

Скоков
Роман
Юрьевич
Ректор "В
ИЭПП"

2026.02.27
15:46:49
+03'00'

Приложение 2 к рабочей программе дисциплины
«Информационные системы в судебной экспертизе»

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОЛЖСКИЙ ИНСТИТУТ ЭКОНОМИКИ, ПЕДАГОГИКИ И ПРАВА»

Факультет информационной безопасности и права

Фонд оценочных средств

«Информационные системы в судебной экспертизе»

Направление подготовки
09.03.03 Прикладная информатика

Направленность (профиль) образовательной программы:
Общий правовой профиль

Уровень высшего образования:
бакалавриат

Квалификация выпускника:
«бакалавр»

Содержание

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы, описание показателей, критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания....	3
2 Методические материалы и типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы	6
2.1 Типовые контрольные задания, используемые для проведения входного контроля	6
2.2 Типовые контрольные задания, используемые для промежуточной аттестации по дисциплине.....	8
2.2.1 Примерный перечень вопросов к зачету.....	8
2.3 Методические материалы и типовые контрольные задания, используемые для текущего контроля по дисциплине	10
2.3.1 Методические материалы, используемые для текущего контроля знаний по дисциплине.....	10
2.3.2 Вопросы, выносимые на самостоятельное изучение	11
2.3.3 Задания для самостоятельной работы	12
2.3.4 Тесты по дисциплине	13
2.3.5 Типовые задания.....	14
2.3.6 Задания для контрольной работы	15
2.3.7 Методика проведения лекции-дискуссии	16
2.3.8 Методика проведения интерактивного решения задач	16
3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков по дисциплине	17
3.1 Балльно-рейтинговая система оценки успеваемости по дисциплине	17

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы, описание показателей, критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Перечень компетенций	Показатели оценивания компетенций	Критерии оценивания компетенций	Этапы формирования компетенций	Шкала оценивания
ПК-6. Способен квалифицированно проводить юридическую экспертизу программного обеспечения в профессиональной деятельности, обеспечивать эксплуатацию комплекса средств автоматизации технологических решений	- знает методологию юридической экспертизы ПО, классификацию ИС судебной экспертизы, нормативно-правовые акты в сфере экспертной деятельности; - умеет проводить юридическую экспертизу ПО на соответствие требованиям законодательства, использовать специализированные программные комплексы для анализа цифровых доказательств; - владеет методиками компьютерно-технической экспертизы, инструментами анализа исходного кода и	- имеет базовые знания методологии юридической экспертизы ПО и нормативно-правовой базы; - умеет на основе типовых примеров проводить простейшие виды экспертизы ПО; - владеет навыками работы с базовыми инструментами анализа цифровых доказательств	Начальный	удовлетворительно (60–74 балла)
		- знает настройки и поддержки автоматизированных рабочих мест (АРМ) и информационных систем и управления информационной безопасности используемых в юридической деятельности; - умеет применять современные технологии для автоматизации юридических технологических решений, включая работу с базами данных правовой информации; - владеет навыками выполнения должностных обязанностей по сбору и анализу информации для автоматизации юридических технологических решений, включая работу с базами данных правовой информации.	Основной	Хорошо (75 – 89 баллов)

	бинарных файлов	- знает содержание обязанностей должностных лиц по поддержки автоматизированных рабочих мест (АРМ) и информационных систем и управления информационной безопасности используемых в юридической деятельности; - умеет самостоятельно определять круг должностных обязанностей по сбору и анализу информации проводить юридическую экспертизу программного обеспечения и ее применения в профессиональной деятельности; - владеет навыки развертывания, настройки и поддержки автоматизированных рабочих мест (АРМ) и информационных систем, используемых в юридической деятельности.	Завершающий	Отлично (90 – 100 баллов)
ПК-7. Способен принимать решения в точном соответствии с законодательством РФ и совершать юридические действия в организации ИТ инфраструктуры и управлении информационной безопасностью	- знает законодательство РФ в области судебной экспертизы, информации и ИБ, требования ФСТЭК и ФСБ к защите информации; - умеет принимать обоснованные решения при проектировании ИТ-инфраструктуры экспертных учреждений, разрабатывать регламенты обработки цифровых доказательств; - владеет методами	- знает законодательство РФ в области судебной экспертизы и ИБ; - умеет разрабатывать регламенты обработки цифровых доказательств с учетом требований законодательства; - владеет опытом применения нормативно-правовых актов при решении сложных задач организации ИТ-инфраструктуры и управления ИБ	Начальный	удовлетворительно (60–74 балла)
		- знает способы и методы анализа норм законодательства РФ, регламентирующие работу с информацией, информационными технологиями и их защитой;	Основной	Хорошо (75 – 89 баллов)

