

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: MG2GSV2JFf312mt4IBynigXCYCfgPLXF

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

Дата: 23.10.2025 г.

И.А. Лебедев , О.В. Капитонова
Цифровой форензик и информационная безопасность

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки

38.03.01 - Экономика,

Образовательная программа «Финансовая разведка и управление рисками бизнеса»

Профиль:

«Финансовая разведка и управление рисками бизнеса»

Рекомендовано

Факультет экономики и бизнеса

(протокол № 8 от 19.05.2026 г.)

Одобрено

Кафедра экономической безопасности и управления рисками

(протокол № 11 от 06.05.2026 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	6
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	7
5.1. Содержание дисциплины	7
5.2. Учебно – тематический план	9
5.3. Содержание семинаров, практических занятий	11
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	13
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	13
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	16
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	18
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	15
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	15
10. Методические указания для обучающихся по освоению дисциплины	29
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)	30
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	30



1. Наименование дисциплины

Цифровой форензик и информационная безопасность

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
ПКП-1	Способность разрабатывать и внедрять мероприятия по управлению рисками в различных функциональных направлениях организации, включая подготовку методических и нормативных документов, а также корректировку реестров рисков в рамках отдельных бизнес-процессов	Анализировать реестры рисков организации и определять ключевые уязвимости в бизнес-процессах.	Знать: Подходы к идентификации, анализу и оценке информационных рисков в разрезе функциональных подразделений и этапов бизнес-процессов, а также методы приоритизации рисков. Уметь: Ориентироваться в реестрах рисков, выделять приоритетные, сопоставлять и группировать по функциональным направлениям деятельности и отдельным этапам бизнес-процессов, вычленять элементы бизнес-процессов, обладающие особой уязвимостью к реализации информационных рисков.
		Разрабатывать методические рекомендации и нормативные документы для управления рисками в различных подразделениях.	Знать: Взаимосвязи рисков, связанных с уязвимостями цифровых носителей и технологий, с направлениями деятельности различных функциональных подразделений; основные методы управления соответствующими рисками, принципы работы с нормативными документами, регулирующими подходы к управлению рисками. Уметь: Устанавливать взаимосвязи рисков, связанных с уязвимостями цифровых носителей и технологий, с на-



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
			правлениями деятельности различных функциональных подразделений; выбирать адекватные методы управления соответствующими рисками, формулировать значимые особенности подходов к управлению рисками для отражения в нормативных документах.
		Формировать предложения по корректировке риск-ориентированных процедур на основе результатов анализа данных.	Знать: Принципы, лежащие в основе риск-ориентированного подхода к управлению рисками, связанными с уязвимостями цифровых носителей и технологий, возможные варианты процедур, снижающих данные риски. Уметь: Учитывать распределение ресурсов организации при разработке риск-ориентированных процедур, адаптировать результаты анализа уязвимостей цифровых носителей и технологий.
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: базовые схемы использования цифровых технологий с целью ОД/ФТ и типовые признаки сомнительных операций и сделок. Уметь: прогнозировать риски, связанные с ОД/ФТ в области использования информационных технологий.
		Документировать выявленные риски и составлять отчеты для представления руководству или контролирующим органам.	Знать: уязвимости процесса сбора и хранения извлеченных данных с целью последующего использования руководством организации, регуляторными и правоохранительными структурами. Уметь: составлять документы и отчеты о выявленных рисках последующего использования руководством орга-



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
			низации, регуляторными и правоохранительными структурами.
		Использовать автоматизированные системы мониторинга для выявления аномалий в финансовых потоках.	Знать: возможности и ограничения инструментов современных цифровых технологий для выявления признаков сомнительных операций и сделок и аномалий финансовых потоков. Уметь: составлять план расследования инцидента и форензик-расследования с учетом возможностей и ограничений автоматизированных систем мониторинга.



3. Место дисциплины в структуре образовательной программы

Дисциплина «Цифровой форензик и информационная безопасность» относится к «Модулю "Выявление и расследование незаконных финансовых операций"».

