

Федеральное государственное образовательное бюджетное учреждение
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

**Кафедра бизнес-информатики
Факультет информационных технологий и анализа больших данных**

Документ подписан усиленной неквалифицированной электронной подписью
Организация: Финансовый университет при Правительстве РФ
Утверждено: Проректор по учебной и методической работе Е.А. Каменева
Сертификат: QID5UnhTK2gTP5pLRgWjvvvCXJ0ufvNm
Дата: 07.05.2025 г.

Н. Н. Римский

Аудит информационных систем

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки

38.03.05 - Бизнес-информатика

Образовательная программа:

Цифровая трансформация управления бизнесом

Профиль

ИТ-менеджмент в бизнесе

Рекомендовано

*Факультет информационных технологий и анализа больших данных
(протокол №55 от 20.05.2025)*

Одобрено

*Кафедра бизнес-информатики
(протокол №9 от 28.04.2025)*

Москва 2025

Содержание

Наименование разделов РПД		Стр.
1.	Наименование дисциплины	5
2.	Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	5
3.	Место дисциплины в структуре образовательной программы	9
4.	Объем дисциплины(модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	9
5.	Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	10
5.1.	Содержание дисциплины	10
5.2.	Учебно-тематический план	12
5.3.	Содержание семинаров, практических занятий	13
6.	Перечень учебно-методического обеспечения для	16

	самостоятельной работы обучающихся по дисциплине	
6.1.	Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	16
6.2.	Перечень вопросов, заданий, тем для подготовки к текущему контролю	18
7.	Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	19
8.	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	26
9.	Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	28
10.	Методические указания для обучающихся по освоению дисциплины	29
11.	Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных	29

	справочных систем	
12.	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	30

1. Наименование дисциплины

«Аудит информационных систем».

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Код компетенции	Наименование компетенции	Индикатор достижения компетенции	Результаты обучения
ПКН-3	Способность применять аналитические системы и консультировать по вопросам разработки и развития аналитических систем работы с данными	1. Применяет аналитические системы работы с данными.	Знать: Типовые риски применения аналитических систем работы с данными. Лучшие практики применения аналитических систем работы с данными. Уметь: Консультировать по вопросам применения аналитических систем работы с данными. Находить недостатки в работе аналитических систем. Консультировать по вопросам разработки аналитических систем.
		2. Проводит анализ рынка аналитических систем работы с данными.	Знать: Типы аналитических систем работы с данными. Ключевая функционально

			<p>сть аналитических систем. Уметь: Выбирать оптимальное решение для современного ИТ по работе с данными.</p>
		<p>3. Консультирует по вопросам применения аналитических систем работы с данными.</p>	<p>Знать: Положительные и отрицательные стороны каждого из классов систем работы с данными. Лучшие практики использования аналитических систем работы с данными в современном ИТ. Уметь: Выявлять риски при использовании систем работы с данными. Выбирать оптимальную аналитическую систему для выбранной организации.</p>
ПКН-6	Способность проводить бизнес-анализ предметной области	1. Проводит обследование предприятия.	<p>Знать: Лучшие практики по влиянию процессов ИТ на организацию. Методологии по выявлению неэффективност и бизнес- процессов ИТ при</p>

			<p>обследовании организации.</p> <p>Уметь:</p> <p>Выявлять точки неэффективности и бизнес-процессов ИТ при обследовании организации. Предлагать рекомендации по их исправлению.</p>
		<p>2. Выявляет потребности и формирует требования к информационной системе.</p>	<p>Знать:</p> <p>Основные недостатки ключевых бизнес-процессов ИТ. Лучшие практики применения ключевых бизнес-процессов ИТ. Основные риски ИТ и ключевых бизнес-процессов ИТ. Основные положения нормативной базы в области защиты информации.</p> <p>Уметь:</p> <p>Формировать выводы по результатам аудита и бизнес-анализа процессов ИТ. Учитывать ИТ-риски при проведении бизнес-анализа ИС. Проводить бизнес-анализ по рискам</p>