	управления ИТ-активами, навыками применения нормативно-правовых актов в экспертной практике	- умеет принимать решения в рамках закона, оформлять юридическую документацию, соблюдать правовой режим защиты информации;	Завершающий	Отлично (90 – 100 баллов)
--	---	--	-------------	------------------------------

ВИЭПП

2 Методические материалы и типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

2.1 Типовые контрольные задания, используемые для проведения входного контроля

1. Что такое судебная экспертиза в соответствии с Федеральным законом № 73-ФЗ?
 - а) Процессуальное действие по установлению обстоятельств, имеющих значение для дела
 - б) Научное исследование объектов с целью установления обстоятельств, имеющих значение для дела
 - в) Деятельность эксперта по установлению обстоятельств, имеющих значение для дела, на основе специальных знаний
 - г) Все перечисленное верно
2. Какой нормативный акт регулирует государственную судебно-экспертную деятельность в РФ?
 - а) Гражданский кодекс РФ
 - б) Федеральный закон № 73-ФЗ от 31.05.2001 г.
 - в) Уголовно-процессуальный кодекс РФ
 - г) Федеральный закон № 149-ФЗ «Об информации»
3. Что такое цифровые доказательства в уголовном процессе?
 - а) Любая информация в электронной форме
 - б) Информация в электронной или цифровой форме, которая может быть использована в качестве доказательства
 - в) Только данные, полученные в результате компьютерно-технической экспертизы
 - г) Только данные, извлеченные из мобильных устройств
4. Какой стандарт определяет требования к экспертным организациям?
 - а) ГОСТ Р ИСО 9001
 - б) ГОСТ Р ИСО/МЭК 17025
 - в) ГОСТ Р 7.0.97-2016
 - г) ГОСТ Р 57580.2-2017
5. Что такое цепочка хранения (chain of custody) цифровых доказательств?
 - а) Процедура фиксации всех операций с доказательствами от изъятия до представления в суд
 - б) Система хранения доказательств в экспертном учреждении
 - в) Программное обеспечение для управления доказательствами
 - г) Метод криптографической защиты доказательств
6. Какой орган утверждает методики судебных экспертиз в РФ?
 - а) Министерство юстиции РФ
 - б) Федеральная служба судебных приставов
 - в) Российский федеральный центр судебной экспертизы при Минюсте России
 - г) Верховный Суд РФ
7. Что такое криптографический анализ в рамках компьютерно-технической экспертизы?
 - а) Анализ алгоритмов шифрования и криптографических протоколов
 - б) Взлом шифрования для получения доступа к данным
 - в) Оценка стойкости криптосистемы и выявление уязвимостей
 - г) Верны варианты а) и в)
8. Какой из перечисленных программных комплексов НЕ относится к средствам цифровой криминалистики?
 - а) Autopsy
 - б) FTK Imager

- в) Microsoft Word
- г) Magnet AXIOM

9. Что регламентирует ст. 79 УПК РФ?

- а) Порядок назначения судебной экспертизы
- б) Порядок производства следственных действий
- в) Порядок изъятия и фиксации электронных данных
- г) Права и обязанности эксперта

10. Какой класс защищенности информационных систем установлен для экспертных учреждений согласно требованиям ФСТЭК России?

- а) K1
- б) K2
- в) K3 или K4 в зависимости от категории информации
- г) K5

11. Что такое метаданные цифровых объектов?

