МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ,
МИНИСТЕРСТВО НАУКИ, ВЫСШЕГО ОБРАЗОВАНИЯ И ИННОВАЦИЙ
КЫРГЫЗСКОЙ РЕСПУБЛИКИ

МОО ВО Кыргызско-Российский Славянский университет
имени первого Президента Российской Федерации Б.Н. Ельцина

УТВЕРЖДАЮ
декан факультета
23 июня 2025 г.

Обеспечение информационной безопасности

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Судебной экспертизы**

Учебный план 400503_21_45 сэ.plx
Специальность 40.05.03 - РФ, 530002 - КР Судебная экспертиза
Специализация "Криминалистические экспертизы"

Квалификация **специалист**

Форма обучения **очная**

Общая трудоемкость **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 32
самостоятельная работа 39,8

Виды контроля в семестрах:
зачет с оценкой 10

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель	9			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	16	16	16	16
Контактная работа в период теоретического обучения	0,2	0,2	0,2	0,2
В том числе инт.	16	16	16	16
В том числе в форме практ.подготовки	4		4	
Итого ауд.	32	32	32	32
Контактная работа	32,2	32,2	32,2	32,2
Сам. работа	39,8	39,8	39,8	39,8
Итого	72	72	72	72

Программу составил(и):
к.э.н., доцент, доцент, Подольский Иван Валерьевич _____

Рецензент(ы):
д.т.н, академик , профессор, Живоглядов Валерий Петрович _____

Рабочая программа дисциплины
Обеспечение информационной безопасности

разработана в соответствии с ФГОС 3++:
Федеральный государственный образовательный стандарт высшего образования - специалитет по специальности 40.05.03 Судебная экспертиза (приказ Минобрнауки России от 31.08.2020 г. № 1136)

составлена на основании учебного плана:
Специальность 40.05.03 - РФ, 530002 - КР Судебная экспертиза
Специализация "Криминалистические экспертизы"
утвержденного учёным советом вуза от ____ _____протокол № _____

Рабочая программа одобрена на заседании кафедры
Судебной экспертизы

Протокол от _ _____ 2025 г. № __
Срок действия программы: уч.г.
Зав. кафедрой доцент, к.ю.н. Калыбаева А.А.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС

__ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Судебной экспертизы

Протокол от __ _____ 2026 г. № __
Зав. кафедрой доцент, к.ю.н. Калыбаева А.А.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС

__ _____ 2027 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Судебной экспертизы

Протокол от __ _____ 2027 г. № __
Зав. кафедрой доцент, к.ю.н. Калыбаева А.А.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС

__ _____ 2028 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры
Судебной экспертизы

Протокол от __ _____ 2028 г. № __
Зав. кафедрой доцент, к.ю.н. Калыбаева А.А.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС

__ _____ 2029 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2029-2030 учебном году на заседании кафедры
Судебной экспертизы

Протокол от __ _____ 2029 г. № __
Зав. кафедрой доцент, к.ю.н. Калыбаева А.А.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Сформировать у будущих судебных экспертов системные знания в области информационной безопасности, необходимые для проведения судебных компьютерно-технических экспертиз. Цель достигается через:
1.2	Понимание контекста: Изучение принципов обеспечения информационной безопасности государства и организаций как объекта потенциальных посягательств.
1.3	Экспертный анализ: Обучение подходам к анализу информационной инфраструктуры жертвы или подозреваемого для выявления следов противоправной деятельности.
1.4	Криминалистический подход: Изучение методов нарушения конфиденциальности, целостности и доступности информации как типичных предметов преступного посягательства.
1.5	Процессуальная грамотность: Закладка терминологического фундамента, обязательного для составления процессуальных документов (заключений эксперта, постановлений).
1.6	Задачи дисциплины:
1.7	Ознакомить студентов с терминологией информационной безопасности, используемой в следственно-судебной практике.
1.8	Сформировать экспертное мышление, направленное на выявление и анализ цифровых следов.
1.9	Изучить методы и средства обеспечения ИБ, чтобы понимать, как они могли быть обойдены или скомпрометированы злоумышленником.
1.10	Научить определять и классифицировать в процессуальных категориях:
1.11	Причины инцидентов информационной безопасности.
1.12	Виды и способы совершения компьютерных преступлений.
1.13	Каналы утечки информации как пути распространения доказательств.
1.14	Каналы искажения информации как способ подлога или фальсификации данных.
1.15	Место дисциплины в образовательной программе:
1.16	Полученные знания и навыки являются критически важными для:
1.17	Последующего изучения специальных дисциплин, таких как "Методика и техника судебной компьютерно-технической экспертизы", "Криминалистика", "Уголовное право".
1.18	Проведения курсовых и дипломных работ, которые часто представляют собой модельные экспертные исследования по конкретным кейсам нарушения ИБ.
1.19	Непосредственного применения в будущей профессиональной деятельности при производстве судебных экспертиз по делам, связанным с компьютерными преступлениями, несанкционированным доступом, утечкой данных и т.д.
1.20	Итог: Для судебного эксперта эта дисциплина — не о том, как защищаться, а о том, как расследовать, что произошло, каким способом и по чьей вине. Она дает техническую основу для юридической квалификации деяния и доказывания его в суде.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.ДВ.03
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Компьютерные технологии в экспертной деятельности
2.1.2	Информационные технологии в экспертной деятельности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Дисциплина является базовым курсом для освоения курса "
2.2.2	Обеспечение информационной безопасности"
2.2.3	"Организация режима секретности"