			защиты информации и выбирать оптимальный подход к защите информации на основе выявленных рисков информационно й безопасности и законодательно й базы РФ.
		3. Проводит анализ рынка и под требования предлагает решения в области ИТ, проводит оценку предложенных решений.	Знать: Типовые риски ключевых бизнес-процессов ИТ. Лучшие практики по выявлению рисков бизнес-процессов ИТ. Уметь: Выбирать наилучшее ИТ решение на основе анализа рисков основных бизнес-процессов ИТ.
ПКП-4	Способность разрабатывать предложения для заказчиков по вопросам использования ИТ для трансформации бизнеса	1. Предлагает вариант изменения бизнес-модели предприятия/организации в условиях трансформации бизнеса.	Знать: Методики аудита процессов ИТ. Ключевые проблемы типовых ИТ процессов. Подходы к трансформации бизнеса. Методики использования ИТ для трансформации бизнеса. Уметь: Делать выводы по

			улучшению ИТ процессов и трансформации бизнеса.
		2. Консультирует заказчиков по выбору направлений изменений ИТ-ландшафта предприятия/организации с учетом целей трансформации бизнеса.	Знать: Лучшие практики по работе бизнес-процессов высокоскоростного ИТ. Уметь: Выбирать оптимальное решение по реализации цифровой трансформации организации.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Аудит информационных систем» относится к «Модулю "Информационные системы управления"»

4. Объем дисциплины(модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Очная форма обучения

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 7 (в часах)
Общая трудоемкость дисциплины	3/108	108
Контактная работа - Аудиторные занятия	30	30
<i>Лекции</i>	14	14
<i>Семинары,</i>	16	16

практические занятия		
Самостоятельная работа	78	78
Вид текущего контроля	Контрольная работа;	Контрольная работа
Вид промежуточной аттестации	Зачет;	Зачет

5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Введение в аудит ИТ и ИС.

Типы аудитов: внутренний и внешний. Применимость каждого из типов аудита для ИТ. Классификация аудита: регулярный независимый внешний аудит, регулярный внутренний ИТ-аудит, специальный ИТ-аудит. Этические основы деятельности аудитора. Подходы к корпоративному управлению (IT Governance) и место аудита в них. Уровни управления компанией и место корпоративного управления. Понятие, цели и задачи стратегического ИТ-аудита. Постановка целей и задач для ИТ и контроль их исполнения посредством проведения аудитов ИТ. Специфика задач, определяющих потребности компании в проведении ИТ-аудита. Обеспечение политик и стандартов в области ИТ корпоративным целям и стратегии. Место и роль аудита в цикле стратегического управления ИТ. Стратегический аудит как этап разработки ИТ-стратегии организации.

Основы управления рисками ИТ. Способы оценки рисков ИТ. Классические риски ИТ процессов. ИТ-аудит как средство управления рисками ИТ. Модель 3-х линий защиты.

Тема 2. Методологическая база аудита ИТ и ИС.

Роль методологической составляющей в организации и проведении ИТ-аудита. Стандарты внешнего аудита и их применение в ИТ. Стандарты внутреннего аудита по методологии Института Внутренних Аудиторов. Использование стандартов для аудита ИС.

С OBIT как методологическая база стратегического ИТ-аудита. COBIT как стандарт аудита ИТ-деятельности организации. Классическая модель стратегического аудита ИТ на основе COBIT . Структура материалов COBIT : руководство по аудиту в сфере ИТ. Мониторинг и контроль в методологии COBIT . Основные виды деятельности и риски ИТ в структуре ключевых доменов COBIT (планирование, реализация, обслуживание и контроль).

Мониторинг результативности использования и соответствия ИТ целям и задачам бизнеса: ISO 38500:2008.

Управление ИТ-процессами компании на основе ITSM (ITIL 4). Связь COBIT и ITSM . Влияние ITSM на аудит ИТ.

Тема 3. Технология и методы проведения аудита ИТ и ИС.

Базовые основы проведения стратегического ИТ-аудита и внутреннего ИТ-аудита (аудита бизнес-процессов). KPI организации и их связь с аудитом. Цели и задачи внутреннего ИТ-аудита. Идентификация причин дискомфорта руководства организации в связи с использованием ИТ. Процессы стратегического аудита. Типовые риски бизнес-процессов ИТ и способы их анализа. Оценка ИТ процессов на соответствие качеству и требованиям контроля. Управление эффективностью, мониторинг внутреннего контроля, соответствие требованиям регулирующих норм и корпоративного управления. Мониторинг и оценка системы внутреннего контроля. Обеспечение корпоративного управления ИТ. Проведение аудиторских процедур. Методы системной диагностики организации: методы выявления и сбора информации, диагностика информационных технологий, методы интервьюирования и анкетирования. Составление аудиторского отчета. Описание рекомендаций для руководства организации по улучшению бизнес-процессов. Жизненный цикл проекта ИТ-аудита. Выходная документация проекта ИТ-аудита. Пакеты прикладных программ для поддержки процедур проведения ИТ-аудита.

