Рабочая программа дисциплины (модуля)*

Цифровой форензик

Направление подготовки (специальность)

38.05.01 Экономическая безопасность

Направленность (профиль)

Судебная экономическая экспертиза и цифровая криминалистика

Присваиваемая квалификация (степень)

экономист (специалист)

Форма обучения

очная

Год(ы) набора 2026

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2026 г.

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре ОПОП
3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)
4. Объем дисциплины (модуля)
5. Структура и содержание дисциплины (модуля)
6. Фонд оценочных средств
6.1. Перечень видов оценочных средств
6.2. Типовые контрольные задания и иные материалы для текущей аттестации
6.3. Типовые контрольные вопросы и задания для промежуточной аттестации
6.4. Критерии оценивания
7. Учебно-методическое и информационное обеспечение дисциплины (модуля)
7.1. Рекомендуемая литература
7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"
7.3. Перечень информационных технологий
8. Материально-техническое обеспечение дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Специальные условия освоения дисциплины обучающимися с инвалидностью и ограниченными возможностями здоровья

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью дисциплины «Цифровой форензик» является формирование у студентов теоретических знаний в области раскрытия преступлений, связанных с компьютерной информацией, а также практических навыков исследования цифровых доказательств, методов поиска, получения и закрепления таких доказательств.

Результаты обучения по дисциплине направлены на достижение индикаторов, соответствующих компетенции ПК-4:

ПК-4.1. Применяет знания для подготовки аналитических материалов и проведения судебных экономических экспертных исследований

ПК-4.2. Владеет методами осуществления экономической экспертизы нормативных правовых актов в целях обнаружения потенциальных угроз экономической безопасности

ПК-4.3. Умеет применять методики судебных экономических экспертных исследований в профессиональной деятельности, в том числе с использованием современных информационных технологий

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.В.18

2.1 Требования к предварительной подготовке обучающегося:

Дисциплина "Цифровой форензик" базируется на знаниях, полученных в ходе освоения следующих ранее изученных дисциплин:

Информационные технологии в профессиональной деятельности

Основы цифровой криминалистики и криминалистического исследования

Информационная безопасность экономических систем

Судебная финансово-экономическая экспертиза

Применение цифровых технологий в деятельности правоохранительных органов

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Освоение дисциплины "Цифровой форензик" необходимо для последующего изучения ряда дисциплин, а также для подготовки к прохождению государственной итоговой аттестации

Подготовка к сдаче и сдача государственного экзамена

Расследование преступлений экономической направленности

Актуальные проблемы экономической безопасности в современных условиях

Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-4: Способен осуществлять экономическую экспертизу нормативных правовых актов в целях обнаружения потенциальных угроз экономической безопасности и применять методики судебных экономических экспертных исследований в профессиональной деятельности, в том числе с использованием современных информационных технологий

Знать:

инструменты для проведения криминалистического анализа и сбора цифровых доказательств;
способы подготовки аналитических материалов и проведения судебных экономических экспертных исследований.

Уметь:

применять методики судебных экономических экспертных исследований в профессиональной деятельности, в том числе с использованием современных информационных технологий;
документировать цифровые доказательства с соблюдением правовых норм;
проводить криминалистический анализ предоставленной информации для ответа на поставленные вопросы.

Владеть:

методиками криминалистических исследований в профессиональной деятельности, в том числе с использованием современных информационных технологий;
навыками поиска цифровых следов в компьютерных системах, фиксации этих следов, анализа собранных материалов с целью выявления источника атаки и восстановления работоспособности системы;
навыками подготовки отчета (заключения) о криминалистическом исследовании.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	инструменты для проведения криминалистического анализа и сбора цифровых доказательств;
3.1.2	способы подготовки аналитических материалов и проведения судебных экономических экспертных исследований.
3.2	**Уметь:**
3.2.1	применять методики судебных экономических экспертных исследований в профессиональной деятельности, в том числе с использованием современных информационных технологий;
3.2.2	документировать цифровые доказательства с соблюдением правовых норм;
3.2.3	проводить криминалистический анализ предоставленной информации для ответа на поставленные вопросы.
3.3	**Владеть:**
3.3.1	методиками криминалистических исследований в профессиональной деятельности, в том числе с использованием современных информационных технологий;
3.3.2	навыками поиска цифровых следов в компьютерных системах, фиксации этих следов, анализа собранных материалов с целью выявления источника атаки и восстановления работоспособности системы;
3.3.3	навыками подготовки отчета (заключения) о криминалистическом исследовании.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость			**4 ЗЕТ**
Часов по учебному плану	:	144	Виды контроля в семестрах:
в том числе	:		
аудиторные занятия	:	68	экзамены 9
самостоятельная работа	:	36,7	
часов на контроль	:	36	
контактная работа: 71,3			
ИКР: 3,3			