- а) Скрытая информация в файлах, не отображаемая пользователем
- б) Данные о данных: время создания, автор, параметры устройства и т.д.
- в) Только техническая информация о формате файла
- г) Информация, добавленная после создания файла

12. Какой метод используется для восстановления удаленных данных?

- а) Анализ неиспользуемых секторов диска
- б) Анализ таблицы размещения файлов (FAT/MFT)
- в) Сканирование свободного пространства носителя
- г) Все перечисленные методы

13. Что такое экспертная информационная система (ЭИС)?

- а) Программный комплекс для автоматизации экспертной деятельности
- б) База данных экспертов
- в) Система документооборота экспертного учреждения
- г) Система связи между экспертными учреждениями

14. Какой из перечисленных видов экспертиз НЕ относится к компьютерно-техническим?

- а) Экспертиза программного обеспечения
- б) Экспертиза баз данных
- в) Дактилоскопическая экспертиза
- г) Экспертиза мобильных устройств

15. Что такое хеширование в контексте фиксации цифровых доказательств?

- а) Метод сжатия данных
- б) Криптографическое преобразование данных в уникальную строку фиксированной длины
- в) Метод шифрования данных
- г) Метод резервного копирования

16. Какой документ оформляется по результатам судебной экспертизы?

- а) Акт экспертизы
- б) Заключение эксперта
- в) Справка эксперта
- г) Протокол исследования

17. Что такое «цифровой след»?

- а) Любая информация, оставленная пользователем в цифровой среде
- б) Только данные о местоположении устройства
- в) Только история посещения веб-сайтов
- г) Только данные из социальных сетей

18. Какой из перечисленных принципов НЕ относится к основным принципам судебной экспертизы?

- а) Принцип объективности
- б) Принцип независимости эксперта
- в) Принцип конфиденциальности
- г) Принцип платности

19. Что такое «облачные» цифровые доказательства?

- а) Данные, хранящиеся на серверах облачных провайдеров
- б) Данные, полученные из социальных сетей
- в) Данные, передаваемые по интернету
- г) Все перечисленные варианты

20. Какой орган осуществляет лицензирование деятельности по проведению судебных экспертиз?

- а) Министерство юстиции РФ
- б) Федеральная антимонопольная служба
- в) Роскомнадзор
- г) Лицензирование не требуется для судебных экспертиз

2.2 Типовые контрольные задания, используемые для промежуточной аттестации по дисциплине

2.2.1 Примерный перечень вопросов к зачету

Теоретические вопросы

1. Понятие и сущность информационных систем в судебной экспертизе. История развития ИС в экспертной деятельности.
2. Нормативно-правовая база применения ИС в судебной экспертизе: Федеральный закон № 73-ФЗ, ГОСТы, методические рекомендации.
3. Классификация ИС судебной экспертизы по видам экспертиз (криминалистические, компьютерно-технические, биометрические).
4. Архитектурные модели ИС судебной экспертизы: клиент-серверные, облачные, распределенные системы.
5. Требования ФСТЭК России к защите информации в экспертных учреждениях.
6. Принципы организации ИТ-инфраструктуры экспертных учреждений.
7. Специализированные программные комплексы для судебной экспертизы: «Эксперт-АИС», «Forensic Toolkit», «Magnet AXIOM».
8. Методы анализа цифровых доказательств: анализ метаданных, восстановление данных, криптографический анализ.
9. Требования законодательства РФ к фиксации и хранению цифровых доказательств (ст. 79 УПК РФ).
10. Понятие и значение цепочки хранения (chain of custody) цифровых доказательств.
11. Юридическая экспертиза программного обеспечения: цели, задачи, методология.
12. Анализ исходного кода ПО на соответствие требованиям законодательства РФ.
13. Верификация и валидация программных продуктов в экспертной практике.
14. Инструменты анализа бинарных файлов и выявления вредоносного кода.
15. Применение искусственного интеллекта и машинного обучения в судебной экспертизе.
16. Этические и правовые аспекты использования ИИ в экспертной деятельности.