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

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	сущность и понятие информационной безопасности, характеристику ее составляющих;
3.1.2	место информационной безопасности в системе национальной безопасности страны;
3.1.3	источники угроз информационной безопасности и меры по их предотвращению;
3.1.4	жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
3.1.5	современные средства и способы обеспечения информационной безопасности.
3.2	**Уметь:**

3.2.1	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
3.2.2	применять основные правила и документы системы сертификации Российской Федерации;
3.2.3	классифицировать основные угрозы безопасности информации.
3.3	**Владеть:**
3.3.1	основами
3.3.2	- обеспечения информационной безопасности государства;
3.3.3	- методологии создания систем защиты информации;
3.3.4	- процессов сбора, передачи и накопления информации;
3.3.5	- оценки защищенности и обеспечения информационной безопасности компьютерных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Пр. подг.	Примечание
	Раздел 1. Модуль 1. Государственная политика и правовые основы информационной безопасности							
1.1	Тема 1. Политика государства в области информатизации и развития ИТ. Стратегия развития информационного общества, цели, принципы, национальные интересы. Понятия: информационное общество, цифровая экономика. /Лек/	10	1					Стратегия развития информационного общества на 2017–2030 гг. Цифровая экономика, информационное пространство, электронное правительство. Основные направления развития ИТ: большие данные, ИИ, интернет вещей, облачные вычисления и др.
1.2	Семинар: Анализ стратегических документов. Обсуждение целей и приоритетов Стратегии. Решение задач и ответы на контрольные вопросы. /Пр/	10	2			2		
1.3	СР (4ч): Проработка конспекта, подготовка к семинару по контрольным вопросам (стр. 10 -11). /Ср/	10	4,2					
1.4	Тема 2. Место ИБ в системе национальной безопасности РФ. Стратегия национальной безопасности. Доктрина ИБ. Основные понятия: угрозы, национальные интересы, система обеспечения ИБ. /Лек/	10	2			2		

1.5	Практикум: Система обеспечения ИБ в РФ. Разбор организационной структуры. Анализ информационных угроз (рис. 2.3). Решение кейсов по противодействию угрозам. /Пр/	10	2					
	Раздел 2. Модуль 2. Классификация и правовой режим защиты информации							
2.1	Тема 3.1. Классификация информации по доступу. Конфиденциальная информация. Федеральный закон № 149-ФЗ. Понятия: информация ограниченного доступа, конфиденциальность. Обзор видов конфиденциальной информации (Указ Президента № 188). /Лек/	10	1					Информационная безопасность в системе национальной безопасности Определения: национальная безопасность, угрозы, стратегические приоритеты. Доктрина информационной безопасности РФ. Роль Президента, Совета Безопасности, государственных органов.
2.2	Семинар: Разграничение видов информации. Работа с классификациями. Анализ перечня сведений конфиденциального характера (табл. 3.1). /Пр/	10	1					
2.3	Тема 3.2. Персональные данные. Федеральный закон № 152-ФЗ «О персональных данных». Основные понятия: оператор, обработка, обезличивание. Требования к защите ПДн. /Лек/	10	2					Подготовка к практикуму.
2.4	Практикум: Обеспечение соответствия 152-ФЗ. Разбор кейсов по нарушениям в обработке ПДн. Составление модели угроз для условной информационной системы ПДн. /Пр/	10	2			2		
2.5	СР (6ч): Изучение нормативных документов в области защиты ПДн (постановления Правительства). /Ср/	10	8					Подготовка к практикуму.
2.6	Тема 3.3. Коммерческая и служебная тайна. Федеральный закон № 98-ФЗ «О коммерческой тайне». Понятия: коммерческая тайна, обладатель, разглашение. Служебная тайна. /Лек/	10	2					Подготовка к деловой игре.

