

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

**Департамент бизнес-информатики  
Факультета информационных технологий и анализа больших данных**

**СОГЛАСОВАНО**

Председатель  
некоммерческой организации  
«Ассоциация крупнейших потребителей  
программного обеспечения и  
оборудования»

\_\_\_\_\_ Р.Ю. Абдулина  
**21.12.2023 г.**

**УТВЕРЖДАЮ**

Проректор по учебной и  
методической работе

\_\_\_\_\_ Е.А. Каменева  
**22.12.2023 г.**

**Н.Н. Римский**

**Аудит информационных систем**

Рабочая программа дисциплины  
для студентов, обучающихся по направлению подготовки  
**38.04.05 Бизнес-информатика**  
направленность программы:  
«Управление информационными технологиями в цифровой экономике»

*Рекомендовано Ученым советом Факультета информационных  
технологий и анализа больших данных  
(протокол № 39 от 20.12.2023 г.)*

*Одобрено Советом учебно-научного Департамента бизнес-информатики  
(протокол № 4 от 18.12.2023 г.)*

## *Содержание*

1. Наименование дисциплины.....	3
2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине.....	3
3. Место дисциплины в структуре образовательной программы.....	4
4. Объем дисциплины в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся.....	5
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий.....	5
5.1. Содержание дисциплины.....	5
5.2. Учебно-тематический план.....	7
5.3. Содержание семинаров, практических занятий.....	8
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.....	10
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы.....	10
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю.....	10
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	11
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.....	15
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	16
10. Методические указания для обучающихся по освоению дисциплины.....	16
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем.....	17
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	17

## 1.Наименование дисциплины

«Аудит информационных систем».

## 2.Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате изучения дисциплины у студентов должны быть сформированы следующие компетенции:

Таблица 1

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ПКН-9	Способность управлять непрерывностью бизнеса с использованием ИТ	1.Демонстрирует понимание необходимости и проектирует системы управления ИТ рисками.	Знать: Основные риски ИТ и ключевых бизнес-процессов ИТ  Уметь: Учитывать ИТ риски при проектировании ИС
		2.Владеет основами нормативного регулирования в области защиты информации.	Знать: Основные положения нормативной базы в области защиты информации  Уметь: Выбирать оптимальный подход к защите информации на основе выявленных рисков информационной безопасности и законодательной базы РФ.
		3.Владеет основными инструментами защиты информации.	Знать: Подходы к инструментам и рискам защиты информации  Уметь: Выбирать оптимальный инструмент защиты информации на основе выявленных рисков информационной безопасности.
ПКН-10	Способность разрабатывать и внедрять ИТ стратегии, проводить стратегический анализ и аудит ИС	1.Демонстрирует понимание особенности стратегического управления ИТ в условиях цифровой трансформации.  2. Владеет организаторскими навыками в ИТ-сфере.	Знать: <ul style="list-style-type: none"><li>• Методологии корпоративного управления</li><li>• Типы анализа и систематизации данных по стратегическому планированию ИТ.</li><li>• Методику проведения ИТ-диагностики (аудита) и критерии ее адаптации по конкретную</li></ul>

			<p>организацию (задачу)</p> <p>Уметь:</p> <ul style="list-style-type: none"> <li>• Составлять стратегию ИТ по результатам ИТ-диагностики (аудита).</li> <li>• Применять методы анализа и систематизации полученных данных для выработки рекомендаций по итогам проведения ИТ-диагностики</li> </ul>
		3.Формирует высокопрофессиональную ИТ-команду для выполнения поставленных задач.	<p>Знать:</p> <p>Специфику ключевых ИТ процессов компании, рисков, присущих данным процессам и квалификацию для управления указанными процессами.</p> <p>Уметь:</p> <p>Оценивать потенциальную возможность эффективно управлять ключевыми ИТ процессами сотрудниками ИТ подразделений компании.</p>
<b>ПК-2</b>	Способность управлять разработкой и внедрением цифровых платформ в деятельность организаций	1.Консультирует по вопросам применения цифровых платформ	<p>Знать:</p> <p>Типовые риски применения цифровых платформ.</p> <p>Уметь:</p> <p>Консультировать по вопросам рисков цифровых платформ.</p>
		Предлагает обоснованный выбор инструментальных средств и методологий для разработки цифровых платформ	<p>Знать:</p> <p>Типовые риски методологий для разработки цифровых платформ</p> <p>Уметь:</p> <p>Выбирать методологию для разработки цифровых платформ исходя из оценки ИТ рисков компании</p>