17. Блокчейн-технологии для фиксации и подтверждения подлинности цифровых доказательств.
18. Ответственность эксперта за нарушение регламентов работы с ИС и цифровыми доказательствами.
19. Судебная практика по оспариванию результатов экспертиз, проведенных с использованием ИС.
20. Перспективы развития ИС в судебной экспертизе: цифровые двойники объектов экспертизы, квантовые вычисления.

Практические вопросы

1. Разработайте регламент обработки цифровых доказательств для экспертного учреждения с учетом требований ФСТЭК России.
2. Проведите анализ метаданных цифрового изображения (файл формата JPG) и определите параметры съемки, устройство и возможные признаки редактирования.
3. Опишите процедуру фиксации цифровых доказательств с мобильного устройства с соблюдением принципа цепочки хранения.
4. Проведите криптографический анализ простого шифрования (шифр Цезаря) и определите метод дешифрования.
5. Разработайте структуру экспертного заключения по результатам анализа программного обеспечения на соответствие требованиям законодательства РФ.
6. Оцените архитектурные решения ИТ-инфраструктуры экспертного учреждения на соответствие требованиям класса защищенности КЗ.
7. Проведите анализ лог-файлов веб-сервера на предмет выявления признаков несанкционированного доступа.
8. Определите методы восстановления удаленных файлов с носителя информации и опишите последовательность действий эксперта.
9. Разработайте сценарий использования ИИ для автоматической классификации цифровых доказательств по типам.
10. Оцените юридические риски при использовании облачных сервисов для хранения цифровых доказательств.
11. Проведите анализ исходного кода фрагмента программы на предмет выявления уязвимостей безопасности.
12. Определите критерии выбора программного комплекса для цифровой криминалистики для экспертного учреждения.
13. Разработайте процедуру аудита ИТ-инфраструктуры экспертного учреждения.
14. Опишите методику анализа цифровых доказательств из мессенджеров (Telegram, WhatsApp).
15. Проведите сравнительный анализ функционала трех программных комплексов для цифровой криминалистики.
16. Разработайте план мероприятий по обеспечению информационной безопасности экспертного учреждения.
17. Определите требования к квалификации специалиста, работающего с ИС судебной экспертизы.
18. Опишите процедуру сертификации программного обеспечения для использования в экспертной деятельности.
19. Разработайте методику оценки достоверности результатов, полученных с использованием ИИ в экспертизе.
20. Проведите анализ судебного решения по делу, в котором оспаривались результаты компьютерно-технической экспертизы.

2.2.2 Примерное задание на зачет

Задание 1. Дайте развернутый ответ на вопрос: «Организация ИТ-инфраструктуры экспертного учреждения: требования законодательства РФ, стандарты ФСТЭК, практические аспекты реализации».

Задание 2. Решите кейс: В ходе расследования уголовного дела изъято мобильное устройство подозреваемого. Необходимо провести комплексную экспертизу устройства с использованием специализированных программных средств. Опишите: а) последовательность действий эксперта с момента получения устройства до формирования заключения; б) программные комплексы, которые могут быть использованы на каждом этапе; в) требования к оформлению результатов экспертизы в соответствии с ГОСТ Р 7.0.97-2016.

2.3 Методические материалы и типовые контрольные задания, используемые для текущего контроля по дисциплине

2.3.1 Методические материалы, используемые для текущего контроля знаний по дисциплине

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде	Наименование оценочного средства
Контрольный опрос	Метод оценки уровня освоения компетенций на основе непосредственного (беседа) или опосредованного (анкета) взаимодействия преподавателя и студента	Примерный перечень вопросов к зачету, вопросы для самостоятельного изучения, задания для СРС	Контрольный опрос
Собеседование	Относительно свободный диалог между преподавателем и студентом на заданную тему с оценкой глубины понимания материала	Вопросы по разделам дисциплины, кейсовые задания	Собеседование
Тестовые задания	Эмпирико-аналитическая процедура оценки уровня освоения компетенций с использованием стандартизированных вопросов	Тесты по дисциплине (раздел 2.3.4)	Тестовые задания
Самостоятельное решение задач	Метод приобретения навыков творческого мышления и самостоятельного	Типовые задания (раздел 2.3.5), задания для контрольной работы	Самостоятельное решение задач

