МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное
учреждение высшего образования
«УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Учёным советом УрГЮУ
протокол № 7 от 05.12.2021
Председатель
Учёного совета УрГЮУ
д.ю.н., профессор Бублик В.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Цифровые технологии в криминалистике»

Основная профессиональная образовательная программа высшего образования – программа подготовки научно-педагогических кадров в аспирантуре по направлению подготовки 40.06.01 Юриспруденция (уровень подготовки кадров высшей квалификации) (направленность: Криминалистика; судебно-экспертная деятельность; оперативно-разыскная деятельность)

Квалификация
Исследователь. Преподаватель-Исследователь

Форма обучения
Очная
Заочная

1. Цели и задачи дисциплины.

Область профессиональной деятельности выпускников, освоивших программу аспирантуры, включает разработку и реализацию правовых норм, проведение научных исследований, образование и воспитание, экспертно-консультационную работу, обеспечение законности и правопорядка.

Целью учебной дисциплины «Особенности расследования преступлений против личности» является формирование знаний, умений и навыков необходимых для осуществления научно-исследовательской деятельности в сфере юриспруденции и педагогической деятельности по образовательным программам высшего образования.

В ходе освоения дисциплины студент готовится к выполнению следующих профессиональных задач:

научно-исследовательская деятельность в области юриспруденции;

преподавательская деятельность по образовательным программам высшего образования.

2. Место дисциплины в структуре образовательной программы.

Дисциплина «Особенности расследования преступлений против личности» относится к дисциплинам по выбору вариативной части Блока 1 Учебного плана.

Требования к входным знаниям.

Необходимым условием изучения дисциплины «Особенности расследования преступлений против личности» является владение аспирантом рядом общепрофессиональных и профессиональных компетенций, сформированных на двух предшествующих уровнях образования в результате освоения им таких дисциплин как Криминалистика, Судебная Экспертиза, Методика расследования преступлений против личности, Криминалистические и оперативно-розыскные аспекты раскрытия и расследования преступлений, Основы оперативно-розыскной деятельности, Уголовное право, Уголовный процесс.

Сформированные по итогам изучения дисциплины «Особенности расследования преступлений против личности» навыки и умения являются базовыми для прохождения практики и государственной аттестации, представления научного доклада об основных результатах подготовки научно-квалификационной работы (диссертации).

Изучению дисциплины предшествуют следующие дисциплины:

1. Научно-исследовательская деятельность
2. Подготовка научно-квалификационной работы (диссертации) на соискание учёной степени кандидата юридических наук.
3. Методология юридической науки
4. Педагогика высшей школы
5. Юридическое источниковедение

3. **Требования к результатам освоения дисциплины**:

Выпускник, освоивший программу, должен обладать следующими компетенциями:

(направленность 12.00.12)

способность проводить теоретические и экспериментальные научные исследования, направленные на дополнение концептуальных основ криминалистики, судебной экспертизы, оперативно-разыскной деятельности, выявлять тенденции развития теории и практики раскрытия и расследования преступлений (ПК-1);

способность применять в научном исследовании современные методологические подходы и основные теории криминалистики, доводить до уровня апробации прикладные разработки в области раскрытия и расследования преступлений (ПК-2);

4. Структура и трудоемкость дисциплины.

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

Очная форма обучения

Вид учебной работы	Всего часов	Семестры					
		3					
Аудиторные занятия (всего)	10	10					
В том числе:	-	-	-	-	-		
Лекции							
Практические занятия (всего):		10					
Самостоятельная работа (всего)	98	98					
В т.ч. промежуточная аттестация	36	36					
Вид промежуточной аттестации (зачет, экзамен)		Зачёт					
Общая трудоемкость час	108	108					
зач.ед.	3						

Тематический план.

№ п/п	Модуль, темы учебной дисциплины	Виды учебной деятельности и трудоемкость (в часах)			Всего часов
		Лекции	Практические занятия	Самостоятельная работа	
I	**Модуль 1. Цифровые следы как объект криминалистического исследования**		**7**	**11**	**14**
1.	Тема 1. Предмет, объект, система и задачи цифровой криминалистики		1	6	8
2	Тема 2. Понятие и сущность цифровой информации как объекта криминалистических исследований		1	7	8
3	Тема 3. Цифровые следы: понятие, признаки, механизм образования, классификация и особенности фиксации		2	7	9
4	Тема 4. Криминалистическое исследование компьютерных устройств и информационно-коммуникационных сетей		1	7	8
5	Тема 5. Основы методики расследования преступлений в сфере компьютерной информации		1	7	8
6	Тема 6. Назначение и производство компьютерно-технических исследований		1	7	8
II	**Модуль 2. Цифровые технологии как методы и средства криминалистического познания**		**3**	**29**	**31**
7	Тема 7. Использование цифровых технологий как средств криминалистической техники в проведении следственных действий		1	7	8
8	Тема 8. Использование информационных		1	7	8

	систем и компьютерных сетей для обеспечения межведомственного взаимодействия правоохранительных органов				
9	Тема 9. Применение цифровых технологий для регистрации и розыска криминалистически значимых объектов		1	7	8
	ВСЕГО:		10	62	72

Заочная форма

Вид учебной работы	Всего часов	Семестры					
		5					
Аудиторные занятия (всего)	12	12					
В том числе:	-	-	-	-	-		
Лекции		6					
Практические занятия (всего):		6					
Самостоятельная работа (всего)	96	96					
В т.ч. промежуточная аттестация	9	9					
Вид промежуточной аттестации (зачет, экзамен)		Зачёт					
Общая трудоемкость час	108	108					
зач.ед.	3	3					

Тематический план.

