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 П3.
- 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

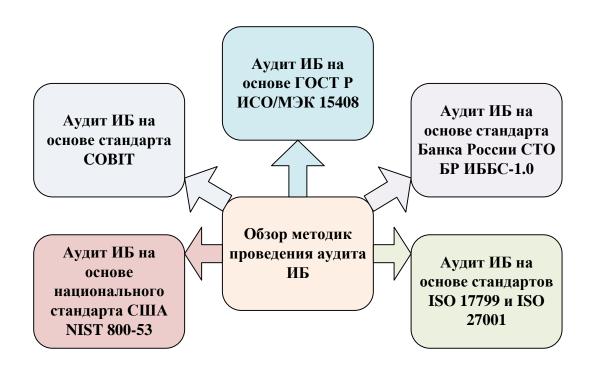
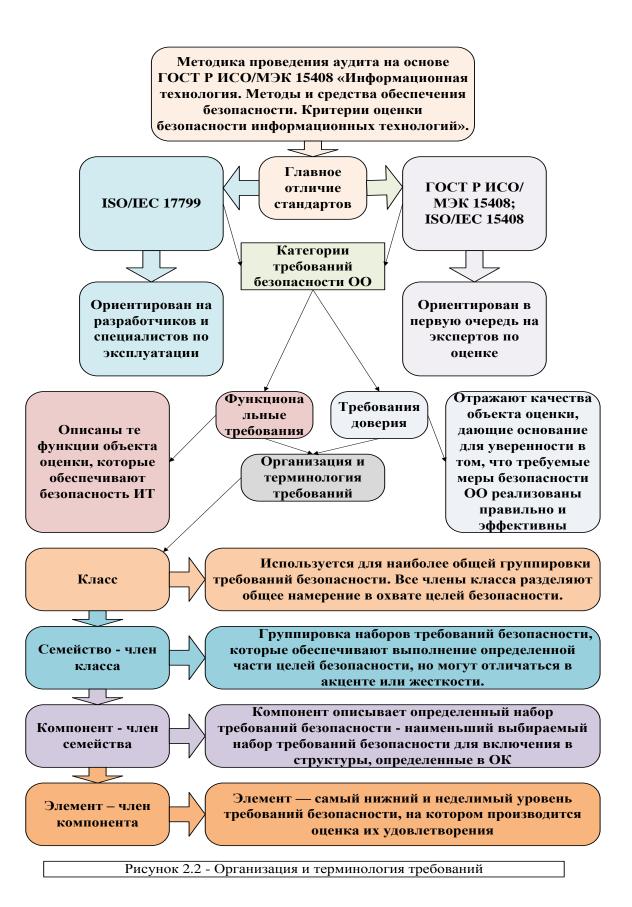


Рисунок 2.1 - Обзор методик проведения аудита ИБ

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

2.3.1 Организация и терминология требований



2.3.2 Понятия, используемые при проведении аудита

Промежуточная комбинация компонентов названа пакетом. Пакет предназначен для многократного использования и определяет требования, которые являются необходимыми для достижения идентифицированных целей. Пакет может использоваться для формирования профилей защиты и заданий по безопасности Зависимости Компонент возникают, когда компонент сам недостаточен для выполнения цели безопасности и необходимо Зависимости наличие другого компонента Чтобы гарантировать законченность требований к В задание по ОО, зависимости должны В профиль защиты быть учтены при включении безопасности компонентов Компоненты могут быть преобразованы с помощью разрешенных действий, чтобы обеспечить выполнение определенной политики безопасности или противостоять определенной угрозе К разрешенным Назначение действиям Обработка относятся $\overline{\overline{\ }}$ Позволяет включить дополнительные детали Выбор в элемент и Разрешает заполнить предполагает спецификацию Процесс выбора интерпретацию идентифицированного одного или требования, правила, параметра при большего константы или условия, использовании основанную на целях количества компонента. Параметр пунктов из списка, безопасности. может быть признаком Обработка не позволяет чтобы или правилом, которое конкретизировать создавать новые конкретизирует возможности требования или удалять требование к элемента существующие и не определенной величине влияет на список или диапазону величин зависимостей, связанных с компонентом

