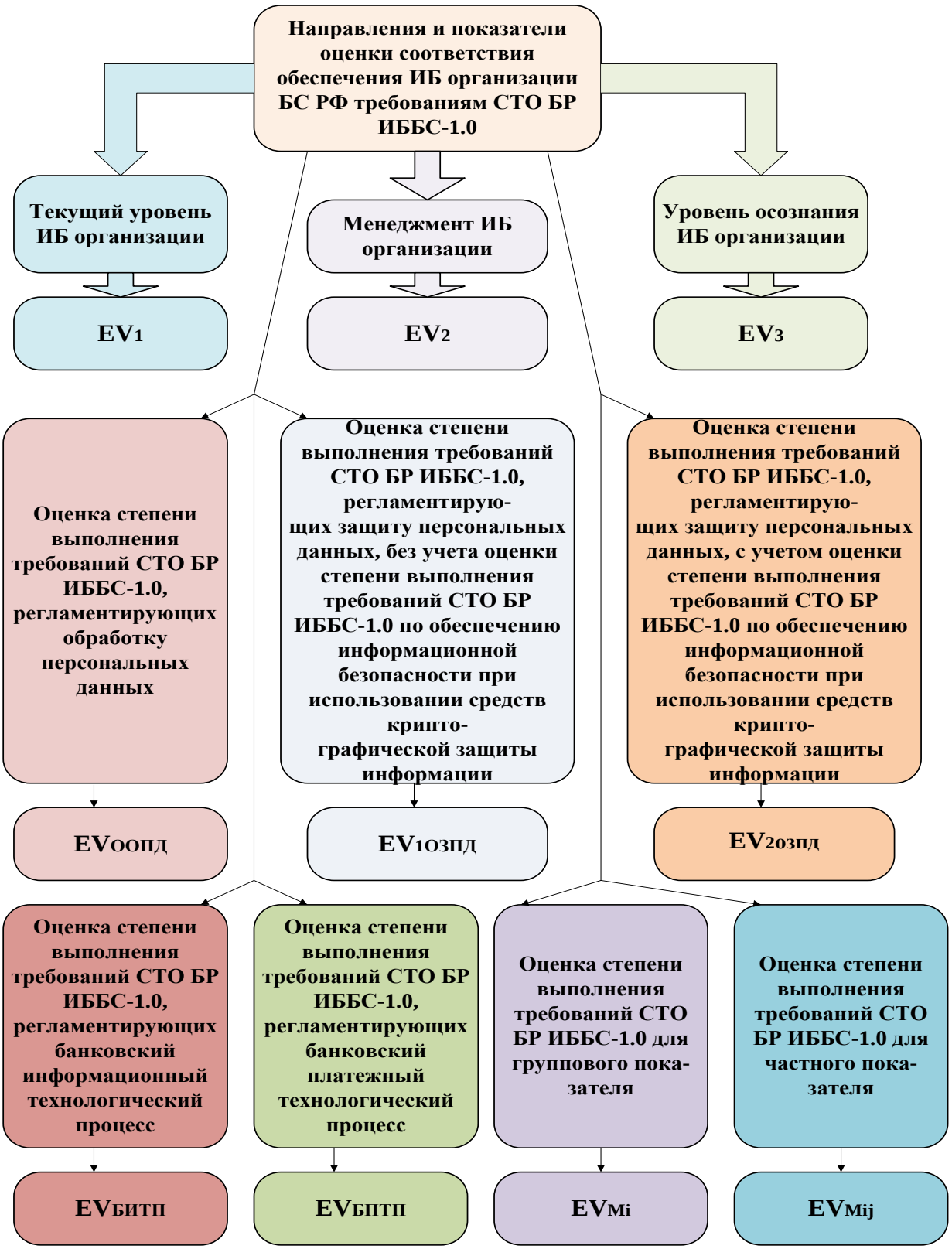

Рисунок 2.8 - Направления и показатели оценки соответствия обеспечения ИБ организации БС РФ требованиям СТО БР ИББС-1.0