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код заняти	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Цифровой форензик: понятие, задачи и сферы применения			
1.1	Понятие и виды цифровых преступлений /Лек/	9	2	Э1 Э2 Э3
1.2	Понятие и виды цифровых преступлений /Пр/	9	2	Э1 Э2 Э3
1.3	Понятие и виды цифровых преступлений /Ср/	9	2	Э1 Э2 Э3
1.4	Цифровые следы: понятие, виды, характеристика /Лек/	9	2	Э1 Э2 Э3
1.5	Цифровые следы: понятие, виды, характеристика /Пр/	9	2	Э1 Э2 Э3
1.6	Цифровые следы: понятие, виды, характеристика /Ср/	9	2	Э1 Э2 Э3
	Раздел 2. Процесс и основные этапы расследования цифровых преступлений			
2.1	Этапы расследования цифровых преступлений и их содержание /Лек/	9	2	Э1 Э2 Э3
2.2	Этапы расследования цифровых преступлений и их содержание /Пр/	9	2	Э1 Э2 Э3

2.3	Этапы расследования цифровых преступлений и их содержание /Ср/	9	1	Э1 Э2 Э3
2.4	Методы и инструменты цифровой криминалистики, применяемые при расследовании компьютерных преступлений /Лек/	9	2	Э1 Э2 Э3
2.5	Методы и инструменты цифровой криминалистики, применяемые при расследовании компьютерных преступлений /Пр/	9	2	Э1 Э2 Э3
2.6	Методы и инструменты цифровой криминалистики, применяемые при расследовании компьютерных преступлений /Ср/	9	1	Э1 Э2 Э3
2.7	Обнаружение и фиксация цифровых доказательств. /Лек/	9	2	Э1 Э2 Э3
2.8	Обнаружение и фиксация цифровых доказательств /Пр/	9	2	Э1 Э2 Э3
2.9	Обнаружение и фиксация цифровых доказательств /Ср/	9	1	Э1 Э2 Э3
2.10	Анализ данных: проведение криминалистических исследований цифровой информации и вредоносных программ /Лек/	9	2	Э1 Э2 Э3
2.11	Анализ данных: проведение криминалистических исследований цифровой информации и вредоносных программ /Пр/	9	2	Э1 Э2 Э3
2.12	Анализ данных: проведение криминалистических исследований цифровой информации и вредоносных программ /Ср/	9	1	Э1 Э2 Э3
	Раздел 3. Исследование инцидентов с жесткими дисками и файловыми системами			
3.1	Исследование инцидентов с жесткими дисками и файловыми системами /Лек/	9	2	Э1 Э2 Э3
3.2	Исследование инцидентов с жесткими дисками и файловыми системами /Пр/	9	2	Э1 Э2 Э3
3.3	Исследование инцидентов с жесткими дисками и файловыми системами /Ср/	9	1	Э1 Э2 Э3
	Раздел 4. Техники, затрудняющие цифровую криминалистическую экспертизу			
4.1	Техники, затрудняющие цифровую криминалистическую экспертизу /Лек/	9	2	Э1 Э2 Э3
4.2	Техники, затрудняющие цифровую криминалистическую экспертизу /Пр/	9	2	Э1 Э2 Э3
4.3	Техники, затрудняющие цифровую криминалистическую экспертизу /Ср/	9	2	Э1 Э2 Э3
	Раздел 5. Криминалистическая экспертиза операционных систем			
5.1	Криминалистическая экспертиза операционных систем /Лек/	9	2	Э1 Э2 Э3
5.2	Криминалистическая экспертиза операционных систем /Пр/	9	2	Э1 Э2 Э3
5.3	Криминалистическая экспертиза операционных систем /Ср/	9	2	Э1 Э2 Э3
	Раздел 6. Сетевая криминалистика: сетевые уязвимости, сетевые атаки, исследование сетевого трафика			
6.1	Сетевая криминалистика: сетевые уязвимости, сетевые атаки, исследование сетевого трафика /Лек/	9	2	Э1 Э2 Э3
6.2	Сетевая криминалистика: сетевые уязвимости, сетевые атаки, исследование сетевого трафика /Пр/	9	2	Э1 Э2 Э3
6.3	Сетевая криминалистика: сетевые уязвимости, сетевые атаки, исследование сетевого трафика /Ср/	9	2	Э1 Э2 Э3
	Раздел 7. Расследование взлома веб-серверов			
7.1	Расследование взлома веб-серверов /Лек/	9	2	Э1 Э2 Э3

