

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Тольяттинский государственный университет»

**Б1.В.08**  
(индекс дисциплины)

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Компьютерная криминалистика

(наименование дисциплины)

по направлению подготовки  
09.03.03 Прикладная информатика

направленность (профиль)  
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2026

Общая трудоемкость: 43Е

**Распределение часов дисциплины по семестрам**

Семестр	6	Итого
Форма контроля	зачет	
Вид занятий		
Лекции	16	16
Лабораторные	-	-
Практические	48	48
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0,25	0,25
Контактная работа	64,25	64,25
Самостоятельная работа	79,75	79,75
Контроль		
<b>Итого</b>	<b>144</b>	<b>144</b>

Рабочую программу составил(и):

К.т.н., доцент, доцент, Полякова Е.В.

*(должность, ученое звание, степень, Фамилия И.О.)*

---

*(должность, ученое звание, степень, Фамилия И.О.)*

---

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

*(должность, ученое звание, степень, Фамилия И.О.)*

---

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

**Срок действия рабочей программы дисциплины до 31.08.2029**

УТВЕРЖДЕНО

На заседании Института инженерной и экологической безопасности

---

(протокол заседания № 1 от «01» сентября 2025 г.).

## 1. Цель освоения дисциплины

Цель дисциплины – изучения методов и средств проведения исследований в компьютерной криминалистике.

В процессе изучения основное внимание уделяется артефактам операционной системы, в частности ОС Windows, которые применяются при проведении криминалистических исследований. Так изучаются методы извлечения и получения данных артефактов. Особое внимание уделяется механизмам получения образов дисков и оперативной памяти исследуемых систем, программным и аппаратным средствам. Помимо этого, изучаются программные средства для анализа как образов, так и полученных из них артефактов.

Особое внимание уделяется расследованию компьютерных инцидентов.

## 2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Организация обработки персональных данных в организации;
- Основы управления информационной безопасностью.

Полученные знания используются при изучении следующих дисциплин:

- Аудит защищенности информационных систем;
- Мониторинг событий информационной безопасности;
- Информационная безопасность компьютерных сетей.

## 3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-6 Способен производить оценку эффективности применения программно-аппаратных средств защиты информации, осуществлять мониторинг функционирования программно-аппаратных средств защиты информации	ПК-6.5 Использует знание сетевых сервисов и протоколов, методов обнаружения атак на уровне сети, хостов и облаков, концепций и методологий анализа вредоносного ПО	Знать: -знание угроз и уязвимостей -знание законодательства (без уточнения какого) -знание категорий инцидентов -знание методов обнаружения атак на уровне сети, хостов и облаков -знание рисков безопасности приложений
		Уметь: -классификация и приоритизация инцидентов -документирование инцидента -оценка тенденций -анализ логов от разных источников -взаимодействие с правоохранительными или иными специальными органами,

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
		<p>проводящими исследование инцидента</p> <p>-координация функций по реагированию на инциденты</p> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- навыками обеспечения целостности цифровых доказательств на разных платформах и в соответствие с требованиями локального законодательства</li> <li>- навыками защиты сетевых коммуникаций</li> <li>- навыками распознавания и категоризации типов уязвимостей и связанных с ними атак</li> <li>- навыками оценки ущерба</li> </ul>
	<p>ПК-6.6 Применяет навыки анализа логов от разных источников, корреляции данных по разным инцидентам, подготовки рекомендаций по их нейтрализации и сбора артефактов по инцидентам</p> <p>ПК-6.7 Владеет навыками идентификации, получения, локализации и репортинга по вредоносному ПО, обеспечения целостности цифровых доказательств на разных платформах и в соответствие с требованиями локального законодательства</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>- сетевые сервисы и протоколы;</li> <li>- основных сетевых концепций, включая топологии, протоколы, компоненты</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- проводить сбор артефактов по инцидентам</li> <li>написание отчетов по инцидентам;</li> <li>- проводить -мониторинг внешних источников данных</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- навыками защиты сети от вредоносного ПО</li> </ul> <p>Знать:</p> <ul style="list-style-type: none"> <li>- знание концепции и методологии анализа вредоносного ПО</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- производить корреляция данных по разным инцидентам и подготовка рекомендаций по их нейтрализации</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- навыками использования средств корреляции событий ИБ;</li> </ul>

