

УТВЕРЖДАЮ

Проректор по учебной работе

О.В. Щербаковой

«26» июня 2025 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Противодействие киберпреступности
Кафедра	Кафедра криминалистики
Год набора	2025

Направление подготовки (специальность) Судебная и прокурорская деятельность
код направления (специальности), полное наименование

Направленность (профиль подготовки/специализация) Прокурорская деятельность
полное наименование

Квалификация: Юрист

Форма обучения: очная, заочная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Программа актуализирована на заседании кафедры: протокол № _____ от 20 г.

Программа актуализирована на заседании кафедры: протокол № _____ от 20 г.

Программа актуализирована на заседании кафедры: протокол № _____ от 20 г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Смушкин Александр Борисович	Кафедра криминалистики	доцент (к/н, доцент),

СОГЛАСОВАНО		СОГЛАСОВАНО	
Заведующий кафедрой криминалистики		И.о. начальника отдела контроля качества образования	
Л.Г. Шапиро <i>ФИО</i>	« 27 » мая 2025 г.	В. А. Неясова <i>ФИО</i>	« 20 » июня 2025 г.

ОДОБРЕНО	
Учебно-методическим советом	
от « 24 » июня 2025 г., протокол №12	

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины: ознакомить с основными понятиями и методами противодействия киберпреступности; получить компетенции, направленные на обеспечение кибербезопасности и противодействие киберпреступности; обеспечить теоретическую и практическую подготовку специалистов к деятельности, связанной с противодействием киберпреступности на различных уровнях

Задачи освоения дисциплины:

- формирование представлений о целях и методах кибербезопасности;
- ознакомление обучающихся с историческими аспектами становления уголовной ответственности за компьютерные преступления,
- структурирование имеющихся и получение новых знаний по вопросам борьбы с киберпреступностью;
- закрепление имеющихся и формирование новых умений и навыков, необходимых для борьбы с киберпреступностью
- формирование навыков работы с юридической, экономической и иной информацией, относящейся к противодействию киберпреступности;
- формирование навыков использования стратегий, техник и методов противодействия киберпреступности в профессиональной деятельности;

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Противодействие киберпреступности» относится к части учебного плана, формируемой участниками образовательных отношений (элективные дисциплины)

Изучение данной дисциплины базируется на знаниях, умениях и навыках, полученных при изучении следующих дисциплин:

- Информационное право;
- Криминалистика;
- Криминология;
- Правоохранительные органы;
- Уголовное право (особенная часть);
- Уголовное право (общая часть);
- Уголовный процесс;
- Основы оперативно-розыскной деятельности;
- Информационные технологии в профессиональной деятельности.

Основные положения дисциплины могут быть использованы в дальнейшем при изучении следующих дисциплин:

- Подготовка к сдаче и сдача государственного экзамена;
- Подготовка к процедуре защиты и защита выпускной квалификационной работы.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ п/п	Код по ФГОС	Компетенция	Код и наименование индикатора достижения компетенции	Приобретаемые знания, умения, навыки
1	ОПК-9	Способен получать юридически значимую информацию из	ОПК-9.1 Определяет правовые основы в сфере обеспечения информационной	Знать: особенности работы со справочно-правовыми системами; способы сбора

		<p>различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационно-коммуникационных технологий с учетом требований информационной безопасности</p>	<p>безопасности; источники, включая правовые базы данных, содержащие юридически значимую информацию ОПК-9.2 Ориентируется в информационном пространстве; применяет информационные технологии, современные цифровые устройства и платформы для решения конкретных задач профессиональной деятельности, проводит статический анализ информации ОПК-9.3 Работает с информационными объектами и сетью Интернет для решения профессиональных задач с учетом требований информационной безопасности</p>	<p>и обработки правовой информации в сети Интернет и иных источниках.</p> <p>Уметь: использовать средства современных информационных технологий в праве, соблюдая меры информационной безопасности и используя возможности антивирусных программ.</p> <p>Владеть: способностью целенаправленно и эффективно собирать сведения, содержащие юридически значимые обстоятельства, из правовых баз и других источников; способностью решать профессиональные задачи с использованием информационных цифровых технологий</p>
2	ПКС-1	<p>Способен к выполнению должностных обязанностей по обеспечению верховенства закона, единства и укрепления законности, защите прав и свобод человека и гражданина, охраняемых законом интересов общества и государства</p>	<p>Способен к выполнению должностных обязанностей по обеспечению верховенства закона, единства и укрепления законности, защите прав и свобод человека и гражданина, охраняемых законом интересов общества и государства</p>	<p>Знать: основные отрасли права; способы обеспечения законности, правопорядка, безопасности личности, общества и государства; систему и специфику правоохранительных и судебных органов; составы преступлений и иных правонарушений;</p> <p>Уметь: толковать и применять нормативные правовые акты с точки зрения законности и правопорядка; анализировать и давать</p>

			оценку социальной значимости правовых явлений и процессов с точки зрения законности и правопорядка, безопасности личности, общества и государства; Владеть: навыками анализа и разрешения правовых проблем и коллизий при выполнении должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства
--	--	--	--

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 3 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах)

Вид учебной работы	Количество часов (форма обучения: <u>Очная</u>)	
	Всего по плану	В т.ч. по семестрам
		9
Контактная работа обучающихся с преподавателем в соответствии с УП (аудиторные занятия)	38	38
Лекции	20	20
Семинарские занятия	18	18
Занятия в форме практической подготовки	4	4
Самостоятельная работа	70	70
Виды промежуточной аттестации	Зачет	Зачет
Всего часов по дисциплине	108	108

Вид учебной работы	Количество часов (форма обучения: <u>Заочная</u>)	
	Всего по плану	В т.ч. по семестрам
		10
Контактная работа обучающихся с преподавателем в соответствии с УП (аудиторные занятия)	6	6
Лекции	2	2
Семинарские занятия	4	4
Занятия в форме практической подготовки	2	2
Самостоятельная работа	98	98
Контроль	4	4
Виды промежуточной аттестации	Зачет	
Всего часов по дисциплине	108	108

Примечание:

Объем практической подготовки при проведении учебных занятий в рамках учебных дисциплин (модулей), связанных с будущей профессиональной деятельностью, как правило, должен составлять не менее 10 % от всего объема контактной работы.

5. СТРУКТУРА УЧЕБНОЙ ДИСЦИПЛИНЫ. РАСПРЕДЕЛЕНИЕ ЧАСОВ ПО ТЕМАМ И ВИДАМ УЧЕБНОЙ РАБОТЫ

5.1. Форма обучения Очная

Название разделов и тем	Общее кол-во часов	Виды учебных занятий				Самостоятельная работа	Форма контроля / наименование оценочного средства	Код индикатора достижения компетенции
		Контактная работа обучающихся с преподавателем (аудиторные занятия)						
		Всего	Лекции	Семинары	Занятия в форме практической подготовки			
Раздел 1. Общие вопросы противодействия киберпреступности								
1. Понятие киберпреступности и кибербезопасности. История развития киберпреступности в России	11	4	2	2	0	7	теоретический опрос	ОПК-9.1
2. Международные основы противодействия киберпреступности	11	4	2	2	0	7	теоретический опрос	ОПК-9.2
3. Цифровизация следственной деятельности в области противодействия киберпреступности. Цифровая криминалистика	11	4	2	2	0	7	теоретический опрос, формирование конкретных ситуаций (кейс-метод)	ОПК-9.1; ОПК-9.3
4. Основы криминалистического исследования цифровой информации	10	3	2	1	0	7	теоретический опрос, формирование конкретных ситуаций	ОПК-9.2; ОПК-9.3

							х ситуаций (кейс- метод)	
Раздел 2. Отдельные аспекты противодействия киберпреступности								
5. Виртуальные следы: понятие, виды и использование в раскрытии и расследовании преступлений	9	2	1	1	2	7	теоретический опрос, формирование конкретных ситуаций (кейс-метод)	ОПК-9.3
6. Исследование отдельных носителей информации и информационных объектов	12	5	3	2	0	7	теоретический опрос	ОПК-9.3
7. Расследование компьютерных преступлений, предусмотренных главой 28 УК РФ	11	4	2	2	2	7	теоретический опрос	ОПК-9.1
8. Особенности расследования преступлений в сфере мобильных телекоммуникаций	11	4	2	2	0	7	теоретический опрос	ОПК-9.2
9. Основы расследования хищений, совершенных с использованием компьютерных устройств.	11	4	2	2	0	7	теоретический опрос	ОПК-9.2
10. Расследование некоторых иных преступлений, совершаемых с	11	4	2	2	0	7	теоретический опрос	ОПК-9.3