Рисунок 2.3 – Понятия, используемые в методике при проведении аудита

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, солержащим необходимый объем требований для данного типа изделий ИТ

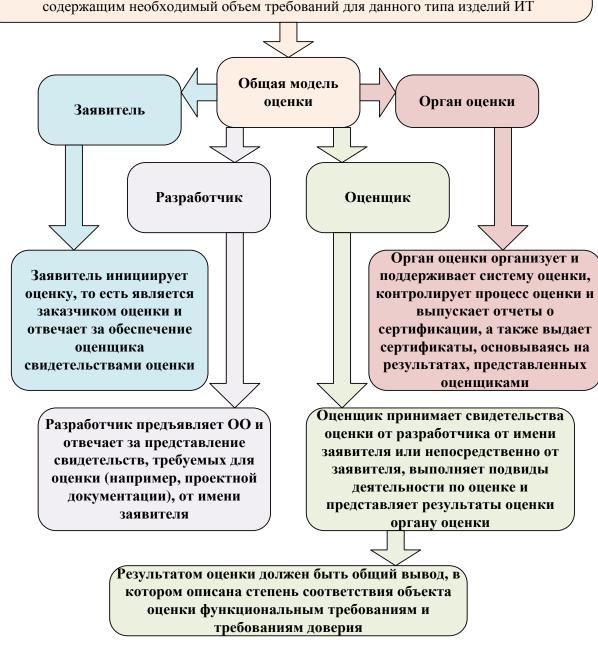


Рисунок 2.4 - Общая модель оценки на основе ГОСТ Р ИСО/МЭК 15408

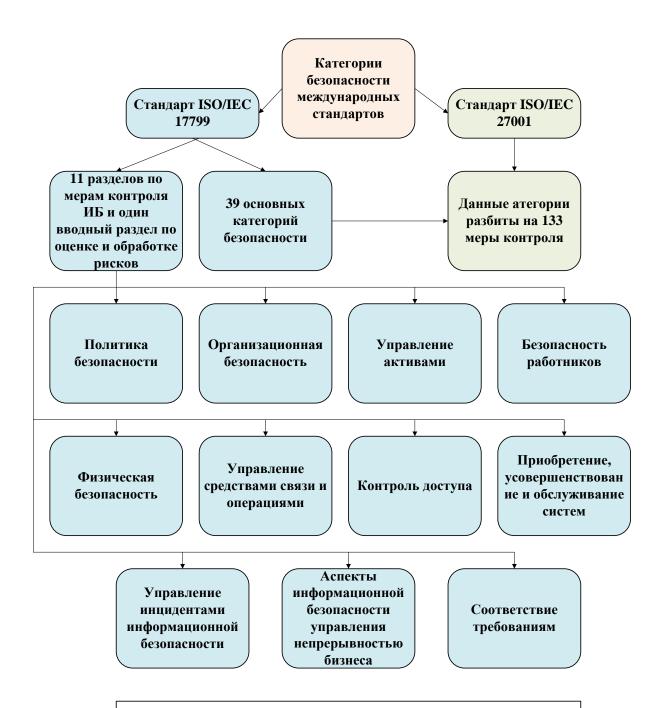


Рисунок 2.5 - Категории безопасности международных стандартов (стандарт ISO/IEC 17799 и стандарт ISO/IEC 27001)

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

Немецкий стандарт «Руководство по обеспечению безопасности ИТ базового уровня» (IT Baseline Protection Manual) разработан Агенством Информационной Безопасности Германии (BSI - Bundesamt für Sicherheit in der Informationstechnik, German Information Security Agency). В отличие от ISO 17799 немецкий стандарт посвящен детальному рассмотрению частных вопросов управления информационной безопасности Компании

Методика на основе стандарта BSI/IT Baseline Protection Manual

Структура стандарта BSI/IT Baseline Protection Manual

Метод управления информационной безопасностью (организация менеджмента в области ИБ, методология использования руководства)

Описания компонентов современных информационных технологий

Описания основных компонентов организации режима информационной безопасности (организационный и технический уровни защиты данных, планирование действий в чрезвычайных ситуациях, поддержка непрерывности бизнеса