2.7	Тема 3.4. Профессиональные и процессуальные тайны. Врачебная, нотариальная, адвокатская, банковская тайна. Тайна связи, усыновления, страхования, исповеди. /Лек/	10	2					Подготовка к круглому столу.
2.8	Круглый стол: Профессиональная этика и конфиденциальность. Анализ правовых коллизий между разными видами тайн. Решение задач на разграничение служебной и профессиональной тайны. /Пр/	10	1					
2.9	СР (6ч): Сравнительный анализ правовых режимов различных профессиональных тайн. /Ср/	10	6					Подготовка к круглому столу.
	Раздел 3. Модуль 3. Защита государственной тайны и информационная безопасность							
3.1	Тема 4.1. Государственная тайна. Закон РФ № 5485-1 «О государственной тайне». Сведения, относящиеся к ГТ. Степени секретности. Допуск и доступ к ГТ. /Лек/	10	2			2		Государственная тайна и система её защиты Закон о государственной тайне, степени секретности. Допуск к гостайне, надбавки, основания для отказа. Органы защиты гостайны, методы и средства защиты информации.
3.2	Практикум: Работа со сведениями, составляющими ГТ. Разбор процедуры допуска и оснований для отказа. Расчет надбавок за работу с ГТ. /Пр/	10	2			2		
3.3	СР (5ч): Изучение степеней секретности (табл. 4.1). Проработка процедуры допуска к ГТ. /Ср/	10	4					схемы данных

3.4	Тема 4.2. Государственная система защиты информации. Органы защиты ГТ. Система защиты информации. Организационно-технические мероприятия по ЗИ. Объекты защиты. /Лек/	10	2			2		Классификация информации, подлежащей защите Виды информации: общедоступная, ограниченного доступа, конфиденциальная. Персональные данные (152-ФЗ), коммерческая, служебная, профессиональная тайны. Особенности защиты разных видов тайн: врачебной, адвокатской, нотариальной, банковской и др.
3.5	Семинар: Планирование мероприятий по защите информации. Разработка паспорта безопасности условного объекта. Анализ типовых нарушений. /Пр/	10	1					
3.6	СР (5ч): Изучение организационно-технических мероприятий по защите информации (рис. 4.3). Подготовка к семинару. /Ср/	10	5,6					
3.7	Тема 5. Основные нормативные документы в области ИБ. Национальные стандарты (ГОСТ Р). Роль ФСТЭК России и ФСБ России. Руководящие документы. /Лек/	10	2			2		
3.8	Практикум: Применение национальных стандартов. Сравнительный анализ ГОСТ Р 50922, ГОСТ Р ИСО/МЭК 27001. Составление реестра мер защиты для ИС. /Пр/	10	2					
3.9	СР (6ч): Ознакомление с ключевыми ГОСТами (список на стр. 54-59). Анализ требований ФСТЭК и ФСБ. /Ср/	10	4					
3.10	/КрТО/	10	0,2					
	Раздел 4. Модуль 4. Контроль и оценка знаний							
4.1	Обобщающая лекция. Актуальные вызовы и тенденции в ИБ. Киберугрозы, импортозамещение, суверенный интернет. /Пр/	10	2			2		

4.2	Подготовка к экзамену. Разбор экзаменационных вопросов, типовых задач, консультации. /Пр/	10	1					
4.3	СР (11ч): Систематизация знаний, повторение всех тем курса, подготовка к экзамену. /Ср/	10	8					

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации

Вопросы для проверки уровня обученности (ЗНАТЬ)
Раздел 1. Правовые и организационные основы информационной безопасности
Правовое регулирование информационной безопасности в Кыргызской Республике и Российской Федерации: сравнительный анализ
Законодательство КР и РФ о защите государственной тайны и конфиденциальной информации
Правовой статус государственных информационных ресурсов в КР и РФ
Защита персональных данных: сравнительный анализ законодательства КР и РФ
Правовые основы борьбы с компьютерными преступлениями в КР (УК КР) и РФ (УК РФ)
Особенности расследования киберпреступлений в соответствии с уголовно-процессуальным законодательством КР и РФ
Международно-правовое регулирование в сфере информационной безопасности

Раздел 2. Технические аспекты информационной безопасности
8. Классификация угроз информационной безопасности современных компьютерных систем
9. Методы и средства идентификации и аутентификации в информационных системах
10. Системы управления доступом: дискреционные и мандатные модели
11. Криптографические методы защиты информации: симметричное и асимметричное шифрование
12. Электронная подпись и цифровые сертификаты в КР и РФ: правовые и технические аспекты
13. Методы и средства защиты от вредоносного программного обеспечения
14. Защита информации в банковских системах и критической информационной инфраструктуре
15. Стандарты и спецификации в области информационной безопасности

