

**Федеральное государственное образовательное бюджетное учреждение
высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

Тульский филиал Финуниверситета

Кафедра «Математика и информатика»

СОГЛАСОВАНО

ЗАО «ЛИМ»

Генеральный директор

В.В. Куликов

«19» декабря 2024 г.



УТВЕРЖДАЮ

Директор филиала

Г.В. Кузнецов

«24» декабря 2024 г.



Н.О. Козлова, Е.В. Манохин

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ
АУДИТ ИНФОРМАЦИОННЫХ СИСТЕМ**

для студентов, обучающихся по направлению подготовки
09.03.02 Информационные системы и технологии,
образовательная программа «Информационные технологии в экономике»,
профиль «Информационные технологии в управлении цифровой
экономикой»

Рекомендовано Ученым советом Тульского филиала Финуниверситета
(протокол от 24 декабря 2024 г. № 22)

Одобрено кафедрой «Математика и информатика»
(протокол от 02 декабря 2024 г. № 5)

Тула 2024

«Аудит информационных систем»

КОД И НАИМЕНОВАНИЕ ОПОП:

09.03.02 Информационные системы и технологии

Образовательная программа - Информационные технологии в экономике

Профиль «Информационные технологии в управлении цифровой экономикой»

Общее количество заданий по дисциплине

Код компетенции	Наименование компетенции	Количество заданий
ПКП-4	Способен осуществлять аудит конфигураций ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению программных систем	40
Всего:		40

Количество заданий по дисциплине в одном варианте

Код компетенции	Наименование компетенции	Количество заданий
ПКП-4	Способен осуществлять аудит конфигураций ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению программных систем	20
Всего:		20

Типы заданий

Наименование типа заданий	Номер типа заданий
Задание закрытого типа на установление последовательности	1
Задание комбинированного типа с выбором одного верного ответа из предложенных	2
Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных	3
Задание открытого типа	4
Задание открытого типа с развернутым ответом	5

Распределение заданий по компетенциям

Код компетенции	Наименование компетенции	Наименование индикаторов сформированности компетенции	Семестр	Номер задания
ПКП-4	Способен осуществлять аудит конфигураций ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению программных систем	1. Организует проведение аудита конфигурации информационной системы, включая разработку программы аудита.	7	1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.1, 4.2, 5.1, 5.2, 6.1, 6.2, 7.1, 7.2, 8.1, 8.2, 9.1, 9.2, 10.1, 10.2
		2. Оценивает конфигурацию информационной системы при создании (модификации) и сопровождению программных систем с целью их улучшения.	7	11.1, 11.2, 12.1, 12.2, 13.1, 13.2, 14.1, 14.2, 15.1, 15.2, 16.1, 16.2, 17.1, 17.2, 18.1, 18.2,

				19.1, 19.2, 20.1, 20.2
--	--	--	--	---------------------------

Типы, уровень сложности и время выполнения заданий

Код компетенции	Индикатор сформированности компетенции	Номер задания	Тип задания	Уровень сложности задания	Время выполнения задания (мин.)
ПКП-4	Организовывает проведение аудита конфигурации информационной системы, включая разработку программы аудита	1.1, 1.2.	2	базовый	2
	Организовывает проведение аудита конфигурации информационной системы, включая разработку программы аудита	2.1, 2.2	2	базовый	2
	Организовывает проведение аудита конфигурации информационной системы, включая разработку программы аудита	3.1, 3.2	2	базовый	2
	Организовывает проведение аудита конфигурации информационной системы, включая разработку программы аудита	4.1, 4.2	2	базовый	2
	Организовывает проведение аудита конфигурации информационной системы, включая разработку программы аудита	5.1, 5.2	2	базовый	2
	Организовывает проведение аудита конфигурации информационной системы, включая разработку программы аудита	6.1, 6.2.	4	повышенный	4
	Организовывает проведение аудита конфигурации информационной системы, включая разработку программы аудита	7.1, 7.2	4	повышенный	4
	Организовывает проведение аудита конфигурации информационной системы, включая разработку программы аудита	8.1, 8.2	1	повышенный	4
	Организовывает проведение аудита конфигурации информационной системы, включая разработку программы аудита	9.1, 9.2	5	высокий	8
	Организовывает проведение аудита конфигурации информационной системы, включая разработку программы аудита	10.1, 10.2	5	высокий	8
	Оценивает конфигурацию информационной системы при	11.1, 11.2.	2	базовый	2