Тема 4. Аудит ключевых направлений ИТ.

Аудит информационных систем: инвентаризация действующих ИТ-решений, степень их документирования, уровень обеспеченности конечных пользователей и качества сопровождения.

Аудит ИТ-инфраструктуры: выявление сильных и слабых сторон конфигурации оборудования и сетевой инфраструктуры, определение надежности и пропускных характеристик.

Аудит бизнес-процессов: аудит ИТ персонала; аудит ИТ активов; аудит управления ИТ.

Аудит информационной безопасности. Метрики информационной безопасности на основе стандартов ISO/IEC, ГОСТ.

Аудит непрерывности бизнеса в контексте ИТ. Disaster recovery план и способы его составления.

Тема 5. Организационные аспекты проведения аудита ИТ и ИС.

Организация рабочих групп, обеспечивающих контроль и аудит ИТ. Роли и ответственности аудиторов. Команда проекта для проведения различных ИТ-аудитов организации. Логика взаимодействия Совета по корпоративному управлению и аудиторов. Российская и зарубежная практика проведения ИТ-аудита и оценка результатов для бизнеса.

5.2. Учебно-тематический план

Очная форма обучения

№ п/п	Наименование тем(разделов) дисциплины	Трудоемкость в часах				
		Всего	Контактная работа - Аудиторная работа			Самостоятельная работа
			Общая, в т.ч.:	Лекции	Семинары, практические занятия	
1	Введение в аудит ИТ и ИС.	20	4	2	2	16
2	Методологическая база аудита ИТ и ИС.	20	6	4	2	14
3	Техноло	22	6	2	4	16

	гия и методы проведения аудита ИТ и ИС.					
4	Аудит ключевых направлений ИТ.	28	10	4	6	18
5	Организационные аспекты проведения аудита ИТ и ИС.	18	4	2	2	14
	Итого	108	30	14	16	78

5.3. Содержание семинаров, практических занятий

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Введение в аудит ИТ и ИС.	Корпоративное управление ИТ: как ответственность высшего руководства и Совета директоров, включающая лидерство, организационные структуры и процессы, обеспечивающие соответствие ИТ текущим и стратегическим целям организации. ИТ аудит: основные понятия. Структура задач, обуславливающих проведение ИТ-аудита. Классификация ИТ-	Дискуссия, обсуждение, выполнение практических заданий.

	аудита. Роль ИТ-аудита в разработке ИТ-стратегии. Базовое управление ИТ рисками в организации и роль рисков при формировании ИТ-стратегии.	
Методологическая база аудита ИТ и ИС.	Стандарты аудита - оценка, использование и распространение. Трехуровневая организация продуктов СОВИТ. Организационные области применения. Взаимосвязь компонентов СОВИТ. Ключевые принципы организации методологии контроля СОВИТ. Определение целей ИТ и корпоративная архитектура. Бизнес и меры контроля в сфере ИТ. Специфика методологии, основанной на контроле. Особенности ITIL /ISO для подготовки и реализации процедур ИТ-аудита.	Дискуссия, разбор кейсов, выполнение и защита практических заданий.
Технология и методы проведения аудита ИТ и ИС.	Описание процесса «Оценка системы внутреннего контроля» для стратегического ИТ-аудита и аудита ИТ процессов, цели контроля (аудит системы внутреннего контроля), рекомендации по управлению. Описание процесса проведения ИТ-аудита. Методы выявления и сбора	Дискуссия, выполнение и защита практических заданий.