№ п/п	Модуль, темы учебной дисциплины	Виды учебной деятельности и трудоемкость (в часах)			Всего часов
		Лекции	Практические занятия	Самостоятельная работа	
I	**Модуль 1. Цифровые следы как объект криминалистического исследования**	**3**	**3**	**49**	**14**
1.	Тема 1. Предмет, объект, система и задачи цифровой криминалистики	1		10	8
2	Тема 2. Понятие и сущность цифровой информации как объекта криминалистических исследований	1		10	8
3	Тема 3. Цифровые следы: понятие, признаки, механизм образования, классификация и особенности фиксации	1	1	9	9
4	Тема 4. Криминалистическое исследование компьютерных устройств и информационно-коммуникационных сетей		1	10	8
5	Тема 5. Основы методики расследования преступлений в сфере компьютерной информации		1	10	8

6	Тема 6. Назначение и производство компьютерно-технических исследований			10	8
II	**Модуль 2. Цифровые технологии как методы и средства криминалистического познания**	**3**	**3**	**28**	**31**
7	Тема 7. Использование цифровых технологий как средств криминалистической техники в проведении следственных действий	1	1	10	8
8	Тема 8. Использование информационных систем и компьютерных сетей для обеспечения межведомственного взаимодействия правоохранительных органов	1	1	9	8
9	Тема 9. Применение цифровых технологий для регистрации и розыска криминалистически значимых объектов	1	1	9	8
	ВСЕГО:	6	10	87	72

5. Планируемые результаты обучения по дисциплине, фонд оценочных средств по дисциплине для текущего контроля и критерии освоения компетенций:

Результаты обучения, достижение которых свидетельствует об освоении компетенции:

ПК-1. Способность проводить теоретические и экспериментальные научные исследования, направленные на дополнение концептуальных основ криминалистики и судебной экспертизы, выявлять тенденции развития теории и практики раскрытия и расследования преступлений

Знания:

предмета, объекта, системы и задач цифровой криминалистики;

понятия, сущности, принципов формирования цифровой доказательственной информации;

понятия и признаков цифровых следов;

механизма следообразования цифровых следов;

способов сокрытия и обнаружения цифровых следов;

способов фиксации цифровых следов;

способов изъятия и копирования цифровых следов;

понятия больших данных и основных компьютерно-технических особенностей их получения и обработки;

принципиальной схемы организации компьютерной техники;

классификационных видов носителей цифровой информации;

общих положений использования телекоммуникационных сетей в раскрытии и расследовании преступлений;

понятия и классификации преступлений в сфере компьютерной информации;

криминалистической характеристики преступлений в сфере компьютерной информации;

понятия, задач и объектов компьютерной-технических экспертиз;

классификации компьютерно-технических экспертиз;

основных ошибок, совершаемых при использовании цифровых технических средств;

программного обеспечения, составляющего АРМ следователя;

основ функционирования и пополнения компьютеризированных учётов, используемых в раскрытии и расследовании преступлений;

основного терминологического инструментария из областей компьютерной техники и сетевых технологий;

требований нормативно-правовых актов в области информационной безопасности и защиты информации.

Умения:

определять типовые цифровые следы и их носители при анализе следственных ситуаций;

описывать механизм следообразования цифровых следов в различных криминальных ситуациях;

классифицировать цифровые следы и носители цифровой доказательственной информации;

классифицировать способы сокрытия цифровых следов;

сравнивать различные подходы к научному определению понятия цифровых следов;

сравнивать различные подходы к научным определениям больших данных;

сопоставлять элементы криминалистической характеристики преступлений в сфере компьютерной информации;

классифицировать направления компьютерно-технических исследований;

использовать корректную терминологию при описании цифровых криминалистически значимых объектов.

Навыки:

юридически правильно квалифицировать факты, события и обстоятельства, связанные с компьютерными инцидентами, и изучать особенности их отражения в непроцессуальных и процессуальных документах;

оценивать корректность применения специальных знаний при проведении служебных и иных документальных проверок по фактам совершения компьютерных инцидентов;

изучать факты применения в профессиональной деятельности следователя и судебного эксперта современных систем и средств электронного документооборота, информационно-телекоммуникационных технологий, информационных систем, в том числе федеральных/государственных;

выявлять и анализировать следственные ошибки при работе с цифровыми объектами;

предлагать способы выявления фактов сокрытия цифровых следов;

осуществлять мануальный и полуавтоматический поиск в телекоммуникационных сетях;

исследовать соблюдение в профессиональной деятельности следователя методик и рекомендаций по расследованию преступлений, связанных с использованием компьютерной информации;

работать с большими объёмами цифровой информации;

адаптировать требования нормативно-правовых актов в области информационной безопасности и защиты информации в криминалистические рекомендации.

Оценочные средства, используемые для оценки сформированности компетенции:

Темы дискуссий:

1. Цифровые, электронные или электронно-цифровые следы?
2. Российский и зарубежный подходы к цифровой криминалистике.
3. Терминологический инструментарий цифровой криминалистики.
4. Криптография и стеганография.
5. Большие данные и криминалистика.
6. Облачные данные и криминалистика.
7. Цифровые источники информации в работе следователя и судебного эксперта.
8. Основные ошибки при работе с носителями цифровой информации.

Критерии освоения компетенции:

Пороговый уровень – обучающийся:

описывает предмет, объект, систему и задачи цифровой криминалистики;

проговаривает понятия цифровых следов, цифровой доказательственной информации, больших данных, преступлений в сфере компьютерной информации;

сравнивает отдельные подходы в определении понятия и сущности цифровых следов;

описывает механизм следообразования цифровых следов;

описывает принципиальную схему организации компьютерной техники;

перечисляет отдельные способы сокрытия, обнаружения, фиксации и изъятия цифровых следов и носителей цифровой доказательственной информации;

разграничивает случаи изъятия и копирования цифровой доказательственной информации;

перечисляет виды носителей цифровой информации;

описывает элементы криминалистической характеристики преступлений в сфере компьютерной информации;

называет основные ошибки, совершаемые при использовании цифровых технических средств в процессе расследования преступлений;

описывает основы функционирования и пополнения компьютеризированных учётов, используемых в раскрытии и расследовании преступлений;