	решения профессиональных задач	(раздел 2.3.6)	
Лекция-дискуссия	Оценочное средство, включающее обучающихся в процесс обсуждения спорного вопроса с оценкой умения аргументировать точку зрения	Методика проведения (раздел 2.3.7), темы для дискуссии	Лекция-дискуссия
Интерактивное решение задач	Метод модерации, при котором все обучающиеся участвуют в решении задач под руководством преподавателя-модератора	Методика проведения (раздел 2.3.8), типовые задания	Интерактивное решение задач

2.3.2 Вопросы, выносимые на самостоятельное изучение

Блок теоретических вопросов

1. История развития информационных систем в судебной экспертизе в России и за рубежом.
2. Международные стандарты в области судебной экспертизы (ISO/IEC 17020, 17025) и их применение в РФ.
3. Сравнительный анализ архитектурных решений ИС судебной экспертизы в различных странах.
4. Правовые основы применения искусственного интеллекта в экспертной деятельности.
5. Требования законодательства РФ к квалификации экспертов, работающих с ИС.
6. Методология оценки эффективности внедрения ИС в экспертных учреждениях.
7. Проблемы идентификации цифровых доказательств в условиях развития криптовалют и анонимных сетей.
8. Этические кодексы экспертов в цифровой криминалистике.
9. Судебная практика по делам, связанным с нарушением порядка работы с цифровыми доказательствами.
10. Перспективы развития квантовых вычислений и их влияние на криптографический анализ в экспертизе.

Блок практических вопросов

1. Анализ реального экспертного заключения по компьютерно-технической экспертизе с точки зрения соответствия требованиям законодательства.
2. Разработка методики анализа цифровых доказательств из социальных сетей.
3. Оценка уязвимостей популярных мессенджеров с точки зрения возможности извлечения доказательств.
4. Разработка регламента работы с облачными сервисами при проведении экспертиз.

5. Анализ кейса: оспаривание результатов экспертизы из-за нарушения цепочки хранения доказательств.
6. Подготовка экспертного заключения по фиктивному делу с использованием демо-версий программных комплексов.
7. Разработка чек-листа для аудита ИТ-инфраструктуры экспертного учреждения.
8. Анализ судебных решений по делам о мошенничестве с использованием криптовалют.
9. Разработка сценария обучения персонала экспертного учреждения работе с новым программным комплексом.
10. Оценка экономической эффективности внедрения ИИ в экспертные процессы.

2.3.3 Задания для самостоятельной работы

Задание 1. Подготовьте реферат на тему: «Сравнительный анализ программных комплексов цифровой криминалистики: «Forensic Toolkit» vs «Magnet AXIOM»» (объем 10-15 страниц).

Задание 2. Разработайте регламент обработки цифровых доказательств для экспертного учреждения с учетом требований ФСТЭК России и ст. 79 УПК РФ. Регламент должен включать:

- процедуру приема и регистрации доказательств;
- порядок фиксации (включая хеширование);
- правила хранения и передачи;
- ответственность за нарушение регламента.

Задание 3. Проведите анализ метаданных 3-5 цифровых изображений (формат JPG) с использованием бесплатных инструментов (ExifTool, Jeffrey's Image Metadata Viewer). Подготовьте отчет с выводами о подлинности изображений.

Задание 4. Изучите судебное решение по делу, в котором оспаривались результаты компьютерно-технической экспертизы (материалы доступны на сайте ГАС «Правосудие»). Подготовьте аналитическую справку с указанием причин оспаривания и судебной позиции.

Задание 5. Разработайте структуру экспертного заключения по фиктивному делу о нарушении авторских прав на программное обеспечение с использованием требований ГОСТ Р 7.0.97-2016.

