



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

Кафедра экономической безопасности и управления рисками
Факультет экономики и бизнеса

Документ подписан усиленной неквалифицированной электронной подписью.

Организация: «ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»

Сертификат: B7MhWXPPlg9wVnM/cb1YzKCKTSv28u1r

Утверждено: Проректор по учебной и методической работе, Е.А. Каменева

Дата: 23.10.2025 г.

А.С. Бабанская

Анализ и выявление схем корпоративного мошенничества

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки
38.03.01 - Экономика,

Образовательная программа «Финансовая разведка и управление рисками бизнеса»

Рекомендовано

*Факультет экономики и бизнеса
(протокол № 7 от 21.04.2026 г.)*

Одобрено

*Кафедра экономической безопасности и управления рисками
(протокол № 09 от 17.03.2026 г.)*



Содержание

1. Наименование дисциплины	3
2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	3
3. Место дисциплины в структуре образовательной программы	
4. Объем дисциплины (модуля) 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	6
5.1. Содержание дисциплины	6
5.2. Учебно – тематический план	9
5.3. Содержание семинаров, практических занятий	10
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	14
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	14
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	18
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	21
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	18
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	18
10. Методические указания для обучающихся по освоению дисциплины	30
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)	8
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	31



1. Наименование дисциплины

Анализ и выявление схем корпоративного мошенничества

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

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
ПКН-4	Способность оценивать показатели деятельности экономических субъектов	Проводит анализ внешней и внутренней среды ведения бизнеса, выявляет основные факторы экономического роста, оценивает эффективность формирования и использования производственного потенциала экономических субъектов.	Знать: методы анализа внешней и внутренней среды организации для выявления факторов, способствующих мошенничеству, и оценки их влияния на экономическую безопасность бизнеса. Уметь: выявлять уязвимые бизнес-процессы и ключевые риски мошенничества на основе анализа макро- и микросреды организации.
		Рассчитывает и интерпретирует показатели деятельности экономических субъектов.	Знать: систему ключевых финансовых и нефинансовых показателей, используемых для выявления признаков мошенничества (в т. ч. индикаторы моделей Бениша, Роскаса и др.). Уметь: рассчитывать и анализировать показатели финансовой отчетности и операционных процессов для обнаружения аномалий данных и признаков мошеннических схем.
ПКП-2	Способность выявлять, документировать и анализировать риски, связанные с отмыванием доходов, полученных преступным путем, и финансированием терроризма, устанавливать признаки сомнительных операций и сделок, а также фиксировать соответствующие сведения в организации	Проводить анализ операций и сделок для выявления признаков сомнительных транзакций.	Знать: инструментарий финансовых расследований, типовые схемы мошенничества в ключевых бизнес-процессах (закупки, продажи, управление активами и др.) и их индикаторы и признаки. Уметь: применять инструментарий финансовых расследований, в т.ч. аналитические и детальные процедуры для выявления подозрительных операций и транзакций в финансовой и операционной деятельности организации.
		Документировать выявленные риски и составлять отчеты для представления руководству или контролирующим органам.	Знать: требования к оформлению документации по выявленным рискам мошенничества, структуру и содержание отчетов для руководства, контрольно-надзорных и правоохранительных органов. Уметь: систематизировать доказательства, оформлять акты расследова-



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
			ний и составлять отчёты о выявленных нарушениях с рекомендациями по их устранению.
		Использовать автоматизированные системы мониторинга для выявления аномалий в финансовых потоках.	Знать: принципы работы и функционал ИТ-систем для противодействия мошенничеству (DLP, фрод-мониторинг и др.), а также типы и виды аномалий. Уметь: моделировать действия оператора автоматизированных систем мониторинга: составлять запросы на проверку контрагентов, задавать фильтры для выявления аномалий, оценивать релевантность срабатываний; формулировать аналитические выводы на основе анализа структурированных и неструктурированных данных.



3. Место дисциплины в структуре образовательной программы

Дисциплина «Анализ и выявление схем корпоративного мошенничества» относится к «Модулю "Управление рисками корпоративного мошенничества (FRAUD)"».

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 6 (в часах)
Общая трудоемкость дисциплины	3/108	108
Контактная работа – Аудиторные занятия	34	34
<i>Лекции</i>	<i>16</i>	<i>16</i>
<i>Семинары, практические занятия</i>	<i>18</i>	<i>18</i>
<i>Самостоятельная работа</i>	<i>74</i>	<i>74</i>
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. Сущность, виды и схемы мошенничества в организациях

Экономическая природа мошенничества в организациях. Факторы и причины развития мошенничества в организациях. Влияние внешней и внутренней среды на развитие мошенничества в организациях. Влияние мошенничества на финансовую устойчивость и обеспечение экономической безопасности бизнеса, риски и угрозы. Современные виды мошенничества в организациях. Классификация видов мошенничества в модели Ассоциации дипломированных экспертов по мошенничеству (Association of Certified Fraud Examiners) известной как «дерево мошенничества». Характеристика отдельных видов мошенничества в бизнес-среде: искажение финансовой отчетности, присвоение активов, коррупция. Классификация видов мошенничества по объекту посягательства и мотивам. Классификация видов мошенничества по субъектам (руководство, сотрудники, контрагенты, внешние злоумышленники). Характеристика отдельных типов мошенничества: мошенничество сотрудников, мошенничество руководства, инвестиционное мошенничество, мошенничество покупателей, мошенничество продавцов. Классификация видов мошенничества по способу реализации (фальсификация документов, злоупотребление полномочиями, сговор и др.). Иные классификации мошенничества.

Наиболее уязвимые бизнес-процессы организаций, подверженные мошенническим действиям. Бизнес-процессы, подверженные риску мошенничества (факторы риска, факторы, снижающие риск, практические примеры схем): закупки, капитальное строительство и ремонт, продажи, управление запасами, управление персоналом, привлечение и размещение денежных средств, искажение финансовой отчетности и другие. Схемы и способы противоправных действий мошенников. Схемы присвоения финансовых результатов, в том числе схемы с участием сбытовых, закупочных, производственных, холдинговых компаний. Основные способы мошенничества в части присвоения активов и манипулирования с отчетностью, а также их последствия. Уязвимости при цифровой трансформации бизнеса. Мошенничество с использованием искусственного интеллекта (deepfake-схемы в виде подделки голоса и видео руководителей, ИИ-фишинговые схемы, создание фальшивых документов нейросетями). Мошенничество с использованием виртуальных активов и криптовалют. Индикаторы мошенничества и злоупотреблений. Признаки мошенничества со стороны менеджеров. Признаки мошенничества со стороны наемных работников. Признаки мошенничества со стороны руководства и топ-менеджмента. Признаки кибермошенничества в отношении компании.