<b>Формируемые и контролируемые компетенции</b> (код и наименование)	<b>Индикаторы достижения компетенций</b> (код и наименование)	<b>Планируемые результаты обучения</b>
		- навыками идентификации, получения, локализации и репортинга по вредоносному ПО
	ПК-6.8 Владеет навыками защиты сетевых коммуникаций, использования средств корреляции событий ИБ	Знать: сетевые коммуникации, средства корреляции событий ИБ Уметь: защищать сетевые коммуникации, использовать средства корреляции событий ИБ Владеть: навыками защиты сетевых коммуникаций, использования средств корреляции событий ИБ

#### 4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек 1	Тема 1 Введение в форензику_1 1.Подразделы форензики. 2.Задачи форензики. 3.Общенаучные методы. 4.Актуальные атаки и известные 5.преступные группировки. 6.Основные источники данных. 7.Организационно-правовые аспекты. 8.Компьютерные преступления 9.Специальные технические средства	6	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Лек 2	Тема 1 Введение в форензику_2 6.Основные источники данных. 7.Организационно-правовые аспекты. 8.Компьютерные преступления 9.Специальные технические средства	6	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Лек 3	Тема 2 Артефакты системы 1.Таймлайны и источники. 2.Оперативно-розыскные мероприятия 3.Файловая система (NTFS). 4.Перехват и исследование трафика. 5.Реестр ОС. 6.Журнал событий Windows. 7.Используемые файлы. 8.История посещения браузеров	6	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 1	Тема 2 Артефакты системы	6	2	2		Практическое задание 1

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		Оформление документации по оперативно-розыскным мероприятиям					
Модуль 1	Пр 2	Тема 2 Артефакты системы Оформление документации по оперативно-розыскным мероприятиям	6	2	2		Практическое задание 1
Модуль 1	Пр 3	Тема 2 Артефакты системы Перехват и исследование трафика с использованием инструментария Kali Linux	6	2	2		Практическое задание 2
Модуль 1	Пр 4	Тема 2 Артефакты системы Перехват и исследование трафика с использованием инструментария Kali Linux	6	2	2		Практическое задание 2
Модуль 1	Пр 5	Тема 2 Артефакты системы Анализ логов, системных журналов, файловой системы	6	2	2		Практическое задание 3
Модуль 1	Пр 6	Тема 2 Артефакты системы Анализ логов, системных журналов, файловой системы	6	2	2		Практическое задание 3
Модуль 1	Лек 4	Тема 3 Компьютерно-техническая экспертиза 1.Фреймворки 2.Методы КТЭ. 3.Работа с файловой системой. 4.Лог-файлы 5.Работа с реестром ОС. 6.Системная конфигурация. 7.Исследование программ. 8.Анализ журнала событий Windows. 9.Исследование дополнительных источников данных.	6	2	-		Банк тестовых заданий/ Устный опрос

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		10.Активность пользовательских браузеров. 11. Поиск нестандартных процессов и подключений					
Модуль 1	Пр 7	Тема 3 Компьютерно-техническая экспертиза  Анатомия атаки	6	2	2		Практическое задание 4
Модуль 1	Пр 8	Тема 3 Компьютерно-техническая экспертиза  Анатомия атаки	6	2	2		Практическое задание 4
Модуль 1	Пр 9	Тема 3 Компьютерно-техническая экспертиза  Практика готовности к инцидентам	6	2	2		Практическое задание 5
Модуль 1	Пр 10	Тема 3 Компьютерно-техническая экспертиза  Практика готовности к инцидентам	6	2	2		Практическое задание 5
Модуль 1	Пр 11	Тема 3 Компьютерно-техническая экспертиза  Выявление необычных служб и нестандартных подключений	6	2	2		Практическое задание 6
Модуль 1	Пр 12	Тема 3 Компьютерно-техническая экспертиза  Выявление необычных служб и нестандартных подключений	6	2	2		Практическое задание 6
Модуль 1	Лек 5	Тема 4 Практика экспертизы 1.Действия специалиста на месте инцидента 2.Следственные действия 3.Тактика обыска	6	2	-		Банк тестовых заданий/ Устный опрос



Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		4.Анализ заражённой системы на месте и его задачи. получение артефактов на месте инцидента. 5.Анализ снимка оперативной памяти. 6.Создание криминалистического образа накопителя 7. Удаление следов					
Модуль 1	Пр 13	Тема 4 Практика экспертизы Порядок сбора улик, действий специалиста	6	2	2		Практическое задание 7
Модуль 1	Пр 14	Тема 4 Практика экспертизы Порядок сбора улик, действий специалиста	6	2	2		Практическое задание 7
Модуль 1	Пр 15	Тема 4 Практика экспертизы Анализ зараженной системы	6	2	2		Практическое задание 8
Модуль 1	Пр 16	Тема 4 Практика экспертизы Анализ зараженной системы	6	2	2		Практическое задание 8
Модуль 1	Лек 6	Тема 5 Реагирование на инциденты_1 1.Готовность к инцидентам 2.Инструменты удаленной сортировки 3.Создание дампа памяти 4.Создание образа диска 5.Инструменты мониторинга сетевой безопасности 6.Анализ событий системы 7Анализ памяти	6	2	-	-	Банк тестовых заданий/ Устный опрос

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		8.Анализ вредоносных программ					
Модуль 1	Лек 7	Тема 5 Реагирование на инциденты_2 9.Извлечение информации с образа жесткого диска 10.Анализ дальнейшего распространения по сети 11. Выявление элементов инфраструктуры, затронутых инцидентом 12.Меры по сглаживанию последствий 13.Эмуляция действий злоумышленника 14. Взаимодействие с НКЦКИ	6	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 17	Тема 5 Реагирование на инциденты_2 Создание образа диска и образа виртуальных машин	6	2	2	-	Практическое задание 9
Модуль 1	Пр 18	Тема 5 Реагирование на инциденты_2 Создание образа диска и образа виртуальных машин	6	2	2	-	Практическое задание 9
Модуль 1	Лек 8	Тема 6 Новые и развивающиеся технологии в области цифровой криминалистики	6	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 19	Тема 6 Новые и развивающиеся технологии в области цифровой криминалистики Применение инструментов сетевой безопасности	6	2	2	-	Практическое задание 10
Модуль 1	Пр 20	Тема 6 Новые и развивающиеся технологии в области цифровой криминалистики Применение инструментов сетевой безопасности	6	2	2	-	Практическое задание 10

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Пр 21	Тема 6 Новые и развивающиеся технологии в области цифровой криминалистики Анализ действий вредоносных программ, обнаружение, нейтрализация	6	2	2	-	Практическое задание 11
Модуль 1	Пр 22	Тема 6 Новые и развивающиеся технологии в области цифровой криминалистики Анализ действий вредоносных программ, обнаружение, нейтрализация	6	2	2	-	Практическое задание 11
Модуль 1	Пр 23	Тема 6 Новые и развивающиеся технологии в области цифровой криминалистики Анализ действий вредоносных программ, обнаружение, нейтрализация	6	2	46	-	Практическое задание 11
	Ср	Самостоятельное изучение материала, не вошедшего в курс лекций	6	79,75	-	-	Банк тестовых заданий
	ПА	Промежуточная аттестация	6	0,25	-	-	Вопросы к зачету
	Псщ	Посещаемость	6	-	10	-	
	Пр 24	Итоговое тестирование	6	2	100	-	Тестовые задания
		Бонусные баллы	6	-	20	-	
<b>Итого:</b>				<b>144</b>			

#### Схема расчета итогового балла

Обучающийся получает до 90 баллов за выполнение практических заданий, до 10 баллов за посещаемость и проходит итоговое тестирование, оцениваемое от 0 до 100 в зависимости от успешности его прохождения. Итоговый балл за курс рассчитывается, как сумма баллов за выполнение практических заданий, баллов за посещаемость и баллов, набранных в ходе тестирования, после чего вся сумма делится на 2. Бонусные баллы выставляются студенту за участие в олимпиадах, конференциях, форумах.

## 5. Образовательные технологии

Технология	Формы обучения	Методы обучения
<b>Технология традиционного обучения</b> – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
<b>Технология модульного обучения</b> – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
<b>Информационные технологии</b> – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.

## 6. Методические указания по освоению дисциплины

Изучение дисциплины предусматривает чтение лекций, проведение практических занятий, самостоятельное изучение специальной литературы по вопросам лекций.

*Изучение теоретического материала* определяется рабочей учебной программой дисциплины, включенным в нее перечнем литературы. Рекомендуется при подготовке к занятиям повторить материал предшествующих тем лекций.