2.3.6.1 Частные и групповые показатели ИБ

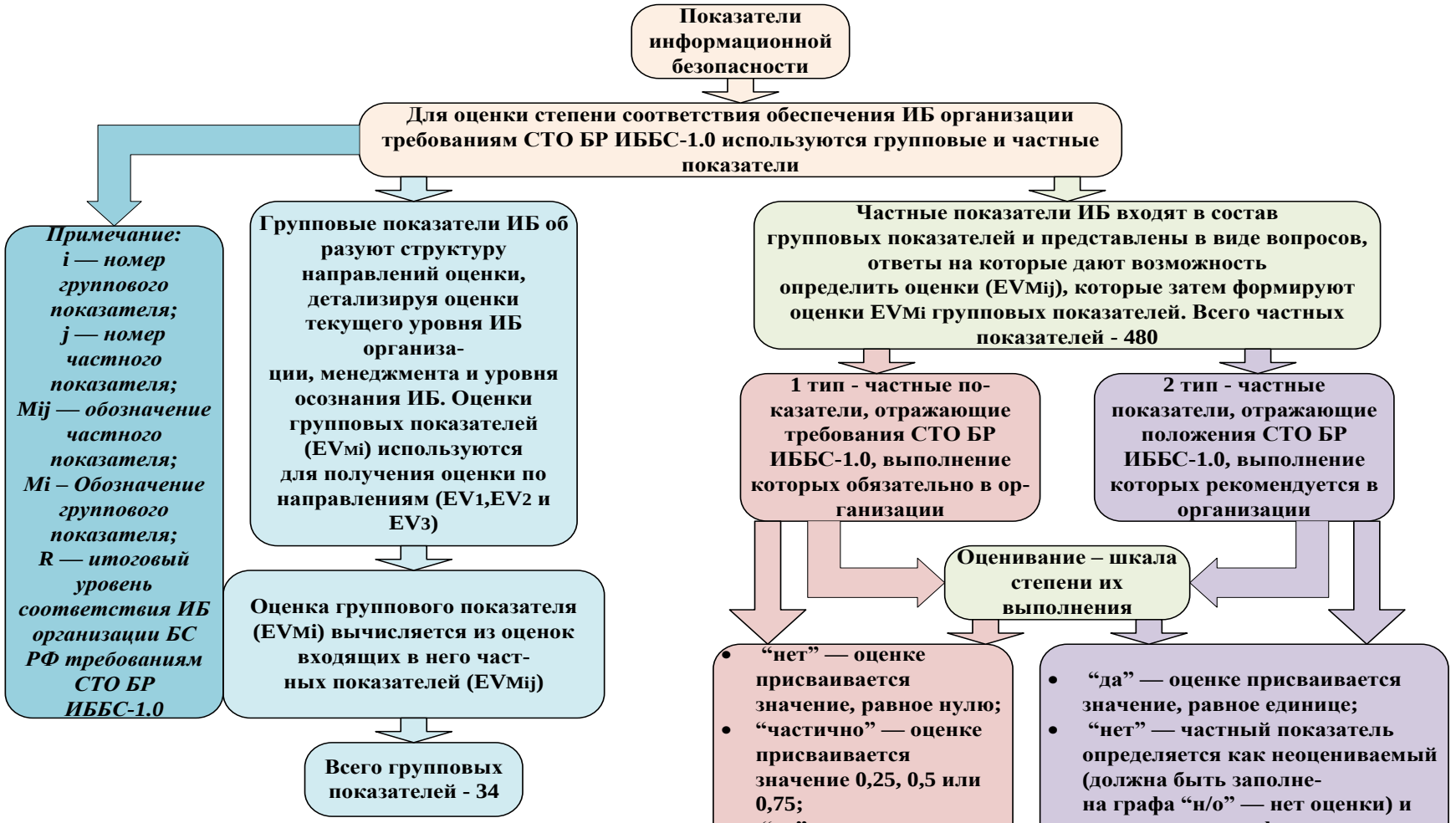

Рисунок 2.8а - Показатели информационной безопасности

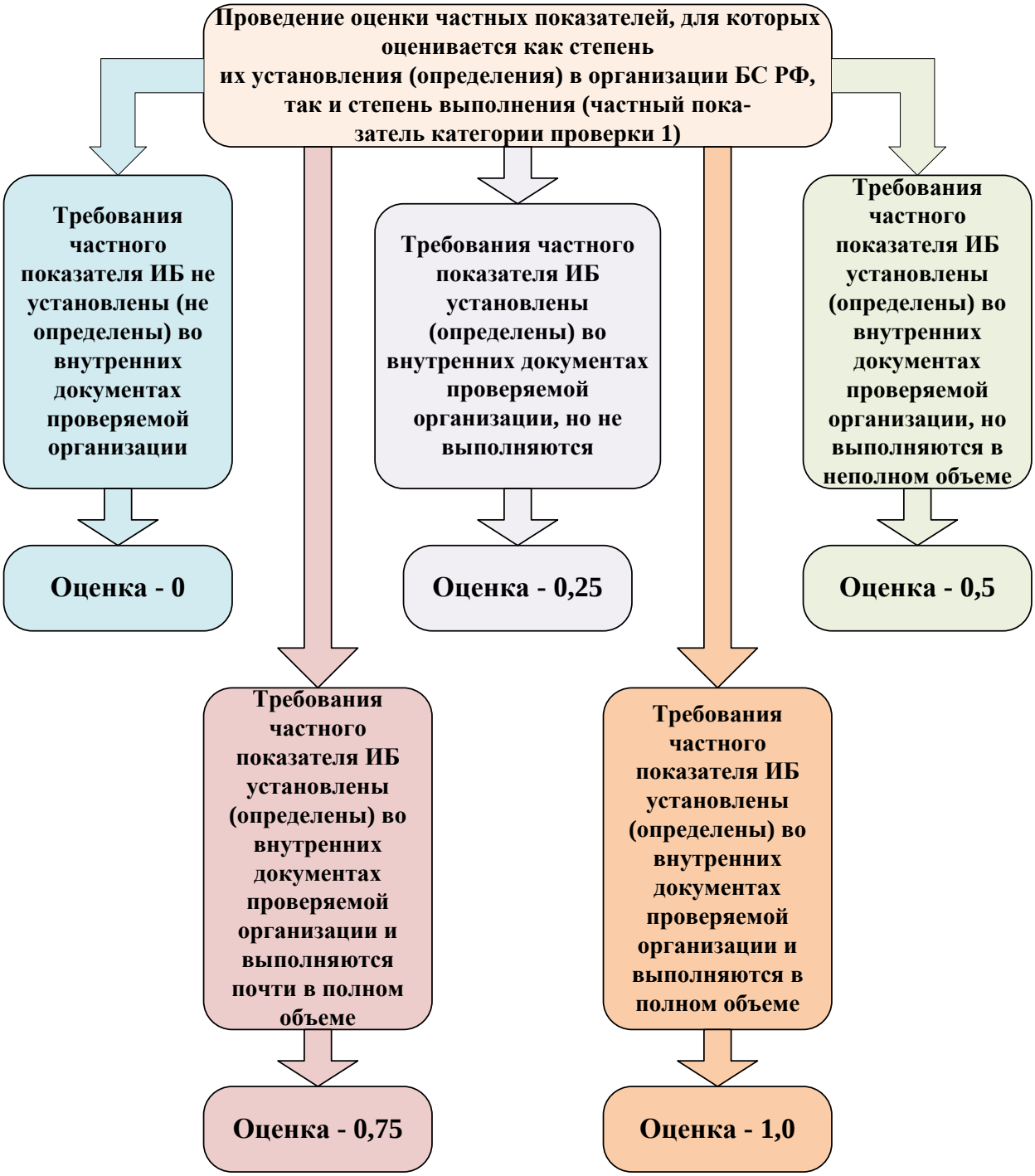

Рисунок 2.8б - Проведение оценки частных показателей, для которых оценивается как степень их установления (определения) в организации БС РФ, так и степень выполнения (частный показатель категории проверки 1)