показывает способность правильно квалифицировать факты, события и обстоятельства, связанные с компьютерными инцидентами, и изучать особенности их отражения в непроцессуальных и процессуальных документах;

использует корректный терминологический инструментарий областей компьютерной техники и сетевых технологий;

изучает факты применения в профессиональной деятельности следователя и судебного эксперта современных систем и средств электронного документооборота, информационно-телекоммуникационных технологий, информационных систем, в том числе федеральных/государственных;

демонстрирует способность осуществлять мануальный и полуавтоматический поиск в телекоммуникационных сетях;

исследует соблюдение в профессиональной деятельности следователя методик и рекомендаций по расследованию преступлений, связанных с использованием компьютерной информации;

перечисляет направления компьютерной-технических исследований;

демонстрирует знания основ нормативно-правовых актов в области информационной безопасности и защиты информации;

формулирует отдельные положения криминалистических рекомендаций, связанных с информационной безопасностью и защитой информации.

Базовый уровень – обучающийся:

описывает отдельные научные подходы к определению предмета, объекта, систему и задач цифровой криминалистики;

анализирует понятия цифровых следов, цифровой доказательственной информации, больших данных, преступлений в сфере компьютерной информации;

анализирует отдельные подходы в определении понятия и сущности цифровых следов;

раскрывает механизм следообразования цифровых следов, в том числе на теоретических примерах;

описывает принципиальную схему организации компьютерной техники;

раскрывает систему способов сокрытия, обнаружения, фиксации и изъятия цифровых следов и носителей цифровой доказательственной информации;

разграничивает случаи изъятия и копирования цифровой доказательственной информации по различным критериям;

классифицирует носители цифровой информации;

раскрывает элементы криминалистической характеристики преступлений в сфере компьютерной информации;

классифицирует основные ошибки, совершаемые при использовании цифровых технических средств в процессе расследования преступлений;

раскрывает основы функционирования и пополнения компьютеризированных учётов, используемых в раскрытии и расследовании преступлений;

правильно квалифицирует факты, события и обстоятельства, связанные с компьютерными инцидентами, и изучать особенности их отражения в непроцессуальных и процессуальных документах;

использует корректный терминологический инструментарий областей компьютерной техники и сетевых технологий;

изучает факты применения в профессиональной деятельности следователя и судебного эксперта современных систем и средств электронного документооборота, информационно-телекоммуникационных технологий, информационных систем, в том числе федеральных/государственных;

демонстрирует способность осуществлять мануальный и полуавтоматический поиск в телекоммуникационных сетях;

исследует соблюдение в профессиональной деятельности следователя методик и рекомендаций по расследованию преступлений, связанных с использованием компьютерной информации;

классифицирует направления компьютерной-технических исследований;

знает основы нормативно-правовых актов в области информационной безопасности и защиты информации;

системно формулирует положения криминалистических рекомендаций, связанных с информационной безопасностью и защитой информации.

Повышенный уровень – обучающийся:

анализирует отдельные научные подходы к определению предмета, объекта, систему и задач цифровой криминалистики;

критически анализирует понятия цифровых следов, цифровой доказательственной информации, больших данных, преступлений в сфере компьютерной информации;

анализирует отдельные подходы в определении понятия и сущности цифровых следов, используя российский и зарубежный подходы;

раскрывает механизм следообразования цифровых следов, в том числе на теоретических и практических примерах;

описывает принципиальную схему организации компьютерной техники;

анализирует систему способов сокрытия, обнаружения, фиксации и изъятия цифровых следов и носителей цифровой доказательственной информации;

систематизирует случаи изъятия и копирования цифровой доказательственной информации по различным критериям;

классифицирует носители цифровой информации;

анализирует элементы криминалистической характеристики преступлений в сфере компьютерной информации;

классифицирует основные ошибки, совершаемые при использовании цифровых технических средств в процессе расследования преступлений;

анализирует процессы функционирования и пополнения компьютеризированных учётов, используемых в раскрытии и расследовании преступлений;

правильно квалифицирует факты, события и обстоятельства, связанные с компьютерными инцидентами, и изучать особенности их отражения в непроцессуальных и процессуальных документах;

использует корректный терминологический инструментарий областей компьютерной техники и сетевых технологий, компьютерных наук;

анализирует факты применения в профессиональной деятельности следователя и

судебного эксперта современных систем и средств электронного документооборота, информационно-телекоммуникационных технологий, информационных систем, в том числе федеральных/государственных;

демонстрирует способность осуществлять мануальный и полуавтоматический поиск в телекоммуникационных сетях, в том числе для исследования прошлого состояния сети;

критически исследует соблюдение в профессиональной деятельности следователя методик и рекомендаций по расследованию преступлений, связанных с использованием компьютерной информации;

классифицирует и анализирует возможности направлений компьютерной-технических исследований;

знает основы нормативно-правовых актов в области информационной безопасности и защиты информации;

системно формулирует положения криминалистических рекомендаций, связанных с информационной безопасностью и защитой информации.

ПК-2. Способность применять в научном исследовании современные методологические подходы и основные теории криминалистики, доводить до уровня апробации прикладные разработки в области раскрытия и расследования преступлений

Знания:

правил изъятия и хранения цифровой техники и носителей цифровой информации;

алгоритмов осмотра компьютерной техники;

алгоритмов осмотра веб-сайтов;

основных операторов поиска информации в сети интернет;

порядка обращения к автоматизированным сервисам мониторинга сети интернет;

алгоритмов осмотра смартфонов;

алгоритмов осмотра содержимого облачных хранилищ;

следственных ситуаций, при которых необходимым и обоснованным действием является назначение компьютерно-технических экспертиз;

порядка назначения компьютерно-технических экспертиз;

основ методики производства компьютерно-технических экспертиз;

основных цифровых технических средств, используемых при производстве следственных действий;

основ использования информационных систем и компьютерных сетей для обеспечения межведомственного взаимодействия правоохранительных органов;

основ оцифровки криминалистически значимых сведений и объектов.