Тема 2. Методы и инструменты для выявления и расследования схем мошенничества

Правовая основа расследования мошенничества в организациях. Руководство по проведению внутренних расследований в организациях ISO/TS 37008:2023. Форензик - как эффективный инструмент выявления и предотвращения мошенничества. Форензик-экспертиза: Методические аспекты форензика как инструмента выявления и предотвращения мошеннических действий в деятельности экономических субъектов. Проведение расследования. Цели и задачи расследования, управление процессом расследования мошенничества, сбор доказательств, взаимодействие с правоохранительными органами (привлечение к ответственности), информационно-технологические средства в расследовании и обнаружении мошенничества, интервью как элемент расследования мошенничества и основные методы его проведения. Управление процессом расследования мошенничества в организации: подготовка и планирование, выполнение и сбор доказательств, отчетность и завершение расследования. Квадрат доказательств. Документирование расследования. Завершение расследования. Отчет по делу о мошенничестве.



Инструменты для привлечения к ответственности и возмещения ущерба. Место и роль правоохранительных органов в расследовании мошенничества в организации.

Инструменты выявления и расследования мошенничества в организации. Анализ существующих методов и способов расследования мошенничества: что можно и что нельзя внутренним службам коммерческой организации (ограничения, накладываемые законодательством Российской Федерации). Способы и приемы выявления мошенничества в деятельности организаций. Процедуры для выявления индикаторов нарушений: аналитические процедуры, детальные процедуры, анализ нефинансовой информации. Использование аналитических процедур для выявления мошенничества. Шесть этапов алгоритма выявления мошенничества в организациях, в том числе анализ качества элементов отчетности, анализ крупных сделок с активами, анализ обоснованности стоимости активов, маркетинговый анализ, анализ соответствия производительности ресурсов отраслевому (рыночному) уровню, анализ рентабельности компании и ее контрагентов. Анализ внешней и внутренней среды ведения бизнеса. Методы и приемы документальной проверки. Признаки искажения и мошенничества, выявляемые при проверке первичной и сводной учетной документации. Методы физической (формальной) проверки. Осмотры, обследования, обмеры, контрольные запуски. Процедуры проверки физического наличия активов (инвентаризации) при наличии признаков мошенничества. Инструменты на основе искусственного интеллекта для предиктивного выявления мошенничества. Цифровые каналы сообщения о нарушениях.

Тема 3. Анализ и признаки противоправных схем мошенничества в организациях

Анализ существующей системы внутреннего контроля. Анализ и сравнение финансовых и нефинансовых показателей. Анализ сообщений, поступивших по горячей линии. Анализ неофициальной информации. Проведение тестирований на основе выборки. Признаки мошенничества, обнаруживаемые в документах бухгалтерского учета. Анализ и выявление схем мошенничества сотрудников и руководства. Признаки мошенничества со стороны сотрудников, наводки и жалобы, изменения в поведении и образе жизни, биографические признаки. Анализ нестандартных решений руководителей, скрытых соглашений, отклонений от корпоративных процедур. Признаки незаконных выплат сотрудникам и кадровые аномалии. Аномалии в операциях с активами и признаки их незаконного вывода. Подходы к выявлению хищений и других нарушений обращения денежных средств (наличные и безналичные). Анализ и выявление нарушений обращения материальных активов (запасы, ТМЦ). Аномалии при анализе операций с внеоборотными активами (основные средства и нематериальные активы). Анализ и выявление схем мошенничества покупателей и поставщиков. Признаки мошенничества в расчетных операциях. Анализ закупочного процесса и кредиторской задолженности, признаки подделки первичных документов и сговора с поставщиками. Анализ продаж и дебиторской задолженности. Выявление фиктивных продаж. Параллельный бизнес и его признаки. Выявление мошенничества с финансовыми результатами. Анализ незаконных схем занижения и завышения финансовых результатов. Анализ и выявление схем инвестиционного мошенничества. Финансовые операции, подверженные риску мошенничества. Признаки мошенничества с ценными бумагами. Признаки мошенничества при кредитовании. Признаки мошенничества при инвестировании в реальные проекты и интеллектуальные ценности. Состав ключевых финансовых индикаторов для выявления схем инвестиционного мошенничества. Выявление злоупотреблений в сфере цифровых финансовых инструментов: анализ аномальных операций с токенами, смарт-контрактами и цифровыми финансовыми активами. Признаки фальсификации, обнаруживаемые через цифровые каналы: анализ метаданных документов, цифровых следов в корпоративных системах.

Искажение и фальсификация информации в бухгалтерской (финансовой) отчетности как признак экономического преступления и способ мошенничества. Недобросовестное составление бухгалтерской (финансовой) отчетности: институционально-правовой аспект. Факторы, побуждающие и создающие условия для мошенничества с бухгалтерской (финансовой) отчетностью. Обзор известных случаев мошенничества с бухгалтерской (финансовой) отчетностью в России и за рубежом. Взаимосвязь между



фальсификацией бухгалтерской (финансовой) отчетности и банкротством экономического субъекта. Последствия мошенничества с бухгалтерской (финансовой) отчетностью. Виды искажений и фальсификации бухгалтерской (финансовой) отчетности. Признаки мошенничества в бухгалтерской (финансовой) отчетности. Анализ и выявление искажений бухгалтерской (финансовой) отчетности. Состав ключевых финансовых индикаторов для выявления мошенничества в бухгалтерской (финансовой) отчетности. Карта нормативных отклонений финансовых индикаторов для моделей Бениша (M-Score) и Роксаса (Roxas' Model). Прочие аналитические модели для выявления фальсификации бухгалтерской (финансовой) отчетности и интерпретация их результатов.

Тема 4. Использование информационных технологий для выявления и расследования мошенничества в организациях

Актуальность и преимущества использования современных информационных технологий при выявлении и расследовании мошенничества в организациях. Особенности информационных решений в сфере противодействия мошенничеству. Перечень информационных технологий для анализа, проведения расследований и выявления мошенничества. Системы DLP, фрод-мониторинга, спам-фильтры, системы мониторинга корпоративной почты, системы контроля за действиями пользователя как инструменты выявления и противодействия мошенничеству в организациях. Аналитика данных. Этапы аналитики данных при расследовании мошенничества. Сбор и подготовка данных при расследовании мошенничества. Методы и алгоритмы обнаружения мошенничества. Автоматизация работы цифровых каналов сообщения о нарушениях. Логика расследования, формулировки и тестирование гипотез о мошенничестве. Виды и группы выявляемых аномалий.

Структурированные и неструктурированные данные. Извлечение и подготовка данных для анализа. Проверка качества и достоверности данных. Характеристика структурированных данных. Анализ структурированных данных: традиционный и современный подходы. Аномалии структурированных данных. Подходы к выявлению аномалий в структурированных данных. Характеристика неструктурированных данных. Информационные источники для анализа неструктурированных данных. Сбор и подготовка информации для анализа. Анализ неструктурированных данных для выявления признаков мошенничества. Возможные риски, связанные с анализом данных в электронном виде. Технологии искусственного интеллекта и машинного обучения в антифрод-системах. Роль блокчейн-аналитики в расследовании инцидентов мошенничества.