Характеристики объектов информатизации (здания, помещения, кабельные сети, контролируемые зоны)

Характеристики компьютерных сетей на основе различных сетевых технологий, например сети Novell NetWare, сети UNIX и Windows)

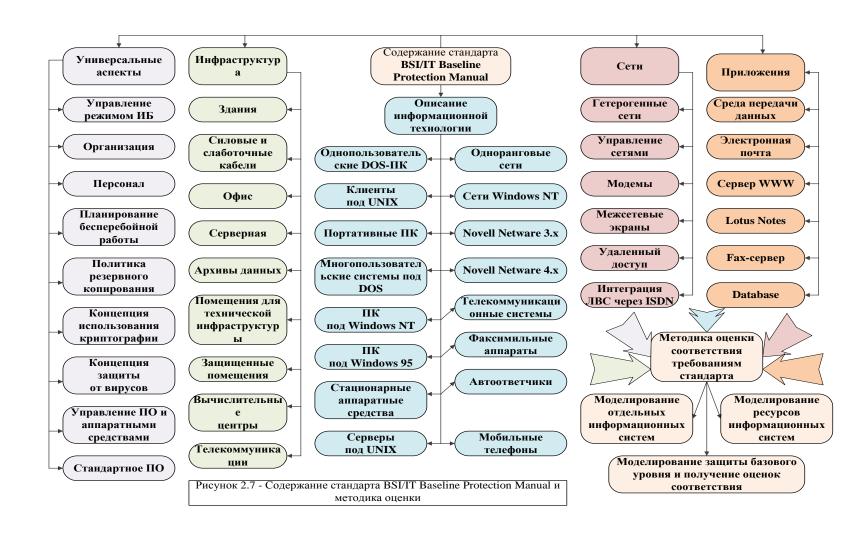
Характеристика активного и пассивного телекоммуникационного оборудования ведущих вендоров, например Cisco Systems

Характеристики основных информационных активов Компании (в том числе аппаратное и программное обеспечение, например рабочие станции и сервера под управлением операционных систем семейства DOS, Windows и UNIX)

Подробные каталоги угроз безопасности и мер контроля (более 600 наименований в каждом каталоге)

Рисунок 2.6 - Структура стандарта BSI/IT Baseline Protection Manual

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



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

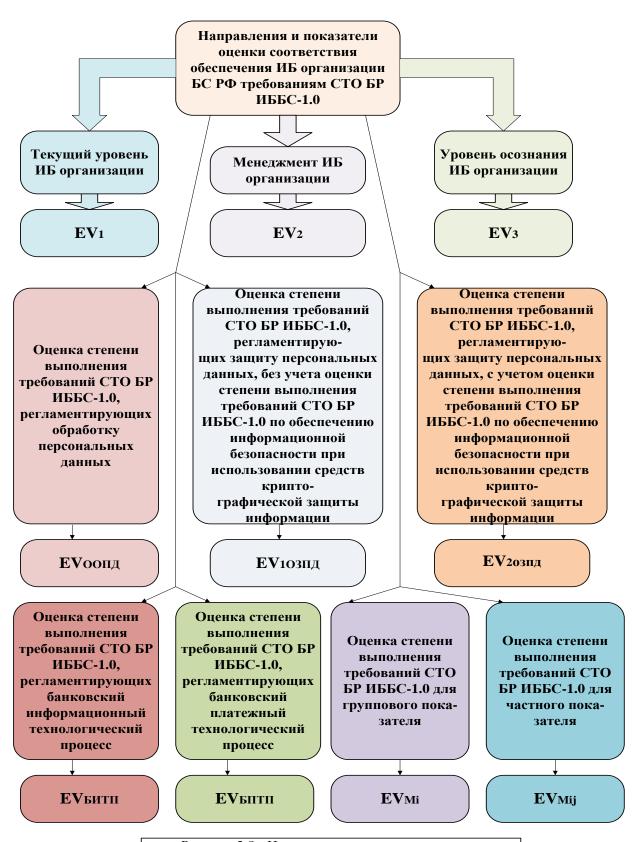
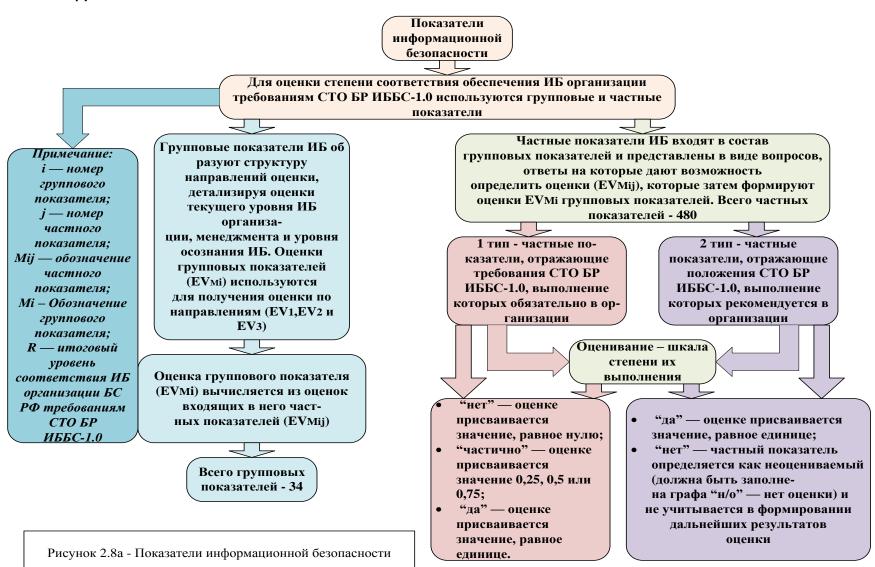