2.3.4 Тесты по дисциплине

Тест по Разделу 1. Теоретические основы ИС в судебной экспертизе

1. Федеральный закон, регулирующий государственную судебно-экспертную деятельность в РФ:

- а) № 149-ФЗ
- б) № 73-ФЗ
- в) № 152-ФЗ
- г) № 272-ФЗ

2. Основная цель применения ИС в судебной экспертизе:

- а) Снижение затрат на экспертизу
- б) Повышение объективности и достоверности экспертных заключений
- в) Ускорение процесса экспертизы
- г) Автоматизация всех этапов экспертной деятельности

3. Какой стандарт определяет общие требования к компетентности испытательных и калибровочных лабораторий?

- а) ГОСТ Р ИСО 9001

- б) ГОСТ Р ИСО/МЭК 17025
- в) ГОСТ Р 7.0.97-2016
- г) ГОСТ Р 57580.2-2017

Тест по Разделу 2. Архитектура и классификация ИС судебной экспертизы

4. К какому виду экспертиз относится анализ программного обеспечения на предмет наличия вредоносного кода?

- а) Криминалистическая
- б) Компьютерно-техническая
- в) Биометрическая
- г) Лингвистическая

5. Какая архитектура ИС обеспечивает работу экспертов из разных географических локаций с единой базой данных?

- а) Локальная
- б) Клиент-серверная
- в) Распределенная
- г) Монолитная

6. Какой принцип является критически важным при проектировании ИС для экспертных учреждений?

- а) Максимальная производительность
- б) Обеспечение целостности и неизменности данных
- в) Минимизация стоимости
- г) Удобство пользовательского интерфейса

Тест по Разделу 3. Программные средства судебной экспертизы

7. Какой программный комплекс специализируется на анализе мобильных устройств и облачных сервисов?

- а) Autopsy
- б) FTK Imager
- в) Magnet AXIOM
- г) Wireshark

8. Для анализа сетевого трафика в рамках экспертизы наиболее подходит:

- а) EnCase
- б) Wireshark
- в) FTK
- г) «Эксперт-АИС»

9. Какой метод используется для подтверждения неизменности цифровых доказательств?

- а) Архивирование
- б) Хеширование
- в) Шифрование
- г) Резервное копирование

Тест по Разделу 4. Правовые и организационные аспекты

10. Статья УПК РФ, регламентирующая порядок производства следственных действий с применением технических средств:

- а) Ст. 77
- б) Ст. 79
- в) Ст. 164
- г) Ст. 195

11. Требования к классу защищенности ИС экспертных учреждений устанавливает:

- а) Министерство юстиции РФ
- б) ФСБ России

- в) ФСТЭК России
- г) Роскомнадзор

12. Что такое «цепочка хранения» (chain of custody) цифровых доказательств?

- а) Система хранения доказательств в экспертном учреждении
- б) Документированный процесс от изъятия до представления в суд с фиксацией всех операций
- в) Программное обеспечение для управления доказательствами
- г) Метод криптографической защиты доказательств

Тест по Разделу 5. Перспективы развития

13. Какая технология позволяет создать неизменяемый реестр операций с цифровыми доказательствами?

- а) Искусственный интеллект
- б) Блокчейн
- в) Облачные вычисления
- г) Квантовые вычисления

14. Основное преимущество применения ИИ в судебной экспертизе:

- а) Полная автоматизация экспертной деятельности
- б) Ускорение обработки больших объемов данных и выявление скрытых закономерностей
- в) Исключение человеческого фактора
- г) Снижение требований к квалификации эксперта

15. Этическая проблема использования ИИ в экспертизе связана с:

- а) Высокой стоимостью внедрения
- б) Отсутствием прозрачности алгоритмов принятия решений («черный ящик»)
- в) Недостаточной производительностью
- г) Сложностью интеграции с существующими системами

Ключи к тестам:

1-б, 2-б, 3-б, 4-б, 5-в, 6-б, 7-в, 8-б, 9-б, 10-б, 11-в, 12-б, 13-б, 14-б, 15-б

2.3.5 Типовые задания

Задача 1: Разработка регламента обработки цифровых доказательств

Описание

задачи:

Вам необходимо разработать регламент обработки цифровых доказательств для государственного экспертного учреждения, выполняющего компьютерно-технические экспертизы. Регламент должен соответствовать требованиям ФСТЭК России и ст. 79 УПК РФ.