Умения:

разграничивать следственные ситуации, требующие изъятия или копирования цифровой доказательственной информации;

выделять следственные ситуации, в которых возможны факты выявления крипто- или стеганографических способов сокрытия цифровой доказательственной информации;

определять следственные ситуации, при которых необходимым является использование специальных знаний в области компьютерной техники, программного обеспечения или сетевых технологий;

изучать направления совершенствования цифровых инструментов следователя или судебного эксперта;

исследовать информационные системы и компьютерные сети, используемые для обеспечения межведомственного взаимодействия правоохранительных органов;

исследовать современное состояние компьютеризированных учётов, используемых при раскрытии и расследовании преступлений.

Навыки:

формулировать криминалистические рекомендации по обнаружению, фиксации, изъятию, хранению и исследованию отдельных цифровых следов и носителей цифровой доказательственной информации;

формулировать проблемы, возникающие при использовании цифровых технических средств во время производства следственных действий;

составлять алгоритмы расследования преступлений в сфере компьютерной информации;

изучать и оценивать эффективность методик экспертных компьютерно-технических исследований;

изучать большие данные и функциональное назначение программного обеспечения;

предлагать направления совершенствования цифровых технологий в следственной и судебно-экспертной деятельности;

предлагать способы преобразования цифровых объектов в традиционные и в обратном направлении.

Оценочные средства, используемые для оценки сформированности компетенции:

Темы дискуссий:

1. Использование информаций базовых станций в расследовании преступлений.
2. Преодоление программных средств защиты данных смартфона.
3. Особенности осмотра и обыска помещений с участием специалиста в области компьютерной информации.
4. Направления совершенствования компьютерно-технических экспертиз.
5. Корреляционные связи между элементами криминалистической характеристики преступлений в сфере компьютерной информации.
6. Совершенствование информационно-криминалистического сопровождения расследования преступлений.
7. Деятельность следователя в сети интернет.
8. Использование сведений из социальных сетей в расследовании преступлений.
9. Необходима ли цифровизация традиционных объектов криминалистических исследований?

Критерии освоения компетенции:

Пороговый уровень – обучающийся:

называет основные правила изъятия и хранения цифровой техники и носителей цифровой доказательственной информации;

воспроизводит алгоритм осмотра компьютерной техники;

воспроизводит алгоритм осмотра веб-сайта;

называет основные операторы поиска информации в сети интернет;

воспроизводит порядок обращения к автоматизированным сервисам мониторинга сети интернет;

воспроизводит алгоритм осмотра смартфонов;

воспроизводит алгоритм осмотра содержимого облачных хранилищ;

называет отдельные следственные ситуации, при которых необходимым и обоснованным действием является назначение компьютерно-технических экспертиз;

воспроизводит порядок назначения компьютерно-технических экспертиз;

анализирует методики производства компьютерно-технических экспертиз;

перечисляет цифровые технические средства, используемые при производстве следственных действий;

анализирует ситуации и способы использования информационных систем и компьютерных сетей для обеспечения межведомственного взаимодействия

правоохранительных органов;

анализирует способы оцифровки криминалистически значимых объектов и сведений;

разграничивает следственные ситуации, требующие изъятия или копирования цифровой доказательственной информации;

называет следственные ситуации, в которых возможны факты выявления крипто- или стеганографических способов сокрытия цифровой доказательственной информации;

определяет следственные ситуации, при которых необходимым является использование специальных знаний в области компьютерной техники, программного обеспечения или сетевых технологий;

изучает направления и предлагает способы совершенствования цифровых инструментов следователя или судебного эксперта;

исследует информационные системы и компьютерные сети, используемые для обеспечения межведомственного взаимодействия правоохранительных органов;

исследует современное состояние компьютеризированных учётов, используемых при раскрытии и расследовании преступлений;

формулирует базовые криминалистические рекомендации по обнаружению, фиксации, изъятию, хранению и исследованию отдельных цифровых следов и носителей цифровой доказательственной информации;

называет проблемы, возникающие при использовании цифровых технических средств во время производства следственных действий;

перечисляет элементы алгоритмов расследования преступлений в сфере компьютерной информации и их последовательность;

изучает и оценивает эффективность методик экспертных компьютерно-технических исследований;

демонстрирует способность работы с большими данными и изучения функционального назначения программного обеспечения;

предлагает направления совершенствования цифровых технологий в следственной и судебно-экспертной деятельности.

Базовый уровень – обучающийся:

анализирует основные правила изъятия и хранения цифровой техники и носителей цифровой доказательственной информации;

анализирует алгоритм осмотра компьютерной техники;

анализирует алгоритм осмотра веб-сайта;

называет основные операторы поиска информации в сети интернет;

раскрывает порядок обращения к автоматизированным сервисам мониторинга сети интернет;

анализирует алгоритм осмотра смартфонов;

анализирует алгоритм осмотра содержимого облачных хранилищ;

раскрывает систему следственных ситуаций, при которых необходимым и обоснованным действием является назначение компьютерно-технических экспертиз;

воспроизводит порядок назначения компьютерно-технических экспертиз;

критически анализирует методики производства компьютерно-технических экспертиз;

раскрывает систему цифровых технических средств, используемых при производстве следственных действий;

анализирует ситуации и способы использования информационных систем и компьютерных сетей для обеспечения межведомственного взаимодействия правоохранительных органов;

анализирует способы оцифровки криминалистически значимых объектов и сведений;

систематизирует следственные ситуации, требующие изъятия или копирования цифровой доказательственной информации;

раскрывает следственные ситуации, в которых возможны факты выявления крипто- или стеганографических способов сокрытия цифровой доказательственной информации;

характеризует следственные ситуации, при которых необходимым является использование специальных знаний в области компьютерной техники, программного обеспечения или сетевых технологий;

анализирует направления и предлагает способы совершенствования цифровых инструментов следователя или судебного эксперта;

исследует информационные системы и компьютерные сети, используемые для обеспечения межведомственного взаимодействия правоохранительных органов;

исследует современное состояние компьютеризированных учётов, используемых при раскрытии и расследовании преступлений;

формулирует криминалистические рекомендации по обнаружению, фиксации, изъятию, хранению и исследованию отдельных цифровых следов и носителей цифровой доказательственной информации;

раскрывает проблемы, возникающие при использовании цифровых технических средств во время производства следственных действий;

анализирует алгоритмы расследования преступлений в сфере компьютерной информации;

изучает и оценивает эффективность методик экспертных компьютерно-технических исследований;

демонстрирует способность работы с большими данными и изучения функционального назначения программного обеспечения;

предлагает направления совершенствования цифровых технологий в следственной и судебно-экспертной деятельности.