*При подготовке к практическому занятию* необходимо изучить материалы лекции, рекомендованную литературу. Изученный материал следует проанализировать в соответствии с планом занятия, затем проверить степень усвоения содержания вопросов.

*Виды самостоятельной работы обучающихся:*

1. Повторение пройденного лекционного материала, чтение рекомендованной литературы.
2. Подготовка к практическим занятиям.
3. Работа с электронными источниками.
4. Подготовка к сдаче зачета.

Самостоятельная работа обучающихся заключается в изучении литературы, дополняющей материал, излагаемый в лекционной части курса. Необходимо овладеть навыками библиографического поиска, в том числе в сетевых Интернет-ресурсах, научиться сопоставлять различные точки зрения и определять методы исследований.

*При подготовке к зачету* следует руководствоваться перечнем вопросов для подготовки к итоговому контролю по курсу. При этом необходимо уяснить суть основных понятий дисциплины.

Предполагается, что, прослушав лекцию, обучающийся должен ознакомиться с рекомендованной литературой из основного списка, осуществить поиск и критическую оценку материала на сайтах Интернет, собрать необходимую информацию.

## 7. Оценочные средства

### 7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
6	ПК-6	Тестовые задания. Вопросы к зачету № 1-60. Практические задания № 1-11

### 7.2. Типовые задания или иные материалы, необходимые для текущего контроля

#### 7.2.1. Практическое задание

(наименование оценочного средства)

Практическое задание 1. Оформление документации по оперативно-розыскным мероприятиям.

Практическое задание 2. Перехват и исследование трафика с использованием инструментария Kali Linux.

Практическое задание 3. Анализ логов, системных журналов, файловой системы.

Практическое задание 4. Анатомия атаки.

Практическое задание 5. Практика готовности к инцидентам.

Практическое задание 6. Выявление необычных служб и нестандартных подключений.

Практическое задание 7. Порядок сбора улик, действий специалиста

Практическое задание 8. Анализ зараженной системы.

Практическое задание 9. Создание образа диска и образа виртуальных машин.

Практическое задание 10. Применение инструментов сетевой безопасности.

Практическое задание 11. Анализ действий вредоносных программ, обнаружение, нейтрализация.

#### Типовой(ые) пример(ы) задания(ий)

Цель: Сформировать навыки законного и процессуально корректного оформления документации, сопровождающей оперативно-розыскные мероприятия в сфере киберпространства, с обеспечением допустимости полученных данных в качестве цифровых доказательств.

Задание:

1. Студент изучает нормативно-правовую базу (Федеральный закон «Об оперативно-розыскной деятельности», Уголовно-процессуальный кодекс РФ, ведомственные инструкции).

2. На основе смоделированного сценария киберинцидента заполняет комплект процессуальных документов: постановление о проведении ОРМ, протокол изъятия цифровых носителей, акт фиксации электронных данных, формуляр цепочки сохранности доказательств. Особое внимание уделяется корректному отражению времени, места, участников, применяемых технических средств и хеш-сумм.

3. Пакет оформленной документации, прошедший проверку на соответствие процессуальным требованиям и готовый для приобщения к материалам проверки/дела.

#### Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.

2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

#### Критерии оценки:

Формы текущего контроля	Критерии и нормы оценки
Отчет по практическим работам № 1-8	2 балла – задание выполнено в полном объеме без замечаний - 2 балла – задание не выполнено
Устный опрос	31-46 балла – дан полный, развернутый, аргументированный ответ на 2 вопроса 21-30 баллов – дан неполный ответ на 2 вопроса 11-20 баллов – дан полный, развернутый, аргументированный ответ на 1 вопрос 1-10 баллов – дан неполный ответ на 1 вопрос 0 баллов – не дан ни один ответ на 2 вопроса
Посещаемость	10 баллов - обучающийся посещает все занятия. Для обучающихся с менее чем 100% посещаемостью оценка рассчитывается пропорционально количеству посещенных занятий

#### 7.2.2. Тестирование

##### Типовой пример тестового задания

Какой метод анализа вредоносного ПО предполагает запуск программы в контролируемой среде (песочнице) для наблюдения за её поведением?

Выберите один из 4 вариантов ответа:

- 1) Статический анализ
- 2) Динамический анализ
- 3) Сигнатурный анализ
- 4) Криптоанализ

#### Критерии оценки:

Баллы начисляются автоматически пропорционально правильным ответам.