использование компьютерных устройств								
Всего	108	38	20	18	4	70	Зачет	ОПК-9.1; ОПК-9.2; ОПК-9.3

5.2. Форма обучения Заочная

Название разделов и тем	Общее кол-во часов	Виды учебных занятий				Самостоятельная работа	Форма контроля / наименование оценочного средства	Код индикатора достижения компетенции
		Контактная работа обучающихся с преподавателем (аудиторные занятия)						
		Всего	Лекции	Семинары	Занятия в форме практической подготовки			
Раздел 1. Общие вопросы противодействия киберпреступности								
1. Понятие киберпреступности и кибербезопасности. История развития киберпреступности в России	14	2	1	1	0	12	теоретический опрос	ОПК-9.1
2. Международные основы противодействия киберпреступности	12	0	0	0	0	12	теоретический опрос	ОПК-9.2
3. Цифровизация следственной деятельности в области противодействия киберпреступности. Цифровая криминалистика	12	0	0	0	0	12	теоретический опрос, формирование конкретных ситуаций (кейс-метод)	ОПК-9.1; ОПК-9.3
4. Основы криминалистического исследования цифровой информации	12	0	0	0	0	12	теоретический опрос, формирование конкретных ситуаций	ОПК-9.2; ОПК-9.3

							х ситуаций (кейс- метод)	
Раздел 2. Отдельные аспекты противодействия киберпреступности								
5. Виртуальные следы: понятие, виды и использование в раскрытии и расследовании преступлений	13	1	0	1	0	12	теоретический опрос, формирование конкретных ситуаций (кейс-метод)	ОПК-9.3
6. Исследование отдельных носителей информации и информационных объектов	8	2	1	1	2	6	теоретический опрос	ОПК-9.3
7. Расследование компьютерных преступлений, предусмотренных главой 28 УК РФ	13	1	0	1	0	12	теоретический опрос	ОПК-9.1
8. Особенности расследования преступлений в сфере мобильных телекоммуникаций	6	0	0	0	0	6	теоретический опрос	ОПК-9.2
9. Основы расследования хищений, совершенных с использованием компьютерных устройств.	6	0	0	0	0	6	теоретический опрос	ОПК-9.2
10. Расследование некоторых иных преступлений, совершаемых с	8	0	0	0	0	8	теоретический опрос, итоговое тестирование	ОПК-9.3

ИСПОЛЬЗОВАНИЕ М КОМПЬЮТЕРНЫХ УСТРОЙСТВ								
Всего	104	6	2	4	2	98	Зачет(4)	ОПК-9.1; ОПК-9.2; ОПК-9.3

Примечание:

При организации ускоренного обучения по индивидуальному учебному плану для обучающихся, имеющих среднее профессиональное или высшее образование различных уровней, количество часов (аудиторная контактная работа), отведенных для изучения учебных дисциплин соответствующего профиля отражено в индивидуальном учебном плане (для обучающегося или группы обучающихся) с учетом особенностей и образовательных потребностей конкретного обучающегося.

Количество часов (аудиторная контактная работа), отведенных для изучения данной учебной дисциплины, тематический план дисциплины для обучающихся, имеющих среднее профессиональное или высшее образование различных уровней с учетом особенностей и образовательных потребностей конкретного обучающегося определяется ежегодно заведующим кафедрой и утверждается в начале учебного года на заседании кафедры приложением к протоколу заседания кафедры.

6. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Общие вопросы противодействия киберпреступности

Тема 1. Понятие киберпреступности и кибербезопасности. История развития киберпреступности в России

Лекция:

1. Понятие кибербезопасности и основные составляющие данной категории
2. Понятие "киберпреступность". Связь с категорией "Компьютерная преступность"
3. Наиболее распространенные преступления, совершаемые с использованием компьютерной техники: хакерство, компьютерное мошенничество, распространение вредоносных программ, компьютерное пиратство.
4. Правовые основания противодействия киберпреступности

Семинарское занятие:

1. Кибербезопасность как правовая и криминалистическая категория
2. Понятие киберпреступности.
3. Основные определения термина «киберпреступность» в правовой науке современной России.
4. Киберпреступность и компьютерные преступления — вопросы соотношения терминов.
5. Классификация киберпреступлений

Самостоятельная работа обучающихся:

1. История развития киберпреступности
2. Основные определения понятия «киберпреступность» в правовой науке иностранных государств.
3. государственная политика в области противодействия киберпреступности

Контрольные вопросы:

1. Возникновение и развитие киберпреступности в ССР и РФ
2. Нормативно-правовые акты и стандарты по основам кибербезопасности.
3. Цели и задачи уголовной политики в сфере противодействия компьютерной преступности.

Тема 2. Международные основы противодействия киберпреступности

Лекция:

1. Hi-Tech Crime Trends 2020/2021 как источник стратегической информации о глобальном ландшафте киберугроз и прогнозах их развития.
2. Международные масштабы киберпреступности.
3. Международное сотрудничество в целях противодействия киберпреступности.
4. Деятельность Интерпола, Европола в борьбе с киберпреступностью.
5. Конвенция о киберпреступности (Будапешт, 2001 г.) и дополнительный протокол к ней

Семинарское занятие:

1. Международный характер киберпреступности
2. Роль Интерпола и Европола в противодействии киберпреступности
3. Информационное обеспечение международного розыска лиц.
4. Конвенция о киберпреступности (Будапешт, 2001 г.)
5. Международные стандарты кибербезопасности

Самостоятельная работа обучающихся:

1. Международный характер явления: причины и дальнейшее развитие.
2. Истоки современных видов киберпреступлений.
3. Международные масштабы киберпреступности.
4. Международное сотрудничество в целях противодействия киберпреступности.

Контрольные вопросы:

1. Основные международные конвенции по противодействию киберпреступности
2. Статистика международных киберпреступлений
3. Интерпол, Европол и другие международные организации в сфере противодействия киберпреступности

Тема 3. Цифровизация следственной деятельности в области противодействия киберпреступности. Цифровая криминалистика

Лекция:

1. Основные категории цифровой трансформации следственной деятельности
2. Понятие цифровой криминалистики..
3. Объект, предмет, цели и задачи цифровой криминалистики
4. Система цифровой криминалистики

Семинарское занятие:

1. Автоматизация, алгоритмизация, компьютеризация, оцифровка и цифровизация расследования
2. Этические основы цифровизации криминалистической деятельности
3. Цифровая трансформация расследования.. Принципы цифровой трансформации расследования
4. Понятие цифровой криминалистики.
5. Объект, предмет, цели и задачи цифровой криминалистики;
6. Методы цифровой криминалистики
7. Система цифровой криминалистики
8. Правовые основы использования информационных технологий в расследовании преступлений

Самостоятельная работа обучающихся:

1. История формирования частной теории электронной цифровой криминалистики (отечественный и зарубежный опыт).
2. Основные подходы к рассматриваемой частной теории
3. Закономерности, изучаемые электронной цифровой криминалистикой
4. Методология частной теории электронной цифровой криминалистики
5. Отечественное, международное и иностранное регулирование рассматриваемых вопросов

Контрольные вопросы:

Что такое цифровизация криминалистической деятельности
Какие взгляды на цифровизацию высказывались в науке
Связь цифровизации с компьютеризацией, оцифровкой, алгоритмизацией
Цифровая трансформация как развитие цифровизации
5. Содержание цифровой трансформации
Что понимается в России и за рубежом под категорией «Форензика»?
Взаимосвязь терминов «электронный», «компьютерный» и «цифровой»
Место частной теории в структуре криминалистического знания ?
Применение достижений цифровой криминалистики к иным видам судопроизводства, корпоративной безопасности и иным видам деятельности

Тема 4. Основы криминалистического исследования цифровой информации

Лекция:

Понятие и виды информации
Основные характеристики информации
Классификация информации
Специфика цифровой информации
Виды цифровой информации
Защита информации

Семинарское занятие:

1. Понятие и виды информации
2. Цифровая информация и аналоговая информация
3. Содержание и виды цифровой информации
3. Способы защиты и сокрытия цифровой информации

Самостоятельная работа обучающихся:

Основные подходы к категории «Информация»
Понятие и виды электронной цифровой информации
Криптография,
Стеганография
Основные угрозы компьютерной информации

Контрольные вопросы:

Виды и содержание криминалистических задач, решаемых с помощью цифровых технологий
Отличия цифровой информации от аналоговой
Основные способы сокрытия содержания информации

Раздел 2. Отдельные аспекты противодействия киберпреступности

Тема 5. Виртуальные следы: понятие, виды и использование в раскрытии и расследовании преступлений

Лекция:

1. Понятие и значение виртуальных следов преступлений
2. Современное состояние, тенденции и перспективы развития учения о виртуальных следах.
3. Классификация электронных- цифровых следов и их возможности в доказывании по уголовным делам и в ходе процессуальных проверок.