Повышенный уровень – обучающийся:

критически анализирует правила изъятия и хранения цифровой техники и носителей цифровой доказательственной информации для различных следственных ситуациях;

критически анализирует алгоритм осмотра компьютерной техники;

критически анализирует алгоритм осмотра веб-сайта;

систематизирует основные операторы поиска информации в сети интернет;

раскрывает порядок обращения к автоматизированным сервисам мониторинга сети интернет;

критически анализирует алгоритм осмотра смартфонов;

критически анализирует алгоритм осмотра содержимого облачных хранилищ;

систематизирует следственные ситуации, при которых необходимым и обоснованным действием является назначение компьютерно-технических экспертиз;

алгоритмизирует процесс назначения компьютерно-технических экспертиз;

критически анализирует методики производства компьютерно-технических экспертиз;

классифицирует цифровые технические средства, используемые при производстве следственных действий;

анализирует ситуации и способы использования информационных систем и компьютерных сетей для обеспечения межведомственного взаимодействия правоохранительных органов;

формулирует новые способы оцифровки криминалистически значимых объектов и сведений;

систематизирует следственные ситуации, требующие изъятия или копирования цифровой доказательственной информации;

систематизирует следственные ситуации, в которых возможны факты выявления крипто- или стеганографических способов сокрытия цифровой доказательственной информации;

критически анализирует следственные ситуации, при которых необходимым является использование специальных знаний в области компьютерной техники, программного обеспечения или сетевых технологий;

анализирует направления и предлагает новые способы совершенствования цифровых

инструментов следователя или судебного эксперта;

критически исследует информационные системы и компьютерные сети, используемые для обеспечения межведомственного взаимодействия правоохранительных органов;

исследует современное состояние компьютеризированных учётов, используемых при раскрытии и расследовании преступлений на основе российского и зарубежного опыта;

формулирует криминалистические рекомендации по обнаружению, фиксации, изъятию, хранению и исследованию отдельных цифровых следов и носителей цифровой доказательственной информации;

анализирует проблемы, возникающие при использовании цифровых технических средств во время производства следственных действий;

анализирует алгоритмы расследования преступлений в сфере компьютерной информации;

изучает и оценивает эффективность методик экспертных компьютерно-технических исследований, предлагает модели повышения эффективности таких методик;

демонстрирует способность работы с большими данными и изучения функционального назначения программного обеспечения;

анализирует и предлагает направления совершенствования цифровых технологий в следственной и судебно-экспертной деятельности.

6. Фонд оценочных средств по дисциплине для промежуточной аттестации; критерии и процедуры оценивания результатов обучения по дисциплине.

При проведении промежуточной аттестации по дисциплине проверяется степень сформированности у обучающихся всех компетенций (полностью или в части), заявленных в п. 3 данной программы дисциплины.

Оценочные средства:

1. **Теоретические вопросы к зачёту:**
    1. Предмет и объект цифровой криминалистики
    2. Задачи и система цифровой криминалистики
    3. Цифровая информация: понятие и сущность
    4. Понятие и признаки цифровых следов преступлений
    5. Классификация цифровых следов
    6. Механизм следообразования цифровых следов
    7. Обнаружение и фиксация цифровых следов
    8. Изъятие и копирование цифровой информации
    9. Мониторинг сети интернет в следственной деятельности
    10. Осмотр смартфона
    11. Осмотр веб-сайта
    12. Осмотр компьютерной техники
    13. Осмотр содержимого облачных хранилищ
    14. Основные ошибки при работе с цифровыми следами и объектами
    15. Криминалистическая характеристика преступлений в сфере компьютерной информации
    16. Криминалистическая классификация преступлений в сфере компьютерной информации;
    17. Следственные ситуации при расследовании преступлений в сфере компьютерной информации
    18. Организация расследования преступлений в сфере компьютерной информации
    19. Понятие, задачи и направления компьютерно-технических исследований
    20. Назначение компьютерно-технической экспертизы
    21. Оценка заключения эксперта компьютерно-технической экспертизы
    22. Характеристика цифровых технико-криминалистических средств

23. Характеристика систем обеспечения межведомственного взаимодействия правоохранительных органов

24. Цифровые технологии в криминалистической регистрации

Критерии и процедуры оценивания результатов обучения по дисциплине. Описание шкал оценивания.

Промежуточная аттестация по дисциплине проходит в виде зачета в 3 семестре (5 семестре на заочной форме обучения).

Зачёт по результатам изучения дисциплины проходит в форме собеседования по экзаменационным вопросам.