7.2	Расследование взлома веб-серверов /Пр/	9	2	Э1 Э2 Э3
7.3	Расследование взлома веб-серверов /Ср/	9	2	Э1 Э2 Э3
	Раздел 8. Расследование взлома серверов баз данных			
8.1	Расследование взлома серверов баз данных /Лек/	9	2	Э1 Э2 Э3
8.2	Расследование взлома серверов баз данных /Пр/	9	2	Э1 Э2 Э3
8.3	Расследование взлома серверов баз данных /Ср/	9	2	Э1 Э2 Э3
	Раздел 9. Облачная криминалистика			
9.1	Облачная криминалистика /Лек/	9	2	Э1 Э2 Э3
9.2	Облачная криминалистика /Пр/	9	2	Э1 Э2 Э3
9.3	Облачная криминалистика /Ср/	9	2	Э1 Э2 Э3
	Раздел 10. Криминалистическая экспертиза вредоносных программ			
10.1	Криминалистическая экспертиза вредоносных программ /Лек/	9	2	Э1 Э2 Э3
10.2	Криминалистическая экспертиза вредоносных программ /Пр/	9	2	Э1 Э2 Э3
10.3	Криминалистическая экспертиза вредоносных программ /Ср/	9	2	Э1 Э2 Э3
	Раздел 11. Криминалистическая экспертиза электронной почты			
11.1	Криминалистическая экспертиза электронной почты /Лек/	9	2	Э1 Э2 Э3
11.2	Криминалистическая экспертиза электронной почты /Пр/	9	2	Э1 Э2 Э3
11.3	Криминалистическая экспертиза электронной почты /Ср/	9	2	Э1 Э2 Э3
	Раздел 12. Криминалистическая экспертиза мобильных устройств			
12.1	Криминалистическая экспертиза мобильных устройств /Лек/	9	2	Э1 Э2 Э3
12.2	Криминалистическая экспертиза мобильных устройств /Пр/	9	2	Э1 Э2 Э3
12.3	Криминалистическая экспертиза мобильных устройств /Ср/	9	2	Э1 Э2 Э3
	Раздел 13. Подготовка отчета об исследовании инцидента. Свидетельство в суде			
13.1	Подготовка отчета об исследовании инцидента. Свидетельство в суде /Лек/	9	2	Э1 Э2 Э3
13.2	Подготовка отчета об исследовании инцидента. Свидетельство в суде /Пр/	9	2	Э1 Э2 Э3
13.3	Подготовка отчета об исследовании инцидента. Свидетельство в суде /Ср/	9	9,7	Э1 Э2 Э3
13.4	Текущий контроль /ИКР/	9	3,3	Э1 Э2 Э3

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Тесты
Контрольные вопросы

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Типовые тесты:

1. По каким причинам может происходить утрата цифровых следов?
1) возникновение и устранение ошибок;
2) изменение цифрового пространства в связи с его обновлением;
3) устаревание, окончание срока эксплуатации или полный расход ресурса материального носителя;
4) утрата цифровых следов невозможна.

2. В качестве следообразующего объекта выступает:
1) информационная среда;
2) программный код;
3) компьютер;
4) машинный код.

3. К физическим носителям можно отнести:
1) облако;
2) QR-код;
3) сервер;
4) дисковое пространство.

4. В классификацию баз данных для использования в судебно-экспертной деятельности по содержанию входят:
1) базы данных, содержащие сведения по объектам судебных экспертиз;
2) базы персональных данных;
3) базы данных, содержащие экспертные заключения по различным видам судопроизводства;
4) базы экспериментальных данных.

5. Причинами возникновения «цифрового мусора» могут быть:
1) любые действия пользователя;
2) аппаратные ошибки;
3) действие вредоносного вируса;
4) ошибки вычислений.

6. Как называется информация, переданная или полученная пользователем информационно-телекоммуникационной сети?
1) электронное сообщение;
2) сайт в сети Интернет;
3) страница сайта в сети Интернет;
4) электронный документ.

7. Цифровые технологии характеризуются:
1) передачей значительного объема информации без потери ее качества;
2) ограниченным сроком хранения информации;
3) большой скоростью передачи информации;
4) объективностью получаемой информации.

8. К цифровым техническим средствам, используемым для запечатления хода следственного действия, окружающей обстановки, обнаруженных следов и объектов, относятся:
1) цифровые технические средства фиксации информации;
2) цифровые технические средства поиска информации;
3) вспомогательные цифровые технико-криминалистические средства;
4) аппаратно-программные комплексы.

9. Что понимается под документированной информацией, представленной в электронной форме, т. е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах?
1) электронный документ;

2) страница сайта в сети Интернет;
3) электронное сообщение;
4) сайт в сети Интернет.