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	Сущность, виды и схемы мошенничества в организациях	26	8	4	4	18
2	Методы и инструменты для выявления и расследования схем мошенничества	26	8	4	4	18
3	Анализ и признаки противоправных схем мошенничества в организациях	30	10	4	6	20
4	Использование информационных технологий для выявления и расследования мошенничества в организациях	26	8	4	4	18
В целом по дисциплине		108	34	16	18	74



5.3. Содержание семинаров, практических занятий

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Сущность, виды и схемы мошенничества в организациях	• Факторы и причины развития мошенничества в организациях. • Современные виды мошенничества в организациях. • Классификация видов мошенничества в модели Ассоциации дипломированных экспертов по мошенничеству (Association of Certified Fraud Examiners) известной как «дерево мошенничества». • Характеристика отдельных видов мошенничества в бизнес-среде: искажение финансовой отчетности, присвоение активов, коррупция. • Классификация видов мошенничества по субъектам (руководство, сотрудники, контрагенты, внешние злоумышленники). • Характеристика отдельных типов мошенничества: мошенничество сотрудников, мошенничество руководства, инвестиционное мошенничество, мошенничество покупателей, мошенничество продавцов. • Бизнес-процессы, подверженные риску мошенничества (факторы риска, факторы, снижающие риск, практические примеры схем): закупки, капитальное строительство и ремонт, продажи, управление запасами, управление персоналом, привлечение и размещение денежных средств, искажение финансовой отчетности и другие. • Схемы присвоения финансовых результатов, в том числе схемы с участием сбытовых, закупочных, производственных, холдинговых компаний. • Основные способы мошенничества в части присвоения активов и манипулирования с отчетностью, а также их последствия. • Индикаторы мошенничества и злоупотреблений. • Признаки кибермошенничества в отношении компании.	Опрос, диспут, кейс-анализ, заслушивание и обсуждение презентаций и учебных научных сообщений.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Методы и инструменты для выявления и расследования схем мошенничества	• Методические аспекты форензика как инструмента выявления и предотвращения мошеннических действий в деятельности экономических субъектов. • Управление процессом расследования мошенничества: подготовка и планирование, выполнение и сбор доказательств, отчетность и завершение расследования. • Взаимодействие с правоохранительными органами и привлечение к ответственности по результатам внутреннего расследования. • Квадрат доказательств. • Документирование расследования. • Процедуры для выявления индикаторов нарушений: аналитические процедуры, детальные процедуры, анализ нефинансовой информации. • Использование аналитических процедур для выявления мошенничества. • Шесть этапов алгоритма выявления мошенничества в организациях, в том числе анализ качества элементов отчетности, анализ крупных сделок с активами, анализ обоснованности стоимости активов, маркетинговый анализ, анализ соответствия производительности ресурсов отраслевому (рыночному) уровню, анализ рентабельности компании и ее контрагентов. • Признаки искажения и мошенничества, выявляемые при проверке первичной и сводной учетной документации. • Процедуры проверки физического наличия активов (инвентаризации) при наличии признаков мошенничества. • Цифровые каналы сообщения о нарушениях. • Инструменты на основе искусственного интеллекта для предиктивного выявления мошенничества.	Опрос, диспут, кейс-анализ, заслушивание и обсуждение презентаций и учебных научных сообщений.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Анализ и признаки противоправных схем мошенничества в организациях	• Анализ существующей системы внутреннего контроля. • Анализ и сравнение финансовых и нефинансовых показателей. • Анализ сообщений, поступивших по горячей линии. • Анализ неофициальной информации. • Анализ и выявление схем мошенничества сотрудников и руководства. • Анализ нестандартных решений руководителей, скрытых соглашений, отклонений от корпоративных процедур. • Подходы к выявлению хищений и других нарушений обращения денежных средств (наличные и безналичные). • Анализ и выявление нарушений обращения материальных активов (запасы, ТМЦ). • Аномалии при анализе операций с внеоборотными активами (основные средства и нематериальные активы). • Анализ и выявление схем мошенничества покупателей и поставщиков. Анализ закупочного процесса и кредиторской задолженности. • Анализ продаж и дебиторской задолженности (признаки мошенничества). • Выявление фиктивных продаж. • Выявление мошенничества с финансовыми результатами. • Анализ незаконных схем занижения и завышения финансовых результатов. • Анализ и выявление схем инвестиционного мошенничества. • Анализ и выявление злоупотреблений в сфере цифровых финансовых и токенизированных активов. • Анализ и выявление злоупотреблений в сфере криптовалютных операций. • Взаимосвязь между фальсификацией бухгалтерской (финансовой) отчетности и банкротством экономического субъекта.	Опрос, диспут, кейс-анализ, заслушивание и обсуждение презентаций и учебных научных сообщений.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	• Последствия мошенничества с бухгалтерской (финансовой) отчетностью. • Виды искажений и фальсификации бухгалтерской (финансовой) отчетности. • Состав ключевых финансовых индикаторов для выявления мошенничества в бухгалтерской (финансовой) отчетности. • Карта нормативных отклонений финансовых индикаторов для моделей Бениша (M-Score) и Роксаса (Roxas' Model).	
Использование информационных технологий для выявления и расследования мошенничества в организациях	• Особенности информационно-технологических решений в сфере противодействия мошенничеству. • Системы DLP, фрод-мониторинга, спам-фильтры, системы мониторинга корпоративной почты, системы контроля за действиями пользователя как инструменты выявления и противодействия мошенничеству в организациях. • Этапы аналитики данных при расследовании мошенничества. • Сбор и подготовка данных при расследовании мошенничества. • Логика расследования, формулировки и тестирование гипотез о мошенничестве. • Виды и группы выявляемых аномалий. • Структурированные и неструктурированные данные. • Проверка качества и достоверности данных. • Анализ структурированных данных: традиционный и современный подходы. • Подходы к выявлению аномалий в структурированных данных. • Сбор и подготовка информации для анализа. • Анализ неструктурированных данных для выявления признаков мошенничества. • Цифровые следы и роль блокчейн-аналитики в расследовании инцидентов мошенничества.	Опрос, диспут, кейс-анализ, заслушивание и обсуждение презентаций и учебных научных сообщений.



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
Сущность, виды и схемы мошенничества в организациях	Экономическая природа мошенничества в организациях. Причины недобросовестного поведения. Теория прирожденности злоумышленника. Влияние мошенничества на финансовую устойчивость и обеспечение экономической безопасности бизнеса, риски и угрозы. Классификация видов мошенничества по объекту посягательства и мотивам. Классификация видов мошенничества по способу реализации (фальсификация документов, злоупотребление полномочиями, сговор и др.). Иные классификации мошенничества. Признаки мошенничества со стороны менеджеров, работников, руководства и топ-менеджмента. Схемы кибермошенничества в отношении компании.	Изучение учебной литературы. Подготовка к опросу и научной дискуссии. Подготовка к интерактивным занятиям. Подготовка и выполнение контрольной работы.
Методы и инструменты для выявления и расследования схем мошенничества	Руководство по проведению внутренних расследований в организациях ISO/TS 37008:2023. Правила организации процесса внутрикорпоративных расследований. Инструменты для привлечения к ответственности и возмещения ущерба. Место и роль правоохранительных органов в расследовании мошенничества в организации. Анализ существующих методов и способов расследования мошенничества: что можно и что нельзя внутренним службам коммерческой организации (ограничения, установленные законодательством Российской Федерации). Анализ внешней и внутренней среды ведения бизнеса. Методы и приемы документальной и физической (формальной) проверки.	Изучение учебной литературы. Подготовка к опросу и научной дискуссии. Подготовка к интерактивным занятиям. Подготовка и выполнение контрольной работы.