#### 7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

##### 7.3.1. Вопросы к промежуточной аттестации

Семестр 6

№ п/п	Вопросы к зачету
1.	Раскройте содержание основных принципов компьютерной криминалистики (неизменность оригинала, документирование, воспроизводимость, независимость). Как каждый принцип реализуется на практике при проведении экспертизы?

2.	Опишите процессуальный порядок назначения и производства судебной компьютерно-технической экспертизы в Российской Федерации. Какие нормативные акты регулируют данный процесс?
3.	Объясните различие между криминалистическим исследованием цифровых носителей и оперативно-розыскными мероприятиями. В каких случаях требуется судебное решение?
4.	Раскройте содержание понятия «цепочка сохранности доказательств». Какие документы и технические меры необходимы для её обеспечения от момента изъятия до представления в суд?
5.	Охарактеризуйте требования к экспертному заключению по результатам компьютерно-технического исследования. Какие разделы обязательны и как формулируются выводы для правоприменителя?
6.	Объясните роль международных стандартов (ISO/IEC 27037, 27041, 27042, 27043) в организации процессов компьютерной криминалистики. Как они соотносятся с национальными методическими рекомендациями?
7.	Раскройте особенности криминалистического анализа данных в рамках расследования инцидентов информационной безопасности. Чем отличается процессуальная экспертиза от внутреннего расследования в коммерческой организации?
8.	Опишите порядок взаимодействия эксперта-криминалиста с правоохранительными органами, адвокатами и техническими специалистами организации-владельца данных. Какие этические нормы при этом соблюдаются?
9.	Объясните, как обеспечивается допустимость цифровых доказательств в судебном процессе. Какие факторы могут привести к признанию доказательств недопустимыми?
10.	Раскройте содержание понятия «криминалистическая гипотеза» при расследовании киберинцидентов. Как формулируются и проверяются гипотезы на основе цифровых артефактов?
11.	Опишите алгоритм криминалистического изъятия персонального компьютера в рабочем состоянии. Какие действия запрещены и почему?
12.	Объясните разницу между физическим и логическим образом цифрового носителя. В каких случаях применяется каждый из методов и как обеспечивается верификация целостности?
13.	Раскройте порядок работы с зашифрованными дисками и разделами. Какие технические и процессуальные сложности возникают при изъятии и исследовании таких носителей?
14.	Охарактеризуйте методы обеспечения сохранности данных при изъятии серверного оборудования в условиях центра обработки данных. Как минимизируется время простоя и риск повреждения данных?
15.	Объясните назначение и принципы использования криминалистических блокираторов записи. Как они работают на аппаратном и программном уровнях?

16.	Раскройте особенности изъятия и анализа данных с устройств хранения, подключённых по интерфейсам NVMe, SAS, Thunderbolt. Какие технические ограничения существуют?
17.	Опишите процедуру создания контрольных хеш-сумм и их роль в доказывании неизменности исследуемой информации. Какие алгоритмы хеширования рекомендованы для судебно-экспертной деятельности?
18.	Объясните порядок работы с виртуальными машинами и контейнерными средами при проведении криминалистического исследования. Как фиксируются снимки состояния и конфигурации?
19.	Раскройте содержание понятия «летучие данные». Какие категории информации относятся к летучим и почему их изъятие требует особой оперативности?
20.	Охарактеризуйте типичные ошибки, допускаемые при изъятии цифровых носителей, и их влияние на допустимость полученных доказательств. Как они предотвращаются на этапе подготовки?
21.	Раскройте структуру файловой системы NTFS. Какие метафайлы и системные структуры наиболее значимы для криминалистического анализа?
22.	Объясните механизм удаления файлов в файловых системах семейства FAT и NTFS. Как происходит освобождение кластеров и почему данные могут быть восстановлены?
23.	Опишите процесс криминалистического восстановления удалённых файлов. Какие методы используются при фрагментации данных и перезаписи секторов?
24.	Раскройте содержание понятия «файловый карвинг». Какие сигнатуры и эвристики применяются для поиска файлов без опоры на метаданные файловой системы?
25.	Объясните роль журналирования в современных файловых системах (ext4, NTFS, APFS). Как анализ журналов помогает восстановить последовательность операций с файлами?
26.	Охарактеризуйте методы анализа альтернативных потоков данных в NTFS. Как они используются для сокрытия информации и как обнаруживаются при исследовании?
27.	Раскройте особенности исследования файловой системы exFAT и её отличия от FAT32 и NTFS. Какие криминалистические артефакты сохраняются после удаления данных?
28.	Объясните порядок анализа временных меток файлов (MACB-времена). Как выявляются признаки подделки времени создания, изменения и доступа к файлам?
29.	Опишите методику исследования файловых систем мобильных устройств (F2FS, ext4 в Android, APFS в iOS). Какие ограничения существуют при их криминалистическом анализе?
30.	Раскройте содержание понятия «slack space» и «unallocated space». Как эти области используются для поиска скрытых или удалённых данных?