Семинарское занятие:

1. Основы поиска цифровых улик в различных операционных системах
2. Понятие и виды виртуальных следов
3. Места расположения виртуальных следов
4. Основы поиска виртуальных следов

Самостоятельная работа обучающихся:

1. Виртуальные следы преступлений

2. Дорожка электронных цифровых следов
3. Применения специальных знаний при поиске следов

Контрольные вопросы:

1. История развития концепции виртуальных следов
2. Основы поиска виртуальных следов
- 3 виртуальные следы в Raid-массивах
4. виртуальные следы распределенной информации

Тема 6. Исследование отдельных носителей информации и информационных объектов

Лекция:

1. Криминалистическое исследование компьютерных устройств
2. Сетевые криминалистические исследования
3. Криминалистическое исследование распределенной информации
4. Криминалистическое исследование мобильных устройств
5. Осмотр и исследование иных информационных объектов

Семинарское занятие:

1. Основы поиска цифровых улик в различных операционных системах
2. Осмотр компьютера, снятие дампа памяти
3. Сетевая криминалистика. Понятие, элементы
4. Использование информации об особенностях построения инфраструктуры компьютерной сети в криминалистических целях
5. Беспроводные сети. Криминалистическое исследование и использование
6. Криминалистическое исследование торрент-трекеров
7. Криминалистическое исследование блокчейна
8. Криминалистическое исследование иных сервисов (пиринговых сетей и т.д.)
9. Основы исследования мобильных телефонов
10. Понятие и основные элементы концепции «Интернета вещей».
11. Криминалистическое исследование и использование «Интернета вещей»

Самостоятельная работа обучающихся:

1. Основы поиска цифровых улик в различных операционных системах
2. Осмотр компьютера, снятие дампа памяти
3. Сетевая криминалистика. Понятие, элементы
4. Использование информации об особенностях построения инфраструктуры компьютерной сети в криминалистических целях
5. Беспроводные сети. Криминалистическое исследование и использование
6. Криминалистическое исследование торрент-трекеров
7. Криминалистическое исследование блокчейна
8. Криминалистическое исследование иных сервисов (пиринговых сетей и т.д.)
9. Основы исследования мобильных телефонов
10. Понятие и основные элементы концепции «Интернета вещей».
11. Криминалистическое исследование и использование «Интернета вещей»

Контрольные вопросы:

1. История компьютерной криминалистики
2. Основные варианты инфраструктуры сети
3. Беспроводные сетевые технологии, их исследование и использование
4. Понятие сервисов распределенного хранения данных
5. Технология блокчейн.
6. Пиринговые сети
7. Облачные сервисы и их исследование
8. Понятие и виды криминалистического исследования мобильных устройств
9. Виды мобильных телефонов. Стандарты сотовой связи. Основные операционные системы смартфонов и планшетных компьютеров

10. Осмотр мобильного телефона и планшета
11. Основные виды носимых «гаджетов» и их исследование.
12. Извлечение криминалистически значимой информации из электронных систем автомобилей
13. Умные вещи и их криминалистическое исследование.
14. Исследование электронных ключей и пропусков
15. Исследование электронных платежных карт

Тема 7. Расследование компьютерных преступлений, предусмотренных главой 28 УК РФ

Лекция:

1. Общая характеристика компьютерных преступлений
2. Организация расследования компьютерных преступлений
3. Тактика отдельных следственных действий при расследовании компьютерных преступлений

Семинарское занятие:

1. криминалистическая характеристика компьютерных преступлений
2. Основные версии при расследовании компьютерных преступлений
3. Планирование расследования в различных следственных ситуациях
4. Первоначальный этап расследования компьютерных преступлений
5. Особенности осмотра компьютерных устройств
6. Последующий этап расследования

Самостоятельная работа обучающихся:

1. Расследование неправомерного доступа к компьютерной информации
2. Расследование создания, использования и распространения вредоносных программ
3. Расследование посягательств на критическую информационную инфраструктуру
4. Расследование нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Контрольные вопросы:

1. Основные типы хакеров
2. Основные мотивы совершения компьютерных преступлений
3. Осмотр компьютерного устройства

Тема 8. Особенности расследования преступлений в сфере мобильных телекоммуникаций

Лекция:

1. Общая характеристика преступлений в сфере мобильных телекоммуникаций
2. Типичные следственные ситуации при расследовании преступлений в сфере мобильных телекоммуникаций. Привлечение специалистов
3. Первоначальный этап расследования
4. Последующий этап расследования

Семинарское занятие:

1. Общая характеристика преступлений в сфере мобильных телекоммуникаций
2. Типичные следственные ситуации при расследовании преступлений в сфере мобильных телекоммуникаций. Привлечение специалистов
3. Первоначальный этап расследования
4. Последующий этап расследования

Самостоятельная работа обучающихся:

1. Понятие и классификация преступлений в сфере мобильных телекоммуникаций
2. Криминалистическая характеристика преступлений в сфере мобильных телекоммуникаций
3. Организация расследования преступлений в сфере мобильных телекоммуникаций

4. Использование специальных знаний

5. Тактика отдельных следственных действий на первоначальном и последующем этапах

Контрольные вопросы:

1. Какие преступления могут быть совершены в сфере мобильных телекоммуникаций

2. Специалисты, привлекаемые к расследованию

3. Назначение экспертиз

4. Тактика иных следственных действий

Тема 9. Основы расследования хищений, совершенных с использованием компьютерных устройств.

Лекция:

1. Общая характеристика хищений, совершенных с использованием компьютерных устройств

2. Расследование хищений денежных средств из банкоматов

3. Хищения с банковских счетов. Предупреждение и расследование

4. Основы расследования компьютерного мошенничества

Семинарское занятие:

1. Общая характеристика компьютерных хищений

2. Типичные следственные ситуации при расследовании компьютерных хищений.

Привлечение специалистов

3. Первоначальный этап расследования

4. Последующий этап расследования

Самостоятельная работа обучающихся:

1. Преступления против собственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

2. Кража с банковского счета, а равно в отношении электронных денежных средств: проблемы квалификации, основные пути совершения, вопросы расследования.

3. Базовый состав мошенничества, совершенный посредством информационно-телекоммуникационных технологий. Мошенничество с использованием электронных средств платежа.. Мошенничество в сфере компьютерной информации (с использованием компьютерных программ, сетей, иных высокотехнологичных средств). Особенности расследования

Контрольные вопросы:

1. Способы хищений, совершаемых, с использованием компьютерных средств

2. Характеристики личности кибермошенника

3. фишинг, скимминг и другие методы,

Тема 10. Расследование некоторых иных преступлений, совершаемых с использованием компьютерных устройств

Лекция:

1. Понятие дистанционной торговли наркотиками

2. Основные способы дистанционной торговли наркотиками

3. Основы противодействия дистанционной торговле наркотиками

4. Кибертерроризм

Семинарское занятие:

1. Дистанционная торговля наркотиками с использованием ИКТ. Понятие и меры выявления

2. Противодействие дистанционной торговле наркотиками с использованием ИКТ.

3. Расследование дистанционной торговли наркотиками

4. Кибертерроризм – определение, предмет и способы совершения.