	создании (модификации) и сопровождению программных систем с целью их улучшения.				
	Оценивает конфигурацию информационной системы при создании (модификации) и сопровождению программных систем с целью их улучшения.	12.1, 12.2	2	базовый	2
	Оценивает конфигурацию информационной системы при создании (модификации) и сопровождению программных систем с целью их улучшения.	13.1, 13.2	2	базовый	2
	Оценивает конфигурацию информационной системы при создании (модификации) и сопровождению программных систем с целью их улучшения.	14.1, 14.2	3	базовый	2
	Оценивает конфигурацию информационной системы при создании (модификации) и сопровождению программных систем с целью их улучшения.	15.1, 15.2	2	базовый	2
	Оценивает конфигурацию информационной системы при создании (модификации) и сопровождению программных систем с целью их улучшения.	16.1, 16.2.	4	повышенный	4
	Оценивает конфигурацию информационной системы при создании (модификации) и сопровождению программных систем с целью их улучшения.	17.1, 17.2	4	повышенный	4
	Оценивает конфигурацию информационной системы при создании (модификации) и сопровождению программных систем с целью их улучшения.	18.1, 18.2	5	высокий	8
	Оценивает конфигурацию информационной системы при создании (модификации) и сопровождению программных систем с целью их улучшения.	19.1, 19.2	5	высокий	8
	Оценивает конфигурацию информационной системы при создании (модификации) и сопровождению программных систем с целью их улучшения.	20.1, 20.2	5	высокий	8

**Задания, позволяющие осуществлять оценку компетенций,
установленных для дисциплины**

Вариант 1

Задание 1.1.

Что такое аудит информационных систем?

А. Независимая оценка состояния информационных технологий и систем организации

Б. Процесс разработки программного обеспечения

В. Проверка финансовой отчетности

Г. Процедура подбора персонала

Ответ:

Задание 2.1.

Какой тип аудит информационных систем предполагает участие специалистов специализированных организаций?

- А. Внешний аудит
- Б. Внутренний аудит
- В. Комплаенс-аудит
- Г. Аналитический аудит

Ответ:

Задание 3.1.

Какой этап аудита информационной системы направлен на проверку выполнения регламентов работы с информационной системой?

- А. Подготовительный этап
- Б. Опрос и интервьюирование
- В. Анализ документации
- Г. Практическая проверка
- Д. Подготовка отчета
- Е. Презентация результатов

Ответ:

Задание 4.1.

Какие документы и материалы не используются для проведения аудита информационной системы?

- А. Политики и процедуры в области ИТ и информационной безопасности
- Б. Бухгалтерский баланс и финансовая отчетность
- В. Регламенты и инструкции по эксплуатации систем
- Г. Лог-файлы и журналы событий
- Д. Результаты предыдущих аудитов и проверок

Ответ:

Задание 5.1.

Какой метод тестирования используется при аудите приложений информационных систем?

- А. Пен-тестинг
- Б. Верификация кода
- В. Мониторинг и анализ лог-файлов
- Г. Тестирование отказоустойчивости
- Д. Социальная инженерия

Ответ:

Задание 6.1.

Перечислите не менее трех основных целей аудита информационных систем.

Ответ:

Задание 7.1.

Какой стандарт используется при проведении аудита информационной безопасности информационных систем?

Ответ:

Задание 8.1.

Укажите правильную последовательность этапов оценки рисков в рамках аудита информационной системы?

1. Оценка возможного ущерба от реализации угроз.
2. Ранжирование рисков по степени критичности.
3. Идентификация активов и угроз.
4. Оценка вероятности возникновения инцидентов.
5. Разработка мер по снижению рисков до приемлемого уровня.

Ответ:

Задание 9.1.

Перечислите не менее трех задач аудитора в процессе аудита информационной системы?

Ответ:

Задание 10.1.

Перечислите не менее трех основных принципов комплаенс-аудита?

Ответ:

Задание 11.1.

Какой метод оценки эффективности управления изменениями в информационной системе направлен на оценку действий специалистов?

- А. Анализ процесса подачи заявок на изменения
- Б. Проверка соблюдения процедур утверждения изменений
- В. Изучение логов и журналов изменений
- Г. Анализ влияния изменений на производительность и безопасность системы
- Д. Интервьюирование сотрудников, участвующих в процессе управления изменениями

Ответ:

Задание 12.1.