	<p>информации.</p> <p>Информационные технологии поддержки проведения процедур сбора и анализа данных для обследования ИТ-департамента (ИТ-процессов и т.п.).</p> <p>Методика диагностики информационных технологий.</p> <p>Разработка отчета о проведении стратегического ИТ-аудита.</p>	
Аудит ключевых направлений ИТ.	<p>Механики и примеры проведения аудита информационных систем и аудита ИТ инфраструктуры.</p> <p>Описание типовых рисков и аудиторских процедур для процессов:</p> <p>управление персоналом ИТ;</p> <p>управление ИТ активами; управление ИТ.</p> <p>Концепция информационной безопасности предприятия.</p> <p>Ключевые процессы информационной безопасности.</p> <p>Метрики информационной безопасности. Аудит ролевой модели доступа, аудит работы с персональными данными, аудит защиты от взломов.</p> <p>Аудит непрерывности ИТ.</p>	<p>Дискуссия, разбор кейсов, выполнение и защита индивидуальных практических заданий.</p>
Организационные аспекты проведения	Критерии выбора аудитора для ИТ-	Дискуссия, разбор кейсов, выполнение пр

аудита ИТ и ИС.	диагностики. Нормы и принципы работы аудитора. Совет по корпоративному управлению и аудиторская команда: практика взаимодействия. Анализ российской практики проведения ИТ-аудита: уровень достижения бизнес-целей.	активных заданий.
-----------------	---	-------------------

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Введение в аудит ИТ и ИС.	Обеспечение политик и стандартов в области ИТ корпоративным целям и стратегии организации. ИТ-аудит как средство управления рисками. Классические риски ИТ процессов. Модель 3-х линий защиты.	Изучение методических материалов по теме в электронном виде и рекомендуемых разделов основной и дополнительной литературы, интернет-источников. Подготовка к практическим занятиям.
Методологическая база аудита ИТ и ИС.	Структура материалов COBIT: Framework. Мониторинг результативности использования и соответствия ИТ целям и задачам бизнеса: ISO 38500:2008. Основы ITSM.	Изучение методических материалов по теме в электронном виде и рекомендуемых разделов основной литературы, интернет источников. Подготовка к

		практическим занятиям. Выполнение самостоятельных заданий.
Технология и методы проведения аудита ИТ и ИС.	Мониторинг системы внутреннего контроля. Подходы к отслеживанию выполнения рекомендаций по результатам ИТ-аудита. Пакеты прикладных программ для поддержки процедур проведения ИТ-аудита.	Изучение методических материалов по теме в электронном виде и рекомендуемых разделов основной и дополнительной литературы, интернет-источников. Выполнение индивидуальных домашних заданий.
Аудит ключевых направлений ИТ.	Основные бизнес-процессы ИТ в организации, их типовые риски и способы организации. Основы непрерывности бизнеса. Методы оценки рисков непрерывности бизнеса. Стандарты ISO и ГОСТ по информационной безопасности. Законодательство РФ и ЕС по персональным данным.	Изучение методических материалов по теме в электронном виде и рекомендуемых разделов основной и дополнительной литературы, интернет-источников. Выполнение индивидуальных домашних заданий.
Организационные аспекты проведения аудита ИТ и ИС.	Логика взаимодействия Совета по корпоративному управлению и аудиторов. Российская и зарубежная практика проведения ИТ-аудита и оценка результатов для бизнеса.	Изучение методических материалов по теме в электронном виде и рекомендуемых разделов основной и дополнительной литературы, интернет-источников. Выполнение индивидуальных домашних заданий.

6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю

Примерные темы для контрольной работы:

1. Разработка проекта проведения ИТ-аудита ИТ-процессов организации и подготовка отчетного документа.
2. Разработка комплектов документов для проведения интервьюирования персонала (высшего, среднего звена) для оценки степен вовлеченности руководства организации в деятельность службы ИТ, его внимания к развитию ИТ и значимости ИТ в основной деятельности.
3. Разработка проекта проведения ИТ-аудита информационных систем организации и подготовка отчетного документа.
4. Разработка программы аудита Информационной безопасности.
5. Разработка программы аудита непрерывности бизнеса.
6. Разработка программы аудита “Ролевая модель доступа”.
7. Разработка карты рисков ИС.
8. Разработка карты рисков бизнес-процесса ИТ.
9. Разработка программы аудита процесса управления инцидентами для компании по производству продуктов питания.
10. Разработка программы аудита процесса управления изменениями для коммерческого банка.