Рисунок 2.8 - Направления и показатели оценки соответствия обеспечения ИБ организации БС РФ требованиям СТО БР ИББС-1.0

2.3.6.1 Частные и групповые показатели ИБ



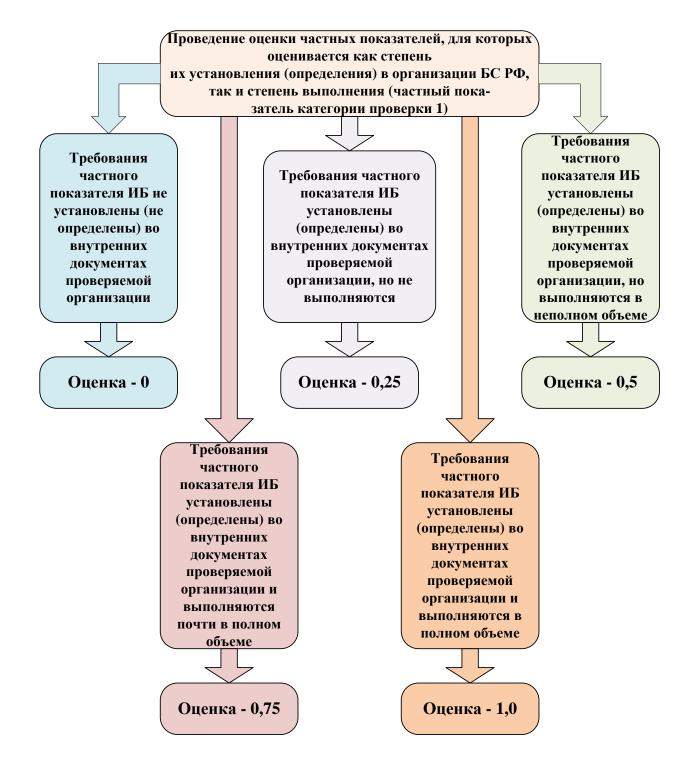


Рисунок 2.8б - Проведение оценки частных показателей, для которых оценивается как степень их установления (определения) в организации БС РФ, так и степень выполнения (частный показатель категории проверки 1)