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

Очная форма обучения

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 7 (в часах)
Общая трудоемкость дисциплины	3/108	108
<i>Контактная работа – Аудиторные занятия</i>	<i>34</i>	<i>34</i>
<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	Домашнее творческое задание	Домашнее творческое задание
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. Понятие, цели и содержание цифрового форензика, взаимосвязь с обеспечением информационной безопасности.

Компьютерная криминалистика. Компьютерное преступление. Роль компьютера и цифровой информации в преступлениях. Инцидент. Цифровые доказательства. Цели и порядок расследования инцидента. Цифровой форензик. Его возможности и ограничения для проведения расследований корпоративных мошенничеств и злоупотреблений. Правовые и этические рамки финансовых расследований. Особенности законодательного регулирования. Необходимые компетенции специалистов.

Тема 2. Носители цифровой информации. Противодействие цифровому форензику (антифорензика).

Классификация носителей цифровой информации. Цифровые устройства и их взаимодействие. Принципы работы файловых систем, операционных систем, клиент-серверных систем и баз данных. Риски информационной безопасности. Антифорензика (анти-криминалистика) и ее методы. Инструменты антифорензики и их возможности. Типы компьютерных преступников. Основные проблемы при борьбе с кибер-преступностью. Риск-ориентированный подход при планировании и осуществлении мероприятий.

Тема 3. Содержание и этапы проведения расследования инцидентов (компьютерная криминалистика).

Расследования по факту инцидентов информационной безопасности, совершенных краж или мошеннических действий. Реагирование на инциденты информационной безопасности. Сбор релевантных данных. Срок жизни цифровой информации и его влияние на планирование оперативных мероприятий. Извлечение данных из носителей и их обработка и анализ. Восстановление хронологии событий удаленных данных. Проведение исследований по фактам утечек цифровых данных. Исследование облачных систем на предмет несанкционированного доступа. Подготовка официального заключения.



Тема 4. Применение средств, методик, инструментов компьютерной криминалистики и eDiscovery-подходов в корпоративных расследованиях.

Роль eDiscovery подхода в корпоративных расследованиях. Типичные сценарии (утечка данных, инсайдерские угрозы, нарушение политики информационной безопасности, трудовые споры). Основные этапы корпоративного расследования и их особенности. Современные методики, инструменты и технологии корпоративных расследований с применением eDiscovery подхода. Анализ больших объемов электронной почты и документации. Взятие под контроль и временное сопровождение ИТ-инфраструктуры при смене менеджмента компании. Помощь в раскрытии цифровых доказательств в ходе судебных разбирательств.

Тема 5. Современные технологические решения в области информационной безопасности, расследований инцидентов и eDiscovery-подходов.

Технологические решения в области защиты инфраструктуры. Технологические решения в области мониторинга, исследования и анализа. Технологические решения в области защиты данных. Технологические сервисы для поддержки бизнеса.

Современные направления развития Fintech-индустрии и их влияние на информационную безопасность участников рынка.



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	Понятие, цели и содержание цифрового форензика, взаимосвязь с обеспечением информационной безопасности.	12	4	2	2	8
2	Носители цифровой информации. Противодействие цифровому форензику (антифорензика).	12	4	2	2	8
3	Содержание и этапы проведения расследования инцидентов (компьютерная криминалистика).	12	4	2	2	8
4	Применение средств, методик, инструментов компьютерной криминалистики и eDiscovery-подходов в корпоративных расследованиях.	37	12	6	6	25