Пример задания для контрольной работы:

Коммерческий банк занимается выдачей потребительских кредитов и привлечением депозитов от физических лиц. В ИТ инфраструктуре банке присутствуют следующие компоненты: фронт-энд решение для кредитных представителей, которые общаются с клиентами; кредитный скорринг, в котором проходит принятие кредитного решения и автоматическая банковская система, в которой учитываются все операции. Все системы соединены между собой интеграционной шиной посредством использования синхронных сервисов. Процесс управления инцидентами описан в банке в специализированной регламенте.

Процесс учитывает в себе регистрацию инцидента, решение инцидента внутри ИТ с разделением зон ответственности и информирование заявителя о решении инцидента. Вся информация о зарегистрированных и решенных инцидентах структурирована и доступна. В среднем в год регистрируется 7500 инцидентов. Каждый год количество инцидентов растет на 15% при сохранении объема операций. Вы ИТ аудитор и вам поставлены следующие задачи:

1. Выявить риски присущие текущему процессу управления инцидентами.
2. Рассчитать объем выборки, который позволит верно оценить проблемы процесса.
3. Сформулировать программу аудита в следующей таблице выявив не менее 5 рисков:

Риск	Контроль	Ответственный	Аудиторские процедуры
Риск %проблема% в связи с %корневая причина проблемы%	Контроль за %описание риска%		Не менее 5 аудиторских процедур на один риск.

Дополнительная информация:

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях Кафедры бизнес-информатики.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень компетенций с указанием индикаторов их достижения в процессе освоения образовательной программы содержится в разделе 2. *Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине.*

Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний

ПКН-3 Способность применять аналитические системы и консультировать по вопросам разработки и развития аналитических систем работы с данными

1) 1. Применяет аналитические системы работы с данными.

Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции

Знать: Типовые риски применения аналитических систем работы с данными. Лучшие практики применения аналитических систем работы с данными.

Уметь: Консультировать по вопросам применения аналитических систем работы с данными. Находить недостатки в работе аналитических систем. Консультировать по вопросам разработки аналитических систем.

Типовые контрольные задания

Задание 1. Подготовьте план и программу аудита аналитической системы

Задание 2. Дайте рекомендации по минимизации рисков внедрения указанной ИС

Задание 3. Расскажите о лучших практиках применения систем типа DWH

2) 2. Проводит анализ рынка аналитических систем работы с данными.

Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции

Знать: Типы аналитических систем работы с данными. Ключевая функциональность аналитических систем.

Уметь: Выбирать оптимальное решение для современного ИТ по работе с данными.

Типовые контрольные задания

Задание 1. Описать функциональность систем типа DWH и предложить вендора по внедрению подобного решения в коммерческом банке.

Задание 2. Сравнить между собой OLAP-кубы и работу с данными на основе SaaS и предложить лучшее решение по внедрению в цифровой ИТ организации.

3) 3. Консультирует по вопросам применения аналитических систем работы с данными.

Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции

Знать: Положительные и отрицательные стороны каждого из классов систем работы с данными. Лучшие практики использования аналитических систем работы с данными в современном ИТ.

Уметь: Выявлять риски при использовании систем работы с данными. Выбирать оптимальную аналитическую систему для выбранной организации.

Типовые контрольные задания

Задание 1. Оцените риски использования массива данных.

Задание 2. Опишите риски, присущие методологии SCRUM.

Задание 3. Выберите оптимальную методологию разработки витрины данных сотового оператора.

ПKN-6 Способность проводить бизнес-анализ предметной области

1) 1. Проводит обследование предприятия.

Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции

Знать: Лучшие практики по влиянию процессов ИТ на организацию. Методологии по выявлению неэффективности бизнес-процессов ИТ при обследовании организации.

Уметь: Выявлять точки неэффективности бизнес-процессов ИТ при обследовании организации. Предлагать рекомендации по их исправлению.

Типовые контрольные задания

Задание 1. Опишите типовые риски ИТ в цифровом стартапе.

Задание 2. Проведите обследование ИТ подразделения в телекоммуникационной организации.

2) 2. Выявляет потребности и формирует требования к информационной системе.

Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции

Знать: Основные недостатки ключевых бизнес-процессов ИТ. Лучшие практики применения ключевых бизнес-процессов ИТ. Основные риски ИТ и ключевых бизнес-процессов ИТ. Основные положения нормативной базы в области защиты информации.