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

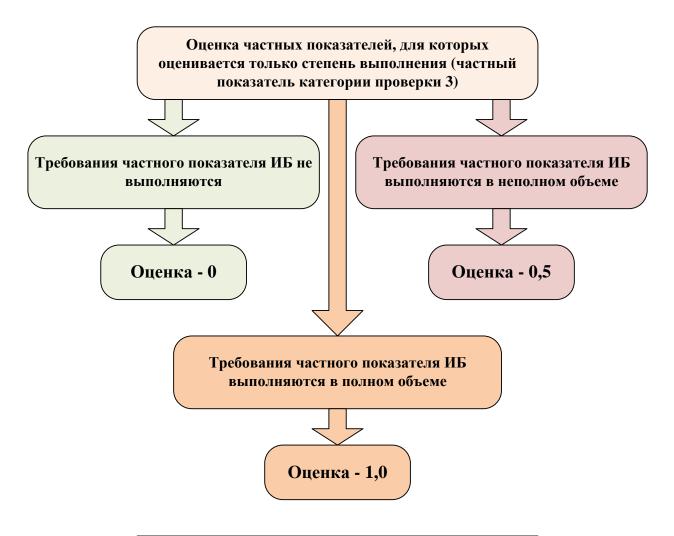


Рисунок 2.8г - Оценка частных показателей, для которых оценивается только степень выполнения (частный показатель категории проверки 3)

2.3.6.2 Порядок оценки соответствия требованиям ИБ в организациях банковской сферы РФ