п/ п	Наименование тем (разделов) дисциплины	Трудоемкость в часах				
		Всего	Контактная работа - Аудиторная работа			Самостоятельная работа
			Общая, в т.ч.:	Лекции	Семинары, практические занятия	
5	Современные технологические решения в области информационной безопасности, расследований инцидентов и eDiscovery-подходов.	35	10	4	6	25
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
Понятие, цели и содержание цифрового форензика, взаимосвязь с обеспечением информационной безопасности.	1. Чем отличается компьютерная криминалистика от цифровой форензики? 2. Какие задачи в области защиты компании от внутренних злоупотреблений может помочь решить цифровой форензик? 3. Каковы основные современные вызовы для обеспечения информационной безопасности?	Устный опрос, выступления с докладами с последующим обсуждением, разбор ситуаций.
Носители цифровой информации. Противодействие цифровому форензику (антифорензика).	1. Какие особенности взаимодействия цифровых носителей следует знать специалистам в области цифрового форензика? 2. Каковы самые эффективные методы антифорензики? 3. Как влияют типы кибер-преступников на подходы к расследованию инцидента?	Устный опрос, выступления с докладами с последующим обсуждением, разбор ситуаций.
Содержание и этапы проведения расследования инцидентов (компьютерная криминалистика).	1. Какая информация об IT-инфраструктуре важна для сбора цифровых доказательств? 2. Каковы порядок и особенности извлечения данных из цифровых носителей? 3. Как влияют удаленные данные на порядок расследования инцидента?	Устный опрос, выступления с докладами с последующим обсуждением, разбор ситуаций.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Применение средств, методик, инструментов компьютерной криминалистики и eDiscovery-подходов в корпоративных расследованиях.	1. В каких случаях проведения корпоративного расследования могут быть полезны средства компьютерной криминалистики. 2. В чем суть e-Discovery подходов? 3. Как используются материалы расследований в ходе судебных разбирательств и досудебных переговоров?	Устный опрос, выступления с докладами с последующим обсуждением, разбор ситуаций.
Современные технологические решения в области информационной безопасности, расследований инцидентов и eDiscovery-подходов.	1. Какие задачи решают современные технологии в области защиты IT-инфраструктуры? 2. Каковы возможности и ограничения современных технологических разработок в области защиты данных? 3. Каковы тренды и перспективы развития рынка форензик-услуг в современной России?	Устный опрос, выступления с докладами с последующим обсуждением, разбор ситуаций.



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
Понятие, цели и содержание цифрового форензика, взаимосвязь с обеспечением информационной безопасности.	1. Особенности форензика в облачных средах и виртуализации. 2. Форензик-анализ блокчейна и криптовалютных операций. 3. Этические дилеммы и конфликт интересов в цифровом форензике.	Изучение учебной литературы. Подготовка к опросу и научной дискуссии. Подготовка и выполнение домашнего творческого задания.
Носители цифровой информации. Противодействие цифровому форензику (антифорензика).	1. Противодействие сетевой форензике. 2. Юридические и тактические проблемы при изъятии цифровых носителей, защищенных антифорензикой. 3. Экономические издержки конфликта юрисдикций мета нахождения цифровых носителей при трансграничных расследованиях.	Изучение учебной литературы. Подготовка к опросу и научной дискуссии. Подготовка и выполнение домашнего творческого задания.
Содержание и этапы проведения расследования инцидентов (компьютерная криминалистика).	1. Судебная экспертиза памяти - анализ оперативной памяти для выявления скрытых процессов. 2. Форензика Интернета вещей и встраиваемых систем.	Изучение учебной литературы. Подготовка к опросу и научной дискуссии. Подготовка и выполнение домашнего творческого задания.



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
	3. Цифровая криминалистика криптовалютных транзакций.	
Применение средств, методик, инструментов компьютерной криминалистики и eDiscovery-подходов в корпоративных расследованиях.	1. Роль экономиста в подготовке цифровых доказательств для суда и регуляторов. 2. Методы противодействия инсайдерским угрозам. 3. Экономический анализ электронной переписки с целью выявления скрытых транзакций и сговоров.	Изучение учебной литературы. Подготовка к опросу и научной дискуссии. Подготовка и выполнение домашнего творческого задания.
Современные технологические решения в области информационной безопасности, расследований инцидентов и eDiscovery-подходов.	1. Использование автоматизация больших данных в расследованиях. 2. Форензика мобильных устройств и мессенджеров. 3. Криптовалютные следы в корпоративных расследованиях.	Изучение учебной литературы. Подготовка к опросу и научной дискуссии. Подготовка и выполнение домашнего творческого задания.



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

Примерные темы для подготовки домашнего творческого задания.