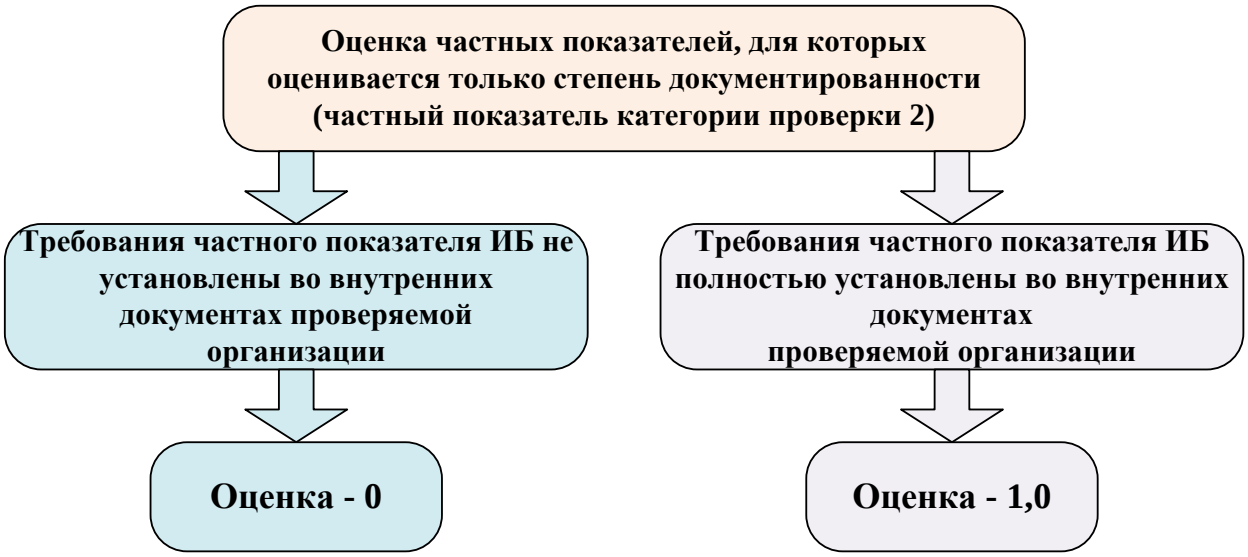

Рисунок 2.8в - Оценка частных показателей, для которых оценивается только сте-пень документированности (частный показатель категории проверки 2)

Рисунок 2.8г - Оценка частных показателей, для которых оценивается только степень выполнения (частный показатель категории проверки 3)

2.3.6.2 Порядок оценки соответствия требованиям ИБ в организациях банковской сферы РФ