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Анализ и признаки противоправных схем мошенничества в организациях	Признаки мошенничества, обнаруживаемые в документах бухгалтерского учета. Признаки мошенничества со стороны сотрудников, наводки и жалобы, изменения в поведении и образе жизни, биографические признаки. Признаки незаконных выплат сотрудникам и кадровые аномалии. Аномалии в операциях с активами и признаки их незаконного вывода. Признаки мошенничества в расчетных операциях. Признаки подделки первичных документов и сговора с поставщиками. Параллельный бизнес и его признаки. Состав ключевых финансовых индикаторов для выявления схем инвестиционного мошенничества. Признаки мошенничества с ценными бумагами. Признаки мошенничества при кредитовании. Признаки мошенничества при инвестировании в реальные проекты и интеллектуальные ценности. Признаки мошенничества с криптовалютой. Признаки мошенничества с цифровыми финансовыми и токенизированными активами. Факторы, побуждающие и создающие условия для мошенничества с бухгалтерской (финансовой) отчетностью. Признаки мошенничества в бухгалтерской (финансовой) отчетности. Прочие аналитические модели для выявления фальсификации бухгалтерской (финансовой) отчетности и интерпретация их результатов.	Изучение учебной литературы. Подготовка к опросу и научной дискуссии. Подготовка к интерактивным занятиям. Подготовка и выполнение контрольной работы.
Использование информационных технологий для выявления и расследования мошенничества в организациях	Преимущества использования современных информационных технологий при выявлении и расследовании мошенничества в организациях. Извлечение и подготовка данных для анализа. Характеристика структурированных данных. Аномалии структурированных данных. Характеристика неструктурированных данных.	Изучение учебной литературы. Подготовка к опросу и научной дискуссии. Подготовка к интерактивным занятиям. Подготовка и выполнение контрольной работы.



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
	Информационные источники для анализа неструктурированных данных. Возможные риски, связанные с анализом данных в электронном виде.	



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

Примерная тематика контрольной работы

Комплексный анализ и выявление схем корпоративного мошенничества с использованием современных методов и информационных технологий (на примере конкретной организации).

Задачи:

1. Провести анализ бизнес-процессов конкретной организации и выявить зоны, уязвимые для мошенничества.
2. Идентифицировать потенциальные схемы мошенничества и описать их признаки («красные флаги»).
3. Определить методы и инструменты для выявления мошенничества (аналитические процедуры, работа с данными и пр.).
4. Разработать карту рисков мошенничества с оценкой вероятности и уровня ущерба для организации.
5. Предложить контрольные процедуры, включая рекомендации по использованию информационных технологий для эффективного выявления мошенничества в организации.

Методические рекомендации по выполнению контрольной работы.

Цель работы: Научиться анализировать и выявлять риски мошенничества в организации, на основе открытых источников.

Что нужно сделать:

1. Выбрать организацию для анализа (коммерческий хозяйствующий субъект с открытой информацией).
2. Собрать информацию из открытых источников:
 - Сервисы ФНС России (в т.ч. государственный информационный ресурс бухгалтерской (финансовой) отчетности (БФО)).
 - Картотека арбитражных дел (судебные споры).
 - СМИ и деловые порталы (новости, расследования).
 - Сервисы проверки контрагентов (СПАРК и др.).
 - Локальные акты организации.
3. Проанализировать и выявить признаки потенциального мошенничества в организации («красные флаги»):
 - Странности в структуре компании (массовая смена директоров, адресов).
 - Финансовые аномалии (резкие скачки отчетности, убытки).
 - Судебные иски (особенно о неисполнении обязательств).
 - Негатив в СМИ и социальных сетях (задержки зарплат, конфликты и пр.).
 - Риски в конкретных бизнес-процессах (закупки, продажи и пр.).
 - Признаки искажения бухгалтерской (финансовой) отчетности и пр.
4. Сделать вывод — насколько компания уязвима для внутреннего и внешнего мошенничества. Определить наиболее вероятные потенциальные схемы мошенничества в организации.
5. Определить методы и инструменты для выявления мошенничества. Для каждой выявленной потенциальной схемы указать, какие методы и инструменты, в т.ч. цифровые могут быть использованы для ее выявления.
6. Построить матрицу рисков мошенничества. Оцените вероятность и уровень потенциального ущерба от рисков мошенничества в организации.
7. Предложить контрольные процедуры, включая рекомендации по использованию информационных технологий для эффективного выявления схем мошенничества в организации.



Объем работы: не более 6 страниц (без учета таблиц, графиков и другого иллюстративного материала).

Критерии оценки контрольной работы.

- 6 баллов — работа демонстрирует высокий уровень аналитики, четкая и последовательная структура, самостоятельные выводы, системное видение проблемы и обобщения, прослеживается авторская позиция.
- 4-5 баллов — работа выполнена качественно и самостоятельно, но недостаточно глубины анализа или есть незначительные пробелы в логике или обобщении, отдельные элементы проработаны поверхностно, прослеживается авторская позиция.
- 2-3 балла — структура соблюдена, формальное соответствие заданию, слабая аргументация, выводы шаблонны, не четко выраженная авторская позиция, поверхностный анализ без признаков генерации текста.
- 0-1 балл — нарушена структура или отсутствуют отдельные обязательные элементы, работа частично соответствует требованиям, поверхностный анализ, имеются признаки генерации текста без осмысления.

Дополнительная информация

Примерная тематика для диспутов

1. Треугольник мошенничества в современных реалиях: работает ли классическая теория?
2. Человеческий фактор в системе контроля — это риск или благо?
3. Топ-менеджмент как источник риска. Почему высокие должности в корпоративной среде не гарантируют честность?
4. Грань между контролем и гибкостью корпоративного управления: где она проходит?
5. Внутренний аудит против внешнего форензика. Как эффективнее выявлять мошенничество в корпоративной среде?
6. Бизнес-процессы группы риска: где искать следы мошенничества в первую очередь?
7. Взаимосвязь экономической нестабильности и санкций с уровнем мошенничества в корпоративной среде. Провоцируют ли внешние шоки рост нарушений?
8. Методы социальной инженерии и кибермошенничества (кейсы руководителей, которые стали невольными соучастниками мошенничества)?
9. Тендеры и подряды: как распознать фиктивный контракт и мошенничество поставщиков?
0. Цифровизация как фактор риска. Защищают ли новые технологии от мошенничества или создают новые уязвимости?
1. Наказание за мошенничество в корпоративной среде (достаточно ли увольнения или нужно уголовное преследование)?
2. Как распознать фальсификацию бухгалтерской (финансовой) отчетности и подлог финансовой документации до прихода аудиторов?
3. Корпоративная культура и этика: работают ли «горячие линии» и кодексы как профилактика?
4. Мошенничество в закупках: схемы откатов и завышения цен, методы выявления.
5. Роль Больших Данных и искусственного интеллекта в прогнозировании мошеннических действий (успешные кейсы и эффективные практики).