1. Экономическая целесообразность внедрения цифрового форензика в компаниях.
2. Правовые риски кредитных организаций при несвоевременном реагировании на инциденты информационной безопасности.
3. Ценные и необходимые компетенции экономиста, занятого форензик-расследованиях.
4. Этические дилеммы при анализе личной переписки сотрудников в корпоративном расследовании.
5. Экономическая модель злоумышленника: отношение затрат на антифорензику и ожидаемого дохода.
6. Основные типы компьютерных преступлений с финансовой точки зрения (ущерб, частота, отраслевая специфика)
7. Риски для финансовой отчетности компании при использовании сотрудниками методов антифорензики.
8. Проблема доказывания умысла киберпреступления со стороны контрагента и значение экономической экспертизы нетипичного поведения.
9. Планирование оперативных мероприятий с учетом "срока жизни" цифровой информации.
10. Применение методик оценки ущерба от утечки цифровых данных для последующего применения в судебном разбирательстве.
11. Использование цифровых следов для восстановления хронологии финансовых махинаций.
12. Анализ больших объемов электронной почты как инструмент выявления картельных сговоров и откатов.
13. Снижение рисков организации путем временного сопровождения ИТ-инфраструктуры при смене топ-менеджмента.
14. Инструменты цифрового форензика для выявления признаков сомнительных операций в области ПОД/ФТ.
15. Особенности подготовки финансово-аналитической части заключения для суда на основе eDiscovery.
16. Эффективность использования eDiscovery-подходов в спорах с налоговыми органами.
17. Технологии "песочницы" для безопасного анализа подозрительных финансовых операций.



18. Риски ОД/ФТ при использовании DeFi-протоколов и некастодиальных кошельков.
19. Цифровой рубль и технология распределенного реестра: новые возможности для форензика и контроля целевого использования бюджетных средств.
20. Экономика преступности: востребованность услуг, формирование цен на услуги хакеров, влияние на приоритезацию угроз со стороны добросовестных участников.
21. Методика расчета стоимости восстановления утраченных по причине атаки цифровых данных для оценки риска и его приоритезации.
22. Возможности и ограничения использования цифровых следов в трансграничных финансовых расследованиях.

Дополнительная информация

Примерные темы докладов.

1. Роль сетей и веб-браузеров в обеспечении доступа пользователей к глобальной информации. Анализ стека и веб-браузеров и его экономическая составляющая.
2. Анализ сетевого трафика, его методики и экономика оптимизации сетевой структуры.
3. Экономические аспекты технологии создания объектно-ориентированных баз данных.
4. Использование мобильной форензики в банковском секторе экономики.
5. Экономические составляющие технологии создания распределенных баз данных для целей форензика и информационной безопасности.
6. Использование Федеральной налоговой службой технологий представления информации и кодирования данных.
7. Применение в форензик-расследованиях технологии моделирования баз данных.
8. Применение методов извлечения данных и инструментов их анализа в целях цифрового форензика.
9. Использование комплексов технических и программных средств (ПАКов) для выполнения задач форензики и обеспечения информационной безопасности на примере банковского сектора экономики.
10. Использование поиска артефактов на HDD и периферии для целей форензика и обеспечения информационной безопасности.
11. Методы деревьев и их использование для расследования инцидентов в рамках проведения мероприятий цифрового форензика.



12. Создание и использование экспертных систем для целей обеспечения информационной безопасности и экономическая целесообразность их применения.

13. Возможности и ограничения анализа e-mail сообщений в целях форензик-расследований на примере крупного банка.

Примеры ситуаций для разбора.

1. В организации был осуществлен сбор данных в ходе форензик-расследования. Совокупный объем извлеченной информации составил 3 терабайта информации. Участники расследования получили непосредственный доступ к двум ПК и двум телефонам, удаленный доступ к другим двум ПК и серверу.

Сколько могло быть кастодианов (владельцев релевантных данных)? Как отразится на расследовании, понимает ли заказчик, где в его инфраструктуре могут храниться потенциально релевантные данные? Имеет ли значение, какого объема носители данных на исследованных устройствах? Какое имеет значение территориальное расположение устройств для целей форензик-расследования?

2. У руководства компании появилось разумное подозрение, что чувствительная корпоративная информация о системе ценообразования для разных категорий дистрибуторов стала известна третьим лицам. Предполагается, что причиной стала утечка инсайдерской информации по вине внутренних сотрудников.