### 3. Место дисциплины в структуре образовательной программы

Дисциплина «Аудит информационных систем» относится к модулю направленности программы магистратуры части, формируемой участниками образовательных отношений ОП направления подготовки 38.04.05 Бизнес-информатика, направленность программы «Управление информационными технологиями в цифровой экономике».

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

Таблица 2

Вид учебной работы по дисциплине	Всего (в з/ед. и часах)	Модуль 4 (в часах)
<b>Общая трудоемкость дисциплины</b>	3 зач.ед. / 108 ч.	3 зач.ед. / 108 ч.
<i>Контактная работа - Аудитор- ные занятия</i>	30	30
<i>Лекции</i>	10	10
<i>Семинары, практические занятия</i>	20	20
<i>Самостоятельная работа</i>	78	78
Вид текущего контроля	контрольная работа	контрольная работа
Вид промежуточной аттестации	экзамен	экзамен

**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.**

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. Поставка целей и задач для ИТ и контроль их исполнения посредством проведения аудитов ИТ. Уровни управления компанией и место корпоративного управления. Понятие, цели и задачи стратегического ИТ-аудита. Место и роль аудита в цикле стратегического управления ИТ. Специфика задач, определяющих потребности компании в проведении ИТ-аудита. Обеспечение политик и стандартов в области ИТ корпоративным целям и финансовой стратегии. Стратегический аудит как этап разработки ИТ-стратегии организации. ИТ-аудит как средство управления рисками. Основы управления рисками. Способы оценки рисков ИТ. Классические риски ИТ процессов. Модель 3-х линий защиты.

**Тема 2. Методологическая база стратегического ИТ-аудита.**

Роль методологической составляющей в организации и проведении ИТ-аудита. COBIT как методологическая база стратегического ИТ-аудита. COBIT как стандарт аудита ИТ-деятельности. 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 ИТ-аудита.**

Базовые основы проведения стратегического ИТ-аудита и внутреннего ИТ-аудита (аудита бизнес-процессов). КРІ 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 бизнес-процессов 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 стратегического аудита ИТ.**

Организация рабочих групп, обеспечивающих контроль и аудит ИТ. Роли и ответственности аудиторов. Команда проекта стратегического ИТ-аудита 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

Таблица 3

№ п/п	Наименование темы (раздела) дисциплины	Трудоемкость в часах					Формы текущего кон- троля успеваемо- сти
		Всего	Контактная работа- Аудиторная работа			Самосто- ятельная работа	
			Общая	Лекции	Семинары, практические занятия		
1	Введение в аудит ИТ	20	4	2	2	16	Дискуссия, обсуждение, выполнение практических заданий
2	Методологическая база стратегического ИТ-аудита	17	3	1	2	14	Дискуссия, обсуждение, выполнение практических заданий
3	Технология и методы проведения ИТ-аудита	22	6	2	4	16	Дискуссия, обсуждение, выполнение практических заданий
4	Аудит ключевых бизнес-процессов ИТ	34	14	4	10	20	Дискуссия, обсуждение, выполнение практических заданий
5	Организационные аспекты проведения стратегического аудита ИТ	15	3	1	2	12	Подготовка к контрольной работе
	В целом по дисциплине	108	30	10	20	78	Контрольная работа
	Итого в %:		28	33	67	72	

\*объем контактной работы в очно-заочной/заочной формах обучения и индивидуальных учебных планах определяется соответствующими учебными планами. Темы, реализуемые в виде контактной работы, определяются преподавателем самостоятельно, исходя из уровня их сложности.