5. Меры противодействия кибертерроризму

Самостоятельная работа обучающихся:

1. Маркетплейсы и их роль в торговле наркотиками
2. Использование мессенджеров для торговли наркотиками
3. Даркнет
4. Закладчики

Контрольные вопросы:

1. Особенности поиска и задержания закладчиков
2. Каналы дистанционной торговли наркотиками
3. Использование специальных знаний для противодействия рассматриваемым преступлениям

7. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Понятие киберпреступности в узком и расширительном толковании термина.
2. Основные определения термина «киберпреступность» в правовой науке современной России; вопросы соотношения с определением термина «компьютерная преступность».
3. Киберпреступность в исторической перспективе (зарождение киберпреступлений, их развитие и эволюция).
4. Современное состояние киберпреступности, ее уровень, структура и динамика.
5. Цифровизация криминалистической деятельности и ее взаимосвязь с компьютеризацией, автоматизацией, алгоритмизацией, оцифровкой
6. Цифровая трансформация раскрытия, расследования и предупреждения преступлений.
7. Принципы цифровой трансформации
8. Понятие электронной цифровой криминалистики. Предмет, объект методическая основа
9. Система теории электронной цифровой криминалистики.
10. История развития электронной цифровой криминалистики.
11. Электронная цифровая информация. Понятие и виды
12. Основные угрозы компьютерной безопасности организации.
13. Виртуальные следы. Понятие, виды, особенности слеодообразования и поиска.
14. Понятие и содержание криминалистического исследования компьютеров и их систем.
15. Осмотр компьютера
16. Криминалистическое исследование беспроводных сетей.
17. Криминалистическое исследование облачных сервисов
18. Криминалистическое исследование торрент-трекеров
19. Криминалистическое исследование блокчейна
20. Криминалистическое исследование мобильных устройств
21. Криминалистическое исследование электронных систем автомобиля
22. Криминалистическое исследование «Умных» вещей и использование концепции «Интернет вещей» в целом
23. Криминалистическое исследование «чипированных» вещей
24. Тактика осмотра электронного объекта
25. Понятие «киберпреступлений». Классификация их
26. Компьютерные преступления. Общая характеристика
27. Использование специальных знаний при расследовании компьютерных преступлений
28. Первоначальный этап расследования компьютерных преступлений
29. Последующий этап расследования компьютерных преступлений.
30. Понятие информационной безопасности РФ.
31. Формы сотрудничества стран СНГ в сфере борьбы с компьютерными

преступлениями.

32. Организационные вопросы взаимодействия правоохранительных России, осуществляющих борьбу с преступлениями в сфере высоких технологий.

33. Основные направления профилактики и пресечение преступлений в сфере высоких технологий

34. . Мошенничество, совершенное с применением киберсредств (компьютерных программ, сетей, иных высокотехнологичных средств). Основы расследования

35. Кибертерроризм – определение, предмет и способы совершения.

36. Основы предупреждения и расследования кибертерроризма

37. Методика расследования совершенных с использованием киберсредств и способов.

38. Основные виды оперативно-розыскной деятельности, применяемые для выявления киберпреступлений.

39. Отдельные оперативно-розыскные мероприятия, применяемые при расследовании киберпреступлений.

40. Вопросы проведения следственных действий при расследовании киберпреступлений.

41. Цифровые доказательства

42. Дорожка электронных цифровых следов

43. Использование специальных знаний при расследовании киберпреступлений

44. Основы расследования компьютерных преступлений

45. Основы расследования преступлений в сфере мобильных телекоммуникаций

46. Расследование иных преступлений, совершенных с помощью компьютерных устройств

47. Основные международно-правовые акты, регулирующие вопросы международного взаимодействия по борьбе с киберпреступностью, включая вопросы расследования киберпреступлений.

48. Международные организации, занимающиеся расследованием киберпреступлений и борьбой с ними.

49. Подразделения правоохранительных органов основных иностранных государств, занимающихся расследованием киберпреступлений.

50. Разграничение юрисдикции при расследовании киберпреступлений.

51. Виды и методы компьютерно-технических экспертиз, их правовые основы.

52. Особенности взаимодействия с негосударственными организациями, направленными на противодействие и расследование компьютерных преступлений

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ

8.1. Методические рекомендации для обучающихся по подготовке к лекционным занятиям

Обязательным условием получения высшего юридического образования является посещение лекции, поскольку специфика данной формы обучения состоит в речевом общении со студенческой аудиторией. Лекция является одной из основных форм освоения учебного материала. Многие обучающиеся Академии весьма активно используют «систему опережающего чтения», то есть предварительно прочитывают лекционный материал, содержащийся в учебниках и учебных пособиях, закладывают базу для более глубокого восприятия лекции.

В то же время бытует такая точка зрения, что «на лекции можно не ходить; так как есть учебники, всегда можно в них потом прочитать материал» или воспользоваться лекциями прилежного сокурсника. Здесь и таится причина получения неудовлетворительных оценок, так как ничто не может заменить живое слово лектора, его общение с аудиторией.

Внимательное слушание лекции, уяснение основного её содержания, краткая, но

разборчивая запись лекции – непереносимое условие успешной самостоятельной работы каждого обучающегося.

Поэтому обучающиеся, присутствующие на лекциях, обязаны не только внимательно слушать преподавателя кафедры, но и конспектировать излагаемый им материал.

При этом конспектирование материала представляет собой запись основных теоретических положений, нормативных материалов, излагаемых лектором. Нужно твердо помнить, что конспектирование лекций дает обучающемуся не только возможность пользоваться записями лекций при самостоятельной подготовке к семинарам и промежуточной аттестации, но и глубже и основательнее вникнуть в существо излагаемых в лекции вопросов, лучше усвоить и запомнить теоретический и нормативный материал. Как уже указывалось, конспектирование представляет собой сжатое и свободное изложение наиболее важных, кардинальных вопросов темы, излагаемой в лекции. Необходимо избегать механического записывания текста лекции без осмысливания его содержания. Не говоря уже о том, что такая запись требует не лекции, а диктовки, что недопустимо и невозможно по данной учебной дисциплине. Главный порок такой системы заключается в том, что при ней основное внимание обучающегося сосредоточивается не на усвоении содержания лекции, а на механическом воспроизведении текста, прочитанного преподавателем. Поскольку обучающийся не обращает внимания на смысл и содержание лекции, а следит лишь за тем, чтобы она была дословно записана в тетради, материал, излагаемый лектором, остается для него непонятным, а само впечатление о содержании излагаемой темы отрывочным, смутным и далеко неполным.

Основная цель лекции, таким образом, остается недостигнутой, к тому же следует иметь в виду и другое: как бы медленно ни читал лекцию лектор и как бы ни старался обучающийся её дословно записать, последнего достигнуть почти невозможно, а так как при такой записи главной целью является – правильно записать лекцию, а не уяснить её смысл, то текст конспекта в ряде случаев искажает смысл и содержание многих разделов лекции. Рекомендуется поэтому высказываемое лектором положение записывать своими словами.

Перед записью надо постараться вначале понять смысл сказанного. Необходимо стараться отделить главное от второстепенного и, прежде всего, записать главное. Качество записи лекции, конечно, во многом зависит от навыков записывающего и от его общей подготовки, от сообразительности, от умения излагать преподаваемое преподавателем своими словами и от многих других факторов чисто индивидуального характера.

Главное для обучающегося, состоит в том, чтобы выработать свой стереотип написания слов. Однако при записи надо по возможности стараться избегать различных ненужных сокращений и записывать слова, обычно не сокращаемые, полностью. Если существует необходимость прибегнуть к сокращению, то надо употреблять общепринятые сокращения, так как произвольные сокращения по истечении некоторого времени забываются, и при чтении конспекта бывает, в связи с этим, очень трудно разобрать написанное.

Обращает на себя внимание единство, взаимообусловленность научных, учебных и воспитательных функций каждой вузовской лекции. Если научная функция лекции состоит в передаче студентам современного состояния науки, ее предмета, метода, основных теоретических категорий, подходов, то учебная и воспитательная функции лекции заключаются в организации и развитии у обучающихся аудиторной и внеаудиторной самостоятельной работы, трудолюбия, формирования научного мышления, в обеспечении эффективного и точного выполнения учебного плана и учебной программы.