Что следует предпринять компании для идентификации лиц, причастных к нарушению? Какие действия помогут установить причины, выявить каналы утечки данных и уязвимые места в ИТ-инфраструктуре? Раскройте значение внутренних регламентов для обеспечения информационной безопасности применительно к данной ситуации.



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
ПКП-1. Способность разрабатывать и внедрять мероприятия по управлению рисками в различных функциональных направлениях организации, включая подготовку мето-	Анализировать реестры рисков организации и определять ключевые уязвимости в бизнес-процессах.	Знать: Подходы к идентификации, анализу и оценке информационных рисков в разрезе функциональных подразделений и этапов бизнес-процессов, а также методы приоритизации рисков. Уметь: Ориентироваться в реестрах рисков, выделять	1. Организация столкнулась с хакерской атакой, которая повлекла за собой утечку данных о движениях материальных ценностей в комплексе складских помещений. На какие функциональные подразделения этот факт оказал влияния? Какие информационные риски связаны с дальнейшей деятельностью компании? 2. Компания по добыче нефти подозревает своего директора по маркетингу в промышленном шпионаже. Поставлена задача составить план мероприятий в рамках форензик-расследования. Какая информация из реестра рисков может быть полезна для составления данного плана?



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
дических и нормативных документов, а также корректировку реестров рисков в рамках отдельных бизнес-процессов		приоритетные, сопоставлять и группировать по функциональным направлениям деятельности и отдельным этапам бизнес-процессов, включать элементы бизнес-процессов, обладающие особой уязвимостью к реализации информационных рисков.	
	Разрабатывать методические рекомендации и нормативные документы для управления рисками в различных подразделениях.	Знать: Взаимосвязи рисков, связанных с уязвимостями цифровых носителей и технологий, с направлениями деятельности различных функциональных подразделе-	1. Компания, работающая в сфере доставки потребительских товаров, выявила риски утечки персональных данных клиентов. На каких функциональных подразделениях отразится реализация такого риска? Какие из подразделений предположительно окажутся в зоне высокого уровня риска. Какие форензик-мероприятия целесообразно порекомендовать руководству для разработки методов снижения данного риска? 2. Раскройте специфику основных методических рекомендаций крупным компаниям для снижения влияния распространенных компьютерных преступлений на деятельность различных функциональных подразделений.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		ний; основные методы управления соответствующими рисками, принципы работы с нормативными документами, регулируемыми подходы к управлению рисками. Уметь: Устанавливать взаимосвязи рисков, связанных с уязвимостями цифровых носителей и технологий, с направлениями деятельности различных функциональных подразделений; выбирать адекватные методы управления соответ-	