31.	Раскройте назначение анализа дампа оперативной памяти в компьютерной криминалистике. Какие типы артефактов можно извлечь из энергозависимой памяти?
32.	Объясните порядок создания криминалистически корректного дампа оперативной памяти. Какие инструменты используются и как минимизируется влияние на систему?
33.	Охарактеризуйте методы поиска процессов, сетевых соединений, загруженных модулей и ключей шифрования в дампе памяти. Какие структуры ядра операционной системы анализируются?
34.	Раскройте содержание понятия «инъекция кода в процессы». Как обнаруживаются признаки внедрения вредоносных библиотек или шелл-кода в легитимные процессы?
35.	Объясните принципы сетевой криминалистики. Какие источники данных (журналы маршрутизаторов, дампы трафика, данные прокси-серверов) наиболее значимы для расследования?
36.	Опишите методику анализа файлов захвата сетевого трафика. Как реконструируются сессии, извлекаются переданные файлы и выявляются аномальные соединения?
37.	Раскройте особенности исследования зашифрованного сетевого трафика. Какие косвенные признаки и метаданные используются для анализа без расшифровки содержимого?
38.	Объясните порядок анализа журналов операционных систем, приложений и средств защиты. Как выявляются признаки несанкционированного доступа и скрытой активности?
39.	Охарактеризуйте методы корреляции событий из разных источников (память, диск, сеть, журналы). Как формируется единая временная шкала инцидента?
40.	Раскройте содержание понятия «сетевые индикаторы компрометации». Как они применяются для ретроспективного анализа и поиска признаков заражения в корпоративной инфраструктуре?
41.	Раскройте особенности изъятия и анализа смартфонов на базе операционных систем Android и iOS. Какие уровни доступа (логический, файловой системы, физический) доступны эксперту?
42.	Объясните порядок работы с облачными сервисами и синхронизированными данными. Какие правовые и технические ограничения существуют при запросе информации у провайдеров?
43.	Охарактеризуйте методы анализа резервных копий мобильных устройств. Какие артефакты (сообщения, геолокация, история браузера) можно извлечь и как они проверяются на достоверность?
44.	Раскройте содержание понятия «криминалистический анализ вредоносного программного обеспечения». Какие этапы включают статический и динамический анализ образцов?

45.	Объясните порядок исследования обфусцированных скриптов и макросов. Как восстанавливается исходная логика выполнения и выявляются скрытые сетевые запросы?
46.	Опишите методику анализа программ-шифровальщиков. Как идентифицируются алгоритмы шифрования, ключи и механизмы распространения полезной нагрузки?
47.	Раскройте особенности исследования устройств интернета вещей и промышленных контроллеров. Какие криминалистические артефакты сохраняются в их прошивках и журналах?
48.	Объясните порядок работы с данными из систем видеонаблюдения, биометрических терминалов и контрольно-пропускных систем. Как обеспечивается достоверность и неизменность таких записей?
49.	Охарактеризуйте методы анализа зашифрованных контейнеров и виртуальных дисков. Как выявляются признаки использования стеганографии или скрытых томов?
50.	Раскройте содержание понятия «антикриминалистические приёмы». Как злоумышленники пытаются затруднить исследование данных и какие методы противодействия применяются экспертами?
51.	Раскройте архитектуру и функциональные возможности современных программно-аппаратных комплексов для компьютерной криминалистики. Какие задачи они решают на разных этапах исследования?
52.	Объясните порядок валидации и верификации криминалистического программного обеспечения. Какие требования предъявляются к инструментарию, используемому в судебной экспертизе?
53.	Охарактеризуйте методику подготовки экспертного заключения. Как технические результаты исследования трансформируются в понятные для суда выводы?
54.	Раскройте содержание понятия «воспроизводимость результатов экспертизы». Как обеспечивается возможность независимой проверки выводов другим специалистом?
55.	Объясните порядок работы с базами данных индикаторов компрометации и хеш-сумм известных вредоносных программ. Как они интегрируются в процесс расследования?
56.	Опишите требования к хранению и архивированию криминалистических образов и промежуточных данных. Какие сроки хранения установлены и как обеспечивается защита от несанкционированного доступа?
57.	Раскройте особенности проведения криминалистического анализа в условиях распределённых и гибридных инфраструктур. Как учитываются данные из нескольких источников и юрисдикций?
58.	Объясните этические ограничения деятельности эксперта-криминалиста. Какие действия могут привести к конфликту интересов или нарушению профессиональных стандартов?