Раздел 3. Судебно-экспертная деятельность в сфере ИБ
16. Особенности назначения и производства судебных компьютерно-технических экспертиз
17. Методика исследования цифровых следов при расследовании киберпреступлений
18. Классификация и характеристика современных вредоносных программных средств
19. Методы выявления и исследования средств несанкционированного доступа
20. Особенности экспертного исследования систем криптографической защиты

Задания для проверки уровня обученности (УМЕТЬ и ВЛАДЕТЬ)
Практические задания по правовым аспектам
Провести сравнительный анализ составов компьютерных преступлений по УК КР и УК РФ
Составить процессуальные документы с учетом требований законодательства КР и РФ о защите конфиденциальной информации
Классифицировать информационные ресурсы по категориям доступа в соответствии с законодательством КР
Практические задания по техническим аспектам
4. Настроить систему разграничения доступа в операционной системе
5. Провести анализ системы аутентификации и предложить меры по ее усилению
6. Исследовать образец вредоносного программного обеспечения с использованием специализированного ПО
7. Реализовать алгоритмы шифрования и электронной подписи для защиты информации
8. Провести аудит безопасности информационной системы
Комплексные экспертные задания
9. Сформировать и обосновать ходатайство о назначении судебной компьютерно-технической экспертизы
10. Составить заключение эксперта по факту неправомерного доступа к компьютерной информации
11. Разработать методику исследования средств криптографической защиты информации
12. Провести анализ системы защиты информации и выявить уязвимости
Критерии оценки:
Полнота и точность применения нормативно-правовой базы КР и РФ
Корректность использования специальной терминологии
Практическая применимость предложенных решений
Соответствие методики проведения исследований современным требованиям
Качество оформления процессуальных документов и заключений
Данные вопросы и задания обеспечивают проверку компетенций ПК-8 и ПК-9 в соответствии с профилем подготовки "Судебная экспертиза".

5.2. Темы курсовых работ (проектов)

Не предусмотрены дисциплиной(модулем)

5.3. Фонд оценочных средств

Фонд оценочных средств (ФОС) по дисциплине «Основы информационной безопасности» формируется для проведения объективной оценки уровня сформированности заявленных компетенций у студентов специалитета «Судебная экспертиза» (ПК-8, ПК-9).

ФОС включает в себя следующие виды контрольно-измерительных материалов, разработанных с учетом профессиональной деятельности судебного эксперта:

1. Контрольные вопросы и тестовый комплекс
Направлены на проверку теоретических знаний и их применения в профессиональном контексте.
Примеры контрольных вопросов:
«Дайте криминалистическую классификацию каналов утечки информации и приведите примеры по делу о нарушении коммерческой тайны». (ПК-8)
«Опишите порядок действий судебного эксперта при обнаружении в материалах дела сведений, составляющих государственную тайну». (ПК-9)
«Какие реквизиты и грифы проставляются на заключении эксперта, если в ходе исследования использовалась информация ограниченного доступа?». (ПК-9)
Тестовый комплекс: Включает ситуационные тестовые задания, где студент должен выбрать юридически и технически верный алгоритм действий эксперта в смоделированной ситуации (например, "При исследовании компьютера обнаружен вредоносный программа-шифровальщик. Ваши первоочередные действия?").

2. Практические задания
Направлены на формирование умений и навыков, моделирующих профессиональную деятельность.
Задание 1 (ПК-8): «По предоставленному образцу вредоносного ПО (хэш-сумме) с использованием официальных баз данных (например, Национальный уязвимостей) составьте его криминалистическую характеристику для внесения в экспертно-криминалистический учет».
Задание 2 (ПК-9): «Составьте вводную часть заключения эксперта по факту несанкционированного доступа к информации, соблюдая требования к защите конфиденциальных данных: замаскируйте персональные данные фигурантов, присвойте документу соответствующий гриф».

3. Задания для самостоятельной работы и интерактивных форм занятий
Направлены на углубленное изучение нормативной базы и отработку навыков в условиях, приближенных к реальным.
Самостоятельная работа (ПК-9): Подготовка аналитической справки на тему: «Сравнительный анализ составов преступлений, предусмотренных ст. 272, 273, 274 УК РФ, с точки зрения предмета доказывания и роли судебной экспертизы».
Интерактивное занятие (деловая игра) (ПК-8, ПК-9): Проведение ролевой игры «Судебное заседание по делу о нарушении ИБ», где студенты выступают в ролях эксперта, обвинителя и защитника, аргументируя свои позиции на основе нормативных актов и результатов модельной экспертизы.