После лекции, не теряя времени, студент должен познакомиться с планом семинарского занятия. Он уясняет обязательную и дополнительную литературу, которую необходимо прочитать, изучить и законспектировать. Обычно разъяснение по этим вопросам студенты получают в конце предыдущего семинарского занятия, когда преподаватель объявляет очередную тему занятия и кратко рассказывает, как к нему

готовиться. В целом, подготовка к семинарскому занятию требует, прежде всего, чтения рекомендуемых нормативных и монографических работ, их реферирования, подготовки докладов и сообщений.

8.2. Методические рекомендации по подготовке к семинарским занятиям

В высших учебных заведениях, в особенности специализированных, учебный процесс, как структурно-сложная деятельность, не должен ограничиваться лишь изучением абстрактного материала. Именно поэтому традиционно в ВУЗах для студенческой аудитории преподавателями сначала читаются лекции, содержащие, как правило, теоретические сведения, после чего они подлежат практическому закреплению. Если лекция закладывает основы научных знаний в обобщенной и абстрактной форме, то семинарские занятия призваны углубить, расширить и детализировать эти знания.

Высокий профессиональный уровень немыслим без выработки практических навыков правильного применения теоретических знаний, ввиду чего трудно переоценить значение практических занятий. Цель занятий: проверить теоретические знания у обучающихся, умение применять усвоенное при решении практических задач. На уровне практического познания происходит усвоение и закрепление полученных теоретических знаний, предоставляется возможность реализации этих знаний в обстановке приближенной к реальности.

В процессе обучения большое значение имеет выработка у обучающегося умений и навыков по применению изучаемого материала на практике.

В ходе практического занятия обсуждаются вопросы, которые задаются студентам в качестве домашнего задания в соответствии с методическими материалами.

Некоторые семинарские занятия проходят в рамках практической подготовки. На таких семинарских занятиях рассматриваются практикоориентированные ситуации, казусы, формируются кейсы и решаются задачи. Семинарские занятия в рамках практической подготовки позволяют обучающимся получить навыки практической работы с конкретными жизненными ситуациями по определенным проблемам, найти правовое решение той или иной ситуации, аргументированно и логично строить правовую позицию по защите прав граждан.

8.3. Методические рекомендации по самостоятельной работе обучающихся

Сами по себе учебные занятия в вузе, как бы они хорошо ни проводились, не могут обеспечить высокого качества подготовки юриста, отвечающего тем требованиям, которые предъявляют в настоящее время социальные и экономические реалии. Главным условием этого является активная и качественная самостоятельная деятельность обучающихся. Именно в процессе самостоятельного изучения курса, вырабатываются необходимые навыки работы с нормативными правовыми актами, появляется способность последовательного, аналитического мышления, что способствует наиболее успешному изучению, осмыслению и запоминанию учебного материала, а также является залогом успешной трудовой деятельности.

На лекциях и семинарских занятиях обучающийся получает существенный объем практического и теоретического материала, нуждающегося в закреплении, углублении в процессе самостоятельного изучения соответствующих вопросов. Однако при организации и осуществлении самостоятельной работы обучающиеся сталкиваются с определенными трудностями и проблемами. Некоторые обучающиеся недостаточно эффективно работают на лекциях и семинарских занятиях, следствием чего является не умение быстро подобрать необходимый нормативный правовой акт. При изучении дисциплины не всем обучающимся удается выделить и понять главное, существенное в тексте, сделать

самостоятельные выводы, определить свое отношение к требованиям норм права и к прочитанному.

В целях более правильной организации самостоятельной работы по учебному курсу обучающимся предлагается ряд рекомендаций, которые необходимо внимательно изучить и использовать с первых же дней обучения.

В период между занятиями при самостоятельной работе над учебным материалом по курсу обучающийся может получить ответы на свои вопросы по предмету непосредственно у преподавателей кафедры в дни их консультаций или письменно обратиться за консультацией к преподавателю кафедры, или непосредственно на кафедру.

Самостоятельная работа по изучению курса складывается из двух элементов: создание условий для работы и сама подготовка, её процесс. К условиям, от которых зависит качество самостоятельной подготовки, следует отнести: а) точное и полное знание задания; б) обеспечение себя необходимой литературой, нормативно-правовыми актами, методическими пособиями; в) наличие конспектов лекций по предмету; г) выделение достаточного количества времени; д) надлежащее рабочее место.

Получив задание и разобравшись в нем, обучающийся обязан принять меры к обеспечению себя необходимыми учебными пособиями: литературой, нормативно-правовыми актами и т.д. Важно к обеспечению себя пособиями приступить своевременно, т.е. немедленно после получения задания или окончания аудиторных занятий. В указанное время обучающийся может посетить научную библиотеку, учебно-методический кабинет кафедры, читальный зал, посмотреть справочные правовые системы или электронные библиотечные системы.

8.4. Методические рекомендации при реализации учебной дисциплины с применением дистанционных образовательных технологий

Вебинар – интерактивное мероприятие, представляющее собой взаимодействие обучающихся и педагогических работников на расстоянии с применением информационно-телекоммуникационных сетей (платформа для проведения он-лайн занятий), включающее в себя интерактивную видеотрансляцию с демонстрацией материалов и обратную видео, аудио и текстовую связь.

Видеолекция – презентация MicrosoftPowerPoint с видео и аудио сопровождением, преобразованная в формат html (может содержать анимацию, видео ролики, элементы управления).

Электронный учебный курс – электронный образовательный ресурс комплексного назначения, расположенный на образовательном портале Академии и обеспечивающий реализацию учебного процесса с применением электронного обучения, проведение учебных занятий, взаимодействие педагогического работника и обучающихся.

8.5. Методические рекомендации по подготовке к сдаче зачета

По итогам изучения курса обучающемуся предстоит сдать зачет. Именно он способен максимально осуществить контроль качества и глубины знаний обучающегося.

На зачете оцениваются полученные теоретические знания, знания нормативных актов, научных статей, степень развития творческого мышления, приобретенные навыки самостоятельной работы, умение систематизировать полученные знания и применять их к решению практических задач.

Оценка «зачтено» по дисциплине выставляется обучающемуся при условии успешного выполнения всех требований рабочей программы по данной дисциплине на основе контроля текущей успеваемости. Форма контроля текущей успеваемости на

семинарских занятиях устанавливается преподавателем. Зачет является итоговой проверкой результатов усвоения обучающимся всего объема учебного курса, способом оценки уровня полученных им знаний по изучаемой дисциплине. При проведении зачета преподаватель должен исходить из того, что при этом реализуются функции обучения, оценки и воспитания обучающегося.

В процессе подготовки к зачету обучающийся должен обратиться к уже изученному материалу, конспектам лекций, учебникам, нормативным актам, информационным ресурсам, собранным и обработанным (тезисы, конспекты, заранее подготовленные ответы на вопросы) студентом в процессе самостоятельной подготовки к семинарским занятиям. Эти знания должны быть систематизированы, обобщены, логически осмыслены.

Оценивая знания обучающегося, преподаватель должен проявлять объективность, доброжелательность, принципиальность, справедливость, демонстрировать уважение аргументированного мнения обучающегося, исходить из принципа научного плюрализма, стимулировать желание студента к творческой учебе. Обучающимся следует показать на примере возможность использования программы учебного курса для выстраивания логики ответа, получения информации о связи вопроса с другими вопросами раздела (темы) учебного курса.

Обучающийся при подготовке к зачету должен усвоить и запомнить важнейшие определения понятий и категорий дисциплины, уяснить смысл специфической терминологии, которая используется для обозначения тех или иных категорий.

В процессе зачета преподаватель должен проверить не только наличие суммы знаний, но и способность обучающегося правильно их использовать, аргументировать собственную позицию, умение анализировать заученные определения понятий и категорий.

Ответ обучающегося на зачете оценивается исходя из следующих критериев: полнота, четкость, информационная насыщенность ответа, новизна используемой информации, знание и использование научных источников, нормативных актов, судебной практики, логичность ответа, доказательность позиции, на которой основывается ответ студента. Также качество и глубина приобретенных знаний фиксируется посредством осуществления сдачи зачета. Оценка «зачтено» ставится на основании устного ответа. Допуск к зачету предполагает успешное выполнение заданий в ходе семинарских занятий.