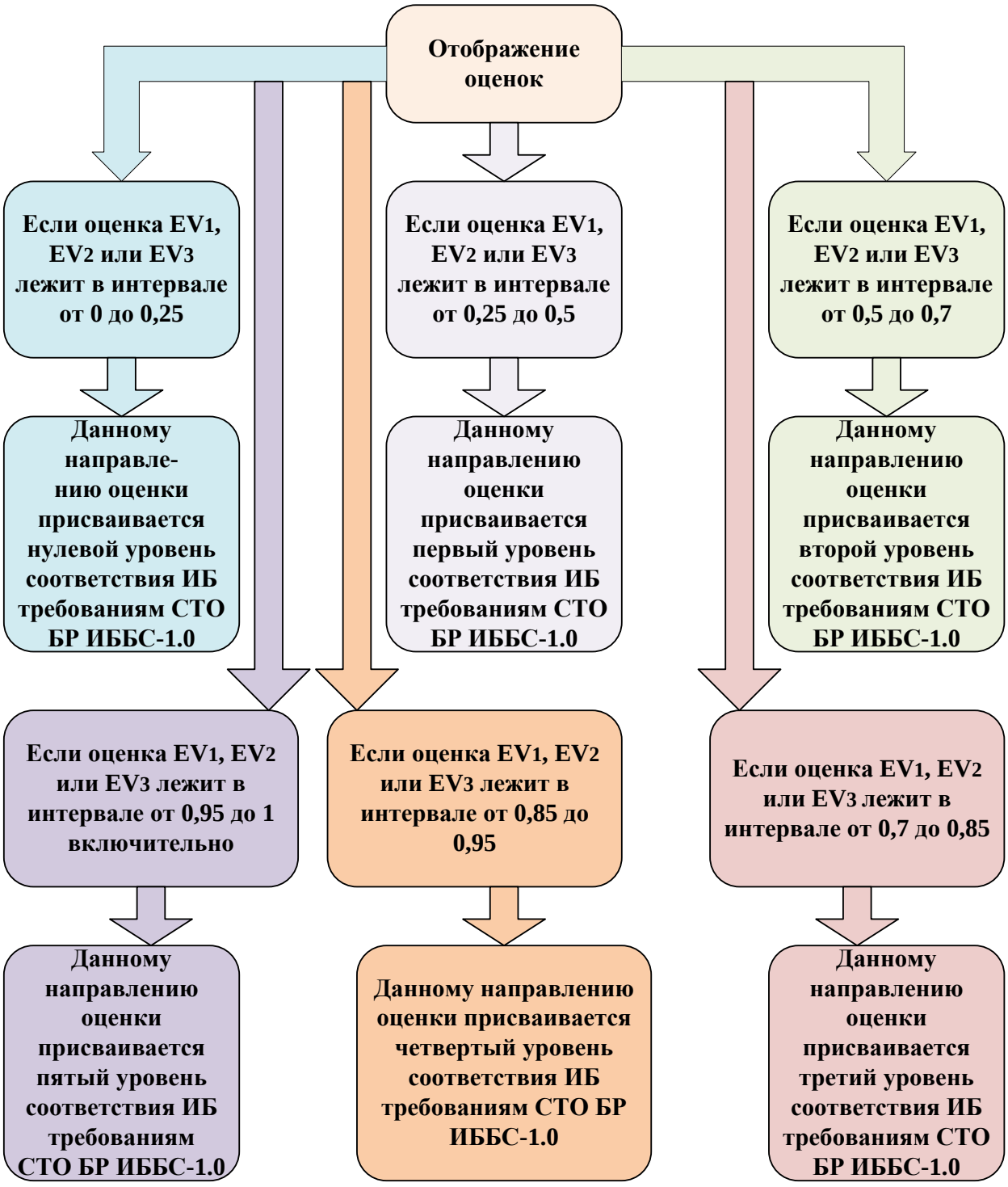

Рисунок 2.9 - Отображение оценок

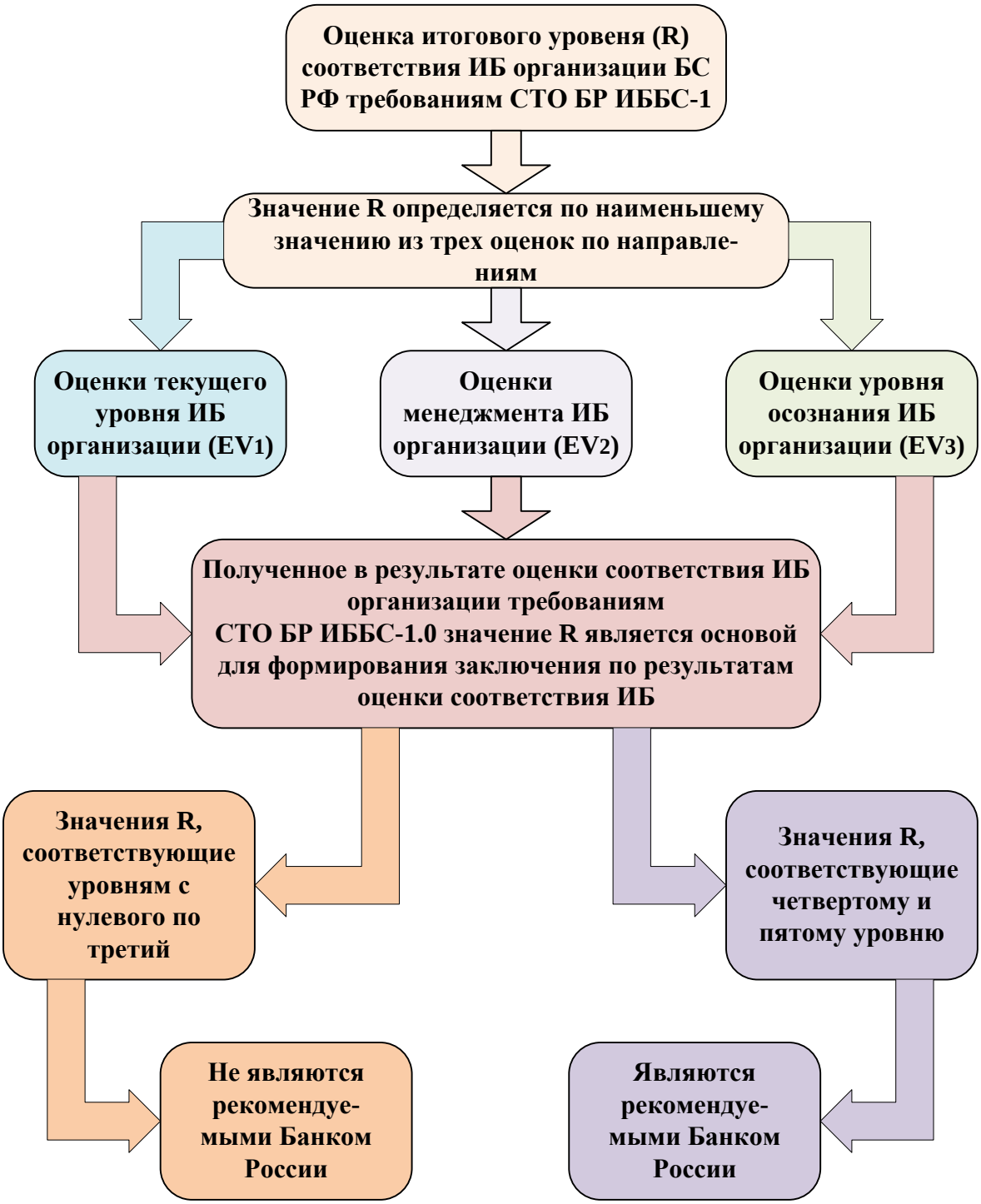

Рисунок 2.9а - Оценка интегрального показателя R

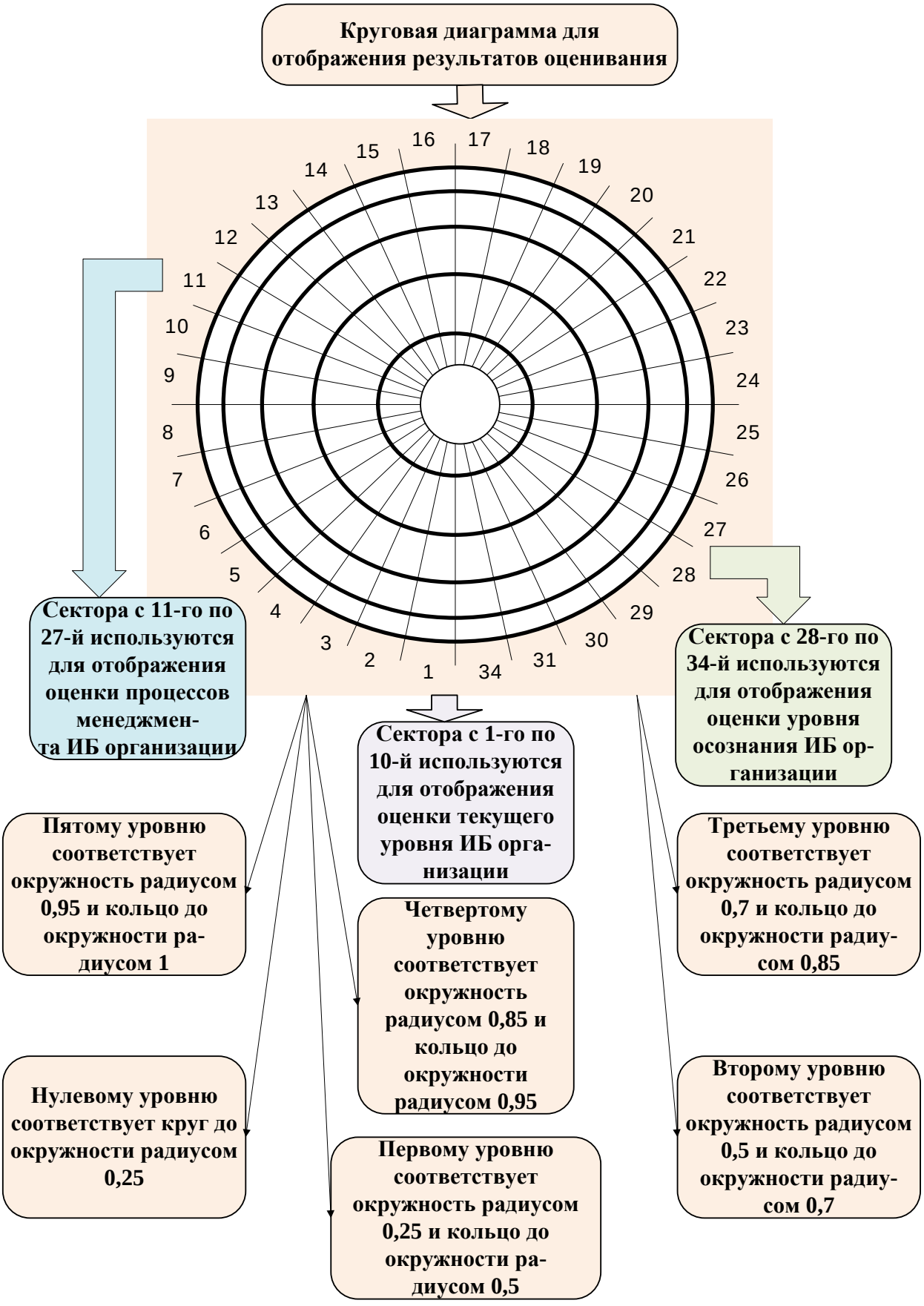

Рисунок 2.9б - Круговая диаграмма для отображения результатов оценивания

С учетом принятых в 2014 изменений в СТО БР ИББС-1 круговая диаграмма для отображения результатов оценивания соответствия ИБ (как пример) может иметь вид, показанный на рисунке 2.9в