Система оценки качества освоения дисциплины
Оценка качества освоения дисциплины и уровня сформированности компетенций осуществляется посредством следующих видов контроля:
Текущий контроль успеваемости: Проводится на практических и семинарских занятиях в форме устного опроса, защиты практических заданий, решения ситуационных задач и тестирования.
Промежуточная аттестация (по модулям): Проводится в форме контрольной работы, направленной на комплексную проверку знаний и умений по ключевым разделам дисциплины.
Итоговая аттестация: Проводится в форме зачета, который представляет собой комплексное испытание, включающее теоретический вопрос и практическую задачу, и оценивает конечный уровень сформированности компетенций ПК-8 и ПК-9.

Оценка качества образовательного процесса
В соответствии с Положением о порядке проведения текущего контроля успеваемости и промежуточной аттестации студентов КРСУ, обучающимся предоставляется возможность анонимного анкетирования с целью оценки содержания, организации и качества учебного процесса по дисциплине.

5.4. Перечень видов оценочных средств

Для контроля уровня сформированности компетенций ПК-8 и ПК-9 в процессе освоения дисциплины используются следующие виды оценочных средств:

Наименование оценочного средства Проверяемые компетенции Краткая характеристика и направленность задания
Контрольная работа ПК-8, ПК-9 Комплексный анализ смоделированного инцидента информационной безопасности. Направлена на проверку умения классифицировать угрозы, определять нарушенные нормы права, формулировать данные для экспертно-криминалистического учета и анализировать соблюдение режима секретности.
Практические работы ПК-8, ПК-9 Серия работ, моделирующих профессиональные задачи эксперта:
• Работа №1 (ПК-8): Работа со справочно-информационными системами (базы уязвимостей, вредоносного ПО) для

идентификации и криминалистического описания угроз.
• Работа №2 (ПК-9): Составление процессуальных документов (фрагменты заключений, постановлений) с соблюдением требований по защите конфиденциальной информации и нанесению соответствующих грифов.
Самостоятельная работа ПК-9 Подготовка аналитического обзора или реферата, посвященного изучению нормативно-правовой базы (ФЗ "О государственной тайне", ведомственные акты) и алгоритмов действий эксперта при работе со сведениями ограниченного доступа.
Зачет ПК-8, ПК-9 Комплексная форма итогового контроля, состоящая из:
• Теоретического вопроса на знание законодательства в области защиты государственной тайны и информации.
• Практической ситуационной задачи, требующей применения знаний о ведении экспертно-криминалистических учетов и информационно-поисковых системах.

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

6.1. Рекомендуемая литература

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Обеспечение информационной безопасности организации	http://www.iccwbo.ru/blog/2016/obespechenie-
Э2	Информационная безопасность	https://pirit.biz/reshenija/informacionnaja-bezopasnost
Э3	Криптографические методы защиты информации	https://www.sites.google.com/site/anisimovkhv/learning
Э4	Нормативно-правовые акты информационной безопасности.	http://kibevs.tusur.ru/sites/default/files/upload/manuals/
Э5	Веб-сайт системы федеральных образовательных порталов	http://www.edu.ru
Э6	Научная электронная библиотека	http://www.elibrary.ru
Э7	ЭБС IPR BOOKS	http://www.iprbookshop.ru/

6.3. Перечень информационных и образовательных технологий

6.3.1 Компетентностно-ориентированные образовательные технологии

6.3.1.1	В соответствии с требованиями ФГОС ВО и для эффективного формирования профессиональных компетенций ПК-8 и ПК-9 у студентов специалитета "Судебная экспертиза" применяется комплекс образовательных технологий, сочетающий традиционные и инновационные подходы.
6.3.1.2	Интерактивные технологии (не менее 40% аудиторных занятий)
6.3.1.3	Деловые игры:
6.3.1.4	"Судебное заседание по делу о нарушении ИБ" - отработка процедуры экспертного заключения
6.3.1.5	"Расследование инцидента информационной безопасности" - междисциплинарный кейс
6.3.1.6	Ролевые игры по процедурам соблюдения режима секретности
6.3.1.7	Кейс-метод:
6.3.1.8	Анализ реальных судебных дел по ст. 271-273 УК КР
6.3.1.9	Решение ситуационных задач по нарушениям режима секретности
6.3.1.10	Кейсы по исследованию цифровых следов компьютерных преступлений
6.3.1.11	Авторские case-study по способам защиты информации
6.3.1.12	Компьютерные симуляции:
6.3.1.13	Виртуальные лабораторные работы по криптографическим методам защиты
6.3.1.14	Симулятор аудита информационной безопасности
6.3.1.15	Тренажер по работе с экспертным программным обеспечением
6.3.1.16	Проектные технологии
6.3.1.17	Разработка моделей систем защиты информации для государственных учреждений
6.3.1.18	Создание методик проведения судебных компьютерно-технических экспертиз