Критерии оценок:

Оценка **«зачтено» выставляется при выполнении следующих минимальных критериев, согласно которым обучающийся:**

описывает предмет, объект, систему и задачи цифровой криминалистики;

проговаривает понятия цифровых следов, цифровой доказательственной информации, больших данных, преступлений в сфере компьютерной информации;

сравнивает отдельные подходы в определении понятия и сущности цифровых следов;

описывает механизм следообразования цифровых следов;

описывает принципиальную схему организации компьютерной техники;

перечисляет отдельные способы сокрытия, обнаружения, фиксации и изъятия цифровых следов и носителей цифровой доказательственной информации;

разграничивает случаи изъятия и копирования цифровой доказательственной информации;

перечисляет виды носителей цифровой информации;

описывает элементы криминалистической характеристики преступлений в сфере компьютерной информации;

называет основные ошибки, совершаемые при использовании цифровых технических средств в процессе расследования преступлений;

описывает основы функционирования и пополнения компьютеризированных учётов, используемых в раскрытии и расследовании преступлений;

показывает способность правильно квалифицировать факты, события и обстоятельства, связанные с компьютерными инцидентами, и изучать особенности их отражения в непроцессуальных и процессуальных документах;

использует корректный терминологический инструментарий областей компьютерной техники и сетевых технологий;

изучает факты применения в профессиональной деятельности следователя и судебного эксперта современных систем и средств электронного документооборота, информационно-телекоммуникационных технологий, информационных систем, в том числе федеральных/государственных;

демонстрирует способность осуществлять мануальный и полуавтоматический поиск в телекоммуникационных сетях;

исследует соблюдение в профессиональной деятельности следователя методик и рекомендаций по расследованию преступлений, связанных с использованием компьютерной информации;

перечисляет направления компьютерной-технических исследований;

демонстрирует знания основ нормативно-правовых актов в области информационной безопасности и защиты информации;

формулирует отдельные положения криминалистических рекомендаций, связанных с информационной безопасностью и защитой информации;

правил изъятия и хранения цифровой техники и носителей цифровой информации;

алгоритмов осмотра компьютерной техники;

алгоритмов осмотра веб-сайтов;

основных операторов поиска информации в сети интернет;

порядка обращения к автоматизированным сервисам мониторинга сети интернет;

алгоритмов осмотра смартфонов;

алгоритмов осмотра содержимого облачных хранилищ;

следственных ситуаций, при которых необходимым и обоснованным действием является назначение компьютерно-технических экспертиз;

порядка назначения компьютерно-технических экспертиз;

основ методики производства компьютерно-технических экспертиз;

основных цифровых технических средств, используемых при производстве следственных действий;

основ использования информационных систем и компьютерных сетей для обеспечения межведомственного взаимодействия правоохранительных органов;

основ оцифровки криминалистически значимых сведений и объектов.

Оценка «незачтено» выставляется при невыполнении заявленных выше минимальных критериев

7. Система оценивания по дисциплине:

Перечень тем/модулей, по которым проводится контрольное мероприятие	Форма и описание контрольного мероприятия	Критерии оценивания
Темы 1–3	Дискуссия организуется по следующей схеме: – обучающиеся выбирают категорию цифровых объектов криминалистического познания – обучающиеся описывают понятие, систему, подходы к криминалистическому изучению выбранного объекта, – проверка преподавателем понимания представленных позиций – критика преподавателем аргументации по проблемным моментам – оценка научной и практической значимости позиции обучающегося	**Выполнено** **Знания:** предмета, объекта, системы и задач цифровой криминалистики; понятия, сущности, принципов формирования цифровой доказательственной информации; понятия и признаков цифровых следов; механизма следообразования цифровых следов; способов сокрытия и обнаружения цифровых следов; способов фиксации цифровых следов; способов изъятия и копирования цифровых следов; понятия больших данных и основных компьютерно-технических особенностей их получения и обработки; принципиальной схемы организации компьютерной техники; классификационных видов носителей цифровой информации; общих положений использования телекоммуникационных сетей в раскрытии и расследовании преступлений; понятия и классификации преступлений в сфере компьютерной информации; криминалистической характеристики преступлений в сфере компьютерной информации; понятия, задач и объектов компьютерной-технических экспертиз; классификации компьютерно-технических экспертиз; основных ошибок, совершаемых при использовании цифровых технических средств; программного обеспечения, составляющего АРМ следователя; основ функционирования и пополнения компьютеризированных учётов, используемых в раскрытии и расследовании преступлений; основного терминологического инструментария из областей компьютерной техники и сетевых технологий;

		требований нормативно-правовых актов в области информационной безопасности и защиты информации; правил изъятия и хранения цифровой техники и носителей цифровой информации; алгоритмов осмотра компьютерной техники; алгоритмов осмотра веб-сайтов; основных операторов поиска информации в сети интернет; порядка обращения к автоматизированным сервисам мониторинга сети интернет; алгоритмов осмотра смартфонов; алгоритмов осмотра содержимого облачных хранилищ; следственных ситуаций, при которых необходимым и обоснованным действием является назначение компьютерно-технических экспертиз; порядка назначения компьютерно-технических экспертиз; основ методики производства компьютерно-технических экспертиз. **Умения:** определять типовые цифровые следы и их носители при анализе следственных ситуаций; описывать механизм следообразования цифровых следов в различных криминальных ситуациях; классифицировать цифровые следы и носители цифровой доказательственной информации; классифицировать способы сокрытия цифровых следов; сравнивать различные подходы к научному определению понятия цифровых следов; сравнивать различные подходы к научным определениям больших данных; сопоставлять элементы криминалистической характеристики преступлений в сфере компьютерной информации; классифицировать направления компьютерно-технических исследований; использовать корректную терминологию при описании цифровых криминалистически значимых объектов; разграничивать следственные ситуации, требующие изъятия или копирования цифровой доказательственной информации; выделять следственные ситуации, в которых возможны факты выявления крипто- или стеганографических способов сокрытия цифровой доказательственной информации; **Навыки:**