8.6. Методические рекомендации по подготовке к теоретическому опросу

Теоретический опрос обучающихся проводится в рамках семинарского занятия и предполагает устное изложение материала по вопросам, предусмотренным планом учебного занятия. Подготовка обучающихся к опросу должна быть системной, включать в себя повторение пройденного материала, изложенного не только на лекции, но и, в ходе самостоятельной работы студентов. В целях эффективного усвоения учебного материала и формирования устойчивых представлений по дисциплине, обучающимся следует изучать не только основную учебную литературу, но и дополнительную научную литературу, в том числе с использованием Интернет-ресурсов, официальных сайтов, справочных правовых систем.

Ответ обучающегося должен представлять собой развернутое, содержательное и логически выстроенное сообщение. При выставлении оценки преподаватель учитывает правильность ответа по содержанию, его последовательность, самостоятельность суждений и выводов, способность устанавливать причинно-следственные связи, соотносить теоретические положения с практикой, в том числе и с будущей профессиональной деятельностью.

8.7. Методические рекомендации по прохождению итогового тестирования

Содержание тестового задания ориентировано на получение от тестируемого однозначного заключения и рассчитано на оценку уровня учебных достижений студентов по конкретной области знаний. Тестовые задания формулируются в виде свернутых кратких суждений. Выбирая ответ на вопрос теста, прежде всего, необходимо внимательно прочитать условия вопроса теста, вдумываясь в его смысл. Следует выбирать наиболее точный и достоверный ответ из всех. Если, по мнению обучающегося, несколько ответов являются правильными, то нужно выбрать тот, который максимально охватывает ответ на поставленный вопрос. Однако нужно учесть, что иногда решение теста предполагает выбор нескольких вариантов из представленных. Это четко определяется в вопросе теста. При решении тестового задания следует сначала прорешать наиболее простые варианты, затем перейти к наиболее сложным. При тестировании на бумажном носителе, следует избегать помарок (допускается аккуратное исправление неверного ответа путем его зачеркивания и проставления рядом правильного варианта).

8.8. Методические рекомендации по подготовке рефератов

Реферат – это научно-исследовательская работа, представляющая собой краткое изложение в письменном виде содержание научных трудов (монографий, учебных пособий, научных статей) по заданной теме. В реферате обучающийся излагает основные положения (идеи, решения, предложения и т.д.), содержащиеся в нескольких источниках, приводит различные точки зрения, обосновывает свое мнение по ним.

Работа над выбранной (заданной) темой проходит следующие этапы: поиск и изучение источников и составление библиографии, разработка плана, написание реферата.

Реферат состоит из титульного листа, оглавления (соответствует плану), введения, основной части и списка использованной литературы.

Объем реферата – не менее и не более 15 страниц, отпечатанных через 2 интервала (11 страниц, отпечатанных через полтора интервала). В реферате следует сделать ссылки на использованные источники. Они должны быть оформлены в соответствии с установленным стандартом.

Готовый реферат представляется преподавателю для проверки. Оценивая реферат, он учитывает умение обучающегося работать с научной литературой, анализировать различные точки зрения по спорным вопросам, аргументировать свое мнение, навыки оформления ссылок, списка использованной литературы.

Если реферат будет оценен положительно, то он может послужить зачетной работой по пройденным темам. Иногда практикуется защита реферата на кафедрах или заседаниях методической комиссии по проверке знаний обучающихся.

8.9. Методические рекомендации по решению предложенных конкретных ситуаций

Обучающемуся необходимо самостоятельно смоделировать жизненную ситуацию по предоставленной тематике, проанализировать ее и выработать алгоритм решения этой ситуации с помощью правовых норм.

Необходимо смоделировать ситуацию, которая возникла в результате происшедших событий, реальных ситуаций или может возникнуть при определенных обстоятельствах в тот или иной момент времени. Обучающиеся должны смоделировать, проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выработать алгоритм решения этой ситуации.

Преимущества метода: • развивает аналитическое мышление обучающихся; • обеспечивает системный подход к решению проблемы; • позволяет выделять варианты правильных и ошибочных решений, выбирать критерии нахождения оптимального решения, принимать коллективные решения; • обучающемуся легко соотносить получаемые теоретические знания с реальной практической ситуацией; •

вносит в обучение элемент загадки, тайны; • разбираемая гипотетическая ситуация не связана ни с каким личным риском ни для одного из участников.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

9.1. Основная литература

1. Арямов А.А., Руева Е.О. Противодействие коррупции в условиях цифровизации : Учебное пособие Российский государственный университет правосудия, 2021. URL: <http://znanium.com/catalog/document?id=397466>
2. Балашов, Д. Н. Криминалистика : учебник / Д.Н. Балашов, Н.М. Балашов, С.В. Маликов. — 3-е изд., перераб. и доп. — Москва : ИНФРА-М, 2024. — 449 с. + Доп. материалы [Электронный ресурс]. — (Среднее профессиональное образование). - ISBN 978-5-16-017344-3. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1905249>
3. Вайл П., Ворнер С. Цифровая трансформация бизнеса: изменение бизнес-модели для организации нового поколения : Научно-популярная литература ООО "Альпина Паблишер", 2019. URL: <http://znanium.com/catalog/document?id=352136>
4. Горшков М. М., Грибунов О. П., Кузнецов А. А., Латышов И. В., Мазунин Я. М., Муравьев К. В., Першин А. Н., Россинская Е. Р., Россинский С. Б., Соколов А. Б., Старичков М. В., Сысенко А. Р., Шаевич А. Криминалистика (общие положения, техника, тактика) : учебник для вузов Юрайт, 2022. URL: <https://urait.ru/bcode/485709>
5. Концепция построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий (ГАС «Доступ к правосудию») : монография / отв. ред. Л. Н. Масленникова. — Москва : Норма : ИНФРА-М, 2024. — 664 с. — DOI 10.12737/1863372. - ISBN 978-5-00156-242-9. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2129522>.
6. Кубанов, В. В. Криминалистика. Ч. 1. Теоретические основы криминалистики. Криминалистическая техника : учебное пособие / В. В. Кубанов. - 2-е изд., испр. и доп. - Самара : Самарский юридический институт ФСИН России, 2023. - 128 с. - ISBN 978-5-91612-413-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2151132>
7. Овчинский В.С. Кибермафия: мировые тенденции и международное противодействие : Монография ООО "Юридическое издательство Норма", 2022. URL: <http://znanium.com/catalog/document?id=400110>
8. Овчинский, В. С. Основы борьбы с киберпреступностью и кибертерроризмом : хрестоматия / сост. В.С. Овчинский. — Москва : Норма : ИНФРА-М, 2024. — 528 с. - ISBN 978-5-91768-814-5. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2098567> (дата обращения: 08.05.2025).
9. Островская, С. Криминалистика компьютерной памяти на практике: Как эффективно анализировать оперативную память : практическое руководство / С. Островская, О. Скулкин ; авторизован. пер. с англ. А. А. Слинкина. - Москва : ДМК Пресс, 2023. - 256 с. - ISBN 978-5-93700-157-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2109510>
10. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебник для вузов / ответственные редакторы С. В. Зуев, В. Б. Вехов. — Москва : Издательство Юрайт, 2025. — 243 с. URL: <https://urait.ru/viewer/rassledovanie-prestupleniy-v-sfere-kompyuternoy-informacii-i-elektronnyh-sredstv-platezha-567677>
11. Россинская Е.Р. Криминалистика : Учебник ООО "Юридическое издательство Норма", 2021. URL: <http://znanium.com/catalog/document?id=365146>
12. Русскевич Е.А. Уголовное право и "цифровая преступность": проблемы и решения : Монография ООО "Научно-издательский центр ИНФРА-М", 2023. URL:

<http://znanium.com/catalog/document?id=415589>

13. Саркисян, А. А. Цифровизация судебно-экспертной деятельности : учебное пособие для вузов / А. А. Саркисян. — Москва : Издательство Юрайт, 2025. — 138 с. URL: <https://urait.ru/viewer/cifrovizaciya-sudebno-ekspertnoy-deyatelnosti-558168#page/1>.
14. Цифровая криминалистика : учебник для вузов / под редакцией В. Б. Вехова, С. В. Зуева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 490 с. URL: <https://urait.ru/viewer/cifrovaya-kriminalistika-568013>
15. Электронные доказательства в уголовном судопроизводстве : учебник для вузов / ответственный редактор С. В. Зуев. — Москва : Издательство Юрайт, 2025. — 193 с. URL: <https://urait.ru/viewer/elektronnye-dokazatelstva-v-ugolovnom-sudoproizvodstve-567334>