59.	Охарактеризуйте методы автоматизации рутинных операций в компьютерной криминалистике. Какие сценарии поддаются автоматизации, а какие требуют обязательного участия специалиста?
60.	Раскройте перспективы развития компьютерной криминалистики в условиях внедрения искусственного интеллекта, квантовых вычислений и новых архитектур хранения данных. Какие вызовы это создаёт для правоохранительной и экспертной практики?

### 7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
6	Зачет (письменно/по накопительному рейтингу)	«зачтено»	55-100 баллов
		«не зачтено»	0-54 баллов

## 8. Учебно-методическое и информационное обеспечение дисциплины

### 8.1. Обязательная литература

<b>№ п/п</b>	<b>Авторы, составители</b>	<b>Заглавие (заголовок)</b>	<b>Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)</b>	<b>Год издания</b>	<b>Количество в научной библиотеке / Наименование ЭБС</b>
1	Нефедов В. С., Криулин А. А., Потерпеев Г. Ю.	Основы обеспечения анонимности в сети Интернет	Учебное пособие	2022	ЭБС Лань
2	Жердев П. А., Мерецкий Н. Е.	Расследование преступлений в сфере компьютерной информации: учебное пособие	Учебное пособие	2024	ЭБС Лань
3	Смирнов С. И., Изергин Д. А., Максимова Е. А., Иванова И. А., Кумуржи Г. М.	Компьютерная экспертиза. Часть 2	Учебное пособие	2025	ЭБС Лань

### 8.2. Дополнительная литература

<b>№ п/п</b>	<b>Авторы, составители</b>	<b>Заглавие (заголовок)</b>	<b>Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)</b>	<b>Год издания</b>	<b>Количество в научной библиотеке / Наименование ЭБС</b>
1	Андреев В. Д.	Аудит и оценка экономической безопасности хозяйствующих субъектов	Учебное пособие	2023	ЭБС Лань

### 8.3. Перечень профессиональных баз данных и информационных справочных систем

1. FREEDOM COLLECTION (Полнотекстовая коллекция электронных журналов Elsevier B.V.) <https://www.sciencedirect.com/> неизвестный
2. Nano Database <http://nano.nature.com/> база данных
3. Springer Materials <http://materials.springer.com/> база данных
4. Springer Nature Protocols and Methods <https://experiments.springernature.com/sources/springer-protocols> база данных
5. zbMath <https://zbmath.org/> база данных
6. Springer Nature (Полнотекстовая коллекция журналов) <https://www.springernature.com/gp/products> неизвестный
7. Springer eBooks (Полнотекстовая коллекция электронных книг издательства Springer Nature) <https://link.springer.com/> неизвестный
8. ORBIT INTELLIGENCE (Патентная база компании QUESTEL) <http://www.orbit.com/> база данных
9. CSD-ENTERPRISE (База данных компании CAMBRIDGE CRYSTALLOGRAPHIC DATA CENTER) <https://www.ccdc.cam.ac.uk/structures/> база данных
10. ELIBRARY.RU (электронная библиотека научных публикаций) <http://elibrary.ru> неизвестный
11. "Гарант" <https://www.garant.ru/> ИСС
12. "КонсультантПлюс" <https://www.consultant.ru/> ИСС
13. "Кодекс" <https://kodeks.ru/> ИСС
14. Техэксперт <https://cntd.ru/> ИСС

### 8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

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

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номера аудитории)	Перечень основного оборудования
1	Помещение для самостоятельной работы обучающихся Д -409	Стол-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор,