Примерная тематика для подготовки презентаций

1. Типовые схемы и методы мошенничества в цифровой экономике.



2. Методы выявления. Использование аналитических процедур для выявления мошенничества.
3. Методы документального контроля: арифметическая проверка, нормативная проверка, сопоставление документов, финансовый анализ и пр.
4. Методы фактического контроля: инвентаризация, контрольные обмеры и пр.
5. Виды доказательств: первичные учетные документы, иные первичные документы, регистры бухгалтерского учета, регистры налогового учета, бухгалтерская отчетность, налоговая отчетность, заключения специалистов, информация в электронном виде и пр.
6. Признаки корпоративного мошенничества, обнаруживаемые в документах бухгалтерского учета.
7. Факторы и индикаторы корпоративного мошенничества на примере производственного сегмента.
8. Факторы и индикаторы корпоративного мошенничества на примере сбытового сегмента.
9. Факторы и индикаторы корпоративного мошенничества на примере закупочного сегмента.
10. Признаки незаконных выплат и вывода активов.
11. Основные способы хищения и другие нарушения обращения с денежными и материальными средствами и их признаки.
12. Методы и порядок расследования фактов хищения внеоборотных активов организации.
13. Проведение инвентаризации при наличии признаков корпоративного мошенничества.
14. Признаки мошенничества, выявляемые в результате анализа, а также при наличии особых отношений с деловыми партнерами.
15. Методы выявления недобросовестных действий контрагентов.
16. Методы выявления недобросовестных действий сотрудников организации.
17. Признаки манипуляции с выручкой и финансовой отчетностью.
18. Система внутреннего контроля и ответственность руководства отчитывающегося экономического субъекта за мошенничество с финансовой отчетностью.
19. Мотивы и методы выявления намеренного занижения прибыли как вида мошенничества в финансовой отчетности.
20. Виды искажений в бухгалтерской отчетности их причины и технология анализа взаимосвязанных показателей.
21. Использование модели М. Бениша (M-score) для выявления признаков искажения бухгалтерской финансовой отчетности.
22. Тестирование системы внутреннего контроля.
23. Матрица расследования корпоративного мошенничества.
24. Предупреждение, обнаружение, расследование корпоративного мошенничества: методы и процедуры.
25. Особенности и порядок сбора доказательств для целей форензика.
26. Фиксация фактов корпоративного мошенничества.
27. Требования к сбору доказательств: относимость, допустимость, достоверность, полнота и достаточность.
28. Цифровые системы и ПО для анализа и выявления фактов мошенничества и коррупции.
29. Особенности анализа структурированных и неструктурированных данных.
30. Способы возмещения ущерба, нанесенного компании в результате мошеннических действий.

Учебные научные сообщения готовятся по результатам чтения отечественных и международных научных публикаций по следующим примерным вопросам:

1. Современные методы выявления корпоративного мошенничества.



2. Роль корпоративного управления и информационных технологий в обнаружении и предотвращении фрод-схем.
3. Применение гибридных моделей для выявления мошенничества в корпоративной среде.
4. Использование альтернативных данных (online-продажи, потребительские транзакции) для обнаружения финансовых манипуляций.
5. Классификация атак с использованием социальной инженерии и методы профилактики корпоративного мошенничества.
6. Эмпирические исследования о влиянии цифровизации на выявление корпоративного мошенничества.
7. Международные стандарты противодействия мошенничеству и их адаптация к российской специфике.
8. Криминологические аспекты корпоративного мошенничества и меры предупреждения.
9. Процедуры и технология проведения служебного расследования фактов мошенничества в корпоративной среде.
10. Контрольные процедуры и ограничения их использования в корпоративной среде при проведении служебных расследований.

Оценка знаний студентов осуществляется в баллах с учетом оценки работы в семестре (самостоятельных работ и домашних заданий, аудиторной работы: участия в опросах и диспутах, решения кейсов, заслушивания и обсуждения презентаций и учебных научных сообщений и др.), оценки итоговых знаний (по результатам зачета) и в соответствии с критериями Финансового университета реализуется следующим образом:

№ п/п	Вид отчетности	Баллы
1.	Работа в модуле	40
2.	Зачет	60
	Итого:	100

Формы текущего контроля успеваемости и их балльная оценка

Формы текущего контроля	Количество баллов
Интерактивная работа в аудитории (диспуты, обсуждение кейсов и учебных научных сообщений, доклады, презентации и т.п.).	16
Посещение	6
Блиц-опросы и проверка знаний по разделам, блокам или темам (на усмотрение преподавателя), тестирование по темам дисциплины.	12
Контрольная работа	6
Итого	40