9.2. Дополнительная литература

1. Арямов А.А., Руева Е.О. Противодействие коррупции в условиях цифровизации : Учебное пособие Российский государственный университет правосудия, 2021. URL: <http://znanium.com/catalog/document?id=397466>
2. Белоус А.И., Солодуха В.А. Кибероружие и кибербезопасность. О сложных вещах простыми словами : Монография Инфра-Инженерия, 2020. URL: <http://znanium.com/catalog/document?id=361651>
3. Богданов А.В., Завьялов И.А. Особенности противодействия киберпреступности подразделениями уголовного розыска : Учеб.-метод, пособие для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» : Учебно-методическая литература Издательство "ЮНИТИ-ДАНА", 2017. URL: <http://znanium.com/catalog/document?id=341355>
4. Борисова И.В. Цифровые методы обработки информации : Учебное пособие Новосибирский государственный технический университет (НГТУ), 2014. URL: <http://znanium.com/catalog/document?id=201992>
5. Бруссард М. Искусственный интеллект: пределы возможного : Научно-популярная литература ООО "Альпина нон-фикшн", 2020. URL: <http://znanium.com/catalog/document?id=368678>
6. Вайпан В.А., Егорова М.А. Проблемы создания цифровой экосистемы: правовые и экономические аспекты : Монография Юридический Дом "Юстицинформ", 2021. URL: <http://znanium.com/catalog/document?id=376573>
7. Мамычев А.Ю., Гайворонская Я.В. Мир в цифровую эпоху: политика, право и экономика в XXI веке : Монография Издательский Центр РИОР, 2020. URL: <http://znanium.com/catalog/document?id=358112>
8. Мартынов В.Г., Андреев А. Ф. Электронные деньги. Интернет платежи : Практическое пособие Маркет ДС, 2010. URL: <http://znanium.com/catalog/document?id=118877>
9. Минин И.В., Минин О.В. Защита конфиденциальной информации при электронном документообороте : Учебное пособие Новосибирский государственный технический университет (НГТУ), 2011. URL: <http://znanium.com/catalog/document?id=174965>
10. Набоких В. А. Датчики автомобильных электронных систем управления и диагностического оборудования : Учебное пособие Издательство "ФОРУМ", 2016. URL: <http://znanium.com/catalog/document?id=95799>
11. Овчинский В.С. Криминология цифрового мира : Учебник ООО "Юридическое издательство Норма", 2018. URL: <http://znanium.com/catalog/document?id=309263>
12. Овчинский В.С. Основы борьбы с киберпреступностью и кибертерроризмом : Учебное пособие ООО "Юридическое издательство Норма", 2017. URL: <http://znanium.com/catalog/document?id=203683>

13. Пашенцев Д.А., Дорская А.А. Концепция цифрового государства и цифровой правовой среды : Монография ООО "Юридическое издательство Норма", 2021. URL: <http://znanium.com/catalog/document?id=379910>
14. Пенькова Т.Г., Вайнштейн Ю.В. Модели и методы искусственного интеллекта : Учебное пособие Сибирский федеральный университет, 2019. URL: <http://znanium.com/catalog/document?id=379870>
15. Ревенков П.В. Кибербезопасность в условиях электронного банкинга : Практическое пособие Прометей, 2020. URL: <http://znanium.com/catalog/document?id=374846>
16. Русскевич Е.А. Уголовное право и "цифровая преступность": проблемы и решения : Монография ООО "Научно-издательский центр ИНФРА-М", 2023. URL: <http://znanium.com/catalog/document?id=415589>
17. Сергеев Н.Е. Системы искусственного интеллекта. Часть 1 : Учебное пособие Издательство Южного федерального университета (ЮФУ), 2016. URL: <http://znanium.com/catalog/document?id=327726>
18. Трофимов В. В., Барабанова М.И. Информационные системы и цифровые технологии: Часть 1 : Учебное пособие ООО "Научно-издательский центр ИНФРА-М", 2021. URL: <http://znanium.com/catalog/document?id=375739>
19. Трофимцева С.Ю. Противодействие киберпреступности: сравнительный анализ международных рекомендаций и норм зарубежного и российского уголовного права : Монография Самарский юридический институт ФСИН России, 2021. URL: <http://znanium.com/catalog/document?id=398245>
20. Уколов В.Ф., Черкасов В.В. Цифровизация. Взаимодействие реального и виртуального секторов экономики : Монография ООО "Научно-издательский центр ИНФРА-М", 2019. URL: <http://znanium.com/catalog/document?id=352967>
21. Харрис Ш., Лазарев Д. Кибервойн@: Пятый театр военных действий ООО "Альпина нон-фикшн", 2016. URL: <http://znanium.com/catalog/document?id=265505>

9.3. Учебно-методическое обеспечение для организации самостоятельной работы обучающихся

1. Криминалистика : Учебно-методическая литература Издательский Центр РИОР, 2016. URL: <http://znanium.com/catalog/document?id=14180>
2. Александров И. В. Криминалистика: тактика и методика. Задачник : учебное пособие для вузов Юрайт, 2022. URL: <https://urait.ru/bcode/489767>
3. Александров И. В., Яблоков Н. П., Джуманбетова А. А., Колдин В. Я., Комаров И. М., Крюкова Е. С., Лушечкина М. А., Махтаев М. Ш., Перепечина И. О., Поташник Д. П., Сотов А. И., Ткачев А. В., Центров Е. Криминалистика. Практикум : учебное пособие для спо Юрайт, 2022. URL: <https://urait.ru/bcode/490337>
4. Леган М.В. Современные цифровые технологии и методики в профессиональной деятельности преподавателя : Учебное пособие Новосибирский государственный технический университет (НГТУ), 2020. URL: <http://znanium.com/catalog/document?id=396970>
5. Ручкин В.Н., Фомин В.В. Современные компьютерные технологии и криминалистика : Учебное пособие Академия ФСИН России, 2019. URL: <http://znanium.com/catalog/document?id=374599>
6. Толстолужинская Е. М. Криминалистика. Практикум : учебное пособие для вузов Юрайт, 2022. URL: <https://urait.ru/bcode/492057>
7. Трофимов В. В., Макаrchук Т.А. Информационные системы и цифровые технологии: практикум : Часть 2 : Учебное пособие ООО "Научно-издательский центр ИНФРА-М", 2021. URL: <http://znanium.com/catalog/document?id=379897>
8. Трофимов В. В., Макаrchук Т.А. Информационные системы и цифровые технологии. Практикум. Часть 1 : Учебное пособие ООО "Научно-издательский центр ИНФРА-М", 2021. URL: <http://znanium.com/catalog/document?id=378608>

9. Яблоков Н. П. Криминалистика : учебник и практикум для спо Юрайт, 2022. URL: <https://urait.ru/bcode/489607>

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа;

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

9.4. Нормативно-правовые акты и иные правовые документы

10. Соглашение о сотрудничестве государств-участников Содружества независимых государств в борьбе с преступлениями в сфере компьютерной информации // Содружество. Информационный вестник Совета глав государств и Совета глав правительств СНГ. -№ 1(37). -С. 138-145
11. Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (в ред. от 08.04.2021)// Собрание законодательства Российской Федерации от 17 июня 1996 г. № 25 ст. 2954
12. Часть четвертая Гражданского кодекса Российской Федерации от 18 декабря 2006 г. N230-ФЗ. (в ред. от 30.04.2021) //Российская газета от 22 декабря 2006 г. N 289,
13. Федеральный закон от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. от 09.03.2021)//Российская газета от 29 июля 2006 г.№ 165
14. Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 07.04.2020) «О связи» (в ред. от 30.04.2021)// Российская газета от 10.07.2003, № 135
15. Закон РФ от 27 ноября 1992 г. № 4015-1 «Об организации страхового дела в Российской Федерации» (в ред. от 24.02.2021)// Российская газета от 12 января 1993 г. N 6
16. Федеральный закон от 27 июня 2011г. N161-ФЗ «О национальной платежной системе» (в ред. от 30 декабря 2020 г)// Российская газета от 30 июня 2011 г. N 139
17. Федеральный закон от 26 июля 2017г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»//Российская газета от 31 июля 2017 г. № 167
18. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (в ред. от 13 июля 2015)// Собрание законодательства Российской Федерации от 10 марта 1997 г. № 10, ст. 1127
19. Указ Президента Российской Федерации от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года»//Российская газета от 22 июля 2020 г. № 159
20. Национальная стратегия развития искусственного интеллекта на период до 2030 г(утв. Указом Президента РФ от 10 октября 2019г. №490 «О развитии искусственного интеллекта в Российской Федерации»)// Официальный сайт Президента РФ URL: <http://www.kremlin.ru/acts/bank/44731/page/1> (дата обращения 26.07.2021)
21. Распоряжение Правительства РФ от 22 октября 1999 г. № 1701-р «Об