		юридически правильно квалифицировать факты, события и обстоятельства, связанные с компьютерными инцидентами, и изучать особенности их отражения в непроцессуальных и процессуальных документах; оценивать корректность применения специальных знаний при проведении служебных и иных документальных проверок по фактам совершения компьютерных инцидентов; выявлять и анализировать следственные ошибки при работе с цифровыми объектами; предлагать способы выявления фактов сокрытия цифровых следов; осуществлять мануальный и полуавтоматический поиск в телекоммуникационных сетях; исследовать соблюдение в профессиональной деятельности следователя методик и рекомендаций по расследованию преступлений, связанных с использованием компьютерной информации; работать с большими объёмами цифровой информации; адаптировать требования нормативно-правовых актов в области информационной безопасности и защиты информации в криминалистические рекомендации; формулировать криминалистические рекомендации по обнаружению, фиксации, изъятию, хранению и исследованию отдельных цифровых следов и носителей цифровой доказательственной информации. При несоблюдении указанных выше критериев мероприятие выставляется оценка «не выполнено».
Темы 4–12	Дискуссия организуется по следующей схеме: – обучающиеся выбирают цифровую технологию, используемую в процессе – обучающиеся приводят типовые следственные ситуации, перечень следственных действий и основных тактических приёмов – проверка преподавателем понимания представленных позиций – критика преподавателем	**Выполнено** **Знания:** основных цифровых технических средств, используемых при производстве следственных действий; основ использования информационных систем и компьютерных сетей для обеспечения межведомственного взаимодействия правоохранительных органов; основ оцифровки криминалистически значимых сведений и объектов; **Умения:** изучать направления совершенствования цифровых инструментов следователя или судебного эксперта; исследовать информационные системы и компьютерные сети, используемые для

	аргументации по проблемным моментам – оценка научной и практической значимости позиции обучающегося	обеспечения межведомственного взаимодействия правоохранительных органов; исследовать современное состояние компьютеризированных учётов, используемых при раскрытии и расследовании преступлений; изучать направления совершенствования цифровых инструментов следователя или судебного эксперта; исследовать информационные системы и компьютерные сети, используемые для обеспечения межведомственного взаимодействия правоохранительных органов; исследовать современное состояние компьютеризированных учётов, используемых при раскрытии и расследовании преступлений. **Навыки:** изучать факты применения в профессиональной деятельности следователя и судебного эксперта современных систем и средств электронного документооборота, информационно-телекоммуникационных технологий, информационных систем, в том числе федеральных/государственных; изучать большие данные и функциональное назначение программного обеспечения; предлагать направления совершенствования цифровых технологий в следственной и судебно-экспертной деятельности; предлагать способы преобразования цифровых объектов в традиционные и в обратном направлении. При несоблюдении указанных выше критериев мероприятие выставляется оценка «не выполнено».

8. Методические указания для обучающихся по освоению дисциплины:

Работа по подготовке к практическим занятиям и активное в них участие - одна из форм изучения дисциплины. Целью проведения практических занятий является выработка у аспирантов практических навыков применения криминалистических рекомендаций, представления о современных достижениях в криминалистической науке. Практические занятия проводятся в активных формах, предполагающих обсуждение практических ситуаций, подготовленных преподавателем, а также в интерактивных формах (работа в малых группах, разбор конкретных ситуаций др.).

Кроме изучения теоретических вопросов, указанных в программе, аспирант должен выполнять к каждому занятию изучать правоприменительную и криминалистическую практику по конкретным вопросам.

Подготовка к практическому занятию включает 2 этапа:

1й – организационный;

2й - закрепление и углубление теоретических знаний.

На первом этапе аспирант планирует свою самостоятельную работу, которая включает:

- уяснение задания на самостоятельную работу;
- подбор рекомендованной литературы и методических материалов;
- составление плана работы, в котором определяются основные пункты предстоящей подготовки.

Второй этап включает непосредственную подготовку аспиранта к занятию. Необходимо помнить, что на занятии обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой и методическими рекомендациями обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. При необходимости следует обращаться за консультацией к преподавателю.

На практическом занятии каждый его участник должен быть готовым к выступлению по всем поставленным вопросам темы, проявлять максимальную активность при их рассмотрении. Выступление должно строиться свободно, убедительно и аргументировано. Необходимо, чтобы выступающий проявлял собственное отношение к тому, о чем он говорит, высказывал свое личное мнение, понимание, обосновывал его и мог сделать правильные выводы из сказанного. Необходимо в подтверждение сказанного приводить мнения ученых, анализировать подходы различных научных школ, указывать на развитие теории конституционного права по конкретной тематике и анализировать развитие практики правоприменения, акцентируя проблемные для теории и практики моменты.

При изучении дисциплины самостоятельная работа аспирантов является главным методом освоения дисциплины. Она предполагает на основе знаний, полученных в ходе практических занятий, изучение учебной и научной литературы, действующего законодательства, следственной и судебной и иной практики, статистических показателей зарубежных стран.

Подготовка к запланированным дискуссиям и круглым столам должна состоять в подборе необходимой учебной, научной литературе, нормативных материалов и изучении практики по тематике, выносимой на данное мероприятие. Аспирант подготавливает краткие выступления по тематике мероприятия, в которых дает обзор научных подходов к проблематике, свое видение решения конкретных проблем и обоснование такого решения. Должен уметь отстаивать свою позицию, аргументировано и корректно отвечая на вопросы коллег и преподавателя и уметь задавать вопросы другим выступающим.

9. Учебно-методическое и информационное обеспечение дисциплины.

Обязательная литература:

9.2.1. Учебная литература:

1. Цифровая криминалистика: учебник для бакалавриата, специалитета и магистратуры / под редакцией В. Б. Вехова; С. В. Зуева. М.: Издательство Юрайт, 2021. 417 с.
2. Электронные доказательства в уголовном судопроизводстве : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственный редактор С. В. Зуев. М.: Издательство Юрайт, 2020. — 193 с.
3. Информационные технологии в уголовном процессе зарубежных стран // Под ред. С.В. Зуева, М. Юрлитинформ, 2020.
4. Основы теории электронных доказательств // Под ред. С.В. Зуева, М. Юрлитинформ, 2019.
5. Электронные носители информации в криминалистике// Под ред. О. С. Кучина, М.

Юрлитинформ, 2017.