10. Какие виды компьютерных атак существуют?
1) DNS-атаки;
2) HTTP-атаки;
3) OS-атаки;
4) TCP-атаки.

11. Какие критерии отличают цифровые технические средства от иных технических средств?
1) способность устройства работать с цифровыми сигналами;
2) наличие программного обеспечения, необходимого для функционирования цифрового технического средства;
3) цифровое техническое средство создано из электронных компонентов и работает за счет потребления электроэнергии;
4) функционирование при условии совместной работы с компьютером.

12. Что такое совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств?
1) информационная система;
2) электронный журнал;
3) информационно-телекоммуникационная сеть;
4) сайт в сети Интернет.

13. Какой тактический прием целесообразно использовать по делам о преступлениях в сфере электронных средств платежа для опровержения алиби подозреваемого в ходе его допроса?
1) задавать подозреваемому вопросы, ответ на которые подсказывается содержанием вопросов;
2) задавать подозреваемому вопросы, активизирующие у него в памяти ассоциативные связи;
3) убеждение подозреваемого в необходимости давать полные и правдивые показания;
4) детализация показаний подозреваемого.

14. Как называется электронный носитель информации, который устанавливается в пользовательском оборудовании (оконечном оборудовании) и с помощью которого осуществляется идентификация абонента, и (или) пользователя услугами связи абонента – юридического лица либо индивидуального предпринимателя, и (или) пользовательского оборудования (оконечного оборудования) и обеспечивает доступ оборудования указанных абонента или пользователя к сети оператора подвижной радиотелефонной связи?
1) электронный ключ;
2) идентификационная карта;
3) идентификационный модуль;
4) электронная подпись.

15. Что в цифровой криминалистике означает машинный носитель информации?
1) сменный носитель данных, предназначенный для записи и считывания данных, представленных в стандартных цифровых кодах;
2) носитель любой цифровой информации;
3) сменный носитель данных;
4) электронный носитель информации.

16. В каком случае не допускается копирование информации?
1) если относительно копирования информации возражает ее владелец;
2) если информация защищена или архивирована;
3) если копированию подлежит большой объем информации;
4) если это может воспрепятствовать расследованию преступления.

17. Как называется система последовательно расположенных по времени и логически взаимосвязанных записей о прохождении компьютерной информации по линиям связи через коммутационное оборудование оператора?
1) трафик электронных следов;
2) путь электронных следов;
3) дорожка электронных следов;
4) цепочка электронных следов.

18. Какие существуют виды электронных ключей?
1) iButton;
2) HASP;
3) HardLock;
4) Blocker.

19. Электронные носители информации с позиций цифровой криминалистики относятся к категории:
1) следов – отображений;
2) следов – веществ;
3) следов – предметов и частей предметов;
4) идеальных следов.

20. В каком нормативном акте предусмотрен порядок изъятия электронных носителей информации при проведении следственных действий?
1) Уголовно-процессуальный кодекс РФ;
2) Уголовный кодекс РФ;
3) Конституция РФ;
4) Федеральный закон «Об информации, информационных технологиях и защите информации».

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

1. Дайте определение понятию «предмет цифровой криминалистики».
2. Дайте определение понятию «объект цифровой криминалистики».
3. Из каких элементов состоит система цифровой криминалистики?
4. Дайте определение понятию «криминалистическое исследование компьютерных устройств, информационных систем и информационно-телекоммуникационных сетей». Какие элементы входят в его систему?
5. Что представляет собой криминалистическое использование компьютерной информации и средств ее обработки? Какова его система?
6. Перечислите задачи цифровой криминалистики.
7. С какими разделами криминалистики, составляющими их частными теориями, и каким образом связана цифровая криминалистика?
8. Что является методологической основой цифровой криминалистики?
9. Назовите и кратко охарактеризуйте общенаучные методы цифровой криминалистики.
10. Назовите и охарактеризуйте специальные методы цифровой криминалистики.
11. Дайте определение понятию «цифровая криминалистика».
12. Дайте определение криминалистической модели преступлений, совершаемых с применением цифровых технологий.
13. Охарактеризуйте объект преступного посягательства как элемент криминалистической модели преступлений, совершаемых с применением цифровых технологий.
14. Назовите и охарактеризуйте особенности способа совершения преступлений с применением цифровых технологий как элемента криминалистической модели.
15. В чем выражается следовая картина преступлений, совершаемых с применением цифровых технологий?
16. Охарактеризуйте обстановку совершения преступлений с применением цифровых технологий как элемента криминалистической модели.
17. Охарактеризуйте мотив преступления, совершаемого с использованием цифровых технологий как структурный элемент криминалистической модели.
18. Что представляет собой цифровая информация?
19. Каковы свойства цифровой информации?
20. Какими специфическими признаками обладает цифровая информация?
21. По каким основаниям можно классифицировать цифровую информацию?
22. Каковы формы представления цифровой информации?
23. Что можно относить к материальным носителям цифровой информации?
24. Дайте определение понятию «электронный след».
25. Назовите цифровые следообразующие и следовоспринимающие объекты.
26. В каких материальных формах может существовать компьютерная программа?
27. На какие виды подразделяются компьютерные программы по своему функциональному назначению?
28. Раскройте особенности механизма образования цифровых следов.
29. Перечислите признаки цифровых следов.
30. Какую роль играют электронные носители информации в механизме образования цифровых следов?
31. В чем состоят информационная сущность и криминалистические особенности фиксации цифровых