### 5.3. Содержание практических и семинарских занятий

Таблица 4

Наименование темы (раздела) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8, 9	Формы проведения занятий
Тема 1. Введение в аудит ИТ	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-аудита. Роль ИТ-аудита в разработке ИТ-стратегии. Базовое управление ИТ рисками в организации и роль рисков при формировании ИТ-стратегии. 8-1,4,5; 9-1-15	Дискуссия, обсуждение, выполнение практических заданий
Тема 2. Методологическая база стратегического ИТ-аудита	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. 8-3,5; 9-1-15	Дискуссия, разбор кейсов, выполнение и защита практических заданий
Тема 3. Технология и методы проведения ИТ-аудита	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 информации. Информационные технологии поддержки проведения процедур сбора и анализа данных для обследования ИТ-департамента (ИТ-процессов и т.п.). Методика диагностики информационных технологий. Разработка отчета о проведении стратегического ИТ-аудита 8-1,3,4,5; 9-1-14	Дискуссия, выполнение и защита практических заданий
Тема 4. Аудит ключевых	Механики и примеры проведения аудита информационных систем и	Дискуссия, разбор кейсов, выполнение и



бизнес-процессов ИТ	аудита ИТ инфраструктуры. Описание типовых рисков и аудиторских процедур для процессов: управление персоналом ИТ; управление ИТ активами; управление ИТ. Концепция информационной безопасности предприятия. Ключевые процессы информационной безопасности. Метрики информационной безопасности. Аудит ролевой модели доступа, аудит работы с персональными данными, аудит защиты от взломов. Аудит непрерывности ИТ. 8-1,2,3,4,5; 9-1-15	защита индивидуальных практических заданий
Тема 5. Организационные аспекты проведения стратегического аудита ИТ	Критерии выбора аудитора для ИТ-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. 8-2; 9-1-15	Дискуссия, разбор кейсов, выполнение практических 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

Таблица 5

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Тема 1. Введение в аудит ИТ	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.
Тема 2. Методологическая база стратегического ИТ-аудита	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.
Тема 3. Технология и методы проведения ИТ-аудита	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.
Тема 4. Аудит ключевых бизнес-процессов 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.
Тема 5. Организационные аспекты проведения стратегического аудита ИТ	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 степеней 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

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

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

Перечень компетенций представлен в разделе 2, который характеризует перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

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

Таблица 6

Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции	Типовые контрольные задания
<b>ПКН-9</b> Способность управлять непрерывностью бизнеса с использованием ИТ	1. Демонстрирует понимание необходимости и проектирует системы управления ИТ рисками.	Знать: Основные риски ИТ и ключевых бизнес-процессов ИТ  Уметь: Учитывать ИТ риски при проектировании ИС	Задание 1. Опишите типовые риски ИТ в цифровом стартапе. Задание 2. Опишите ключевые риски непрерывности бизнеса в части ИТ.
	2. Владеет основами нормативного регулирования в области защиты информации.	Знать: Основные положения нормативной базы в области защиты информации	Задание 1. Опишите 10 ключевых по вашему мнению ограничений по работе с персональными данными на основе ФЗ-152 “О персональных данных”