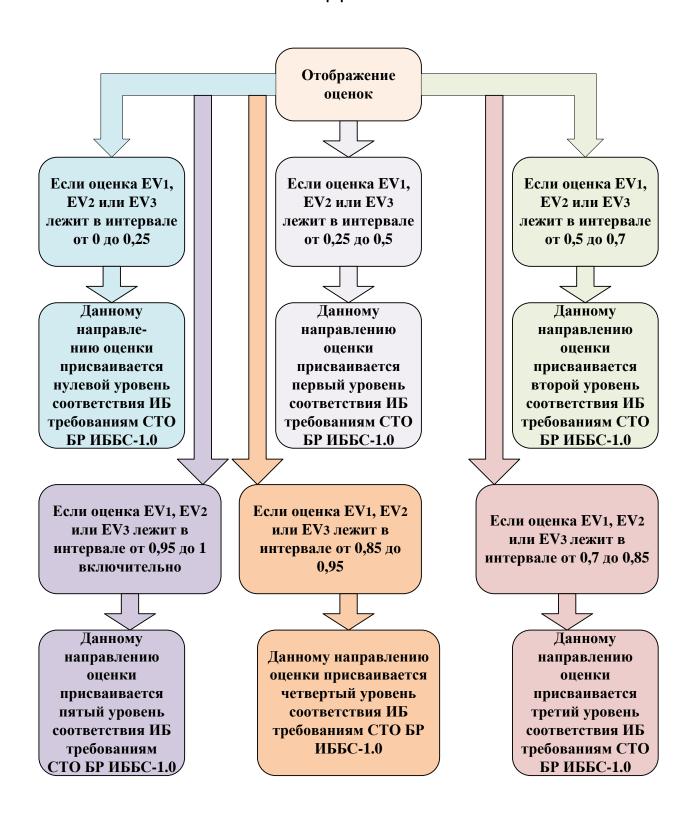


Рисунок 2.9 - Отображение оценок

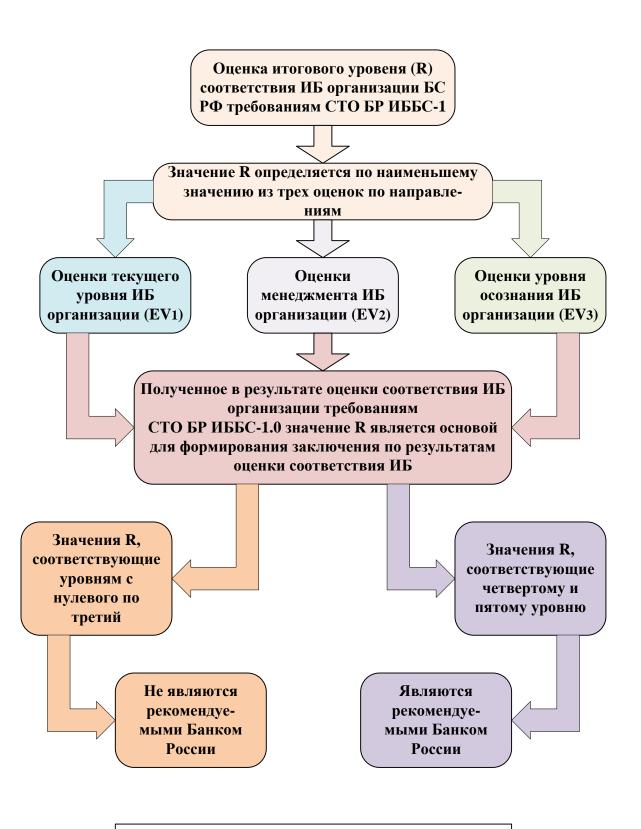


Рисунок 2.9а - Оценка интегрального показателя R

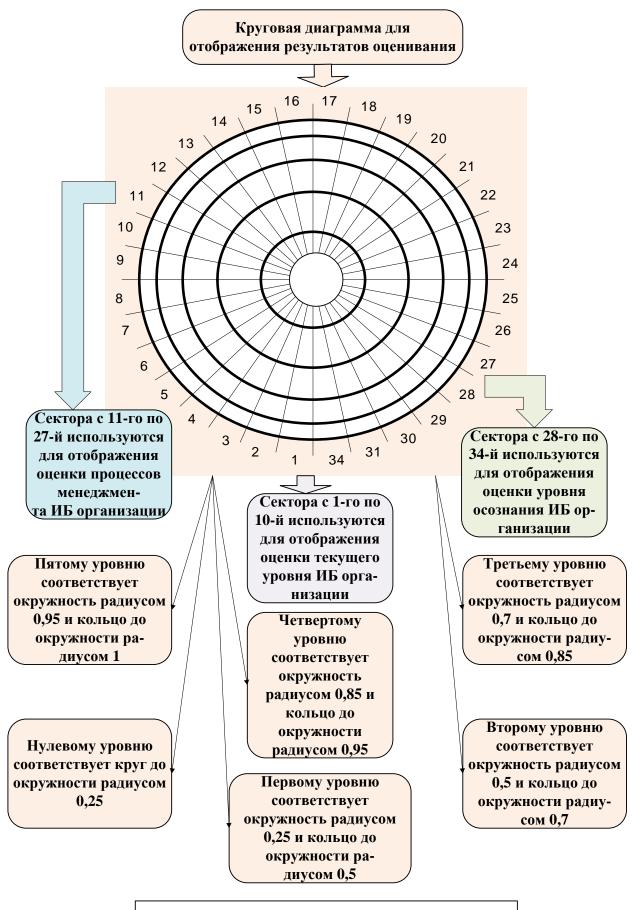


Рисунок 2.9б - Круговая диаграмма для отображения результатов оценивания

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

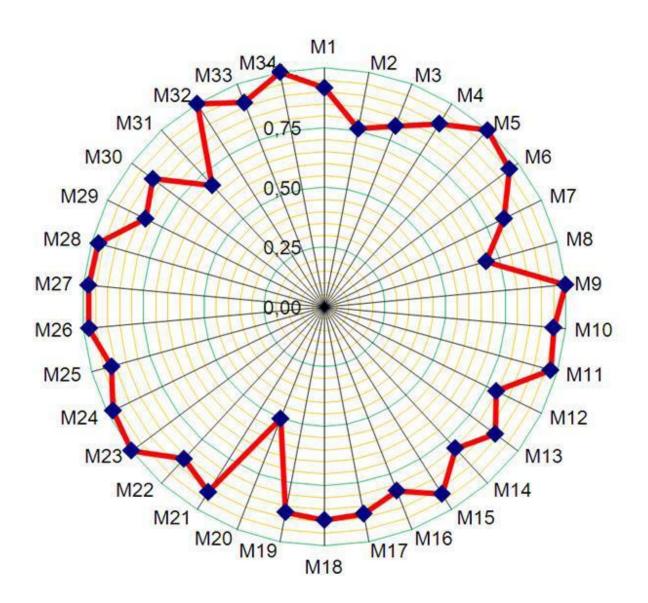


Рисунок 2.9в - результаты оценивания соответствия ИБ

проведения оценки соответствия По результатам проведения оценки соответствия формируется документ — "Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-2014" Документ формируется на основе Аудиторского Отчета самооценки в заключения в случае случае проведения проведения оценки оценки соответствия соответствия силами организации внешней организа-БС РФ (внутренний цией аудит) В этот документ следует включать, как минимум, следующие оценки/ EVOОПД — оценка степени выполнения требований СТО R — итоговый уровень БР ИББС-1.0, соответствия ИБ организации регламентирующих БС РФ требованиям СТО БР обработку персональных ИББС-1.0 данных EVм6 — оценка группового показателя М6 "Обеспечение информационной безопасности при использовании средств EV103ПД — оценка степени криптографической защиты выполнения требований СТО БР информации", применительно к банковскому технологическому процессу, ИББС-1.0, регламентирующих защиту персональных данных, в рамках которого обрабатываются персональные без учета оценки степени выполнения требований данные (оценка степени выполнения СТО БР ИББС-1.0 по обеспечению требований СТО БР ИББС-1.0, регламентирующих защиту информационной безопасности при персональных данных при использовании использовании средств средств криптографической защиты криптографической защиты информации) информации