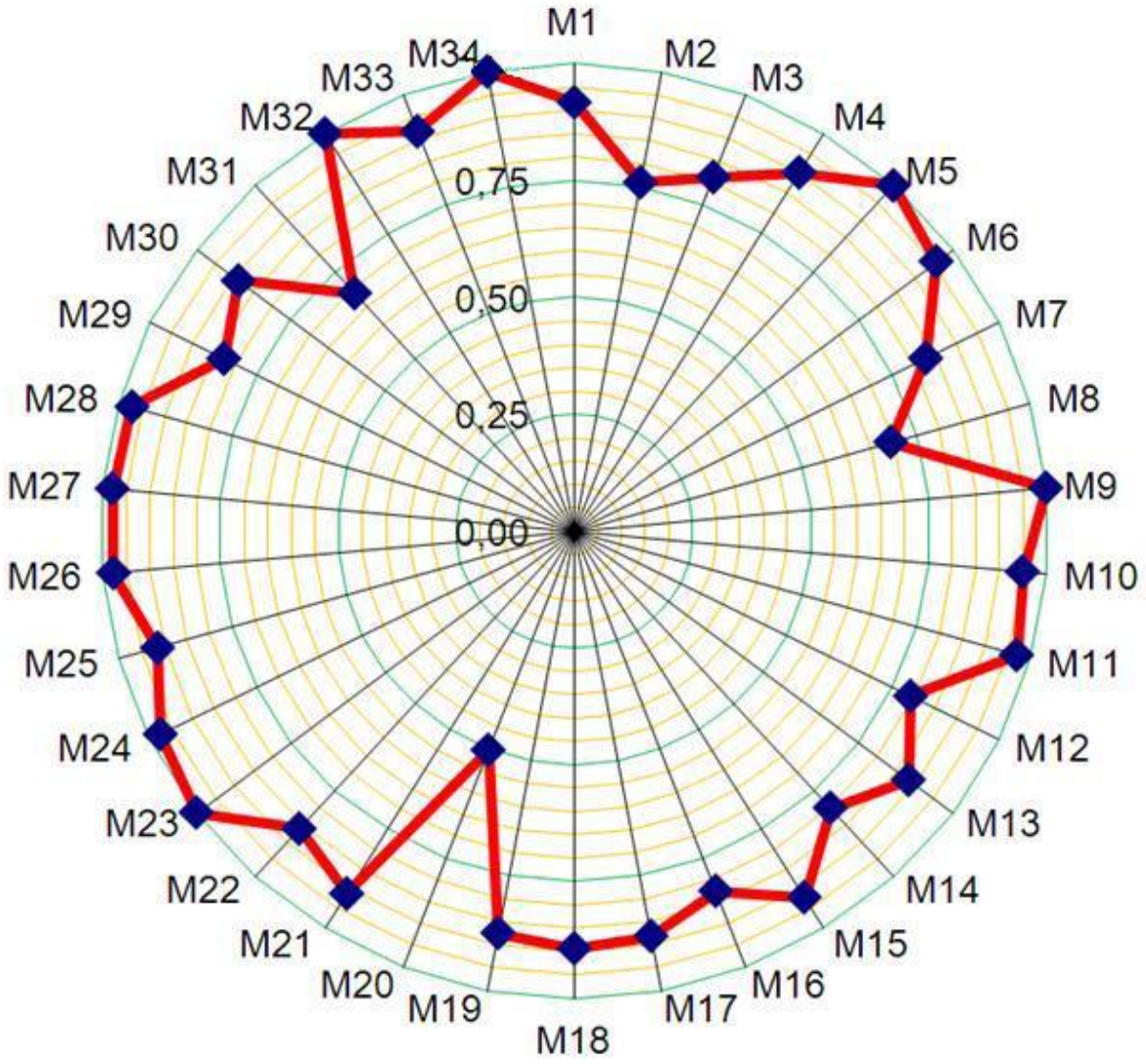

Рисунок 2.9в - результаты оценивания соответствия ИБ

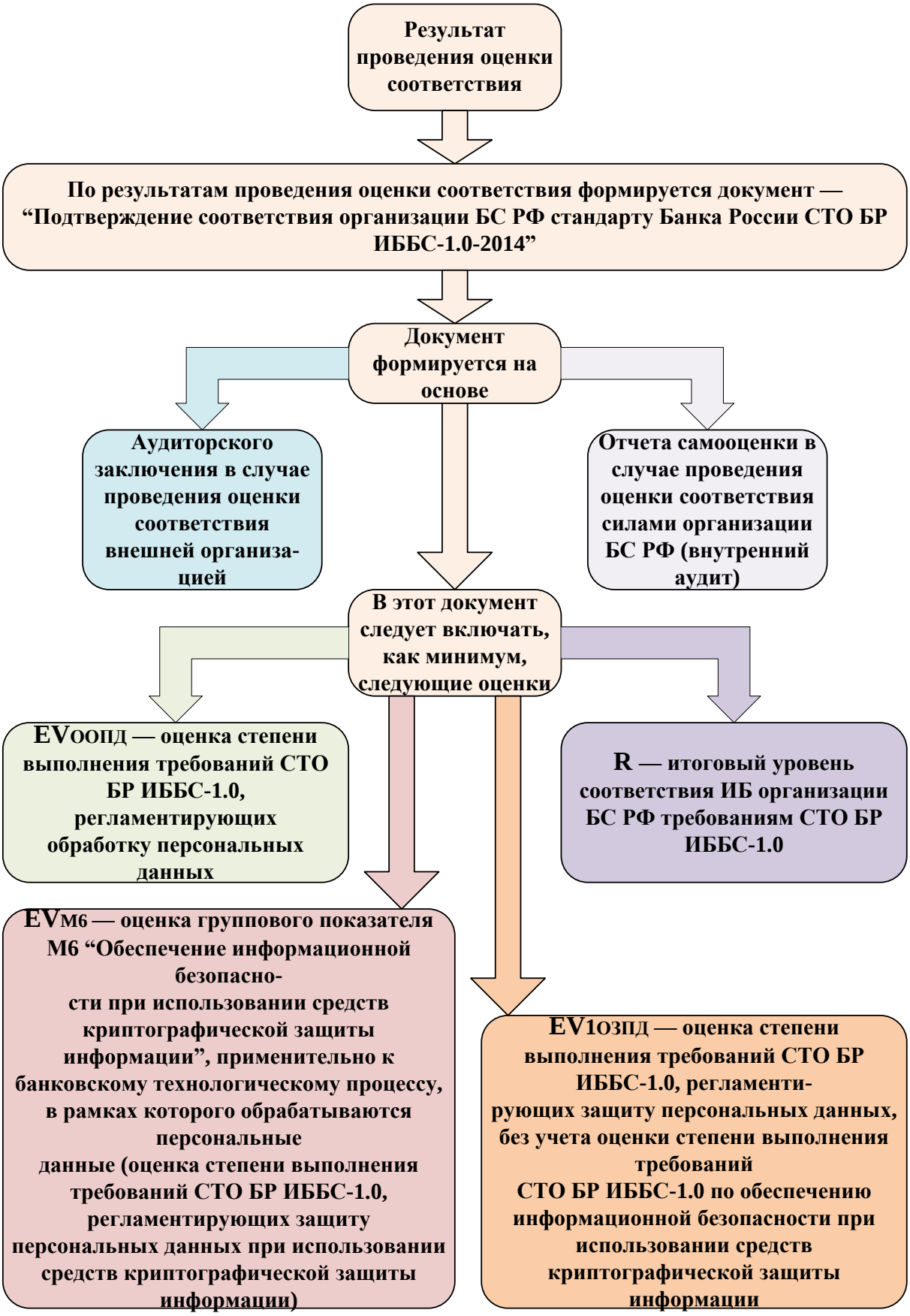

Рисунок 2.9в - Результат проведения оценки соответствия

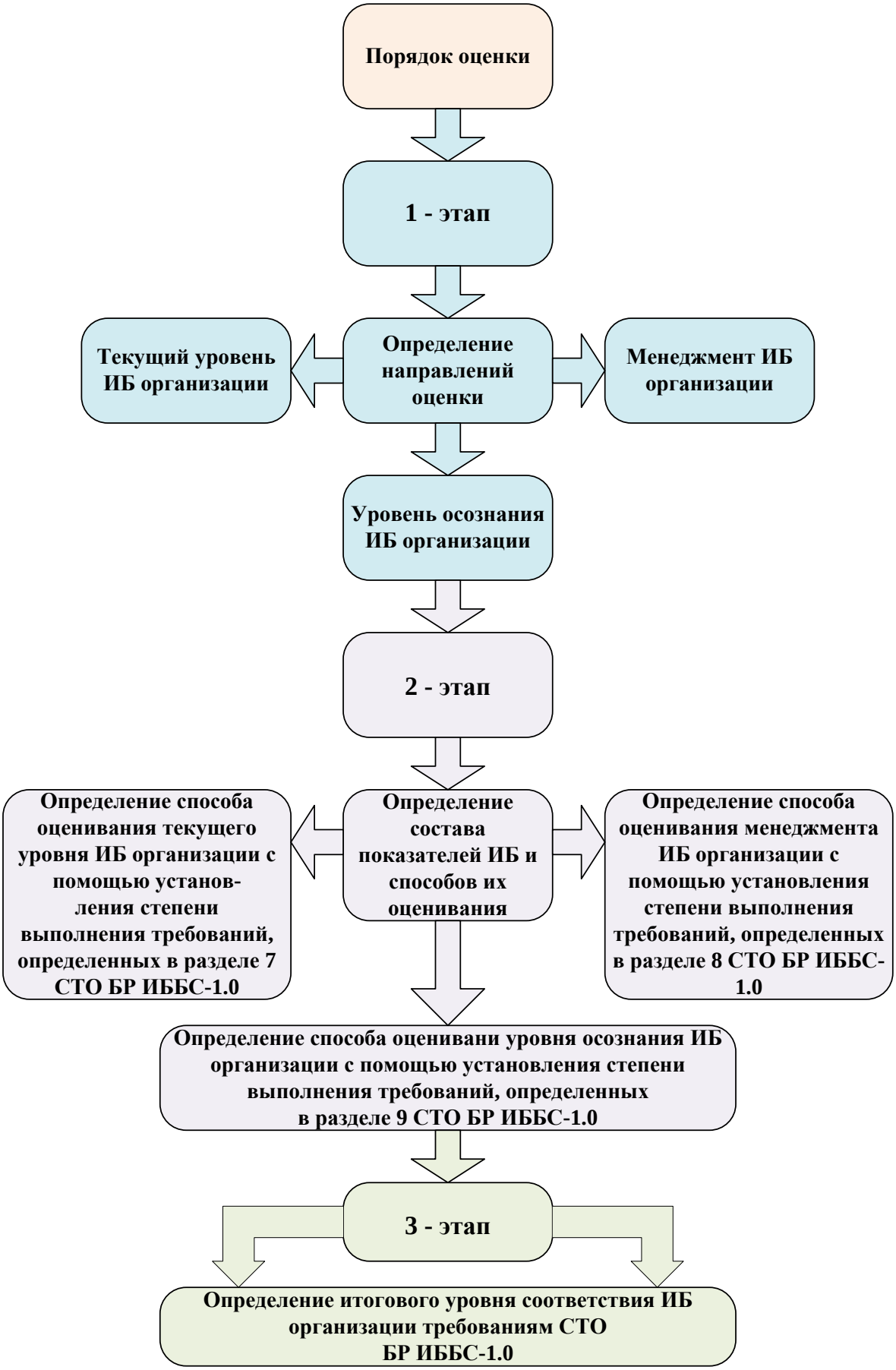

Рисунок 2.9г - Порядок оценки

2.3.7 Методика на основе национального стандарта США NIST 800-53

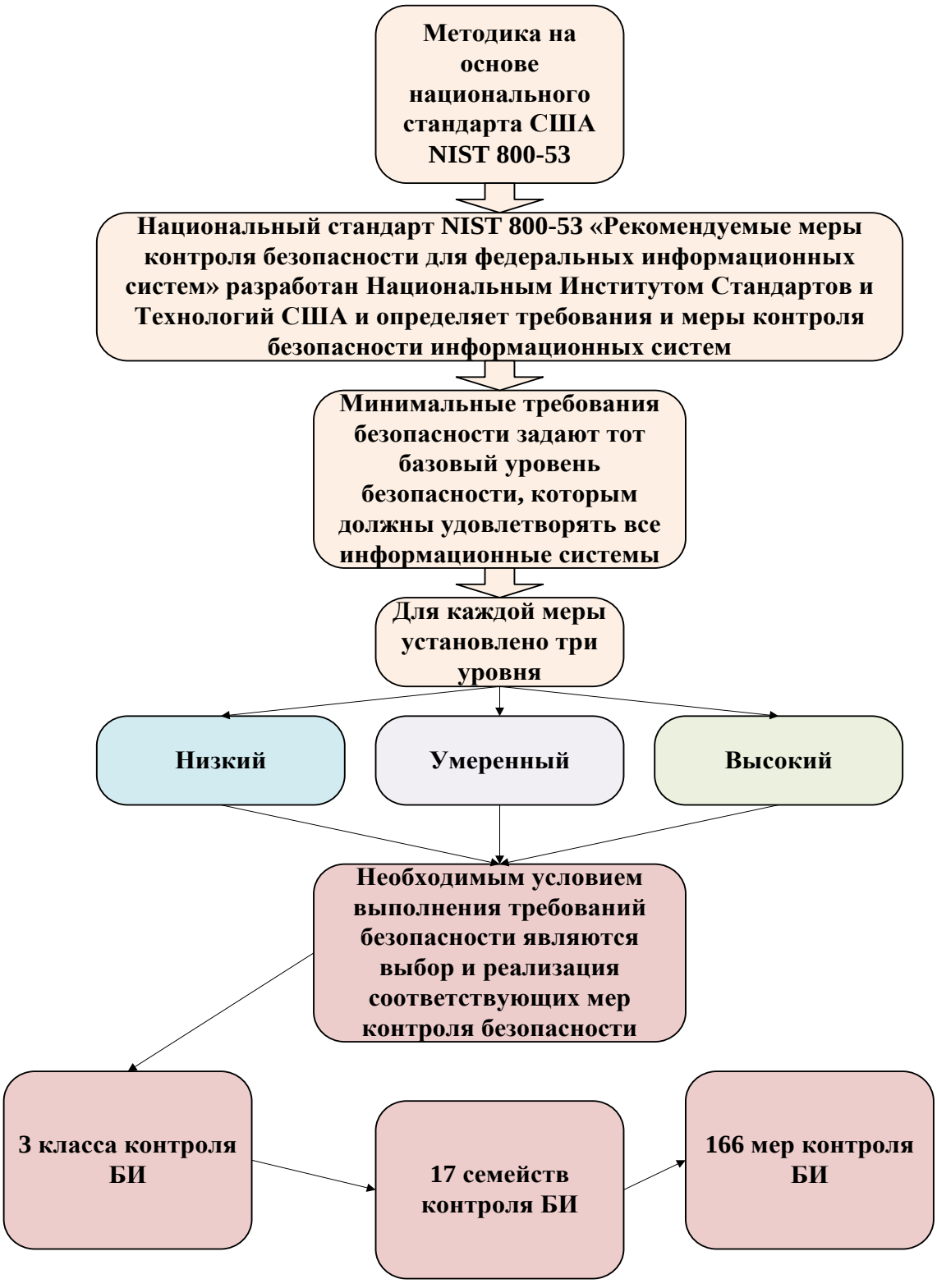

Рисунок 2.10 - Методика на основе национального стандарта США NIST 800-53

2.3.7.1 Меры контроля БИ стандарта NIST SP 800-53