следов?
32. Перечислите способы, с помощью которых документы в электронном виде направляются адресату.
33. Раскройте понятие «личный кабинет» и поясните способы доступа к нему.
34. Поясните назначение Единой системы идентификации и аутентификации.
35. Как с позиций цифровой криминалистики классифицируются документы в электронном виде?
36. Дайте определение понятию «электронный документ» и перечислите его криминалистические признаки.
37. Раскройте понятия «электронная подпись», «средства электронной подписи», «ключ электронной подписи», «ключ проверки электронной подписи», «сертификат ключа проверки электронной подписи», «квалифицированный сертификат».
38. Перечислите информацию, которую должен содержать квалифицированный сертификат.
39. На какие виды подразделяются электронные подписи по юридической силе?
40. Назовите криминалистические признаки неквалифицированной электронной подписи.
41. Назовите криминалистические признаки квалифицированной электронной подписи.
42. Перечислите участников электронного взаимодействия.
43. Какие признаки необходимо устанавливать и анализировать в процессе криминалистического исследования электронных юридически значимых документов?
44. Дайте определение понятию «электронный образ документа».
45. Какие признаки необходимо устанавливать и анализировать в процессе криминалистического исследования электронных образов юридически значимых документов?
46. Дайте понятие и назовите общие криминалистические признаки вредоносной компьютерной программы.
47. Раскройте содержание понятия «Ботнет».
48. Раскройте содержание понятия «компьютерная атака».
49. Дайте определение понятию «компьютерный инцидент». Как оно связано с понятием «компьютерная атака»?
50. Перечислите объекты и назовите субъектов критической информационной инфраструктуры.
51. Раскройте классификацию компьютерных атак.
52. Комплекс каких действий необходимо выполнить в случае деструктивного воздействия вредоносных компьютерных программ на критическую информационную инфраструктуру пользователей компьютерной сети?
53. Назовите криминалистически значимую информацию, которую необходимо установить специалисту в сфере судебных компьютерно-технических исследований и экспертиз в ходе предварительного исследования применения вредоносной компьютерной программы.
54. Какие действия необходимо осуществить при обнаружении признаков компьютерной атаки?
55. На что необходимо обратить особое внимание при исследовании доказательственной информации по факту совершения компьютерной атаки?
56. Дайте определение понятию «криминалистическое исследование компьютерных устройств и информационно-телекоммуникационных сетей».
57. Раскройте содержание понятия «электронный носитель информации». Какое криминалистическое значение он имеет?
58. Поясните, что представляет собой запись (регистрация, фиксация) информации.
59. На какие группы подразделяют электронные носители информации в цифровой криминалистике и почему?
60. Дайте определение понятию «машинный носитель информации».
61. По каким основаниям в цифровой криминалистике осуществляется их классификация и почему?
62. Каковы особенности предварительного криминалистического исследования электронного носителя и содержащейся в его памяти информации?
63. Какие фактические данные должны быть зафиксированы в протоколе осмотра электронного носителя и содержащейся в его памяти информации?
64. Раскройте структуру и содержание типового протокола получения криминалистической копии накопителя на жестком магнитном диске.
65. Назовите компьютерные программы, которые могут быть использованы для создания криминалистической копии электронного носителя информации.
66. Поясните понятие «хэш-функция». Назовите компьютерные программы, которые могут быть использованы для вычисления значений хэш-функций.
67. Какие компьютерные программы возможно использовать для блокирования записи информации на электронный носитель, с которого получается криминалистическая копия?
68. Дайте определение понятию «электронный ключ».
69. Поясните принцип работы электронного ключа.
70. Из каких компьютерных устройств состоит электронный ключ?
71. На какие виды подразделяются электронные ключи в зависимости от интерфейса подключения к ЭВМ?
72. Назовите типичные виды электронных ключей и раскройте особенности их работы.