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		ствующими рисками, формулировать значимые особенности подходов к управлению рисками для отражения в нормативных документах.	
	Формировать предложения по корректировке риск-ориентированных процедур на основе результатов анализа данных.	Знать: Принципы, лежащие в основе риск-ориентированного подхода к управлению рисками, связанными с уязвимостями цифровых носителей и технологий, возможные варианты процедур, снижающих данные риски. Уметь: Учитывать распределение ресур-	1. Компания, работающая в сфере авиаперевозок, выявила риски уязвимостей к кибератакам своих информационных баз. Какие форензик-мероприятия целесообразно порекомендовать руководству для разработки методов снижения данного риска? 2. Строительная компания регулярно участвует и часто выигрывает тендеры на выполнение гособоронзаказа. Обозначьте не менее трех направлений, которая могут стать приоритетными для разработки мероприятия обеспечения информационной безопасности. В рамках этих направлений выделите основные возможные цели злоумышленников. Выдвинете предположения, какие типы кибер-преступников могут быть наиболее активны. Раскройте, как данная информация может быть использована в формировании предложений по корректировке риск-ориентированных процедур.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		сов организации при разработке риск-ориентированных процедур, адаптировать результаты анализа уязвимостей цифровых носителей и технологий.	
ПКП-2. Способность выявлять, документировать и анализировать риски, связанные с отмыванием доходов, полученных преступным путем, и финансированием терро-	Проводить анализ операций и сделок для выявления признаков сомнительных транзакций.	Знать: базовые схемы использования цифровых технологий с целью ОД/ФТ и типовые признаки сомнительных операций и сделок. Уметь: прогнозировать риски, связанные с ОД/ФТ в области использования информационных технологий.	1.Банк внедрил новое мобильное приложение с биометрической идентификацией. Предложите чек-лист для проверки с целью выявления уязвимостей проекта в области ПОД/ФТ. 2.Раскройте, какие характеристики работы криптобирж позволяют использовать их для проведения транзакций с признаками сомнительных операций и сделок в области ОД/ФТ.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ризма, устанавливать признаки сомнительных операций и сделок, а также фиксировать соответствующие сведения в организации	Документировать выявленные риски и составлять отчеты для представления руководству или контролирующим органам.	Знать: уязвимости процесса сбора и хранения извлеченных данных с целью последующего использования руководством организации, регуляторными и правоохранительными структурами. Уметь: составлять документы и отчеты о выявленных рисках последующего использования руководством организации, регуляторными и правоохранительными структурами.	1. Компания, предоставляющая FTech услуги, провела форензик-расследование по заказу крупной высокотехнологичной производственной компании, которая столкнулась с налаженной системой утечек чувствительной информации о технических разработках. Были проверены несколько массивов лог-файлов с различных цифровых носителей и подготовлен отчет для предоставления цифровых доказательств в суде. Какие уязвимости использования данного отчета следует учесть при подготовке к судебному разбирательству? 2. Раскройте основные значимые для составления итогового отчета моменты, которые следует учитывать с начала и на протяжении форензик-расследования.
	Использовать автоматизированные си-	Знать: возможности и ограничения ин-	1. Крупный банк планирует внедрить API-доступ для финтех-партнеров, чтобы сторонние сервисы могли инициировать платежи для клиентов банка. Предложите список со-



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
	стемы мониторинга для выявления аномалий в финансовых потоках.	струментов современных цифровых технологий для выявления признаков сомнительных операций и сделок и аномалий финансовых потоков. Уметь: составлять план расследования инцидента и форензик-расследования с учетом возможностей и ограничений автоматизированных систем мониторинга.	мнительных операций для рекомендации разработчикам автоматизированной системы мониторинга. 2.В строительной компании выявили инцидент хищения средств через двойную оплату счета на крупную сумму, которая была осуществлена за месяц до увольнения директора по закупкам. Проведенная операция выявила наличие уязвимостей в автоматизированной системе внутренней проверки соответствия счетов договорным обязательствам. Составьте план форензик-расследования.



Примеры практико-ориентированных заданий

1. В ходе расследования сделана выгрузка цифровых данных и получен дамп почтового ящика менеджера по закупкам, преобразованный в электронную таблицу с полями: дата, от кого, кому, тема, тело письма. Рассматривается подозрение, что с одним из участников тендера на поставку сырья были согласованы условия до официального объявления торгов. Предложите ключевые слова и словосочетания для анализа переписки. Какие коммуникации будут подозрительными в данном контексте?

2. Уходящий генеральный директор имеет доступ к корпоративной CRM, облачному хранилищу и почте. В компании произошла смена собственника, и новый владелец опасается, чтобы уходящий генеральный директор не уничтожил и не скопировал важную финансовую информацию. Составьте пошаговый план действий, указывая какие цифровые активы следует защитить. Укажите для каждого шага риск, который снижается или предотвращается.

Примеры вопросов для подготовки к промежуточной аттестации

1. Роль компьютерной криминалистики и цифрового форензика в обеспечении информационной безопасности организаций.

2. Цели и этапы проведения форензик-расследований.

3. eDiscovery подходы и этапы eDiscovery проекта.

4. Сбор цифровых доказательств и особенности цифровых носителей.

5. Ключевые цифровые и технологические инновации в контуре системы безопасности

6. Возможные варианты применения в контуре СБ технологий Big data.

7. Возможные варианты применения в контуре СБ технологий распознавания видео/фото/голоса.