Рисунок 2.11 - Меры контроля БИ стандарта NIST SP 800-53

2.3.8 Структура стандарта COBIT

Рисунок 2.12 – Структура стандарта COBIT

2.4 Сравнение методик проведения аудитов

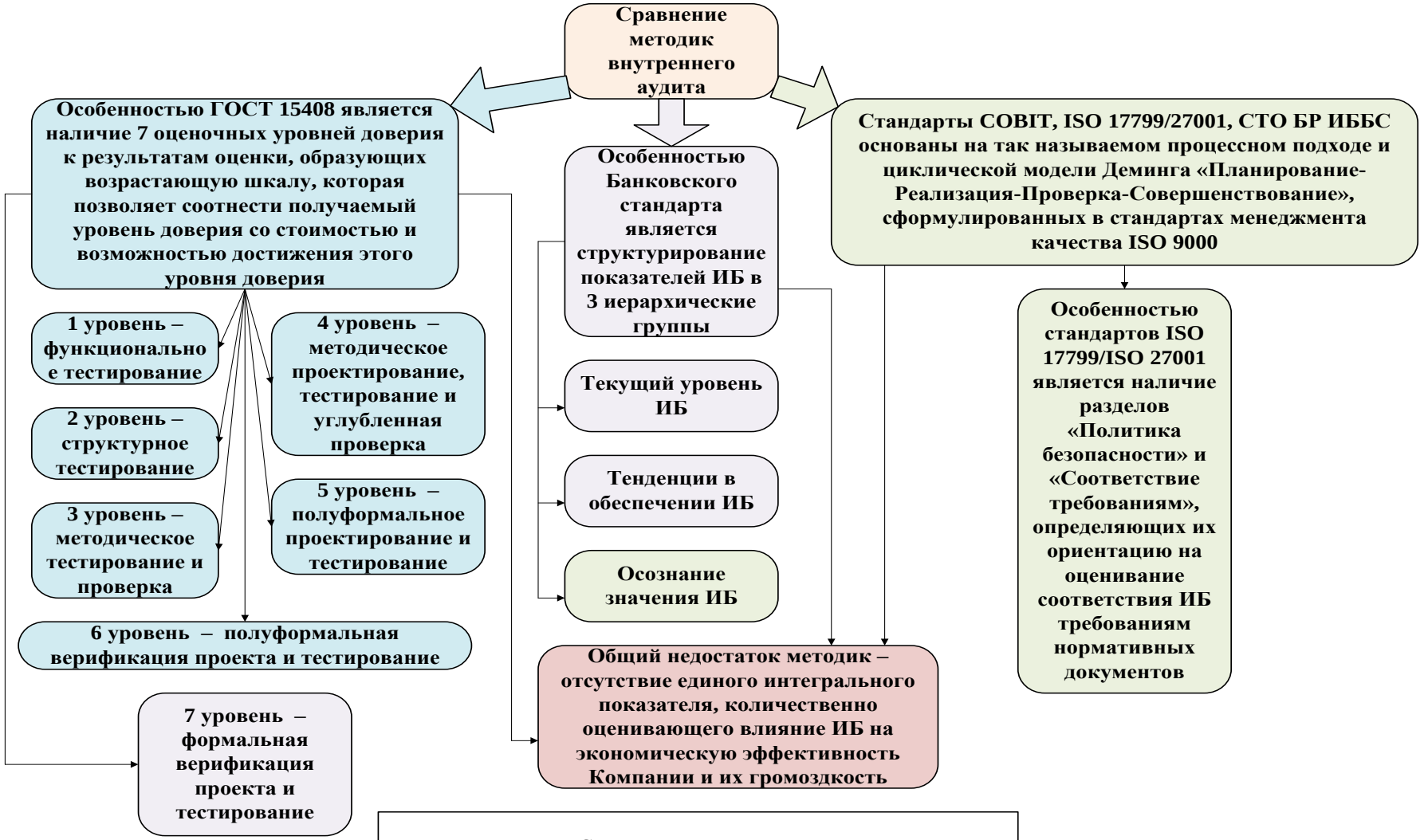

Рисунок 2.13 - Сравнение методик внутреннего аудита

Таблица 2.4 Сравнительные характеристики методик оценивания ИБ

Характеристика	ГОСТ 15408	СТО БР ИББС	ISO 17799/ 27001	BSI	NIST	COBIT
Разработчик (страна, организация)	РФ (на основе м/н)	РФ	м/н	ФРГ	США	компания ISACA
Уровни ИБ	технический	организа-ционный	организа-ционный, процедур-ный	организа-ционный, техничес-кий	организа-ционный, процедур-ный, техничес-кий	организа-ционный, процедур-ный
Структурирован-ность	11 классов, 61 семейство функц. требований, 7 классов, 26 семейств треб. доверия	3 группы, 32 груп. показателя, 237 частных показате-лей	11 разделов, 133 требования	5 групп, 46 объектов контроля	3 класса, 17 семейств, 163 меры контроля	4 домена, 34 цели контроля, 318 средств контроля
Подход	системный, функциональный	процес-сный	процессный	функцио-нальный	функцио-нальный	процесс-сный