73. Раскройте криминалистически значимые сведения о типичных способах обхода программно-аппаратных средств защиты, функционирующих на основе электронных ключей.
74. Поясните алгоритмы выявления признаков подделки электронного ключа и установления местонахождения его эмулятора.
75. Раскройте понятие «электронная вычислительная машина (ЭВМ)».
76. Назовите основания, по которым ЭВМ классифицируют в криминалистике.
77. Каковы цели осмотра ЭВМ и какие снимки необходимо сделать в ходе его производства?
78. Какие действия необходимо предпринять специалисту в начале осмотра ЭВМ?
79. Какие фактические данные необходимо зафиксировать в протоколе осмотра ЭВМ?
80. Назовите типичные следы и места их локализации, которые необходимо обнаружить и исследовать при производстве осмотра ЭВМ.
81. В чем состоит специфика предварительного криминалистического исследования сотовых радиотелефонов, как разновидности мобильных ЭВМ, и содержащейся в их памяти компьютерной информации?
82. Назовите действия, которые необходимо выполнить на подготовительном этапе осмотра сотового радиотелефона.
83. Раскройте алгоритм действий, осуществляемых во время рабочего этапа осмотра сотового радиотелефона.
84. Что такое идентификатор мобильного оборудования — IMEI? Как его определить? Какое криминалистическое значение он имеет?
85. Какие основные тематические разделы содержит меню пользователя сотового радиотелефона?
86. Какую криминалистически значимую компьютерную информацию можно получить с помощью программно-аппаратного комплекса UFED?
87. Что не следует делать при изъятии работающего сотового радиотелефона?
88. Какое криминалистическое значение имеют коды блокировки SIM-карты?
89. Перечислите действия, которые производятся на завершающем этапе осмотра сотового радиотелефона.
90. Перечислите современные технико-криминалистические средства, которые используют для обнаружения, фиксации, предварительного исследования и изъятия цифровых следов.
91. Дайте определение понятию «информационно-телекоммуникационная сеть».
92. По какому основанию и на какие виды классифицируют информационно-телекоммуникационные сети в цифровой криминалистике?
93. Дайте определение понятию «дорожка электронных следов» и раскройте содержание ее основных элементов.
94. Назовите оперативно-розыскные мероприятия и следственные действия, в ходе которых осуществляется обнаружение, фиксация, изъятие и предварительное исследование криминалистически значимой цифровой информации, обрабатываемой с помощью глобальных компьютерных сетей мобильной радиосвязи и Интернет.
95. Кто такие «операторы связи» и какую цифровую информацию они обязаны хранить на территории Российской Федерации и предоставлять в порядке, предусмотренном действующим законодательством?
96. Кто такие «организаторы распространения информации в сети «Интернет» и какие цифровые данные они обязаны хранить на территории Российской Федерации и предоставлять в установленном порядке для целей уголовного судопроизводства?
97. Назовите оперативно-розыскные мероприятия и следственные действия, направленные на обнаружение, фиксацию, изъятие и предварительное исследование криминалистически значимой цифровой информации, обрабатываемой с помощью глобальных компьютерных сетей мобильной радиосвязи и Интернет.
98. Назовите основания и раскройте порядок проведения оперативно-розыскных мероприятий, направленных на обнаружение, фиксацию, изъятие и предварительное исследование криминалистически значимой цифровой информации, обрабатываемой с помощью глобальных компьютерных сетей мобильной радиосвязи и Интернет.
99. Какие следственные действия могут быть использованы для получения цифровой доказательственной информации?
100. Какие оперативно-розыскные мероприятия могут быть использованы для получения цифровой доказательственной информации?
101. Каковы принципы операций с цифровой доказательственной информацией?
102. В чём состоит различие операций по изъятию носителя цифровой информации и её копированию?
103. В каких случаях целесообразно производить изъятие, а не копирование цифровой информации?
104. Какие критерии отличают цифровые технические средства от иных технических средств?
105. Перечислите и кратко охарактеризуйте цифровые технологии, используемые в качестве средств криминалистической техники.
106. Обоснуйте преимущества применения цифровых технологий, в качестве средств криминалистической техники.
107. Дайте определение понятию «цифровые технические средства».
108. Назовите и кратко охарактеризуйте цифровые технические средства фиксации информации.
109. Для решения каких криминалистических задач используются специализированные криминалистические