9.2.2. Официальные издания:

1) Вестник Конституционного Суда Российской Федерации [Электронный ресурс]// Режим доступа: http://vestnik.ksrf.ru/

2) Бюллетень Верховного суда Российской Федерации [Электронный ресурс] // Режим доступа: http://www.supcourt.ru/documents/newsletters/?year=2017

9.2.3. Справочно-библиографические издания

1) Экспертиза [Электронный ресурс] : юрид. слов.-справ. / под ред. А. В. Малько. – Москва : Проспект, 2018. – (Юридические словари России). – Доступ с сайта электрон.-библ. системы изд-ва «Проспект». – URL: http://ebs.prospekt.org/book/38659/page/1 .

2) Словарь по криминалистике. 1250 терминов и определений [Электронный ресурс] / под ред. А. И. Бастрыкина. – Москва : ЮНИТИ-ДАНА, 2017. – Доступ с сайта электрон.-библ. системы «Ipr Books». – URL: http://www.iprbookshop.ru/72434.html .

9.2.4. Специализированные периодические издания:

1) Наука. Общество. Государство [Электронный ресурс] : электрон. науч. журн. – Пенза : Пенз. гос. ун-т, 2013-2016; 2017, № 1-4; 2018, № 1-2. – Доступ с сайта электрон.-библ. системы изд-ва «Лань». – URL: https://e.lanbook.com/journal/2689#journal_name .

2) Пробелы в российском законодательстве [Электронный ресурс]. – Москва : Юр-ВАК, 2012-2016; 2017, № 1-7; 2018, № 1-3. – Доступ с сайта электрон.-библ. системы изд-ва «Лань». – URL: https://e.lanbook.com/journal/2105#journal_name .

3) Юридическая наука и практика: Вестник Нижегородской академии МВД России [Электронный ресурс]. – Нижний Новгород : Нижегор. акад. М-ва внутрен. дел Рос. Федерации, 2013-2017; 2017, № 1-4; 2018, № 1-2. – Доступ с сайта электрон.-библ. системы изд-ва «Лань». – URL: https://e.lanbook.com/journal/2581#journal_name.

Нормативно-правовые и правоприменительные акты:

1. Конституция Российской Федерации;
2. Федеральный закон «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ. СЗ РФ от 17 июня 1996 г. № 25 ст. 2954. (ред. от 19.02.2018).
3. Федеральный закон «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ. СЗ РФ от 24 декабря 2001, № 52 (ч. 1) (в ред. от 19.02.2018).
4. Федеральный закон от 31 мая 2001г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации».
5. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. ГОСТ Р 57429-2017 «Судебная компьютерно-техническая экспертиза. Термины и определения».

Современные профессиональные базы данных:

1. Центральная база статистических данных (ЦБСД) - официальный сайт Федеральной службы государственной статистики - www.gks.ru;
2. Единая межведомственная информационно – статистическая система (ЕМИСС) - официальный сайт Федеральной службы государственной статистики - www.gks.ru;
3. База данных показателей муниципальных образований - официальный сайт Федеральной службы государственной статистики - www.gks.ru;
4. Сведения о государственной регистрации юридических лиц, индивидуальных предпринимателей, крестьянских (фермерских) хозяйств - https://egrul.nalog.ru/
5. Государственная автоматизированная система Российской Федерации «Правосудие» - https://bsr.sudrf.ru/bigs/portal.html
6. Банк решений арбитражных судов - https://ras.arbitr.ru/
7. Правовые акты Федеральной антимонопольной службы - https://solutions.fas.gov.ru/
8. Банк решений Конституционного Суда Российской Федерации - http://www.ksrf.ru/ru/Decision/Pages/default.aspx
9. Государственная система правовой информации– www.pravo.gov.ru;

Международные реферативные базы данных научных изданий

1. Политематическая реферативно-библиографическая и наукометрическая (библиометрическая) база данных Web of Science - https://www.usla.ru/science/uniims/spravochnye-materialy.php
2. Единая реферативная база данных Scopus - https://www.usla.ru/science/uniims/spravochnye-materialy.php

Информационные справочные и поисковые системы:

1. Информационно-правовой портал «Гарант» - www.garant.ru;
2. Справочная правовая система «КонсультантПлюс» - www.consultant.ru;
3. Информационно-правовая система «Кодекс» - www.kodeks.ru.
4. CrimLib.info – Энциклопедия криминалистики и уголовного процесса [Электронный ресурс] – URL: https://crimlib.info.

Электронно-библиотечные системы:

1. Электронно-библиотечная система ZNANIUM.COM - znanium.com;
2. Электронно-библиотечная система «Лань» - e.lanbook.com;
3. Электронно-библиотечная система «Юрайт» - www.biblio-online.ru;
4. Электронно-библиотечная система BOOK.ru - www.book.ru;
5. Электронно-библиотечная система «IPR-books» - www.iprbookshop.ru;
6. Электронно-библиотечная система «Проспект» - ebs.prospekt.org

Комплект лицензионного программного обеспечения:

1. Libre Office;
2. Microsoft Windows 7 Профессиональная;
3. Microsoft Office Professional Plus 2010
4. НЭБ РФ, версия 1.0.15 – Национальная электронная библиотека;
5. Kaspersky Endpoint Security 10 для Windows;
6. Справочная Правовая Система «КонсультантПлюс»;
7. Информационно-справочная система «Кодекс»;
8. Информационно-правовая система «Законодательство стран СНГ»;
9. Справочная правовая система «ГАРАНТ».

10. Материально-техническое обеспечение дисциплины.

Учебные аудитории для проведения занятий лекционного типа, укомплектованные специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: рабочие места для обучающихся, рабочее место преподавателя, кафедра с сенсорным экраном и компьютером, экран проекционный, проектор, доска магнитно-меловая.

Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническим средствами обучения, служащими для представления учебной информации большой аудитории: рабочее место преподавателя, рабочие места для обучающихся, доска магнитно-меловая.

Помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.