6.3.1.19	Проектирование систем экспертно-криминалистического учета
6.3.1.20	Традиционные технологии (модернизированные)
6.3.1.21	Проблемные лекции с разбором сложных случаев из судебной практики
6.3.1.22	Практические занятия репродуктивного типа для освоения базовых способов действий
6.3.1.23	Практикумы по работе с средствами криптографической защиты информации
6.3.1.24	Семинары-дискуссии по сравнительному анализу законодательства КР и РФ
6.3.1.25	Информационно-коммуникационные технологии
6.3.1.26	Электронный курс с видео-лекциями и интерактивными материалами
6.3.1.27	Виртуальные лаборатории для практических работ
6.3.1.28	Online-тестирование и система автоматической проверки заданий
6.3.1.29	Использование специализированного ПО для судебных экспертов
6.3.1.30	Цифровой образовательный контур с использованием онлайн-платформ (Quizlet), облачных хранилищ и мессенджеров для оперативного сопровождения
6.3.1.31	Авторские педагогические технологии
6.3.1.32	Визуализация сложного материала с помощью интерактивных схем и ментальных карт
6.3.1.33	Гибридная форма обучения с использованием платформы СДО МУДЛ «Цифровой КРСУ»
6.3.1.34	Интеграция реальных задач юридической и экспертной практики в учебный процесс
6.3.1.35	Технологии самостоятельной работы
6.3.1.36	Работа с базами данных нормативно-правовых актов КР и РФ
6.3.1.37	Подготовка аналитических справок по судебной практике
6.3.1.38	Дистанционные консультации через систему LMS
6.3.1.39	Выполнение виртуальных практикумов
6.3.1.40	Оценочные технологии:
6.3.1.41	Портфолио учебных достижений
6.3.1.42	Защита проектов с участием практикующих экспертов
6.3.1.43	Сквозной кейс-чемпионат по расследованию киберпреступлений
6.3.1.44	Экзамен в форме решения комплексной профессиональной задачи
6.3.1.45	Данный комплекс образовательных технологий обеспечивает формирование системного мышления и способности к практическому применению полученных знаний в профессиональной деятельности судебного эксперта, что соответствует требованиям современной цифровой экономики и потребностям правоприменительной практики.
6.3.2 Перечень информационных справочных систем и программного обеспечения	
6.3.2.1	Программное обеспечение, используемое при освоении дисциплины
6.3.2.2	Базовое программное обеспечение:

6.3.2.3	Операционные системы: Windows 10/11
6.3.2.4	Пакет Microsoft Office: Word, Excel, PowerPoint, Access
6.3.2.5	Средства разработки и анализа: Python с библиотеками криптографии
6.3.2.6	Специализированное программное обеспечение для судебно-экспертной деятельности:
6.3.2.7	StegoTC G2 TC - для анализа стеганографических методов
6.3.2.8	S-Tools (Steganography Tools) - для исследования скрытых каналов передачи информации
6.3.2.9	FTK Imager - для создания и анализа образов цифровых носителей
6.3.2.10	Autopsy - для комплексного анализа цифровых следов
6.3.2.11	Wireshark - для анализа сетевого трафика
6.3.2.12	Технические средства обучения
6.3.2.13	Интерактивная доска Whiteboard DualPenS
6.3.2.14	Система видеоконференцсвязи для дистанционных занятий
6.3.2.15	Компьютерные классы с доступом к специализированному ПО
6.3.2.16	Информационно-справочные системы
6.3.2.17	Правовые базы данных:
6.3.2.18	ициальные интернет-порталы правовой информации Кыргызской Республики
6.3.2.19	Государственные информационно-справочные системы в сфере ИБ
6.3.2.20	Базы данных судебной практики по киберпреступлениям
6.3.2.21	Специализированные ресурсы:
6.3.2.22	Национальный центр обработки инцидентов КР
6.3.2.23	Базы данных уязвимостей и вредоносного ПО
6.3.2.24	Открытые образовательные ресурсы по криптографии и защите информации
6.3.2.25	Организация доступа
6.3.2.26	Обеспечен круглосуточный доступ к сети «Интернет» для самостоятельной работы
6.3.2.27	Дистанционный доступ к электронным образовательным ресурсам через СДО МУДЛ «Цифровой КРСУ»
6.3.2.28	Возможность удаленной работы со специализированным ПО через облачные сервисы
6.3.2.29	Перспективы развития
6.3.2.30	Планируется интеграция с MS Teams для организации collaborative learning
6.3.2.31	Внедрение виртуальных лабораторий для практических работ
6.3.2.32	Развитие мобильного доступа к образовательным ресурсам
6.3.2.33	Примечание: Перечень программного обеспечения регулярно актуализируется в соответствии с развитием технологий и потребностями судебно-экспертной практики.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Учебные аудитории для проведения занятий лекционного типа