		<p>Уметь:</p> <p>Выбирать оптимальный подход к защите информации на основе выявленных рисков информационной безопасности и законодательной базы РФ.</p>	<p>Задание 2.</p> <p>Какие существуют уровни обеспечения информационной безопасности согласно требованиям ФСТЭК.</p>
	<p>3. Владеет основными инструментами защиты информации.</p>	<p>Знать:</p> <p>Подходы к инструментам и рискам защиты информации</p> <p>Уметь:</p> <p>Выбирать оптимальный инструмент защиты информации на основе выявленных рисков информационной безопасности.</p>	<p>Задание 1. Опишите программу аудита непрерывности бизнеса в коммерческом банке.</p> <p>Задание 2.</p> <p>Составьте disaster recovery план для конкретного риска.</p>
<p><b>ПKN-10</b></p> <p>Способность разрабатывать и внедрять ИТ стратегии, проводить стратегический анализ и аудит ИС</p>	<p>1. Демонстрирует понимание особенности стратегического управления ИТ в условиях цифровой трансформации.</p> <p>2. Владеет организаторскими навыками в ИТ-сфере.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>• Методологии корпоративного управления</li> <li>• Типы анализа и систематизации данных по стратегическому планированию ИТ.</li> <li>• Методику проведения ИТ-диагностики (аудита) и критерии ее адаптации по конкретную организацию (задачу)</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>• Составлять стратегию ИТ по результатам ИТ-диагностики (аудита).</li> <li>• Применять методы анализа и</li> </ul>	<p>Задание 1. Выявите риски, присущие описанному процессу. На основе выявленных рисков составьте стратегию развития ИТ.</p> <p>Задание 2. Опишите бизнес-процесс проведения аудита по указанному процессу</p> <p>Задание 3. Опишите данные, на основе которых строится ИТ стратегия указанной организации</p>

		систематизации и полученных данных для выработки рекомендаций по итогам проведения ИТ-диагностики	
	3.Формирует высокопрофессиональную ИТ-команду для выполнения поставленных задач.	<p>Знать:          Специфику ключевых ИТ процессов компании, рисков, присущих данным процессам и квалификацию для управления указанными процессами.</p> <p>Уметь:          Оценивать потенциальную возможность эффективно управлять ключевыми ИТ процессами сотрудниками ИТ подразделений компании.</p>	<p>Задание 1. Опишите программу аудита по указанному ИТ процессу.</p> <p>Задание 2. Опишите типовые риски указанного ИТ процесса</p>
<b>ПК-2</b> Способность управлять разработкой и внедрением цифровых платформ в деятельность организаций	1.Консультирует по вопросам применения цифровых платформ	<p>Знать:          Типовые риски применения цифровых платформ.</p> <p>Уметь:          Консультировать по вопросам рисков цифровых платформ.</p>	<p>Задание 1. Подготовьте план и программу аудита ИС</p> <p>Задание 2. Дайте рекомендации по минимизации рисков внедрения указанной ИС</p>
	2.Предлагает обоснованный выбор инструментальных средств и методологий для разработки цифровых платформ	<p>Знать:          Типовые риски методологий для разработки цифровых платформ</p> <p>Уметь:          Выбирать методологию для разработки цифровых платформ исходя из оценки ИТ рисков компании</p>	<p>Задание 1. Опишите риски, присущие методологии SCRUM</p> <p>Задание 2. Выберете оптимальную методологию разработки нового мобильного предложения сотового оператора.</p>

*Примерные вопросы к экзамену:*

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 соответствовать регулирующим требованиям через соответствие с общепринятыми стандартами корпоративного управления (COSO) и мерами контроля в сфере ИТ, которые ожидают видеть регулирующие органы и внешние аудиторы.
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.

*Примерные практические задания к экзамену:*

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.

*Пример экзаменационного билета:*

1. 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:

4. Основные цели и задачи проведения аудиторской проверки ролевой модели доступа (10 баллов);
  5. Риски, присущие описанной ситуации (15 баллов);
  6. Рекомендации по изменению бизнес-процесса на основе рисков из буллита 2 (15 баллов).
2. Раскройте: непрерывность бизнеса, ключевые риски непрерывности бизнеса, disaster recovery plan. (20 баллов).

***Методические материалы, определяющие процедуры оценивания  
знаний, умений***

Приказ от 23.03.2017 №0557/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по программам бакалавриата и магистратуры в Финансовом университете».