Задание:

1. Определите этапы работы с цифровыми доказательствами от момента поступления до возврата (или уничтожения).
2. Для каждого этапа разработайте:
 - перечень обязательных действий эксперта;
 - требования к документальному оформлению;
 - методы фиксации неизменности данных (хеширование и др.);
 - ответственность за нарушение процедуры.
3. Разработайте форму «Акт приема-передачи цифровых доказательств» с учетом требований законодательства.
4. Определите технические средства, необходимые для обеспечения целостности доказательств на каждом этапе.

Критерии оценки:

- полнота охвата всех этапов работы с доказательствами;
- соответствие требованиям нормативных актов;
- практическая применимость регламента;

- качество оформления документов.

Задача 2: Анализ цифровых доказательств с мобильного устройства

Описание

задачи:

В рамках учебного кейса предоставлен образ диска мобильного устройства (в формате .img). Необходимо провести анализ с целью выявления доказательств несанкционированного доступа к корпоративной сети.

Задание:

1. Выберите программный комплекс для анализа (используйте демо-версию или открытые инструменты).
2. Проведите анализ образа диска с целью выявления:
 - истории подключений к Wi-Fi сетям;
 - установленных приложений с функциями удаленного доступа;
 - логов сетевой активности;
 - учетных данных (логины/пароли).
3. Подготовьте экспертное заключение по форме, соответствующей ГОСТ Р 7.0.97-2016, с указанием:
 - методики исследования;
 - выявленных фактов;
 - выводов по поставленным вопросам.

Критерии оценки:

- корректность выбора инструментов анализа;
- полнота выявленных доказательств;
- соответствие оформления заключения требованиям ГОСТ;
- обоснованность выводов.

2.3.6 Задания для контрольной работы

2.3.6.1 Задание к теоретической части контрольной работы

Вариант

1. Проанализируйте нормативно-правовую базу, регулирующую применение ИС в судебной экспертизе. Выделите пробелы и противоречия в законодательстве. Разработайте предложения по совершенствованию правового регулирования с учетом развития цифровых технологий.

Вариант

2. Сравните архитектурные решения ИС судебной экспертизы для трех типов учреждений: государственная экспертная организация, негосударственная экспертная организация, экспертное подразделение правоохранительного органа. Обоснуйте различия в требованиях к ИТ-инфраструктуре для каждого типа.

2.3.6.2 Задание к практической части контрольной работы

Задача

1. В ходе экспертизы предоставлен исходный код программного модуля на языке Python. Необходимо:

1. Провести анализ кода на предмет соответствия требованиям безопасности (выявить уязвимости типа SQL-инъекции, XSS).
2. Определить наличие признаков вредоносной функциональности.
3. Подготовить фрагмент экспертного заключения с выводами.

Исходные данные: Фрагмент кода в приложении к заданию.

Задача

2. Разработайте архитектуру ИТ-инфраструктуры для экспертного учреждения, выполняющего компьютерно-технические экспертизы с требованиями:

- класс защищенности КЗ по ФСТЭК;
- работа с данными до грифа «Секретно»;
- одновременная работа 15 экспертов;
- хранение архива доказательств объемом до 500 ТБ. Представьте схему архитектуры с пояснениями по каждому компоненту.

2.3.7 Методика проведения лекции-дискуссии

Цель: Достижение обоснованной позиции по спорным вопросам применения ИИ в судебной экспертизе путем осознания участниками своих мнений, суждений и выработки уважительного отношения к альтернативным точкам зрения.

Задачи:

- развитие умений анализировать этические и правовые дилеммы в экспертной деятельности;
- поиск и разработка перспективных подходов к регулированию ИИ в экспертизе;
- развитие способности продуцировать множество решений для сложных ситуаций;
- нахождение оптимального баланса между автоматизацией и ответственностью эксперта.