Результат

Рисунок 2.9в - Результат проведения оценки соответствия

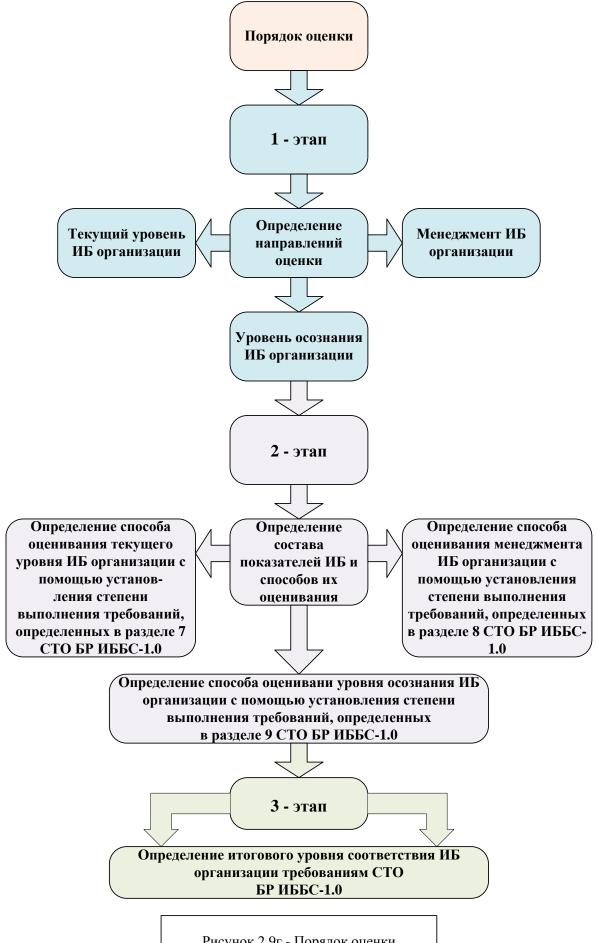


Рисунок 2.9г - Порядок оценки



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

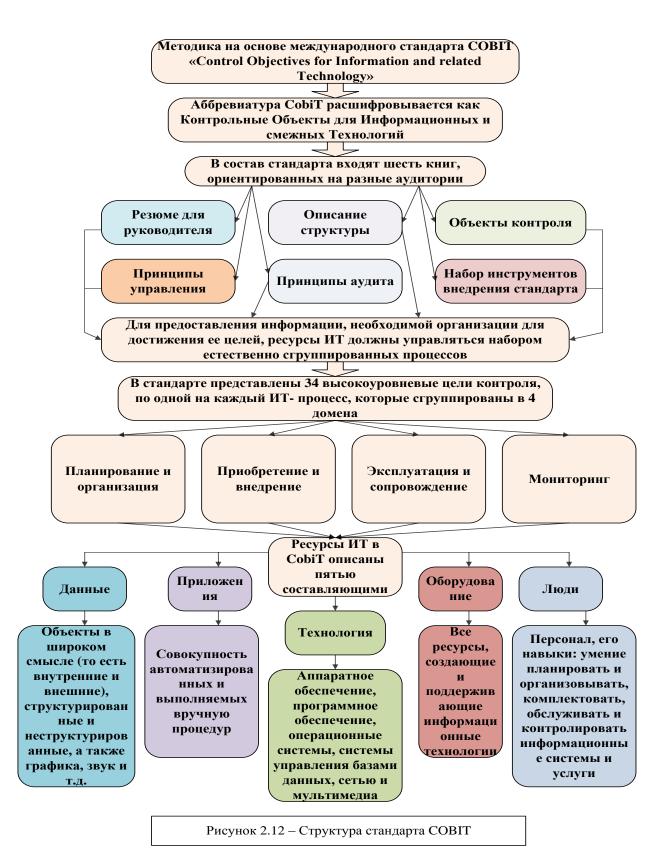
Меры контроля БИ стандарта NIST SP 800-53 Класс Административный Технический Операционный $\forall \vdash$ Семейства, Семейства, идентификаторы, Семейства, идентификаторы, количество мер идентификаторы, количество мер контроля количество мер контроля контроля Оценка рисков $\forall \vdash$ Идентификация и Идентификатор - RA Кадровая безопасность аутентификация Идентификатор - PS Количество мер Идентификатор – ІА контроля - 5 Количество мер Количество мер контроля - 7 контроля - 8 Планирование Контроль доступа Физическая зашита и безопасности Идентификатор – АС Идентификатор – PL защита от внешней Количество мер контроля -Количество мер среды 20 Идентификатор –РЕ контроля - 5 Аудит и протоколирование Количество мер Закупка систем и контроля - 17 Идентификатор – AU сервисов Количество мер контроля -Планирование Идентификатор – SA 11 нештатных ситуаций Количество мер контроля - 11 Идентификатор – СР Защита систем и Количество мер коммуникаций Сертификация, Идентификатор – SC контроля - 10 аккредитация и оценка Количество мер контроля безопасности Управление 19 Идентификатор – СА конфигурацией Идентификатор – СМ Целостность систем и Количество мер контроля - 7 Количество мер данных контроля - 7 Идентификатор – SI Реагирование на Количество мер контроля инциденты 12 Сопровождение Идентификатор – IR Идентификатор – МА Зашита носителей Количество мер Количество мер информации контроля - 7 контроля - 6 Идентификатор – МР Информирование и Количество мер контроля - 7,

обучение Идентификатор – АТ

Количество мер

контроля - 4

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



2.4 Сравнение методик проведения аудитов



Таблица 2.4 Сравнительные характеристики метолик оценивания ИБ

Таблица 2.4 Сравнительные характеристики методик оценивания ИБ									
Характеристика	ГОСТ 15408	СТО БР ИББС	ISO 17799/ 27001	BSI	NIST	СОВІТ			
Разработчик	РФ	РФ	м/н	ФРГ	США	компания			
(страна,	(на основе					ISACA			
организация)	м/н)								
Уровни ИБ	технический	организа-	организа-	организа-	организа-	организа-			
		ционный	ционный,	ционный,	ционный,	ционный,			
			процедур-	техничес-	процедур-	процедур-			
			ный	кий	ный,	ный			
					техничес-				
					кий				
Структурирован-	11 классов,	3 группы,	11	5 групп, 46	3 класса, 17	4 домена,			
ность	61 семейство	32 груп.	разделов,	объектов	семейств,	34 цели			
	функц.	показателя	133	контроля	163 меры	контроля,			
	требований,	, 237	требования	-	контроля	318 средств			
	7 классов, 26	частных				контроля			
	семейств	показате-							
	треб.	лей							
	доверия								
Подход	системный,	процес-	процессный	функцио-	функцио-	процесс-			
	функциональ	сный		нальный	нальный	сный			
	ный								