Уметь: Формировать выводы по результатам аудита и бизнес-анализа процессов ИТ. Учитывать ИТ риски при проведении бизнес-анализа ИС. Проводить бизнес-анализ по рискам защиты информации и выбирать оптимальный подход к защите информации на основе выявленных рисков информационной безопасности и законодательной базы РФ.

Типовые контрольные задания

Задание 1. Проведите бизнес-анализ рисков архитектуры организации.

Задание 2. Опишите 10 ключевых по вашему мнению ограничений по работе с персональными данными на основе ФЗ-152 “О персональных данных”

Задание 3. Какие существуют уровни обеспечения информационной безопасности согласно требованиям ФСТЭК.

3) 3. Проводит анализ рынка и под требования предлагает решения в области ИТ, проводит оценку предложенных решений.

Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции

Знать: Типовые риски ключевых бизнес-процессов ИТ. Лучшие практики по выявлению рисков бизнес-процессов ИТ.

Уметь: Выбирать наилучшее ИТ решение на основе анализа рисков основных бизнес-процессов ИТ.

Типовые контрольные задания

Задание 1. Опишите ключевые риски непрерывности бизнеса в части ИТ.

Задание 2. На основе анализа рисков выберите лучшую ИТ систему для кредитной организации.

ПКП-4 Способность разрабатывать предложения для заказчиков по вопросам использования ИТ для трансформации бизнеса

1) 1. Предлагает вариант изменения бизнес-модели предприятия/организации в условиях трансформации бизнеса.

Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции

Знать: Методики аудита процессов ИТ. Ключевые проблемы типовых ИТ процессов. Подходы к трансформации бизнеса. Методики использования ИТ для трансформации бизнеса.

Уметь: Делать выводы по улучшению ИТ процессов и трансформации бизнеса.

Типовые контрольные задания

Задание 1. Провести аудит процесса цифровизации.

Задание 2. Сформировать выводы по результатам аудита мобильного приложения.

2) 2. Консультирует заказчиков по выбору направлений изменений ИТ-ландшафта предприятия/организации с учетом целей трансформации бизнеса.

Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции

Знать: Лучшие практики по работе бизнес-процессов высокоскоростного ИТ.

Уметь: Выбирать оптимальное решение по реализации цифровой трансформации организации.

Типовые контрольные задания

Задание 1. На основе аудита ИТ процессов предложите оптимальное решение по цифровой трансформации книгопечатного производства.

Задание 2. Сформулируйте как будет работать процесс управления инцидентами в логике высокоскоростного ИТ.

Примеры практико-ориентированных заданий

В компании внедряется новая информационная система типа ERP . В процессе внедрения выяснилось, что для нее не разработана ролевая модель доступа. Известно, что в компании есть еще три информационных системы, для каждой из которых разработана своя ролевая модель доступа. Также известно, что текущие информационные системы будут передавать всю свою информацию в неизменном виде в новую систему типа ERP . ИТ-директор поручил вам провести аудиторскую проверку ролевой модели доступа в компании и предоставить рекомендации по изменению бизнес-процесса. Опишите:

1. Основные цели и задачи проведения аудиторской проверки ролевой модели доступа;

2. Риски, присущие описанной ситуации;
3. Рекомендации по изменению бизнес-процесса на основе рисков из буллита 2.

Примерные вопросы для подготовки к Зачету

1. Какие рекомендации хотело бы получить руководство организации по результатам аудита?
2. Проанализируйте логическую структуру периметра основных видов деятельности контроля и аудита.
3. Перечислите основные виды ИТ-аудита и их цели.
4. Какая информация должна быть собрана в процессе проведения внутреннего аудита?
5. Чем обусловлена необходимость приведения в соответствие сферы ИТ потребностям бизнеса и какова в этом роль ИТ-аудита?
6. В чем состоит помощь методологии COBIT
7. Сформулируйте основной принцип методологии COBIT
8. Что Вы понимаете под соответствиями требованиям регулирующих норм и корпоративного управления?
9. Может ли менеджмент быть уверен в том, что меры внутреннего контроля результативны и эффективны?
10. Сформируйте шаги проведения аудита информационной системы.

Методические материалы, определяющие процедуры оценивания знаний, умений

Приказ от 01.10.2024 №2187/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования в Финансовом университете».