7.2	Аудитории, оборудованные мультимедийными проекторами и экранами
7.3	Лекционные залы с интерактивными досками (Whiteboard DualPenS)
7.4	Система усиления звука для презентаций и видео-материалов
7.5	Специализированная аудитория 314 для лекций и практических занятий
7.6	Компьютерные классы для практических занятий
7.7	Специализированные компьютерные классы с ПК не менее 15 рабочих мест
7.8	Установленное базовое ПО: ОС Windows, Microsoft Office
7.9	Специализированное ПО: StegoTC G2 TC, S-Tools, FTK Imager, Autopsy, Wireshark
7.10	Наличие лицензионного программного обеспечения
7.11	Обеспечение регулярного обновления ПО и антивирусной защиты
7.12	Лабораторное оборудование
7.13	Мобильные лабораторные комплексы для исследования компьютерной техники
7.14	Устройства для создания образов цифровых носителей
7.15	Сетевое оборудование для моделирования корпоративных сетей
7.16	Криптографические средства защиты информации
7.17	Переносной мультимедийный комплекс для выездных занятий
7.18	Технические средства обучения
7.19	Интерактивные панели и доски для визуализации учебного материала
7.20	Документ-камеры для демонстрации работы с техническими средствами
7.21	Системы видеоконференцсвязи для дистанционного обучения
7.22	Планшеты и мобильные устройства для мобильного обучения
7.23	Библиотечный фонд и электронные ресурсы
7.24	Читальные залы с рабочими местами, оснащенными компьютерами
7.25	Доступ к электронной библиотечной системе КРСУ
7.26	Подписка на специализированные базы данных и периодические издания
7.27	Аудитория 504 - читальный зал библиотеки на 40 посадочных мест с 18 компьютерами
7.28	Информационно-телекоммуникационная инфраструктура
7.29	Высокоскоростной доступ к сети Интернет во всех учебных аудиториях
7.30	Защищенные каналы связи для работы с конфиденциальной информацией
7.31	Корпоративная сеть КРСУ с доступом к электронным образовательным ресурсам
7.32	Система дистанционного обучения "Цифровой КРСУ"
7.33	Обеспечение доступности для лиц с ограниченными возможностями здоровья
7.34	Специально оборудованные рабочие места в компьютерных классах
7.35	Пандусы и лифты в учебных корпусах
7.36	Адаптированные образовательные материалы и программное обеспечение
7.37	Материально-техническая база соответствует требованиям реализации компетентностного подхода и обеспечивает формирование практических навыков в области информационной безопасности и судебной экспертизы.

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

1. Организация аудиторной работы

Лекционные занятия:
Изучите план лекции заранее, ознакомьтесь с основными понятиями темы
Во время лекции ведите конспект, выделяя ключевые положения и термины
Используйте рекомендованные источники для углубленного изучения материала
Активно участвуйте в обсуждениях, задавайте уточняющие вопросы

Практические занятия:
Подготовьтесь к занятию: изучите теоретический материал и методические указания
Имейте при себе необходимые материалы: методички, нормативные документы, зачетную книжку
Выполняйте задания последовательно, следуя предложенному алгоритму
Используйте специализированное ПО в аудиториях 304, 305

Самостоятельная работа
Работа с литературой
Составьте индивидуальный график изучения материалов
Используйте различные источники: учебники, научные статьи, нормативные акты

Ведте тематический словарь терминов и понятий
Регулярно работайте с электронной библиотечной системой КРСУ

Выполнение расчетно-практических работ (РПР)
Выбирайте тему в соответствии с профессиональными интересами
Составьте детальный план работы и согласуйте с преподавателем
Систематически работайте над РПР в течение семестра
Соблюдайте сроки выполнения этапов работы

Подготовка к контрольным мероприятиям

Текущий контроль
Регулярно повторяйте пройденный материал
Выполняйте все предусмотренные задания
Анализируйте ошибки и затруднения

Рубежный контроль
Составьте план подготовки к каждому модулю
Используйте различные формы повторения материала
Выполняйте типовые задания по каждой теме

Промежуточный контроль
Начните подготовку заблаговременно
Повторите основные понятия и методы работы
Прорешайте задания из пройденных РПР

Работа с электронными ресурсами
Электронная образовательная среда

Регулярно проверяйте обновления в СДО "Цифровой КРСУ"
Используйте электронные курсы для повторения материала
Участвуйте в онлайн-консультациях и обсуждениях
Специализированное программное обеспечение
Осваивайте возможности специализированного ПО
Используйте демо-версии для домашней подготовки
Изучайте руководства пользователя и методические материалы