Методика проведения:

1. Назначение секретаря лекции-дискуссии, его инструктаж по фиксации ключевых аргументов участников.
2. Объявление темы дискуссии: «Может ли искусственный интеллект заменить эксперта в судебной экспертизе? Этические и правовые аспекты».
3. Представление лектором базовой информации по теме (15 минут).
4. Свободный обмен мнениями с разделением на «за» и «против» автоматизации экспертной деятельности.
5. Подведение итогов дискуссии с формулированием консенсусной позиции по ключевым вопросам.
6. Переход к информационной части лекции с учетом результатов дискуссии.

Критерии

оценки:

Секретарь лекции-дискуссии – 0,5–1,5 балла;
Активное участие в дискуссии с аргументированными выступлениями – 0,5–1 балл.

2.3.8 Методика проведения интерактивного решения задач

Цель: Проверка навыков решения профессиональных задач в области анализа цифровых доказательств и развитие мыслительных операций, направленных на достижение практических результатов.

Задачи:

1. Проверка навыков применения знаний при решении кейсов по анализу цифровых доказательств.
2. Формирование навыков совместной деятельности экспертов при проведении комплексных исследований.
3. Овладение общими принципами решения проблемных ситуаций в экспертной практике.
4. Развитие коммуникативных навыков и умения аргументировать экспертную позицию.

Методика проведения:

Первый этап

этап

«подготовка»:

Преподаватель разрабатывает кейс с фрагментами решения и определяет ключевые точки для обсуждения.

Второй этап «организационный»:

1. Объявление темы и цели решения задачи (анализ доказательств из мессенджера).

2. Назначение секретаря и его инструктаж.
3. Объявление критериев оценки.

Третий этап «интеллектуальный»:

1. Представление условий задачи и исходных данных.
2. Индивидуальное предварительное решение задачи каждым студентом.
3. Высказывание мнений по ходу решения, обсуждение альтернативных подходов.

4. Коллективная выработка оптимального алгоритма решения.

Четвертый этап «подведение итогов»:

1. Формулирование выводов по решению задачи.
2. Подведение итога преподавателем с указанием лучших практик.
3. Оценка участников по материалам секретаря.

Критерии

Секретарь – 1 балл;
Активное участие в решении задачи с предложением конструктивных идей – 1–3 балла.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков по дисциплине

3.1 Балльно-рейтинговая система оценки успеваемости по дисциплине

В целях оперативного контроля уровня усвоения материала учебной дисциплины и стимулирования активной учебной деятельности студентов (очной формы обучения) используется балльно-рейтинговая система оценки успеваемости. В соответствии с этой системой оценки студенту в ходе изучения дисциплины предоставляется возможность набрать не менее 60 баллов за текущую работу в семестре и до 40 баллов на зачете (итоговый контроль). Результирующая оценка по дисциплине складывается из суммы баллов текущего и итогового контроля.

К зачету допускаются студенты, посетившие не менее 70% лекций и практических занятий и имеющие рейтинг не менее 30 баллов.

Балльно-рейтинговая система по дисциплине «Информационные системы в судебной экспертизе»

Виды контроля	Максимальная сумма баллов на выполнение одного вида задания	Всего возможных за семестр работ	Итого максимальная сумма баллов
Присутствие на лекционных и практических занятиях	0,25	18 (лекции) + 36 (практика) = 54	13,5
Работа на практических занятиях (активность, решение задач)	1,0	27	27
СРС, в т.ч.:			19,5
– написание конспектов лекций	0,5	9	4,5
– защита рефератов/докладов	2,0	3	6,0
– выполнение практических заданий по СРС	1,5	6	9,0
Текущий контроль	2,0	5	10

(тестирование, контрольные опросы)			
Итого за семестр	—	—	60
Зачет (итоговый контроль)	40,0	1	40
Итого по дисциплине	—	—	100

Нормы выставления дополнительных (премиальных) баллов

Виды работ	Максимальная сумма баллов
Решение дополнительных практических задач повышенной сложности	3
Участие в научно-практических конференциях по тематике дисциплины	4
Публикация научной статьи по тематике дисциплины	3
Итого	10

Шкала итоговой оценки

Количество баллов	Оценка
90–100	«отлично»
75–89	«хорошо»
60–74	«удовлетворительно»
0–59	«не зачтено»