операционные системы?
110. Что относится к цифровым техническим средствам поиска и измерения?
111. Что такое специальное программное обеспечение?
112. Назовите разновидности тактических приемов работы с электронными доказательствами.
113. Определите общий порядок представление электронных доказательств прокурором в суде.
114. Какова правовая основа представления результатов оперативно-розыскной деятельности в электронном виде?
115. Раскройте порядок представления результатов оперативно-розыскной деятельности в электронном виде в суд.
116. Назовите основные объекты судебной компьютерно-технической экспертизы.
117. Выделите виды судебной компьютерно-технической экспертизы.
118. В каких случаях назначается судебная компьютерно-техническая экспертиза?
119. Сформулируйте требования, предъявляемы к определению содержания и формулировке вопросов для судебной компьютерно-технической экспертизы.
120. Определите виды вопросов, выносимых на судебную компьютерно-техническую экспертизу.
121. Приведите примеры вопросов, выносимых на судебную компьютерно-техническую экспертизу.
122. Из каких стадий состоит процесс экспертного исследования?
123. Из чего состоит оценка заключения эксперта по итогам проведения судебной компьютерно-технической экспертизы?

6.4. Критерии оценивания

Критерии оценивания тестовых заданий:

"Отлично" - 96-100% правильных ответов;
"Хорошо" - 76-95% правильных ответов;
"Удовлетворительно" - 60-75% правильных ответов;
"Неудовлетворительно" - менее 60 % правильных ответов.

Критерии оценивания результатов сдачи экзамена:

Оценка «отлично» (высокий уровень сформированности компетенций) выставляется в том случае, если обучающийся:
- свободно владеет научным стилем изложения материала, демонстрирует глубокое знание учебного материала, основополагающих категорий и понятий, знаком с дополнительной литературой, свободно оперирует нормами действующего законодательства Российской Федерации;
- дает аргументированный исчерпывающий ответ по существу, самостоятельно, без наводящих вопросов преподавателя;
- демонстрирует понимание причинно-следственных связей между явлениями и процессами, сопровождая их примерами, фактами, данными научных исследований;
- умеет объяснять проявление процессов и явлений на национальном, региональном и локальном уровнях, увязывает их с особенностями мирохозяйственного развития;
- владеет навыками обоснования собственных суждений по излагаемому вопросу, демонстрирует профессионально-личностную позицию.

Оценка «хорошо» (средний уровень сформированности компетенций) выставляется в том случае, если:
- ответ обучающегося соответствует указанным выше критериям, но содержание ответа имеет отдельные неточности (несущественные ошибки) в изложении теоретического и практического материала, отличается меньшей обстоятельностью, глубиной, полнотой;
- обучающийся допускает в своём ответе отдельный нечеткие формулировки и (или) излагает информацию, не относящуюся к раскрываемому вопросу;
- допущенные неточности (ошибки) исправляются обучающимся после уточняющих вопросов экзаменатора.

Оценка «удовлетворительно» (базовый уровень сформированности компетенций) выставляется в том случае, если:
- обучающийся демонстрирует знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности и существенные ошибки в определении понятий, формулировке положений;
- допускает неточности при обосновании причинно-следственных связей;
- не привлекает для аргументации ответа основные положения исследовательских, концептуальных и нормативных документов, не умеет обосновывать свои суждения;
- наблюдается нарушение логики изложения;

- ответ отличается низким уровнем самостоятельности суждений, не содержит собственной профессионально-личностной позиции.

Оценка «неудовлетворительно» (проверяемые компетенции не сформированы) выставляется в том случае, если:
- обучающийся демонстрирует разрозненные, бессистемные знания, допускает ошибки в определении понятий, формулировке теоретических положений, искажающие их смысл;
- учебный материал излагается беспорядочно и неуверенно, ответ на вопрос в целом неправильный и (или) содержащий в основном ошибочные положения;
- обучающийся не может дать обоснование причинно-следственных связей социально-экономических явлений и процессов, не умеет применять знания для объяснения реальных фактов, событий, явлений на национальном, региональном и локальном уровнях;
- имеет значительное количество пропусков аудиторных занятий по неуважительным причинам.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Инструменты для компьютерной криминалистики https://habr.com/ru/
Э2	Подборка ресурсов по цифровой форензике (искусству расследования кибер-преступлений) https://www.securitylab.ru/blog/
Э3	Образовательная платформа "Юрайт" https://urait.ru/

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

LMS Moodle

Adobe Reader

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. – Москва, [1999-]. – Доступ к полным текстам из сети ЧелГУ. – Режим доступа : http://elibrary.ru/defaultx.asp.

2. Консультант Плюс [Электронный ресурс] : официальный сайт компании Консультант Плюс. – Режим доступа : http://consultant.ru/, свободный.

3. ГАРАНТ [Электронный ресурс] : информационно-правовой портал [сайт]. – Режим доступа : http://garant.ru/, свободный.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран).

При проведении занятий лекционного типа используются аудитории, оборудованные проектором и компьютером с установленным на нем браузером и программным обеспечением для демонстрации презентаций (PowerPoint).