8. Контроль ИТ-инфраструктуры при смене менеджмента компании.

9. Уязвимости сбора и хранения данных в ходе и по результатам расследования: проверка целостности данных и их анализ.

10. Сетевая криминалистика, работа с метаданными и временными метками.

11. Инструменты и методы борьбы с экономическими преступлениями в цифровом форензике.

12. Основные разделы цифровой криминалистики (компьютерная форензика, сетевая форензика, форензика мобильных устройств и криминалистика криптографических схем)

13. Основные вехи развития кибер-преступности и современные цели цифрового форензика



14.Методы противодействия со стороны преступников цифровому форензику (криптография, стеганография, уничтожение данных)

15.Основные проблемы при борьбе с кибер-преступностью и их влияние на масштаб различных видов кибер-преступлений.

16.Информационные риски (опасность возникновения убытков или ущерба в результате применения информационных носителей и информационных технологий).

17.Доказательная сила логов и цепочка доказательности.

18.Срок жизни цифровой информации и оперативность в цифровой форензике.

19.Криминалистическая характеристика, типология компьютерных преступников, их применение в рамках риск-ориентированного подхода к расследованиям.

20.Современные программные разработки для целей цифрового форензика и обеспечения информационной безопасности организации.



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

Основная литература:

1. Вехов, Виталий Борисович Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. 3-е изд., пер. и доп Электрон. дан. Москва : Юрайт, 2026 485 с (Высшее образование) URL: <https://urait.ru/bcode/581669> (дата обращения: 27.02.2026). Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей <https://urait.ru/bcode/581669> ISBN 978-5-534-21152-8 : 2479.00. [БИК ID: RU2fURAIT2f581669]
2. Нестеров, А.В. Виртуальные следы в криминалистике : Учебник / А.В. Нестеров Электрон. дан. Москва : КноРус, 2024 153 с. Режим доступа: book.ru Internet access <https://book.ru/book/950616> ISBN 978-5-406-12176-4. [БИК ID: RU\bookru\bibl\950616]

Дополнительная литература:

1. Калмыков, И. А. Компьютерная криминалистика [Электронный ресурс] : лабораторный практикум. специальность 10.05.03 (090303.65) информационная безопасность автоматизированных систем. специализация «защищенные автоматизированные системы управления» / Калмыков И. А., Пелешенко В. С. Ставрополь : СКФУ, 2017 84 с. Книга из коллекции СКФУ - Информатика <https://e.lanbook.com/book/155227>. [БИК ID: RU-LAN-BOOK-155227]
2. Жердев, П. А. Расследование преступлений в сфере компьютерной информации [Электронный ресурс] : учебное пособие / Жердев П. А., Мерецкий Н. Е. Хабаровск : ДВГУПС, 2024 92 с. Рекомендовано Методическим советом в качестве учебного пособия Книга из коллекции ДВГУПС - Право. Юридические науки <https://e.lanbook.com/book/506837>. [БИК ID: RU-LAN-BOOK-506837]

Нормативные правовые акты:

1. Конституция РФ (ст. 23, 24, 29)
2. Уголовный кодекс РФ в текущей редакции.
3. Кодекс РФ об административных правонарушениях в текущей редакции.



4. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне" (с изменениями и дополнениями) .

5. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями)

6. Федеральный закон от 27 июля 2006 г. 152-ФЗ «О персональных данных» (с изменениями и дополнениями)

7. Федеральный закон от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (с изменениями и дополнениями)

8. Национальный стандарт ГОСТ Р ИСО/МЭК 27001 (информационные технологии) — Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности.

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 Znanium <http://www.znanium.com>
4. Электронно-библиотечная система "Университетская библиотека ОНЛАЙН" <http://biblioclub.ru/>
5. Образовательная платформа "ЮРАЙТ" <https://urait.ru/>



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 г. № 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. Браузеры (Chrome, Firefox) с драйверами (ChromeDriver, GeckoDriver)
2. Kaspersky
3. Microsoft Office (Windows)

Современные профессиональные базы данных и информационные справочные системы

1. Информационно-правовая система «Гарант»
2. Информационно-правовая система «Консультант Плюс»

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