- усилении борьбы с преступлениями в сфере высоких технологий и реализации международных договоренностей и обязательств РФ»//Собрание законодательства РФ от 1 ноября 1999г № 44 ст. 5335.
22. Приказ Генерального прокурора РФ от 14 сентября 2017г. №627 Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2025 года// Официальный сайт Генеральной Прокуратуры РФ URL: <https://genproc.gov.ru/documents/orders/627.pdf> (дата обращения 23.07.21)
 23. ГОСТ 2.051-2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения (введен в действие Приказом Росстандарта № 1628-ст от 22.11.2013). М.: Стандартинформ, 2014. С.2.
 24. Межгосударственный стандарт ГОСТ 2.051-2013 Единая система конструкторской документации (ЕСКД). Электронные документы. Общие положения (с Поправкой). Введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. N 1628-ст// Текст приказа официально опубликован не был
 25. ГОСТ7.69–95 СИБИБД «Аудиовизуальные документы. Основные термины и определения. М.: ИПК Издательство стандартов, 1996
 26. Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст)// Текст приводится по официальному изданию М.: Стандартинформ, 2008
 27. Методические рекомендации по цифровой трансформации государственных корпораций и компаний с государственным участием (утв. Минцифры, одобр. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности 6 ноября 2020)// Документ официально опубликован не был.
 28. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ// СЗ РФ. 1996.№ 25. Ст. 29.
 29. Уголовно-процессуальный кодекс РФ от 18 декабря 2001 г. № 174-ФЗ//Российская газета от 22 декабря 2001 г. № 249.
 30. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»// Российская газета от 8 апреля 2011 г. № 75
 31. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»// Российская газета от 29 июля 2006 г. № 165
 32. ГОСТ Р 34.10-2012. Национальный стандарт Российской Федерации. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (утв. и введен в действие Приказом Росстандарта от 07.08.2012 N 215-ст). М.: Стандартинформ, 2013
- 9.5. Ресурсы информационно-телекоммуникационной сети «Интернет»**
33. Судебные и нормативные акты РФ URL: <http://sudact.ru/>
 34. Портал правовой статистики URL: <http://crimestat.ru/>
 35. genproc.gov.ru/stat/
 36. Официальная статистика МВД РФ
URL:<http://mvd.ru/presscenter/statistics/reports>
 37. Судебная практика:URL:<https://rospravosudie.com/>.

10. ИНФОРМАЦИОННОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Программное обеспечение

Для успешного освоения дисциплины обучающийся использует следующие программные средства:

1. операционная система Windows или Linux;
2. пакет офисных программ Microsoft Office или Libre Office.
3. программа видеоконференцсвязи.

2. Информационно-справочные системы и профессиональные базы данных:

1. справочная правовая система «Консультант Плюс».
2. Электронные каталоги научной библиотеки СГЮА – автоматизированная библиотечная программа ИРБИС.
3. LEXPRO - информационно-правовая база данных (<https://online.lexpro.ru/>)
4. Электронно-библиотечная система ZNANIUM.COM (<https://znanium.com/>)
5. Университетская библиотека ONLINE (<https://biblioclub.ru/>)
6. Электронная библиотечная система Юрайт (<https://urait.ru/>)
7. Электронная библиотечная система IPRTSMART (<http://www.iprbookshop.ru>)
8. ЭИОС Академии (<http://portal.ssla.ru/>; <https://wp2.ssla.ru/>; <http://online.ssla.ru/>)

Обучающимся обеспечивается доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, указанным в рабочей программе дисциплины.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Для проведения лекционных занятий используются аудитории, укомплектованные необходимой специализированной учебной мебелью и техническими средствами для предоставления учебной информации обучающимся, а именно: преподавательский стол; стол обучающихся; скамьи; стулья; кафедра; мультимедийный комплекс (проектор, экран), компьютер, колонки или мобильный комплект; лицензионное программное обеспечение; подключение к Интернету, учебно-наглядные пособия: презентации.

Для проведения занятий семинарского типа, групповых и индивидуальных консультаций, курсового проектирования, текущего контроля и промежуточной аттестации используются аудитории, укомплектованные преподавательским столом; столами для обучающихся; стульями; классной доской; мультимедийным комплексом (проектор, экран); компьютером, колонками или мобильным комплектом; лицензионным программным обеспечением; подключением к сети Интернет; учебно-наглядными пособиями: презентациями.

Для подготовки студентов к семинарским (практическим) занятиям оборудованы кабинеты для самостоятельной работы. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе.

При изучении дисциплины также используются: Центр деловых игр, лекционная, семинарская.

12. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

При необходимости обучающемуся инвалиду и лицу с ОВЗ предоставляется дополнительное время для подготовки ответа на зачете или экзамене.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Педагогические работники, относящиеся к профессорско-преподавательскому составу кафедры, знакомятся с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Медиа материалы также следует использовать и адаптировать с учетом индивидуальных особенностей обучения лиц с ОВЗ.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету является важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей в соответствии с фондом оценочных средств, адаптированных для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в ОПОП ВО результатов обучения и уровень сформированности всех компетенций, заявленных образовательной программой.

Категории обучающихся по нозологиям	Формы оценочных средств, адаптированные к ограничениям здоровья и восприятия информации обучающихся инвалидов и лиц с ОВЗ	Виды оценочных средств
--	--	-------------------------------

с нарушениями зрения	<ul style="list-style-type: none"> – в печатной форме увеличенным шрифтом, – в форме электронного документа, – в печатной форме шрифтом Брайля. 	– собеседование
с нарушениями слуха	<ul style="list-style-type: none"> – в печатной форме, – в форме электронного документа. 	– тестирование
с нарушениями опорно-двигательного аппарата	<ul style="list-style-type: none"> – в печатной форме, – в форме электронного документа. 	– решение дистанционных тестов, контрольные вопросы

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием средств обучения общего и специального назначения:

– лекционная аудитория – мультимедийное оборудование, мобильный радиокласс (для студентов с нарушениями слуха);

– учебная аудитория для самостоятельной работы – стандартные рабочие места с персональными компьютерами; рабочее место с персональным компьютером оснащенным специализированным программным и техническим обеспечением для студентов с нарушениями зрения.

В аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, должно быть предусмотрено соответствующее количество мест для обучающихся с учетом ограничений их здоровья.

В аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, должен быть обеспечен беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья.

В Саратовской государственной юридической академии имеются специальные технические средства обучения, программное обеспечение для инвалидов и лиц с ограниченными возможностями здоровья.

Категории обучающихся по нозологиям	Материально-техническое и программное обеспечение для инвалидов и лиц с ограниченными возможностями здоровья
С нарушениями зрения	<p>Специальные технические средства:</p> <ul style="list-style-type: none"> - компьютер; - программное обеспечение экранного доступа " ZoomTextFusion "; - электронный ручной видео-увеличитель; - тифлоплеер; - принтер для печати рельефно-точечным шрифтом Брайля; - электронный стационарный видео увеличитель.
С нарушениями слуха	<p>Специальные технические средства:</p> <ul style="list-style-type: none"> - радиокласс – беспроводная технология передачи звука (FM-система); - звукоусиливающее оборудование; - средства отображения информации; - компьютер.
С нарушениями опорно-	<p>Специальные технические средства:</p> <ul style="list-style-type: none"> - компьютер;

двигательного аппарата	- специальная клавиатура (с увеличенным размером клавиш, со специальной накладкой, ограничивающей случайное нажатие соседних клавиш) - джойстик со сменными насадками; - выносная кнопка.
------------------------	---

Разработчик _____ доцент (к/н, доцент) кафедры криминалистики _____ Смушкин
А.Б.

подпись

должность

ФИО