Для проведения занятий лекционного типа предлагаются наборы учебно-наглядных пособий, включающие в себя презентации по разделам и темам дисциплины.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические рекомендации по изучению дисциплины для студентов представляют собой комплекс рекомендаций и разъяснений, позволяющих студенту оптимальным образом организовать процесс изучения данной дисциплины.
Обучение по дисциплине «Цифровой форензик» предполагает проведение аудиторных занятий (лекций, практических занятий) и самостоятельную работу обучающихся.
Лекции – форма учебного занятия, цель которого состоит в рассмотрении основных теоретических вопросов излагаемой дисциплины в логически выдержанной форме. Одно из основных назначений лекций состоит не только в получении необходимых знаний, но и в организации самостоятельной работы студентов. Работать самостоятельно

студент должен до лекции, во время лекции и после нее. С целью обеспечения успешного освоения материала дисциплины обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, так как:
- знакомит с новым учебным материалом;
- разъясняет учебные элементы, трудные для понимания;
- систематизирует учебный материал;
- ориентирует в учебном процессе;
- формирует компетенции раскрываемые в данной дисциплине.

Подготовка к лекции для обучающихся заключается в следующем:
- внимательно прочитать материал предыдущей лекции;
- изучить дополнительный материал, рекомендуемый преподавателем;
- узнать тему предстоящей лекции (по тематическому плану, по информации лектора);
- ознакомиться с учебным материалом по учебнику и учебным пособиям;
- уяснить место изучаемой темы в своей профессиональной подготовке;
- ознакомиться с компетенциями данной дисциплины и уровнями их освоения;
- записать возможные вопросы, которые следует задать лектору на лекции.

На практическом занятии участие обучающегося сводится к следующему:
- определение темы и цели работы;
- проверка теоретических знаний, которые необходимы для рациональной работы и практической деятельности;
- разработка алгоритма проведения практического задания;
- ознакомление со способами фиксации полученных результатов;
- непосредственное выполнение практического задания;
- обобщение и систематизация полученных результатов (порядок оформления определяет преподаватель);
- подведение итогов занятия.

При выполнении самостоятельной работы обучающимся прививается знание и умение работы с нормативной, специальной литературой, а также навыки владения самостоятельного научного поиска и исследовательской работы. Такие занятия помогают осуществлять обратную связь и оказать практическую помощь обучающимся при подготовке к практическим занятиям, текущей и промежуточной аттестации.

Для выполнения ситуационных задач необходимо:
- изучить материал лекций соответствующих заданию;
- разобраться в предлагаемой ситуации;
- определить возможное влияние внутренних и внешних факторов на предлагаемую ситуацию - используя полученные знания и профессиональное суждение выполнить задание (вариантов решения может быть несколько);
- оформить задачу в соответствии с порядком оформления письменных работ.

Подготовка к экзамену. К экзамену необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по дисциплине. Обучающемуся необходимо познакомиться: с рабочей программой дисциплины; с примерами заданий для текущей и промежуточной аттестации; рекомендуемыми учебниками, учебными пособиями по дисциплине, а также электронными ресурсами; перечнем фондов оценочных средств и критериями оценивания сформированности компетенций по данной дисциплине.

Систематическое выполнение учебной работы на лекциях и практических занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи экзамена.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося (мобильные специальные технические средства для лиц с нарушениями зрения и с нарушением слуха, ассистивные информационные технологии).

При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации, речевые синтезаторы, экранные лупы).

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся с инвалидностью и с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.

Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ с помощью специальных технических и программных средств к электронным источникам, представленным в

форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах.
Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и особенностям восприятия информации.
Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий.
При проведении промежуточной аттестации по дисциплине обучающимся с инвалидностью и с ограниченными возможностями здоровья обеспечивается по их заявлению предоставление в доступной форме в зависимости от их индивидуальных особенностей инструкции о порядке проведения промежуточной аттестации, оценочных средств и возможности ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).
При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование предоставленных ЧелГУ или собственных технических средств, необходимых им в связи с их индивидуальными особенностями. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

38.05.01, Экономическая безопасность, Судебная экономическая экспертиза и цифровая криминалистика, Цифровой форензик, 2026 год набора, очная форма обучения

Проректор по учебной работе утверждено 20.02.2026 А.А. Саламатов

Ученым советом факультета экономики и управления

Протокол заседания № 11 от 24.02.2026

Председатель Ученого совета
факультета экономики и управления согласовано А.А. Егорова

Заседанием кафедры экономической теории и регионального развития

Протокол заседания № 7 от 17.02.2026

Заведующий кафедрой согласовано А.А. Саламатов

Автор (составитель) Г.А. Косарева

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1