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

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ПКН-4. Способность оценивать показатели деятельности экономических субъектов	Проводит анализ внешней и внутренней среды ведения бизнеса, выявляет основные факторы экономического роста, оценивает эффективность формирования и использования производственного потенциала экономических субъектов.	Знать: методы анализа внешней и внутренней среды организации для выявления факторов, способствующих мошенничеству, и оценки их влияния на экономическую безопасность бизнеса. Уметь: выявлять уязвимые бизнес-процессы и ключевые риски мошенничества на основе анализа макро- и микросреды организации.	• Перечислите и дайте характеристику ключевым методам анализа внешней среды организации, применимые для выявления рисков мошенничества. • Какие внутренние факторы организации могут создавать уязвимости для мошеннических схем? Приведите примеры с пояснением механизма воздействия. • Какие индикаторы нестабильности внутренней среды могут сигнализировать о повышенном риске корпоративного мошенничества? • Проанализируйте макроэкономические показатели отрасли (темпы роста, уровень конкуренции, регуляторные изменения). Определите факторы, которые могут стимулировать мошенничество в компаниях конкретной отрасли. • Какие инструменты анализа конкурентной среды помогают прогнозировать риски мошенничества? • Проанализируйте описание бизнес-процесса продаж. Определите точки, где возможны манипуляции с отчётностью. Разработайте контрольные процедуры. • Используя данные о динамике рынка труда в отрасли, оцените риски мошенничества со стороны персонала в конкретном регионе. Составьте план профилактических мероприятий. • На примере кейса с изменением налогового законодательства определите потенциальные схемы уклонения от обязательств. Предложите способы их обнаружения.
	Рассчитывает и интерпретирует показатели деятельности экономических субъектов.	Знать: систему ключевых финансовых и нефинансовых показателей, используемых для выявления признаков мошенничества (в т. ч. индикаторы моделей Бе-	• Перечислите ключевые индикаторы модели Бениша (M-Score) и объясните их связь с рисками мошенничества. • В чём принципиальные отличия моделей Роксаса и Бениша? Для каких типов компаний подходит каждая из них? • Какие нефинансовые показатели (кроме финансовых коэффициентов) могут сигнализировать о фальсификации отчётности? Приведите примеры.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соответствующие с индикаторами достижения компетенции	Типовые контрольные задания
		ниша, Роскаса и др.). Уметь: рассчитывать и анализировать показатели финансовой отчётности и операционных процессов для обнаружения аномалий данных и признаков мошеннических схем.	- Предложите показатели для анализа и мониторинга, указывающие на возможные схемы вывода средств из организации. - Как интерпретировать расхождения между динамикой выручки и денежными потоками? Приведите пример мошеннической схемы. - Какие операционные показатели (кроме финансовых) следует анализировать для выявления хищений в цепочке поставок? - На основе отчёта о финансовых результатах одной из компаний выявите аномалии, указывающие на возможное завышение выручки. Предложите методы проверки. - Рассчитайте коэффициенты оборачиваемости запасов за 2 года. Сопоставьте их с иными данными бухгалтерской (финансовой) отчетности. Сделайте вывод о возможных манипуляциях с себестоимостью. - Используя данные о зарплатах и производительности, оцените риски мошенничества в кадровом блоке. Составьте план проверки.
ПКП-2. Способность выявлять, документировать и анализировать риски, связанные с отмыванием доходов, полученных преступным путем, и финансированием терроризма, устанавливать признаки сомнительных операций и сделок, а также фиксировать соответ-	Проводить анализ операций и сделок для выявления признаков сомнительных транзакций.	Знать: инструментарий финансовых расследований, типовые схемы мошенничества в ключевых бизнес-процессах (закупки, продажи, управление активами и др.) и их индикаторы и признаки. Уметь: применять инструментарий финансовых расследований, в т.ч. аналитические и детальные процедуры для выявления подозрительных операций и транзакций в финансовой	- Опишите типовую схему мошенничества в процессе закупок. Какие документы и показатели позволят её выявить? - Какие признаки указывают на фиктивные продажи в отчётности? - В чём заключаются особенности схем мошенничества при управлении нематериальными активами? - Как анализ банковских выписок помогает обнаружить подозрительные транзакции? - Составьте чек-лист для проверки операций с основными средствами на предмет мошеннических схем. - Опишите порядок проведения аналитических процедур при проверке закупочного процесса. - Какие детальные процедуры применяются для верификации подлинности первичных документов? - На основе данных о платежах компании постройте граф взаимосвязей контрагентов. Выделите узлы, соответствующие признакам схем обналичивания. - Проанализируйте договор поставки и сопутствующие документы. Найдите признаки сговора с поставщиком. - Используя данные о продажах и остатках товаров, определите, есть ли признаки создания «мертвых душ» в клиентской базе.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ствующие сведения в организации		и операционной деятельности организации.	
	Документировать выявленные риски и составлять отчеты для представления руководству или контролирующим органам.	Знать: требования к оформлению документации по выявленным рискам мошенничества, структуру и содержание отчетов для руководства, контрольно-надзорных и правоохранительных органов. Уметь: систематизировать доказательства, оформлять акты расследований и составлять отчеты о выявленных нарушениях с рекомендациями по их устранению.	• Перечислите обязательные разделы отчета о выявленном факте мошенничества для руководства компании. • Какие данные должны быть включены в приложение к отчету для правоохранительных органов? • В чём отличия формата отчёта для внутреннего аудита и внешнего регулятора? • Какие требования предъявляются к оформлению доказательств мошенничества? • Разработайте шаблон отчета для ежемесячного мониторинга рисков мошенничества. Выделите в нем ключевые блоки. • Какие критерии определяют приоритетность включения данных в акт расследования? • В чем специфика оформления электронных доказательств (переписка, логи систем)? • Какие ошибки в отчетах снижают их доказательную силу в суде или при проверке надзорными органами? • На основе приведенного набора доказательств (выписки, договоры, переписка) составьте акт расследования по факту мошенничества в отделе продаж. Структурируйте доказательства по категориям, укажите источники и степень достоверности. На основе приведённого кейса оформите приложение с перечнем доказательств (документы, выписки, скриншоты). • Разработайте раздел «Рекомендации» для отчета о выявленном случае фальсификации бухгалтерской (финансовой) отчетности. Предложите конкретные меры по усилению внутреннего контроля на данном участке. • Оформите приложение к отчету для правоохранительных органов, включив: перечень изъятых документов; скриншоты подозрительных транзакций; сводную таблицу аномалий. • Проанализируйте образец отчета о расследовании. Выделите недостатки в оформлении доказательств и предложите исправления.
	Использовать автоматизированные системы мониторинга для выявления аномалий	Знать: принципы работы и функционал ИТ-систем для противодействия мошенничеству (DLP,	• Перечислите ключевые функции систем фрод-мониторинга. В чем их отличие от DLP-систем? • Какие типы аномалий в финансовых потоках выявляют автоматизированные системы? Приведите примеры для каждой категории. • Как алгоритмы машинного обучения применяются для обнаружения мошеннических схем?



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
	малый в финансовых потоках.	фрод-мониторинг и др.), а также типы и виды аномалий. Уметь: моделировать действия оператора автоматизированных систем мониторинга: составлять запросы на проверку контрагентов, задавать фильтры для выявления аномалий, оценивать релевантность срабатываний; формулировать аналитические выводы на основе анализа структурированных и неструктурированных данных.	- Каковы ограничения ИТ-систем в выявлении сговора между сотрудниками? - Какие данные (структурированные/неструктурированные) анализируют системы противодействия мошенничеству? Приведите по 2 примера для каждого типа. - На основании логов системы фрод-мониторинга выделите 3 транзакции, соответствующие критериям подозрительных операций. Обоснуйте выбор, указав параметры срабатывания системы. - Составьте список фильтров для DLP-системы, направленных на выявление утечки конфиденциальной информации о контрактах. Включите не менее 4 правил. - Проанализируйте отчет автоматизированной системы о аномалиях в зарплатных выплатах. Определите 2–3 случая, требующих ручной проверки. - Опишите сценарий срабатывания системы при обнаружении цепочки платежей, соответствующих схеме «транзитного» обналичивания. Укажите ключевые индикаторы. - Как настроить фильтр для выявления операций с «фирмами-однодневками»? Приведите основные критерии. - Сформулируйте запрос на проверку контрагента по ИНН в системе «СПАРК». Укажите ключевые параметры анализа (например, аффилированность, судебные иски). - На основе отчета системы о подозрительных платежах составьте аналитическую записку с выводами: количество срабатываний за период; доля подтвержденных случаев мошенничества; рекомендации по корректировке фильтров. - Проанализируйте переписку из корпоративной почты (фрагмент). Выделите ключевые слова и контексты, указывающие на возможный сговор. Сформулируйте гипотезу для проверки.