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

***Основная:***

1. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 269 с. - ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/1843184> (дата обращения: 14.02.2024). – Текст : электронный.
2. Бирюков, А. Н. Процессы управления информационными технологиями: учебное пособие для направлений бакалавриата и магистратуры "Бизнес-информатика" / А. Н. Бирюков; Финуниверситет – Москва : Кнорус, 2021. - 208 с. - Бакалавриат и магистратура.- Текст : непосредственный. – То же. – 2021. – ЭБС BOOK.ru. - URL: <https://book.ru/book/936559> (дата обращения: 14.02.2024). – Текст : электронный.

***Дополнительная:***

3. Грекул, В. И. Аудит информационных технологий: учебник для вузов / Грекул В. И. - Москва : Гор. линия-Телеком, 2015. - 154 с. - ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/555524> (дата обращения: 14.02.2024). – Текст : электронный.
4. Булыга, Р. П. Аудит бизнеса: учебник для студентов магистратуры, обучающихся по направлениям подготовки "Экономика", "Финансы и кредит", "Государственный аудит", "Менеджмент"/ Р. П. Булыга. – Москва : Юнити-Дана, 2017, 2021. - 264 с. - (Серия «Magister»). - Текст : непосредственный. - То же. - 2021. - ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/1352931> (дата обращения: 14.02.2024); ЭБС Университетская библиотека online. - URL: <https://biblioclub.ru/index.php?page=book&id=682405> (дата обращения: 14.02.2024). - Текст : электронный.

5. Ситнов, А. А. Международные стандарты аудита: учебник для студ. вузов, обуч. по напр. "Экономика", квалификация (степень) "Магистр" / А. А. Ситнов; Финуниверситет. – Москва : Юнити-Дана, 2014. - 239 с. – Текст: непосредственный. - (Серия «Magistei»). - То же. - 2017. - ЭБС ZNANIUM. - URL: <http://znanium.com/catalog/product/1028688> (дата обращения: 14.02.2024). – Текст : электронный.
6. Ситнов, А. А. Аудит информационных систем: Монография для магистров, обуч. по спец. 08.00.13 "Математич. и инструментальные методы экономики", 08.00.12 "Бух. учет, статистика" и др. междисциплинарным спец. / А. А. Ситнов, А. И. Уринцов; Финуниверситет. – Москва : Юнити-Дана, 2014. - 239 с. – Текст : непосредственный.

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

1. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru>
2. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
3. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru>
4. Электронно-библиотечная система Znanium <http://www.znanium.com>
5. Электронно-библиотечная система издательства «ЮРАЙТ» <https://www.urait.ru>
6. Электронно-библиотечная система издательства «Лань» <https://e.lanbook.com>
7. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru>
8. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
9. Национальная электронная библиотека <http://нэб.рф>
10. Информационный портал [www.cnews.ru](http://www.cnews.ru) [Электронный ресурс], режим доступа: [www.cnews.ru](http://www.cnews.ru)
11. Информационный портал [habrahabr.ru](http://habrahabr.ru) [Электронный ресурс], режим доступа: [habrahabr.ru](http://habrahabr.ru), 2014
12. Gartner - аналитический ресурс в области ИТ <http://www.gartner.com>
13. COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2019 [Электронный ресурс], режим доступа <https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9ZEAS>
14. CIT forum <http://www.citforum.ru>
15. Портал iTeam – Технологии корпоративного управления <http://www.iteam.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**

11.1. Комплект лицензионного программного обеспечения:

1. ОС Astr Linux,
2. LibreOffice
3. Антивирус Kaspersky

11.2 Современные профессиональные демонстрационные и информационные справочные системы:

1. Консультант Плюс.

11.3 Сертифицированные программные и аппаратные средства защиты информации:

Не предусмотрены.

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

Помещения для проведения лекций, семинарских занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.