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
		компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф
2	Помещение для самостоятельной работы обучающихся УЛК-105	Стол, стулья, стеллажи (в т.ч. выставочные) с книгами, персональные компьютеры, мобильные рабочие места
3	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
4	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. Д-402	Стол, стулья, стол преподавательский, стул преподавательский, доска аудиторная (меловая), кафедра напольная, проектор, экран выкатной.
5	Лаборатория "Техносферная безопасность. Здания, сооружения и их устойчивость при пожаре". Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной	Стол, стулья, стол преподавательский, стул преподавательский, стулья ученические, доска аудиторная (меловая), шкаф, стенд для размещения документов по охране труда, пожарной безопасности, стол для манекена, манекен, тонометр механический, торс реанимационный, тренажер для постановки клизмы и в/м инъекций, тренажер сердце-легкие и мозговой реанимации максимум 2-01, носилки санитарные., секундомер

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	аттестации. Институт инженерной и экологической безопасности Д-403	
6	<p>Лаборатория "Техносферная безопасность. Автоматизированные системы управления и связи. Производственная и пожарная автоматика".</p> <p>Учебная аудитория для проведения занятий семинарского типа.</p> <p>Учебная аудитория для курсового проектирования (выполнения курсовых работ).</p> <p>Учебная аудитория для проведения групповых и индивидуальных консультаций</p> <p>Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.</p> <p>Д-405</p>	<p>Стол учебный двухместный, стол преподавательский, стул преподавательский, стулья учебные, доска аудиторная (меловая), шкаф, стенд для размещения документов по охране труда, пожарной безопасности, стенд для размещения и хранения лабораторных принадлежностей по дисциплине «Пожарная безопасность», огнетушитель ОУБ-7, песочница мини, противогазы в сумке, учебно-лабораторное оборудование «Автоматическая система пожаротушения», учебно-лабораторное оборудование "Охранно-пожарная сигнализация" стенд «Сигнализация пожарно-охранная сигнализация», стенд «Оросители автоматические системы пожаротушения»</p>
7	<p>Лаборатория "Техносферная безопасность".</p> <p>Учебная аудитория для проведения занятий семинарского типа.</p> <p>Учебная аудитория для курсового проектирования (выполнения курсовых работ).</p> <p>Учебная аудитория для проведения групповых и индивидуальных консультаций</p> <p>Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.</p> <p>Д-407</p>	<p>Стол учебный двухместный, стол преподавательский, стул преподавательский, стулья учебные, доска аудиторная (меловая), шкаф, стенд для размещения документов по охране труда, пожарной безопасности, экран на треноге Da-Lite Versatol 152x152, проектор №265910 Acer P1, ноутбук №6512 BWL HP Compaq nx 7300 CM-430 -, стенд для размещения нормативных документов по дисциплине «Безопасность грузоподъемных машин и механизмов», стенд к лабораторной работе № 2 «Браковка канатных строп».</p>
8	<p>Лаборатория "Техносферная безопасность".</p> <p>Учебная аудитория для проведения занятий семинарского типа.</p> <p>Учебная аудитория для курсового проектирования (выполнения курсовых работ).</p> <p>Учебная аудитория для проведения групповых и индивидуальных консультаций</p>	<p>Стол учебный двухместный, стол преподавательский, стул преподавательский, стулья учебные, доска аудиторная (меловая), шкаф, тумба на колесиках, стенд "Средства индивидуальной защиты", стенд для размещения документов по охране труда, пожарной безопасности, стенд «Материалы и отходы», магнитные доски на колесиках</p>

№ п/п	<b>Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)</b>	<b>Перечень основного оборудования</b>
	Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. Д-408	
9	Лаборатория "Техносферная безопасность". Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. Д-410	Столы ученические двухместные, стол преподавательский, стул преподавательский., стулья ученические, доска аудиторная (меловая), шкаф, стенд для размещения документов по охране труда, пожарной безопасности, стенд «Низковольтная защитная аппаратура», шкаф распределительный, стойка с изолирующими штангами (6 шт), стенд испытательный (щитовая), огнетушитель -, стенд «Электросхемы», стенд проверки электроинструментов СПЭИ-1, стенд «Виды ламп», стенд «Защитные средства и приспособления», установка лабораторная «Модель электродвигателя», стенд «Низковольтная защитная аппаратура»
10	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. Д-413	Столы ученические двухместные , стол преподавательский, стул преподавательский, стулья ученические, доска аудиторная, кафедра напольная, проектор подвесной, экран (с автоматическим приводом), системный блок .