Примеры практико-ориентированных заданий

Примеры кейс заданий

Задание 1. В филиале частной строительной фирмы квартальная выручка оказалась ниже прогнозируемой. Это было странно, так как продажи были хорошие. Руководитель проверил финансовые отчеты, но нарушений не было. Специалисты службы безопасности, изучив отчет «Категории / отклонения» выявили, что входящие звонки от клиентов подозрительно короткие. Тогда они прослушали записи разговоров и «Аудио» с микрофонов ноутбуков сотрудников. В результате работы тайного покупателя выяснилось, что, менеджеры принимали звонок от клиента по корпоративному номеру, а потом перезванивали с личного мобильного: они предлагали клиенту пообедать и обсудить предпочтения. На встрече они озвучивали заказчикам повышенные скидки в обмен на личную материальную выгоду (откат). Хотя в компании были предусмотрены скидки для особо важных клиентов, но менеджеры за откат давали их в качестве индивидуальных.

Определите тип и вид деяния ответ аргументируйте. Дайте экономико-правовую оценку действиям должностных лиц. Проведите анализ ситуации и выделите «красные флаги» и специфические индикаторы, свидетельствующие о мошенничестве / коррупции в организации. Какие методы контроля были использованы в описанной ситуации? Разработайте программу проведения внутреннего расследования в организациях по выявленному инциденту.

Задание 2. По данным заполненных расходных-кассовых ордеров проведите документальную проверку, определите признаки подозрительных операций. Оформите отчеты сотрудника службы экономической безопасности о выявленных нарушениях:

- а) для представления руководству;
- б) для представления контролирующим органам.

Ответьте на вопросы:

1. Какие процедуры и методы были использованы для выявления нарушений?
2. Требуется ли служебное расследование по факту выявленных нарушений?
3. С кем необходимо взаимодействовать при выявлении подобных нарушений?

Задание 3. Используя данные Государственного информационного ресурса Бухгалтерской (финансовой) отчетности ФНС России <https://bo.nalog.gov.ru/> проанализируйте финансовое состояние трех коммерческих организаций, осуществляющих схожие виды деятельности (в одном экономическом сегменте) за последние 3-4 года.

По представленным финансовым данным рассчитайте модели, используемые для выявления вероятности манипуляций с прибылью и фальсификации финансовой отчетности компаниями (модификации М. Бениша, Роксаса и пр.). Сделайте аналитический вывод о наличии признаков манипуляции с данными бухгалтерской (финансовой) отчетности компаний. Подготовьте аналитическую записку руководству о ваших наблюдениях и возможных рисках сотрудничества (совместного инвестиционного проекта) с данными компаниями.

Примеры тестовых заданий:

1. Какая из перечисленных ситуаций с наибольшей вероятностью свидетельствует о скрытом риске внутреннего мошенничества и требует немедленного расследования?

А) Руководитель отдела заключает краткосрочные контракты с проверенными поставщиками по рыночным ценам, но в обход обязательной процедуры проведения тендера, формально аргументируя это «срочностью выполнения критически важного заказа».

Б) Бухгалтер дважды за месяц допустил арифметические погрешности в расчете налога на прибыль.

В) Сотрудник службы безопасности, следуя регламенту, не внес в базу данных посетителя, разовый пропуск для которого был оформлен с нарушением установленной процедуры.



Г) Менеджер по развитию инициировал списание морально устаревшего оборудования, рыночная стоимость которого близка к нулю, с целью освобождения складских площадей.

2. Мошенничество с целью сокрытия убытков компании чаще всего направлено на:

А) Улучшение условий труда.

Б) Сохранение курса акций и привлечение инвестиций.

В) Снижение налоговой нагрузки.

Г) Занижение зарплат и социальных отчислений.

3. Какой из перечисленных индикаторов с наибольшей вероятностью указывает на потенциальное корпоративное мошенничество со стороны руководителей?

А) Увеличение операционных расходов из-за глобального роста цен на сырье и энергоносители.

Б) Падение рентабельности основных продуктовых линий на фоне роста аналогичных показателей у ключевых конкурентов.

В) Систематический отказ руководства от делегирования полномочий на подписание ключевых документов, даже во время плановых отпусков, сочетающийся с нежеланием принимать отпуск одновременно с заместителем.

Г) Наличие неформальных отношений между членами совета директоров и исполнительным руководством.

Примеры вопросов для подготовки к промежуточной аттестации

1. Экономическая природа, факторы и причины развития мошенничества в организациях.
2. Влияние внешней и внутренней среды на развитие мошенничества в организациях.
3. Классификация видов мошенничества.
4. Дерево мошенничества ACFE и характеристика его элементов.
5. Последствия мошенничества и его влияние на финансовую устойчивость и экономическую безопасность бизнеса.
6. Бизнес-процессы, подверженные риску мошенничества.
7. Общие индикаторы мошенничества и злоупотреблений.
8. Форензик как инструмент выявления и предотвращения мошенничества.
9. Логика и этапы расследования фактов мошенничества (ISO/TS 37008:2023).
10. Технология проведения и управления процессом расследования мошенничества в организации.
11. Поиск доказательств мошенничества (квадрат доказательств).
12. Виды и группы выявляемых аномалий в данных.
13. Документирование расследования.
14. Классификация способов и приемов для выявления мошенничества в деятельности организаций.
15. Аналитические процедуры для выявления мошенничества.
16. Детальные процедуры для выявления мошенничества.
17. Анализ нефинансовой информации для выявления мошенничества.
18. Шесть этапов алгоритма выявления мошенничества в организации.
19. Анализ качества элементов отчетности при выявлении мошенничества.
20. Анализ крупных сделок с активами: индикаторы мошенничества.
21. Анализ обоснованности стоимости активов: методы и критерии.
22. Маркетинговый анализ как инструмент выявления мошеннических схем.
23. Анализ соответствия производительности ресурсов отраслевому уровню.
24. Анализ рентабельности компании и ее контрагентов: признаки аномалий.
25. Методы и приемы документальной проверки на наличие признаков мошенничества.
26. Методы и приемы фактической проверки на наличие признаков мошенничества.
27. Инвентаризация как метод контроля и выявления фактов мошенничества.



28. Сравнение финансовых и нефинансовых показателей при выявлении мошенничества.
29. Анализ сообщений по «горячей линии»: методы обработки и оценки.
30. Анализ неофициальной информации в расследовании мошенничества.
31. Критерии эффективности субъектов корпоративного управления и признаки мошенничества руководителей, менеджеров и персонала.
32. Признаки незаконных выплат сотрудникам и кадровые аномалии.
33. Признаки мошенничества в документах бухгалтерского учета.
34. Анализ нестандартных решений руководителей и скрытых соглашений.
35. Признаки параллельного бизнеса и противоправного присвоения финансовых результатов (сбытовые, закупочные, производственные и пр.).
36. Анализ и выявление хищений денежных средств (наличные и безналичные).
37. Анализ нарушений обращения материальных активов (запасы, ТМЦ).
38. Аномалии при анализе операций с устойчивыми внеоборотными активами (основные средства, нематериальные активы).
39. Признаки инвестиционного мошенничества (ценные бумаги, кредитование, реальные проекты, интеллектуальные ценности).
40. Анализ закупочного процесса: индикаторы сговора с поставщиками.
41. Выявление фиктивных продаж и аномалий дебиторской задолженности.
42. Анализ и выявление мошенничества с финансовыми результатами: схемы занижения и завышения.
43. Признаки и виды мошенничества с бухгалтерской (финансовой) отчетностью.
44. Ответственность руководства отчитывающегося экономического субъекта за мошенничество с бухгалтерской (финансовой) отчетностью.
45. Выявление махинаций с бухгалтерской (финансовой) отчетностью (модели М. Бениша, Роксаса и др.).
46. Информационные технологии, группы программных продуктов для выявления и расследования мошенничества в организации.
47. Характеристика структурированных и неструктурированных данных, их извлечение и подготовка для анализа.
48. Анализ структурированных данных при расследовании мошенничества.
49. Анализ неструктурированных данных при расследовании мошенничества.
50. Проблемы и риски, связанные с качеством информации и анализом данных в расследовании.