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Нормативно-правовые акты:

1. Федеральный закон РФ "О персональных данных" от 27.07.2006 N 152-ФЗ
2. Федеральный закон РФ "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
3. Федеральный закон РФ "О коммерческой тайне" от 29.07.2004 N 98-ФЗ
4. Федеральный закон РФ "Об электронной подписи" от 06.04.2011 N 63-ФЗ
5. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ
6. General Data Protection Regulation, GDPR; Постановление 2016/679; EU

Основная литература:

1. Процессы управления информационными технологиями : Учебное пособие / А.Н. Бирюков Электрон. дан. Москва : КноРус , 2021 207 с. Режим доступа: book.ru Internet access <https://book.ru/book/936559> ISBN 978-5-406-02703-5
2. Внутренний аудит информационных систем : Монография / Л.В. Каширская, А.А. Ситнов Электрон. дан. Москва : КноРус , 2021 216 с. Режим доступа: book.ru Internet access <https://book.ru/book/941560> ISBN 978-5-406-08993-4

Дополнительная литература:

1. Методология и организация контроля в сфере информационных технологий : Монография / Л.В. Каширская, А.А. Ситнов Электрон. дан. Москва : Русайнс , 2020 271 с. Режим доступа: book.ru Internet access <https://book.ru/book/939714> ISBN 978-5-4365-5081-7
2. Практические основы бухгалтерского учета имущества организации. Практикум : Учебно-практическое пособие / С.М. Догучаева, Ж.А. Кеворкова Электрон. дан. Москва : КноРус , 2024 185 с. Режим доступа: book.ru Internet access <https://book.ru/book/952044> ISBN 978-5-406-12510-6

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Электронная библиотека Финансового университета (ЭБ)
<http://elib.fa.ru/> (<http://library.fa.ru/files/elibfa.pdf>)
2. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
3. Электронно-библиотечная система "Университетская библиотека ОНЛАЙН" <http://biblioclub.ru/>
4. "Деловая онлайн библиотека" издательства "Альпина Паблишер"
<http://lib.alpinadigital.ru/en/library>
5. Электронно-библиотечная система издательства "Лань"
<https://e.lanbook.com/>
6. Образовательная платформа "ЮРАЙТ" <https://urait.ru/>
7. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
8. Информационно-образовательный портал Финуниверситета:
<https://org.fa.ru>
9. •Электронная библиотека Финансового университета (ЭБ)
<http://elib.fa.ru/>
10. •Электронно-библиотечная система BOOK.RU <http://www.book.ru>
11. •Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
12. •Электронно-библиотечная система Znanium <http://www.znanium.ru/>
13. •Электронно-библиотечная система издательства «ЮРАЙТ»
<https://urait.ru/>
14. •Электронно-библиотечная система издательства Проспект
<http://ebs.prospekt.org/books>
15. •Электронно-библиотечная система издательства Лань
<https://e.lanbook.com/>

16. •Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>
17. •Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
18. •Национальная электронная библиотека <http://нэб.рф/>
19. •Электронная библиотека «Русская история» <http://history-lib.ru/>

10. Методические указания для обучающихся по освоению дисциплины

Студентам необходимо руководствоваться «Методическими рекомендациями по планированию и организации внеаудиторной самостоятельной работы по образовательным программам бакалавриата и магистратуры в Финансовом университете» (Приказ ректора № 1040_о от 11.05.2021) и данной рабочей программой дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

- Комплект лицензионного программного обеспечения:

1. Kaspersky
2. Microsoft Office (Windows)
3. Astra Linux

- Современные профессиональные базы данных и информационные справочные системы:

1. Информационно-правовая система «Гарант»
2. Информационно-правовая система «Консультант Плюс»
3. Электронная энциклопедия: <http://ru.wikipedia.org/wiki/Wiki>
4. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>

5. Электронно-библиотечная система Znanium <http://www.znanium.com>
6. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
7. Компьютерная техника
8. Консультант+

- Сертифицированные программные и аппаратные средства защиты информации

1. не предусмотрены

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. **Учебная аудитория** для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), набор демонстрационного оборудования (проектор, экран)

2. **Компьютерный класс** для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенный оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), персональные компьютеры, набор демонстрационного оборудования (проектор, экран)