Какая задача НЕ относится к процессу внутреннего аудита информационной системой?

- А. Постоянный мониторинг состояния информационных систем
- Б. Поддержание высокого уровня безопасности и соответствия стандартам
- В. Выявление слабых мест и своевременное устранение недостатков
- Г. Помощь руководству в принятии решений по развитию ИТ-инфраструктуры
- Д. Повышение производительности труда в организации

Ответ:

Задание 13.1.

Как определить, насколько эффективно используется ИТ-бюджет?

- А. Сопоставление запланированных и фактических затрат
- Б. Анализ возврата инвестиций (ROI) от реализованных проектов
- В. Сравнение стоимости аналогичных решений у конкурентов
- Г. Опрос пользователей и сотрудников о полезности и удобстве внедряемых технологий
- Д. Исследование экономической выгоды от повышения производительности и снижения рисков
- Е. Комплексный подход, включающий все перечисленные методы

Ответ:

Задание 14.1.

Каковы основные проблемы, возникающие при проведении аудита информационных систем? (возможны несколько вариантов ответа)

- А. Ограниченное время и ресурсы для проведения аудита
- Б. Недоступность необходимой документации и информации
- В. Противодействие со стороны сотрудников, опасющихся критики своей работы
- Г. Кибератаки
- Д. Изменчивость и сложность современных информационных систем

Ответ:

Задание 15.1.

На каком этапе аудита информационных систем осуществляется тестирование системы?

- А. Подготовительный этап
- Б. Анализ документации
- В. Опрос и интервьюирование
- Г. Практическая проверка
- Д. Подготовка отчета
- Е. Презентация результатов

Ответ:

Задание 16.1.

Приведите не менее трех аспектов организации взаимодействия между аудиторами и внутренними службами организации?

Ответ:

Задание 17.1.

Приведите не менее трех критериев для выбора аудиторской компании для проведения внешнего аудита?

Ответ:

Задание 18.1.

Перечислите основные разделы отчета по результатам аудита информационной системы?

Ответ:

Задание 19.1.

Перечислите этапы аудита информационной безопасности?

Ответ:

Задание 20.1.

Каким образом можно оценить влияние результатов аудита на общую стратегию развития организации?

Ответ:

Вариант 2

Задание 1.2.

Какие основные цели аудита информационных систем?

- А. Проверять соответствие ИТ-инфраструктуры требованиям законодательства и стандартов
- Б. Выявлять уязвимости и недостатки в защите информации
- В. Оценивать эффективность и оптимальность использования ресурсов
- Г. Все вышеперечисленное

Ответ:

Задание 2.2.

Какой стандарт используется при проведении аудита информационной безопасности?

- А. ISO/IEC 27001
- Б. COBIT
- В. NIST SP 800-53
- Г. GDPR

Ответ:

Задание 3.2.

Какова роль аудитора в процессе аудита?

- А. Проводить опросы сотрудников
- Б. Выполнять техническую проверку оборудования
- В. Оценивать текущее состояние информационных систем и давать рекомендации по улучшению
- Г. Заниматься разработкой программного обеспечения

Ответ:

Задание 4.2.

В результате выполнения какой задачи оценки рисков в рамках аудита информационных систем, составляется спецификация рисков?

- А. Идентификация активов и угроз
- Б. Оценка вероятности возникновения инцидентов
- В. Оценка возможного ущерба от реализации угроз
- Г. Ранжирование рисков по степени критичности
- Д. Разработка мер по снижению рисков до приемлемого уровня

Ответ:

Задание 5.2.

Что НЕ относится к принципам комплаенс-аудита?

- А. Соответствие законодательству и нормативным актам
- Б. Соблюдение внутренних политик и процедур
- В. Прозрачность и доступность информации
- Г. Эффективность оценки

Ответ:

Задание 6.2.

Независимая оценка состояния информационных технологий и систем организации, направленная на выявление рисков, несоответствий стандартам и рекомендациям, а также на проверку эффективности и надежности функционирования ИТ-инфраструктуры – это ...

Ответ:

Задание 7.2.

К какому типу аудита информационных систем относится проверка соответствия законодательству и нормативным актам?

Ответ:

Задание 8.2.

Расположите в правильном порядке основные этапы проведения аудита информационной системы?

Ответ: Основные этапы аудита включают:

1. Подготовительный этап
2. Анализ документации
3. Опрос и интервьюирование
4. Презентация результатов
5. Практическая проверка
6. Подготовка отчета

Ответ:

Задание 9.2.