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

Основная литература:

1. Глотов, В.И. Международная практика в области противодействия легализации активов полученных в результате мошенничества и коррупции : Учебное пособие / В.И. Глотов, Н.М. Чуйкова Электрон. дан. Москва : Русайнс, 2024 276 с. Режим доступа: book.ru Internet access <https://book.ru/book/952863> ISBN 978-5-466-05298-5. [БИК ID: RU\bookru\bibl\952863]
2. Земсков, В. В. Анализ и выявление схем корпоративного мошенничества : учебник / В. В. Земсков Москва : Прометей, 2025 176 с. : ил., табл. Библиогр. в кн Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация <https://biblioclub.ru/index.php?page=book&id=721459> ISBN 978-5-00172-788-0. [БИК ID: BIBLIOCLUB\0000721459]
3. Жариков, Ю.С. Уголовно-правовая охрана недвижимого имущества от хищения путем обмана или злоупотребления доверием (мошенничества) : Учебное пособие / Ю.С. Жариков Электрон. дан. Москва : КноРус, 2026 148 с. Режим доступа: book.ru Internet access <https://book.ru/book/961123> ISBN 978-5-406-15784-8. [БИК ID: RU\bookru\bibl\961123]

Дополнительная литература:

1. Сотникова, Л.В. Мошенничество в финансовой отчетности: обнаружение и предупреждение : Учебник / Л.В. Сотникова Электрон. дан. Москва : Русайнс, 2026 394 с. Режим доступа: book.ru Internet access <https://book.ru/book/959548> ISBN 978-5-466-09961-4. [БИК ID: RU\bookru\bibl\959548]
2. Романов, В. Г. Социальная инженерия мошенничества [Электронный ресурс] : монография / Романов В. Г., Романова И. В. Чита : ЗабГУ, 2021 240 с. Рекомендовано к изданию Советом по научной и инновационной деятельности Забайкальского государственного университета Книга из коллекции ЗабГУ - Право. Юридические науки <https://e.lanbook.com/book/271808> ISBN 978-5-9293-2771-1. [БИК ID: RU-LAN-BOOK-271808]
3. Маркелов, А.Г. Расследование мошенничества: использование данных о преступных навыках и их значение в особых (компромиссных) производствах : Монография / А.Г. Маркелов, С.А. Алексеев, В.Н. Чулахов; под ред. В.Н. Чулахов Электрон. дан. Москва : Русайнс, 2025 162 с. Режим доступа: book.ru Internet access <https://book.ru/book/960230> ISBN 978-5-466-10378-6. [БИК ID: RU\bookru\bibl\960230]
4. Тарасов, Александр Николаевич Психология корпоративного мошенничества : учебник и практикум для вузов / А. Н. Тарасов. Электрон. дан. Москва : Юрайт, 2025 320 с (Высшее образование) URL: <https://urait.ru/bcode/560622> (дата обращения: 01.09.2025). Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей <https://urait.ru/bcode/560622> ISBN 978-5-534-01053-4 : 1289.00. [БИК ID: RU2fURAIT2f560622]
5. Петров, А. М. Аналитическое обеспечение методов выявления мошенничества [Электронный ресурс] : учебник / Петров А. М. Москва : Центркаталог, 2024 160 с. Книга из коллекции Центркаталог - Экономика и менеджмент <https://e.lanbook.com/book/417245> ISBN 978-5-907825-01-7. [БИК ID: RU-LAN-BOOK-417245]

Нормативные правовые акты:

1. Уголовный кодекс Российской Федерации [Электронный ресурс]: Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ с (изм. и доп.) // Справочная система «Гарант».



2. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (с изм. и доп.) // Справочная система «Гарант».
3. Федеральный закон «О противодействии коррупции» от 25.12.2008 г. № 273-ФЗ
4. Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 г. № 115-ФЗ.
5. ГОСТ Р ИСО 31000-2010 «Менеджмент риска. Принципы и руководство».
6. ГОСТ Р ИСО 31010:2009 «Менеджмент риска. Методы оценки риска».
7. ГОСТ Р ИСО 37001:2025 «Системы менеджмента противодействия коррупции – Требования и рекомендации по применению».
8. ГОСТ Р ИСО 71025:2023 «Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента. Часть 9. Требования к компетентности персонала для проведения аудита и сертификации систем менеджмента противодействия коррупции».
9. ГОСТ Р ИСО 37003:2025 «Системы управления противодействием мошенничеству. Руководство для организаций по управлению рисками мошенничества».
10. ГОСТ Р ИСО 37008:2023 «Внутренние расследования в организациях. Руководство»
11. МСА 240 «Обязанности аудитора в отношении недобросовестных действий».
12. МСА 400 «Оценка рисков и внутренний контроль».

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 издательства "Лань" <https://e.lanbook.com/>
4. Образовательная платформа "ЮРАЙТ" <https://urait.ru/>
5. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
6. • Электронные коллекции книг и журналов издательства Springer: <http://link.springer.com/>
7. СПАРК <https://spark-interfax.ru/>
8. Цифровой архив научных журналов: <https://arch.neicon.ru/xmlui>.
9. Сайт «Анализ финансового состояния предприятия»: www.afdanalyse.ru
10. Справочно-образовательная система Акцион 360 <https://action360.ru/>
11. Библиотека электронных публикаций Организации экономического сотрудничества и развития OECD iLibrary <https://www.oecd-ilibrary.org/>
12. Web of Science <http://apps.webofknowledge.com>
13. Министерство экономического развития Российской Федерации URL: <https://economy.gov.ru/>
14. Государственный информационный ресурс бухгалтерской отчетности



10. Методические указания для обучающихся по освоению дисциплины

Студентам при подготовке следует использовать нормативные документы Финансового университета, Методические рекомендации по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете, утвержденные приказом Финуниверситета от 11.05.2021 № 1040, использовать методические рекомендации кафедры.



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 «Консультант Плюс»
2. Информационно-правовая система «Гарант»
3. Информационно-справочная система «СПАРК»

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. **Помещение для самостоятельной работы** обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде Университета.
3. Библиотека, читальный зал