Формирование профессиональных компетенций

Развитие практических навыков
Участвуйте в деловых играх и case-study
Анализируйте реальные ситуации из судебной практики
Осваивайте современные методы исследования цифровых следов

Работа с нормативной базой
Изучайте актуальные версии нормативных документов
Следите за изменениями в законодательстве
Анализируйте правоприменительную практику

Рекомендации по организации времени
Планирование учебной деятельности:
Составьте семестровый план работы
Еженедельно корректируйте планы
Равномерно распределяйте учебную нагрузку

Эффективная работа с информацией:
Используйте различные методы конспектирования
Развивайте навыки критического анализа
Применяйте техники запоминания и повторения

Критерии успешного освоения дисциплины:
Систематическое посещение аудиторных занятий
Своевременное выполнение всех видов работ
Активная работа на практических занятиях
Успешное прохождение контрольных мероприятий
Умение применять полученные знания в профессиональном контексте

Дополнительные рекомендации:

Участвуйте в научных мероприятиях кафедры
Используйте возможности дополнительного образования
Консультируйтесь с преподавателем при возникновении трудностей
Формируйте профессиональное портфолио достижений
Следование данным методическим указаниям позволит успешно освоить дисциплину и сформировать необходимые профессиональные компетенции.

ТЕХНОЛОГИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ:

СИСТЕМА КОНТРОЛЯ И ОЦЕНКИ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ
1. Текущий контроль
Посещение и активность на аудиторных занятиях
Выполнение обязательных заданий для самостоятельной работы
Работа на практических занятиях и лабораторных работах
Тестирование по отдельным темам дисциплины
2. Рубежный контроль
Контрольные работы по модулям дисциплины
Защита практических работ и проектов
Модульные тестовые задания
Проверка расчетно-практических работ
3. Промежуточный контроль (экзамен в 9 семестре)
Комплексная проверка знаний по всем модулям дисциплины
Соответствие требованиям ФГОС ВО и профессиональным стандартам

КРИТЕРИИ ОЦЕНКИ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
Теоретическая часть (20-25 баллов):
Правильное определение основных понятий и терминов
Владение специальной терминологией
Понимание принципов информационной безопасности
Знание нормативно-правовой базы КР и РФ
Практическая часть (25-30 баллов):
Умение применять методы защиты информации
Навыки работы со специализированным программным обеспечением
Способность анализировать и решать профессиональные задачи
Качество интерпретации результатов

ОРГАНИЗАЦИЯ УЧЕБНОГО ПРОЦЕССА
Подготовка к занятиям:
Изучение конспектов лекций и рекомендованной литературы
Работа с глоссарием и методическими указаниями
Использование электронных образовательных ресурсов
Подготовка к практическим занятиям по методическим рекомендациям

Практические занятия:
Проводятся в специализированных аудиториях 304, 305, 313
Оборудованы персональными компьютерами и специализированным ПО
Направлены на формирование профессиональных умений и навыков
Включают работу с криминалистическим оборудованием и программными комплексами

САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ
Расчетно-практическая работа (РПР):
Самостоятельное исследование по актуальным проблемам информационной безопасности
Этапы выполнения: выбор темы, подбор источников, анализ информации, оформление отчета
Цели: систематизация знаний, развитие аналитических способностей, формирование исследовательских компетенций

Методическое обеспечение:
Электронные курсы и образовательные платформы
Специализированное программное обеспечение
Базы данных и справочно-правовые системы
Методические рекомендации по всем видам работ

ПОРЯДОК ОТРАБОТКИ ПРОПУЩЕННЫХ ЗАНЯТИЙ
Пропуски по уважительной причине - отработка по индивидуальному графику
Пропуски без уважительной причины - обязательная отработка в установленные сроки
Формы отработки: устный опрос, письменные работы, тестирование, дополнительные задания
Контроль со стороны деканата и кафедры за своевременностью отработок

РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ
Тестовые работы:
Комплексная подготовка по ключевым темам дисциплины
Развитие аналитического мышления и способности к рассуждению
Рациональное распределение времени при выполнении заданий
Использование методики "от простого к сложному"
Практические и контрольные работы:
Следование методическим рекомендациям
Применение профессионального программного обеспечения
Соответствие требованиям к оформлению работ
Качественная интерпретация полученных результатов

ОСОБЫЕ УСЛОВИЯ
Студенты - от и с более 60 баллами по текущему и рубежному контролю могут быть освобождены от ответа на экзамене
Использование справочных материалов и технических средств на контрольных мероприятиях

Индивидуальный подход к студентам с ограниченными возможностями здоровья
Технологическая карта обеспечивает прозрачность системы оценки и способствует качественному освоению дисциплины в соответствии с требованиями ФГОС ВО и профессиональными стандартами.