Перечислите документы и материалы необходимы для проведения аудита информационной системы?

Ответ:

Задание 10.2.

Перечислите и охарактеризуйте не менее трех методов тестирования, которые используются при аудите информационных систем.

Ответ:

Задание 11.2.

Какой критерий НЕ используется при выборе аудиторскую компанию для проведения внешнего аудита?

- А. Репутация и опыт компании в сфере ИТ-аудита
- Б. Наличие сертификатов и лицензий на проведение аудита
- В. Специализация на конкретных отраслях и стандартах
- Г. Стоимость услуг и условия сотрудничества
- Д. Местоположение компании

Ответ:

Задание 12.2.

На каком этапе аудита информационной безопасности проверяется актуальность процедур безопасности?

- А. Оценка текущего состояния защиты информации
- Б. Идентификация уязвимостей и угроз
- В. Проверка наличия и актуальности политик и процедур безопасности
- Г. Оценка эффективности используемых средств защиты
- Д. Анализ соответствия требованиям международных стандартов

Ответ:

Задание 13.2.

В каком разделе отчета по результатам аудита информационной системы отражают текущее состояние информационной системы?

- А. Введение с описанием целей и задач аудита
- Б. Подробное описание проведенного анализа и тестов
- В. Выводы и рекомендации по устранению выявленных недостатков
- Г. Приоритезация найденных проблем по уровню риска
- Д. План мероприятий по улучшению состояния информационных систем
- Е. Приложения с дополнительными материалами и доказательствами

Ответ:

Задание 14.2.

Какие аспекты готовности организации к инцидентам и катастрофам проверяют при аудите информационных систем? (возможны несколько вариантов ответа)

- А. Наличие плана реагирования на инциденты и катастрофы.
- Б. Система охраны организации.
- В. Периодический аудит резервных копий и планов восстановления.
- Г. Повышение квалификации персонала.
- Д. Наличие соглашений с внешними поставщиками услуг по восстановлению.

Ответ:

Задание 15.2.

Какой аспект общего влияния результатов аудита на общую стратегию развития организации отражает экономию от предотвращения возможных потерь вследствие инцидентов, связанных с информационной системой?

- А. Анализировать предложенные рекомендации и планы действий
- Б. Рассматривать возможные экономические последствия устранения выявленных проблем
- В. Оценивать улучшение безопасности и стабильности информационных систем

Г. Прогнозировать влияние улучшений на конкурентоспособность и репутацию организации

Д. Включать результаты аудита в стратегические планы развития ИТ-инфраструктуры

Ответ:

Задание 16.2.

Какую задачу выполняет аудит доступа??

Ответ:

Задание 17.2.

Что такое "план восстановления после сбоев"??

Ответ:

Задание 18.2.

Какие методы позволяют определить, насколько эффективно используется ИТ-бюджет?

Ответ:

Задание 19.2.

Перечислите основные проблемы, возникающие при проведении аудита информационных систем?

Ответ:

Задание 20.2.

Перечислите критерии готовности организации к инцидентам и катастрофам?

Ответ:

Ключи к оцениванию заданий

Вариант 1

№ задания	Верный ответ	Критерии оценивания
1.1	А	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
2.1	А	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
3.1	Г	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
4.1	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
5.1	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
6.1	Возможные варианты ответа: оценка соответствия ИТ-инфраструктуры требованиям законодательства и стандартов; выявление уязвимостей и недостатков в защите информации; проверка эффективности и оптимальности использования ресурсов; оценка уровня готовности к инцидентам и катастрофам; определение возможностей для улучшения процессов и технологий.	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
7.1	Международный стандарт ISO/IEC 27001 Управление информационной безопасностью.	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
8.1	3-4-1-2-5	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
9.1	Возможные варианты ответа: Независимо оценивать текущее состояние информационных систем и процессов. Идентифицировать риски и уязвимости. Формулировать рекомендации по устранению выявленных недостатков. Составлять объективные и обоснованные заключения. Консультировать руководство по вопросам улучшения ИТ-инфраструктуры.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
10.1	Возможные варианты ответа: Соответствие законодательству и нормативным актам. Соблюдение внутренних политик и процедур. Прозрачность и доступность информации. Независимость и объективность оценки. Своевременное реагирование на нарушения и недостатки.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие

11.1	Д	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
12.1	Д	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
13.1	Е	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
14.1	А, Б, В, Д	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
15.1	Г	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
16.1	Возможные варианты ответа: Распределение ролей и ответственности Регулярные встречи и обсуждения промежуточных результатов Обмен информацией и документами в режиме реального времени Совместное участие в разработке рекомендаций и планов действий Обратная связь и консультации по возникающим вопросам.	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
17.1	Возможные варианты ответа: Репутация и опыт компании в сфере ИТ-аудита. Наличие сертификатов и лицензий на проведение аудита. Специализация на конкретных отраслях и стандартах. Стоимость услуг и условия сотрудничества. Опыт работы с аналогичными организациями и проектами.	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
18.1	Отчет по результатам аудита должен содержать: Введение с описанием целей и задач аудита. Подробное описание проведенного анализа и тестов. Выводы и рекомендации по устранению выявленных недостатков. Приоритезация найденных проблем по уровню риска. План мероприятий по улучшению состояния информационных систем. Приложения с дополнительными материалами и доказательствами.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
19.1	Аудит информационной безопасности включает: Оценку текущего состояния защиты информации. Идентификацию уязвимостей и угроз. Проверку наличия и актуальности политик и процедур безопасности. Оценку эффективности используемых средств защиты (антивирусы, фаерволы, VPN и др.).	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие

	Анализ соответствия требованиям международных стандартов (ISO/IEC 27001, GDPR и др.)	
20.1	Влияние результатов аудита можно оценить следующим образом: Анализируя предложенные рекомендации и планы действий. Рассматривая возможные экономические последствия устранения выявленных проблем. Оценивая улучшение безопасности и стабильности информационных систем. Прогнозируя влияние улучшений на конкурентоспособность и репутацию организации. Включая результаты аудита в стратегические планы развития ИТ-инфраструктуры	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие

Вариант 2

№ задания	Верный ответ	Критерии оценивания
1.2	Г	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
2.2	А	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
3.2	В	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
4.2	А	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
5.2	Г	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
6.2	Аудит информационных систем	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
7.2	Комплаенс-аудит	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
8.2	1-3-2-5-6-4	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
9.2	Для проведения аудита могут потребоваться следующие документы и материалы: Политики и процедуры в области ИТ и информационной безопасности. Регламенты и инструкции по эксплуатации систем. Лог-файлы и журналы событий. Результаты предыдущих аудитов и проверок. Документация по проектированию и внедрению систем. Лицензии и сертификаты на программное обеспечение. Контракты с поставщиками и подрядчиками.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
10.2	Методы тестирования могут включать: Пен-тестинг (penetration testing) - имитация атак злоумышленников для выявления уязвимостей. Верификация кода - анализ исходного кода программ на наличие ошибок и уязвимостей. Мониторинг и анализ лог-файлов - отслеживание активности пользователей и систем. Тестирование отказоустойчивости - моделирование сбоев и аварий для проверки готовности к инцидентам. Социальная инженерия - тесты на подверженность сотрудников обманным манипуляциям.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
11.2	Д	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
12.2	В	1 балл – полное совпадение с верным ответом

		0 баллов – неверный ответ или его отсутствие
13.2	В	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
14.2	А, В, Д	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
15.2	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
16.2	Проверку прав и привилегий пользователей	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
17.2	Документ, описывающий действия в случае кризисной ситуации	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
18.2	Эффективность использования ИТ-бюджета можно оценить следующими методами: Сопоставление запланированных и фактических затрат. Анализ возврата инвестиций (ROI) от реализованных проектов. Сравнение стоимости аналогичных решений у конкурентов. Опрос пользователей и сотрудников о полезности и удобстве внедряемых технологий. Исследование экономической выгоды от повышения производительности и снижения рисков.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
19.2	Проблемы могут включать: Ограниченное время и ресурсы для проведения аудита. Недоступность необходимой документации и информации. Противодействие со стороны сотрудников, опасющихся критики своей работы. Отсутствие четких критериев оценки эффективности. Изменчивость и сложность современных информационных систем.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
20.2	К критериям готовности организации к инцидентам и катастрофам можно отнести: Наличие плана реагирования на инциденты и катастрофы. Проведение тренировок и симуляций Периодический аудит резервных копий и планов восстановления Обучение персонала действиям в чрезвычайных ситуациях Наличие соглашений с внешними поставщиками услуг по восстановлению	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие