МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОСВЕЩЕНИЯ»
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОСВЕЩЕНИЯ)

Юридический факультет
Кафедра уголовного права, уголовного процесса и криминалистики

Согласовано
деканом юридического факультета
«18» марта 2026 г.
_____
/Узденов Ш.Ш./

Рабочая программа модуля

Особенности квалификации и расследования преступлений в сфере информационных технологий

Направление подготовки
40.04.01 Юриспруденция

Программа подготовки:
Криминалистика и уголовное судопроизводство

Квалификация
Магистр

Форма обучения
Очная

Согласовано учебно-методической
комиссией юридического факультета
Протокол «13» марта 2026 г. № 7
Председатель УМКом_____
/Софинская Е.Д./

Рекомендовано кафедрой уголовного права,
уголовного процесса и криминалистики
Протокол от «27» февраля 2026 г. № 6
Зав. кафедрой_____
/Москалев М.А./

Москва
2026

Авторы-составители:
Дукманов М.В., кандидат юридических наук, доцент
Колесова А.С., кандидат юридических наук, доцент

Рабочая программа модуля «Особенности квалификации и расследования преступлений в сфере информационных технологий» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 40.04.01 Юриспруденция, утверждённого приказом МИНОБРНАУКИ РОССИИ от 25.11.2020 г. №1451.

Модуль входит в часть, формируемую участниками образовательных отношений, Блока 1 «Дисциплины (модули)» и является обязательным для изучения.

Модуль состоит из дисциплин: «Особенности квалификации и расследования преступлений в сфере компьютерной информации» и «Актуальные проблемы квалификации и расследования преступлений, совершенных с использованием информационных технологий».

Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

Год начала подготовки (по учебному плану) 2026.

СОДЕРЖАНИЕ

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

1.1 Цель освоения модуля

Цель освоения модуля «Особенности квалификации и расследования преступлений в сфере информационных технологий» состоит в формировании у студентов твердых знаний о правовых основаниях и содержании актуальных проблем и особенностей квалификации и расследования преступлений в сфере информационных технологий.

Задачи дисциплины:

- Формирование знаний о понятии, сущности и составе преступлений в сфере информационных технологий.
- Формирование научно обоснованного подхода к проблемам квалификации преступлений в сфере информационных технологий.
- Изучение основных положений о квалификации преступлений в сфере информационных технологий с целью последующего использования полученных знаний и умений в самостоятельной научной и практической профессиональной деятельности в сфере обеспечения безопасности личности, общества, государства.
- Формирование у обучающихся компетенций, установленных образовательной программой в соответствии с ФГОС ВО.
- Овладение обучающимися знаниями, умениями, навыками и опытом деятельности, характеризующими процесс формирования компетенций и обеспечивающими достижение планируемых результатов освоения данного модуля.

1.2 Планируемые результаты обучения

В результате освоения данной дисциплины у обучающихся формируются следующие компетенции:

По модулю «Особенности квалификации и расследования преступлений в сфере информационных технологий»:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

СПК-2. Способен квалифицированно применять нормативные правовые акты и реализовывать нормы материального и процессуального права в профессиональной деятельности.

СПК-4. Способен консультировать по вопросам законодательства, требующим специальных знаний, давать квалифицированные разъяснения и заключения по вопросам применения действующих правовых норм.

По дисциплине «Особенности квалификации и расследования преступлений в сфере компьютерной информации»:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

СПК-4. Способен консультировать по вопросам законодательства, требующим специальных знаний, давать квалифицированные разъяснения и заключения по вопросам применения действующих правовых норм.

По дисциплине «Актуальные проблемы квалификации и расследования преступлений, совершенных с использованием информационных технологий»:

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

СПК-2. Способен квалифицированно применять нормативные правовые акты и реализовывать нормы материального и процессуального права в профессиональной деятельности.

2. МЕСТО МОДУЛЯ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Модуль входит в часть, формируемую участниками образовательных отношений, Блока 1 «Дисциплины (модули)» и является обязательным для изучения.

Модуль состоит из дисциплин: «Особенности квалификации и расследования преступлений в сфере компьютерной информации» и «Актуальные проблемы квалификации и расследования преступлений, совершенных с использованием информационных технологий».

Модуль «Особенности квалификации и расследования преступлений в сфере информационных технологий» имеет тесные связи с такими дисциплинами как: «Национальная безопасность и основные направления устойчивого развития Российской Федерации», «Правовое обеспечение информационной безопасности», «Теоретические основы квалификации преступлений», «Особенности процессуальной деятельности органов дознания и предварительного следствия».

Приступая к изучению данного модуля, студенты должны понимать, уметь анализировать, правильно толковать правовые нормы, владеть навыками работы с нормативными правовыми актами с целью последующего их практического применения.

В рамках изучения данного модуля могут быть предусмотрены встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов.

Освоение данного курса является важным элементом подготовки магистрантов в области юриспруденции. Знания и навыки, полученные при изучении модуля, будут полезны обучающимся в последующей правоохранительной, исследовательской и научно-

п

е Указанные связи и содержание дисциплин модуля «Особенности квалификации и р расследования преступлений в сфере информационных технологий» дают обучающемуся а системное представление о комплексе изучаемых дисциплин в соответствии с ФГОС ВО, что о обеспечивает соответственный теоретический уровень и практическую направленность в о системе обучения будущей деятельности магистра юриспруденции.

г

и

3. ОБЪЕМ И СОДЕРЖАНИЕ МОДУЛЯ

ч

3.1 Объем модуля

е **Модуль «Особенности квалификации и расследования преступлений в сфере а информационных технологий»**

к **Показатель объема модуля**	**Форма обучения**
о	**Очная**
й Объем модуля в зачетных единицах	5
Объем модуля в часах	180 (62)[1]
д Контактная работа:	82,7 (54,4)[2]
е Лекции	40 (40)[3]
я Практические занятия	40 (12)[4]
Т Контактные часы на промежуточную аттестацию:	2,7 (2,4)[5]
е Контрольная работа	0,4 (0,4)[6]
л Экзамен	0,3
Б Предэкзаменационная консультация	2 (2)[7]
н Самостоятельная работа	80

о

с

т

и

[1] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[2] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[3] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[4] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[5] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[6] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[7] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

Контроль	17,3 (7,6)[8]

Формы промежуточной аттестации:

По дисциплине «Особенности квалификации и расследования преступлений в сфере компьютерной информации» – контрольная работа в 3 семестре.

По дисциплине «Актуальные проблемы квалификации и расследования преступлений, совершенных с использованием информационных технологий» – контрольная работа в 4 семестре.

По модулю «Особенности квалификации и расследования преступлений в сфере информационных технологий» – экзамен в 4 семестре.

Объем дисциплины «Особенности квалификации и расследования преступлений в сфере компьютерной информации»

Показатель объема дисциплины	**Форма обучения**
	Очная
Объем дисциплины в зачетных единицах	2
Объем дисциплины в часах	72 (30)[9]
Контактная работа:	36,2 (26,2)[10]
Лекции	18 (18)[11]
Практические занятия	18 (8)[12]
Контактные часы на промежуточную аттестацию:	0,2 (0,2)[13]
Контрольная работа	0,2 (0,2)[14]
Самостоятельная работа	32
Контроль	3,8 (3,8)[15]

Форма промежуточной аттестации по дисциплине: контрольная работа в 3 семестре.

Объем дисциплины «Актуальные проблемы квалификации и расследования преступлений, совершенных с использованием информационных технологий»

Показатель объема дисциплины	**Форма обучения**
	Очная
Объем дисциплины в зачетных единицах	2
Объем дисциплины в часах	72 (30)[16]
Контактная работа:	44,2 (26,2)[17]
Лекции	22 (22)[18]
Практические занятия	22 (4)[19]
Контактные часы на промежуточную аттестацию:	0,2 (0,2)[20]
Контрольная работа	0,2 (0,2)[21]
Самостоятельная работа	24

[8] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[9] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[10] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[11] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[12] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[13] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[14] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[15] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[16] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[17] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[18] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[19] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[20] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[21] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

Контроль	3,8 (3,8)[22]

Форма промежуточной аттестации по дисциплине: контрольная работа в 4 семестре.

3.2 Содержание модуля

Дисциплина «Особенности квалификации и расследования преступлений в сфере компьютерной информации»

Наименование разделов (тем) дисциплины с кратким содержанием	**Кол-во часов**	
	Лекции	**Практические занятия**
Тема 1. Преступления в сфере компьютерной информации - новый вид преступных посягательств в уголовном законодательстве Российской Федерации Сложность в квалификации деяний, совершенных в сфере компьютерной информации. Соотношение состава неправомерного доступа к компьютерной информации и состава создания, использования и распространения вредоносных компьютерных программ по объективным и субъективным признакам. Разграничение составов неправомерного доступа к компьютерной информации и нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Соотношение со смежными составами.	4	4 (4)[23]
Тема 2. Информационные отношения как объект уголовно-правовой охраны Понятие родового объекта преступных посягательств в сфере компьютерной информации. Понятие предмета компьютерного преступления. Понятие и виды преступлений в сфере компьютерной информации.	2	2
Тема 3. Виды и способы совершения преступлений в сфере компьютерной информации Многообразие способов совершения преступлений в сфере компьютерной информации. Классификация способов совершения компьютерных преступлений по законодательству России. Сложность в квалификации деяний, совершенных в сфере компьютерной информации. Перечень смежных составов, предусматривающих неправомерное обращение с информацией по уголовному кодексу Российской Федерации. Проблема ответственности за компьютерное мошенничество.	4	4 (4)[24]
Тема 4. Вопросы уголовной ответственности за неправомерный доступ к компьютерной информации. Характеристика объективных признаков составов преступлений. Понятие охраняемой законом компьютерной информации. Понятие «вируса» и «вредоносной» компьютерной программы. Характеристика субъективных признаков составов преступлений. Совершение неправомерного доступа к компьютерной информации по	2	2

[22] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[23] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[24] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

неосторожности. Особенности субъекта преступлений.		
Тема 5. Типология личности компьютерного преступника Особенности субъектов компьютерных преступлений. Классификация субъектов компьютерных преступлений. Личностный аспект субъекта компьютерного преступления. Основные характеристики личности компьютерного преступника.	2	2
Тема 6. Мировой опыт правового регулирования предупреждения преступности в сфере компьютерной информации Международное сотрудничество как форма борьбы с преступностью в сфере компьютерной информации. Понятие, задачи и средства комплексного контроля над преступностью в сфере компьютерной информации. Международный опыт борьбы с преступлениями в сфере компьютерной информации. Опыт правового регулирования общественных отношений в сфере компьютерной информации в Российской Федерации.	4	4
Итого	**18 (18)[25]**	**18 (8)[26]**

Дисциплина «Актуальные проблемы квалификации и расследования преступлений, совершенных с использованием информационных технологий»

Наименование разделов (тем) дисциплины с кратким содержанием	**Кол-во часов**	
	Лекции	**Практические занятия**
Тема 1. Информационное обеспечение борьбы с преступлениями в области информационных технологий. Информационное обеспечение борьбы с преступлениями, связанными с подделкой документов. Информационное обеспечение международного розыска лиц. Общие положения.	2	2 (2)[27]
Тема 2. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Ст. 272 УК РФ. Неправомерный доступ к компьютерной информации. Ст. 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ. Ст. 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Анализ объективных и субъективных признаков.	4	4 (2)[28]
Тема 3. Понятие и отличительные особенности киберпреступности. Кибертерроризм в России: его свойства и особенности. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности. Кибертерроризм как реальная угроза внешнему и внутреннему контурам национальной безопасности России. Ответственность за киберпреступления. Зарубежная практика по формированию	4	4

[25] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[26] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[27] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[28] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

борьбы с кибермошенничеством. Российская практика противодействия кибермошенничеству.		
Тема 4. Мошенничество в сфере компьютерной информации (статья 159.6 УК РФ). Общая характеристика преступления ст. 159.6 УК РФ. Уголовно-правовой анализ. Выделение объекта, объективной стороны, субъекта, субъективной стороны. Проблемы квалификации. Анализ правоприменения. Криминологическая характеристика лиц, совершающих деяния, предусмотренные статьей 159.6 УК РФ. Риски недостаточного обеспечения информационной безопасности.	2	2
Тема 5. Криминалистическая характеристика компьютерных преступлений. Проблемы криминалистической тактики при расследовании преступлений, предусмотренных главой 28 УК РФ. Высокая латентность указанных преступлений и причины. Сложность сбора доказательств и процесса доказывания. Широкий спектр криминалистически значимых признаков преступлений. Отсутствие единой программы борьбы с киберпреступлениями. Сложность расследования и раскрытия компьютерных преступлений. Отсутствие обобщенной судебной и следственной практики по делам данной категории. Нехватка высокопрофессиональных специалистов, представителей правоохранительных органов.	4	4
Тема 6. Современная уголовная политика в сфере борьбы с компьютерными преступлениями. Понятие и многоаспектность компьютерных преступлений. Наиболее распространенные преступления, совершаемые с использованием компьютерной техники: хакерство, компьютерное мошенничество, распространение вредоносных программ, компьютерное пиратство. Цели и задачи уголовной политики в сфере противодействия компьютерной преступности. Правовая основа противодействия компьютерной преступности.	4	4
Тема 7. Криминалистические и иные (междисциплинарные) средства противодействия преступлениям в сфере экономической деятельности с использованием современных информационных технологий. Программы обеспечения информационной безопасности. Проблемы защиты объектов собственности, в том числе и интеллектуальной, в сфере экономической деятельности.	2	2
Итого	**22 (22)[29]**	**22 (4)[30]**

[29] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[30] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Дисциплина «Особенности квалификации и расследования преступлений в сфере компьютерной информации»

Темы для самостоятельного изучения	Изучаемые вопросы	Кол-во часов	Формы самостоятельной работы	Методическое обеспечение	Формы отчетности
Тема 1. Преступления в сфере компьютерной информации - новый вид преступных посягательств в уголовном законодательстве Российской Федерации	1. Сложность в квалификации деяний, совершенных в сфере компьютерной информации. 2. Соотношение состава неправомерного доступа к компьютерной информации и состава создания, использования и распространения вредоносных компьютерных программ по объективным и субъективным признакам. 3. Разграничение составов неправомерного доступа к компьютерной информации и нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. 4. Соотношение со смежными составами.	6	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад
Тема 2. Информационные отношения как объект уголовно-правовой охраны	1. Понятие родового объекта преступных посягательств в сфере компьютерной информации. 2. Понятие предмета компьютерного преступления. 3. Понятие и виды преступлений в	4	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад

	сфере компьютерной информации.				
Тема 3. Виды и способы совершения преступлений в сфере компьютерной информации	1. Многообразие способов совершения преступлений в сфере компьютерной информации. 2. Классификация способов совершения компьютерных преступлений по законодательству России. 3. Сложность в квалификации деяний, совершенных в сфере компьютерной информации. 4. Перечень смежных составов, предусматривающих неправомерное обращение с информацией по уголовному кодексу Российской Федерации. 5. Проблема ответственности за компьютерное мошенничество.	6	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад
Тема 4. Вопросы уголовной ответственности за неправомерный доступ к компьютерной информации.	1. Характеристика объективных признаков составов преступлений. 2. Понятие охраняемой законом компьютерной информации. 3. Понятие «вируса» и «вредоносной» компьютерной программы. 4. Характеристика субъективных признаков составов преступлений. 5. Совершение неправомерного доступа к компьютерной информации по неосторожности.	6	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад

	6. Особенности субъекта преступлений				
Тема 5. Типология личности компьютерного преступника	1. Особенности субъектов компьютерных преступлений. 2. Классификация субъектов компьютерных преступлений. 3. Личностный аспект субъекта компьютерного преступления. 4. Основные характеристики личности компьютерного преступника.	4	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад
Тема 6. Мировой опыт правового регулирования предупреждения преступности в сфере компьютерной информации	1. Международное сотрудничество как форма борьбы с преступностью в сфере компьютерной информации. 2. Понятие, задачи и средства комплексного контроля над преступностью в сфере компьютерной информации. 3. Международный опыт борьбы с преступлениями в сфере компьютерной информации. 4. Опыт правового регулирования общественных отношений в сфере компьютерной информации в Российской Федерации.	6	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад
Итого		**32**			

Дисциплина «Актуальные проблемы квалификации и расследования преступлений, совершенных с использованием информационных технологий»

Темы для самостоятельного изучения	Изучаемые вопросы	Кол-во часов	Формы самостоятельной работы	Методическое обеспечение	Форма отчетности
Тема 1. Информационное обеспечение борьбы	1. Информационное обеспечение борьбы с преступлениями,	4	Подготовка к занятиям, изучение	Учебно-методическое и ресурсное	Устный опрос, доклад

с преступлениями в области информационных технологий.	связанными с подделкой документов. 2. Информационное обеспечение международного розыска лиц. 3. Общие положения.		литературы и судебной практики, подготовка доклада	обеспечение дисциплины (п. 6.1, 6.2, 6.3)	
Тема 2. Уголовно-правовая характеристика преступлений в сфере компьютерной информации.	1. Ст. 272 УК РФ. Неправомерный доступ к компьютерной информации. 2. Ст. 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ. 3. Ст. 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. 4. Анализ объективных и субъективных признаков.	4	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад
Тема 3. Понятие и отличительные особенности киберпреступности.	1. Кибертерроризм в России: его свойства и особенности. 2. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности. 3. Кибертерроризм как реальная угроза внешнему и внутреннему контурам национальной безопасности России. 4. Ответственность за киберпреступления.	4	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад

	5. Зарубежная практика по формированию борьбы с кибермошенничеством. 6. Российская практика противодействия кибермошенничеству.				
Тема 4. Мошенничество в сфере компьютерной информации (статья 159.6 УК РФ).	1. Общая характеристика преступления ст. 159.6 УК РФ. 2. Уголовно-правовой анализ. 3. Выделение объекта, объективной стороны, субъекта, субъективной стороны. 4. Проблемы квалификации. 5. Анализ правоприменения. 6. Криминологическая характеристика лиц, совершающих деяния, предусмотренные статьей 159.6 УК РФ. 7. Риски недостаточного обеспечения информационной безопасности.	2	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад
Тема 5. Криминалистическая характеристика компьютерных преступлений.	1. Проблемы криминалистической тактики при расследовании преступлений, предусмотренных главой 28 УК РФ. 2. Высокая латентность указанных преступлений и причины. 3. Сложность сбора доказательств и процесса доказывания. 4. Широкий спектр	4	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад

	криминалистически значимых признаков преступлений. 5. Отсутствие единой программы борьбы с киберпреступлениям и. 6. Сложность расследования и раскрытия компьютерных преступлений. 7. Отсутствие обобщенной судебной и следственной практики по делам данной категории. 8. Нехватка высокопрофессионал ьных специалистов, представителей правоохранительных органов.				
Тема 6. Современная уголовная политика в сфере борьбы с компьютерными преступлениями.	1.Понятие и многоаспектность компьютерных преступлений. 2.Наиболее распространенные преступления, совершаемые с использованием компьютерной техники: хакерство, компьютерное мошенничество, распространение вредоносных программ, компьютерное пиратство. 3.Цели и задачи уголовной политики в сфере противодействия компьютерной преступности. 4.Правовая основа противодействия компьютерной преступности.	4	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад

Тема 7. Криминалистические и иные (междисциплинарные) средства противодействия преступлениям в сфере экономической деятельности с использованием современных информационных технологий.	1. Программы обеспечения информационной безопасности. 2. Проблемы защиты объектов собственности в том числе и интеллектуальной в сфере экономической деятельности.	2	Подготовка к занятиям, изучение литературы и судебной практики, подготовка доклада	Учебно-методическое и ресурсное обеспечение дисциплины (п. 6.1, 6.2, 6.3)	Устный опрос, доклад
ИТОГО		**24**			

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.1 Перечень компетенций с указанием этапов их формирования в процессе освоение образовательной программы

Дисциплина «Особенности квалификации и расследования преступлений в сфере компьютерной информации»

Код и наименование компетенции	Этапы формирования
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.	1. Работа на учебных занятиях 2. Самостоятельная работа
СПК-4. Способен консультировать по вопросам законодательства, требующим специальных знаний, давать квалифицированные разъяснения и заключения по вопросам применения действующих правовых норм.	1. Работа на учебных занятиях 2. Самостоятельная работа

Дисциплина «Актуальные проблемы квалификации и расследования преступлений, совершенных с использованием информационных технологий»

Код и наименование компетенции	Этапы формирования
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.	1. Работа на учебных занятиях 2. Самостоятельная работа
СПК-2. Способен квалифицированно применять нормативные правовые акты и реализовывать нормы материального и процессуального права в профессиональной деятельности.	1. Работа на учебных занятиях 2. Самостоятельная работа

5.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оцениваемые компетенции	Уровень сформированности	Этап формирования	Описание показателей	Критерии оценивания	Шкала оценивания
Дисциплина «Особенности квалификации и расследования преступлений в сфере компьютерной информации»					

УК-1	Пороговый	1. Работа на учебных занятиях 2. Самостоятельная работа	**Знать:** правила правоприменения в области уголовного права и уголовно-процессуального права, регулирующие порядок принятия решений и совершения юридических действий. **Уметь:** выбирать соответствующие нормы права, обеспечивающие расследование компьютерных преступлений; толковать нормы уголовного права, уголовно-процессуального права и других отраслей, которые составляют правовую основу расследования компьютерных преступлений; составлять юридические документы.	Устный опрос, доклад	Шкала оценивания устного опроса, Шкала оценивания доклада
	Продвинутый	1. Работа на учебных занятиях 2. Самостоятельная работа	**Знать:** правила правоприменения в области уголовного права и уголовно-процессуального права, регулирующие порядок принятия решений и совершения юридических действий. **Уметь:** выбирать соответствующие нормы права, обеспечивающие расследование компьютерных преступлений; толковать нормы уголовного права, уголовно-процессуального права и других отраслей, которые составляют правовую основу расследования компьютерных преступлений; составлять юридические документы. **Владеть:** навыками принятия решений и совершения юридических действий в точном соответствии с нормами отраслевого законодательства, которые составляют правовую основу расследования компьютерных преступлений; навыками анализа и применения судебной и иной практики в соответствующей отрасли права.	Устный опрос, доклад, тестирование	Шкала оценивания устного опроса, Шкала оценивания доклада, Шкала оценивания тестирования

СПК-4	Пороговый	1.Работа на учебных занятиях. 2.Самостоятельная работа.	**Знать:** - законодательство в сфере в сфере компьютерной информации; - систему и принципы построения и функционирования отношений, складывающихся в сфере компьютерной информации; - основные научные подходы к пониманию права и дискуссионные проблемы современной юридической науки и правоприменительной практики по вопросам преступлений в сфере компьютерной информации. **Уметь:** - консультировать по вопросам законодательства по отношениям в сфере компьютерной информации; - давать квалифицированные разъяснения и заключения по вопросам применения действующих правовых норм по вопросам преступлений в сфере компьютерной информации.	Устный опрос, доклад	Шкала оценивания устного опроса, Шкала оценивания доклада
	Продвинутый	1.Работа на учебных занятиях. 2.Самостоятельная работа**.**	**Знать:** - законодательство в сфере в сфере компьютерной информации; - систему и принципы построения и функционирования отношений, складывающихся в сфере компьютерной информации; - основные научные подходы к пониманию права и дискуссионные проблемы современной юридической науки и правоприменительной практики по вопросам преступлений в сфере компьютерной информации. **Уметь:** - консультировать по вопросам законодательства по отношениям в сфере компьютерной информации; - давать квалифицированные разъяснения и заключения по вопросам применения	Устный опрос, доклад, тестирование	Шкала оценивания устного опроса, Шкала оценивания доклада, Шкала оценивания тестирования

			действующих правовых норм по вопросам преступлений в сфере компьютерной информации. **Владеть:** - навыками разработки и представления собственных вариантов правовых решений в конкретной ситуации или исходя из заданных (поставленных) условий; - способностью к креативному развитию ранее полученных знаний, а также накоплению новых в целях их применения для решения конкретных отношений и вопросов, возникающих в правовой сфере; - навыками систематизации источников, принципов и нормы права для квалифицированного их применения.		
Дисциплина «Актуальные проблемы квалификации и расследования преступлений, совершенных с использованием информационных технологий»					
УК-1	Пороговый	1. Работа на учебных занятиях 2. Самостоятельная работа	**Знать:** процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения при квалификации и расследовании преступлений, совершенных с использованием информационных технологий. **Уметь:** принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий при квалификации и расследовании преступлений, совершенных с использованием информационных технологий.	Устный опрос, доклад	Шкала оценивания устного опроса, Шкала оценивания доклада
	Продвинутый	1. Работа на учебных занятиях 2. Самостоятельная работа	**Знать:** процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения	Устный опрос, доклад, тестирование	Шкала оценивания устного опроса, Шкала оценивания

			при квалификации и расследовании преступлений, совершенных с использованием информационных технологий. **Уметь:** принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий при квалификации и расследовании преступлений, совершенных с использованием информационных технологий. **Владеть:** методами установления причинно-следственных связей и определения наиболее значимых среди них при квалификации и расследовании преступлений, совершенных с использованием информационных технологий; методиками постановки цели и определения способов ее достижения; методиками разработки стратегий действий при проблемных ситуациях.		доклада, Шкала оценивания тестирования
СПК-2	Пороговый	1. Работа на учебных занятиях 2. Самостоятельная работа	**Знать:** способы, виды, стадии реализации правовых актов; содержание норм материального и процессуального права о преступлениях, совершенных с использованием информационных технологий. **Уметь:** использовать нормы материального и процессуального права в профессиональной деятельности; выбирать нормы материального и процессуального права, необходимые для применения в конкретных обстоятельствах дела, при квалификации и расследовании преступлений, совершенных с использованием информационных технологий.	Устный опрос, доклад	Шкала оценивания устного опроса, Шкала оценивания доклада

	Продвинутый	1. Работа на учебных занятиях 2. Самостоятельная работа	**Знать:** способы, виды, стадии реализации правовых актов; содержание норм материального и процессуального права о преступлениях, совершенных с использованием информационных технологий. **Уметь:** использовать нормы материального и процессуального права в профессиональной деятельности; выбирать нормы материального и процессуального права, необходимые для применения в конкретных обстоятельствах дела, при квалификации и расследовании преступлений, совершенных с использованием информационных технологий. **Владеть:** навыками работы с нормами процессуального и материального права в профессиональной деятельности, реализации норм материального и процессуального права в профессиональной деятельности квалификации и расследовании преступлений, совершенных с использованием информационных технологий.	Устный опрос, доклад, тестирование	Шкала оценивания устного опроса, Шкала оценивания доклада, Шкала оценивания тестирования

Описание шкал оценивания

Шкала оценивания тестирования

Критерии оценивания	Баллы
Количество правильных ответов: 11-10	8-10
Количество правильных ответов: 9-7	5-7
Количество правильных ответов: 6-4	3-4
Количество правильных ответов: 3	0-2

Шкала оценивания доклада

Критерии оценивания	Баллы
Содержание доклада соответствует его названию. Доклад оформлен в соответствии с требованиями. В тексте полностью раскрыты ключевые аспекты проблемы, содержится список литературы. Студент хорошо ориентируется в тексте доклада и рассматриваемой проблеме, самостоятельно отвечает на вопросы, не пользуясь текстом доклада или прибегая к нему в минимальном объеме, иллюстрирует свой ответ практическими примерами, делает необходимые обоснованные выводы.	8-10

Содержание доклада соответствует его названию. Доклад оформлен в соответствии с требованиями. В тексте раскрыты ключевые аспекты проблемы, содержится список литературы. Студент ориентируется в тексте доклада и рассматриваемой проблеме, отвечает на вопросы, пользуясь текстом доклада, делает необходимые выводы.	5-7
Содержание доклада соответствует его названию. Доклад оформлен в соответствии с требованиями, содержит список литературы. Студент отвечает на вопросы, пользуясь текстом доклада, делает необходимые обоснованные выводы при условии оказания наводящей помощи.	3-4
Содержание доклада соответствует его названию. Доклад оформлен в соответствии с требованиями, содержит список литературы. Студент отвечает на вопросы, только путем обращения к тексту доклада, делает необходимые выводы только при условии оказания ему активной помощи.	0-2

Шкала оценивания устного опроса

Критерии оценивания	Баллы
Дан верный и исчерпывающий ответ на поставленный вопрос; соблюдается последовательность и логика изложения при ответе; студент правильно использует терминологию; отсутствуют фактические ошибки в ответе.	8-10
В целом, дан верный ответ на поставленный вопрос, однако не все ключевые аспекты затронуты и раскрыты; может незначительно нарушаться последовательность изложения; правильно используется юридическая терминология; отсутствуют фактические ошибки в ответе.	5-7
В целом, дан верный, но неполный ответ на поставленный вопрос; нарушаться последовательность изложения; допущены ошибки в использовании юридической терминологии; прослеживается неясность и нечеткость изложения	3-4
Ответ дан неверный либо студент отказался отвечать на поставленный вопрос	0-2

5.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Дисциплина «Особенности квалификации и расследования преступлений в сфере компьютерной информации»

Примерный перечень вопросов для устного опроса

1. Классификация компьютерных преступлений, предложенная экспертами ООН.
2. Категория объекта в современной уголовно – правовой теории.
3. Понятие информации в различных аспектах.
4. Понятие преступления в сфере компьютерной информации.
5. Основные классификации способов совершения преступлений в сфере компьютерной информации.
6. Понятие охраняемой законом компьютерной информации.
7. Особенности субъекта преступлений в сфере компьютерной информации.
8. Виды охраняемой законом информации.

Примерный перечень тем для докладов

1. Ретроспектива создания первых счетных машин и их модификация в современные компьютеры.

2. Международный опыт противодействия преступлениям в сфере компьютерной информации.

3. Основные этапы межгосударственного сотрудничества в борьбе с преступностью в сфере компьютерной информации.

4. Проблема создания эталонной схемы закона об уголовной ответственности за совершение компьютерных преступлений Organization for Economic Cooperation and Development.

5. Характеристика точек зрения на понятие «компьютерное преступление».

6. Компьютерное преступление как вид информационного преступления, посягающего на информационные отношения.

7. Способы совершения компьютерных преступлений по уголовному законодательству некоторых государств-участников СНГ.

8. Совершение неправомерного доступа к компьютерной информации по неосторожности.

9. Сущность уголовно-правового запрета, установленного собственником на доступ к компьютерной информации.

Примерные задания для тестирования

1. Наименее опасным является следующий тип личности киберпреступника:
○ случайный
○ ситуативный
○ злостный
○ особо злостный

2. Конвенция Совета Европы о преступности в сфере компьютерной информации:
○ не ратифицирована Россией, подпись отозвана
○ не подписывалась Россией
○ подписана и ратифицирована Россией
○ подписана, но не ратифицирована Россией

3. По образовательной, социальной и материальной характеристике личности киберпреступников они схожи с:
○ «беловоротничковыми» преступниками
○ профессиональными преступниками
○ насильственными преступниками
○ «ворами в законе»

4. В уголовном праве РФ преступные деяния должны обладать признаками:
○ общественной опасности и противоправности
○ только общественной опасности
○ только противоправности
○ общественной опасности и (или) противоправности

5. Основным федеральным законом, регулирующим информационный оборот в РФ, является:
○ Федеральный закон РФ «Об информации, информационных технологиях и защите информации»
○ Закон РФ «О средствах массовой информации»
○ Закон РСФСР «Об ответственности за правонарушения при работе с информацией»
○ Федеральный закон РФ «Об информации, информатизации и защите информации»

6. ФЗ «Об информации, информационных технологиях и защите информации» не регулирует отношения, связанные с:

○ защитой авторского права
○ применением информационных технологий
○ осуществлением права на поиск информации
○ обеспечением защиты информации

7. Право на поиск, получение, передачу, производство и распространение информации является:

○ конституционным
○ закреплённым в международных документах
○ закреплённым в федеральном законодательстве
○ не закреплённым в законодательстве

8. Информация в РФ может являться объектом отношений:

○ всех перечисленных
○ публичных
○ гражданских
○ административно-правовых

9. Возможность получения информации и её использования:

○ доступ к информации
○ защита информации
○ право на информацию
○ информационный оборот

10. Отличительным признаком компьютерной информации, согласно УК РФ, является:

○ представление в форме электрических сигналов
○ хранение в машинночитаемой форме
○ обработка в компьютерах
○ передача через компьютерные сети

Примеры заданий для контрольной работы

1 вариант.

Вопрос. Понятие компьютерной информации.

Задача. Боровиков, являясь оператором ЭВМ в одной из организаций, на своем компьютере изготовил электронное почтовое сообщение с рекламой товаров, приложив к нему в качестве подробного каталога с ценами составленную им программу ЭВМ, и распространил ее в сети Интернет 350 адресатам. В результате массового распространения этой программы после ее запуска пользователями сети Интернет, Боровиков несанкционированно получил по своему электронному адресу 87 учетных имен и паролей для доступа в Интернет, которые скопировал на жесткий диск своего компьютера и в дальнейшем использовал для доступа в сеть Интернет.

Квалифицируйте содеянное.

2 вариант.

Вопрос. Виды преступлений в сфере компьютерной информации.

Задача. АО «Окно» разработало и продавало компьютерную игру. При установке игры на компьютер некоторые стандартные драйверы устройств заменялись на драйверы, разработанные АО «Окно», в результате была нарушена нормальная работа нескольких тысяч компьютеров. При установке программа тестировала компьютерное оборудование и

программное обеспечение пользователя, сведения о которых при регистрации с помощью модема сообщались в АО «Окно». В документации к игре не сообщалось об этом.

Квалифицируйте содеянное.

Дисциплина «Актуальные проблемы квалификации и расследования преступлений, совершенных с использованием информационных технологий»

Примерный перечень вопросов для устного опроса

1. Понятие преступлений и правонарушений в сфере информационных технологий.
2. Факторы роста преступлений в сфере информационных технологий.
3. Законодательство России, регламентирующее ответственность за преступления в сфере информационных технологий.
4. Понятие информационной безопасности РФ.
5. Соотношение доктрины информационной безопасности РФ и доктрины национальной безопасности РФ.
6. Основные составляющие национальных интересов России в информационной сфере.
7. Методы обеспечения информационной безопасности: понятие и общая характеристика (правовые, организационно-технические, экономические).
8. Какие преступления в соответствии с действующим уголовным кодексом РФ могут быть отнесены к преступлениям в сфере информационных технологий?
9. Кибертерроризм в России: его свойства и особенности.
10. Проблемы криминалистической тактики при расследовании преступлений, предусмотренных главой 28 УК РФ.

Примерный перечень тем для докладов

1. Использование или принуждение к использованию компьютерных систем для совершения преступлений против собственности.
2. Использование компьютерных технологий в целях извлечения прибыли путем создания финансовых «пирамид» и аналогичных махинаций.
3. Проблемы квалификации мошенничества с использованием банковских пластиковых карт.
4. Раскрытие и распространение сообщений электронной почты, сведений, хранящихся в электронных базах данных.
5. Террористические акты, связанные с деяниями в области информационных технологий.
6. Международное законодательство и законодательство России в области борьбы с преступлениями в сфере информационных технологий: сравнительная характеристика.
7. Актуальные вопросы предупреждения и противодействия преступлениям в сфере информационных технологий

Примерные задания для тестирования

1. Какие преступления относятся к преступлениям в сфере компьютерной информации?

а) создание вредоносных компьютерных программ;

б) распространение порнографических материалов с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

в) проведение азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

г) все ответы правильные.

2. Родовым объектом преступлений в сфере компьютерной информации являются:

а) экономическая безопасность;

б) отношения в сфере охраны авторского права;

в) информационная безопасность;

г) общественная безопасность и общественный порядок.

3. Субъектом преступлений в сфере компьютерной информации является:

а) юридическое или физическое лицо, не имеющие разрешения для работы с информацией определенной категории;

б) физическое, вменяемое лицо, достигшее 18-летнего возраста;

в) физическое, вменяемое лицо, достигшее 16-летнего возраста;

г) физическое лицо, не имеющее права на доступ к компьютеру или информационно-телекоммуникационным сетям.

4. К компьютерной информации относятся:

а) собственно информационные ресурсы (базы данных, текстовые, графические файлы и т.д.), представленные в форме электрических сигналов;

б) программы, обеспечивающие функционирование компьютера или информационно-телекоммуникационных сетей, хранение, обработку и передачу данных;

в) информация на машинном носителе, в компьютере или информационно-телекоммуникационных сетях;

г) все ответы правильные.

5. Преступление, предусмотренное ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» считается оконченным:

а) с момента совершения неправомерного доступа к охраняемой законом компьютерной информации;

б) только в случае уничтожения, блокирования, модификации либо копирования компьютерной информации;

в) только при наступлении тяжких последствий в случае уничтожения, блокирования, модификации либо копирования компьютерной информации;

г) все ответы правильные.

6. В ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» не предусмотрена уголовная ответственность за:

а) внесение изменений в существующие программы;

б) распространение машинных носителей с вредоносными программами;

в) несанкционированное копирование охраняемой законом компьютерной информации;

г) нет правильного ответа.

7. Преступление, предусмотренное ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», считается оконченным:

а) только при наступлении тяжких последствий;

б) только в случае несанкционированного уничтожения, блокирования, модификации либо копирования компьютерной информации;

в) с момента использования или распространения вредоносной программы;

г) с момента создания, использования или распространения вредоносной программы.

8. Субъектом преступления, предусмотренного ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», является:

а) физическое, вменяемое лицо, достигшее 16-летнего возраста;

б) физическое, вменяемое лицо, достигшее 18-летнего возраста;

в) лицо, имеющее право на доступ к компьютеру или информационно-телекоммуникационным сетям;

г) лицо, не имеющее права на доступ к компьютеру или информационно-телекоммуникационным сетям.

9. В числе квалифицирующих признаков в ст. 273 УК РФ предусмотрено совершение данного преступления:

а) с целью скрыть другое преступление или облегчить его совершение;

б) из корыстной заинтересованности;

в) из хулиганских побуждений;

г) по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы.

10. Преступление, предусмотренное ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», считается оконченным:

а) с момента нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

б) с момента уничтожения, блокирования, модификации либо копирования компьютерной информации;

в) если это деяние причинило крупный ущерб;

г) только при наступлении тяжких последствий.

Примеры заданий для контрольной работы

1 вариант.

Вопрос. Ст. 272 УК РФ. Неправомерный доступ к компьютерной информации: общая характеристика.

Задача. Служащий банка «Южный» Игрунков приобрел на рынке компакт–диск с компьютерной игрой «Звездные войны II». На следующий день Игрунков установил игру на своем рабочем компьютере, связанном по сети с другими компьютерами банка. В результате распространения вируса, записанного на компакт–диске, компьютерная система банка была выведена из строя и не могла нормально функционировать более суток, из–за чего банк понес существенные убытки.

Как квалифицировать действия Игрункова?

2 вариант.

Вопрос. Ст. 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ: общая характеристика

Задача. Студент Технического университета Артемов, преодолев ради любопытства систему защиты коммерческого вебсайта, распространил информацию о способе взлома системы защиты этого сайта в компьютерной сети. Там же он поместил информацию о зарегистрированных пользователях упомянутого сайта, включая сведения о номерах их кредитных карт. В последующие несколько часов сайт подвергся массированным атакам сетевых хулиганов, в результате чего прекратил функционирование на несколько дней.

Кроме того, нелегальным использованием кредитных карт был причинен ущерб их законным владельцам.

Дайте юридическую оценку действиям Артемова.

Примерный перечень вопросов к экзамену по модулю

1. Internet – государство в государстве.
2. Ответственность за компьютерные преступления по уголовному законодательству государств-участников СНГ.
3. Понятие компьютерной информации.

4. Виды преступлений в сфере компьютерной информации.

5. Особенности законодательной конструкции составов преступлений в сфере робототехники.

6. Характеристика основных групп способов совершения преступлений в сфере компьютерной информации.

7. Зарубежный опыт классификации способов совершения преступлений в сфере компьютерной информации.

8. Ответственность за несанкционированное проникновение к охраняемой законом компьютерной информации с неосторожной формой вины.

9. Внутренние пользователи: опасность изнутри компании.

10. Преступные последствия неправомерного доступа к компьютерной информации.

11. Специальный субъект неправомерного доступа к компьютерной информации.

12. Создание компьютерной программы как процесс написания её алгоритма.

13. Способы распространения вредоносных компьютерных программ.

14. Понятие «вируса».

15. Особенности формы вины при создании, использовании и распространении вредоносных компьютерных программ, повлекшие тяжкие последствия или создавших угрозу их наступления.

16. Правила эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации и информационно-телекоммуникационных сетей.

17. Правила эксплуатации информационно-телекоммуникационных сетей и оконечного оборудования.

18. Правила доступа к информационно-телекоммуникационным сетям.

19. Особенности субъектов компьютерных преступлений.

20. Хакер: компьютерный преступник или рядовой пользователь компьютерной техники?

21. Личностный аспект субъекта компьютерного преступления.

22. Робот как субъект компьютерного преступления.

23. Новейшие виды источников угроз информационной безопасности.

24. Мировой опыт противодействию преступлениям в сфере компьютерной информации.

25. Правовое регулирование ответственности за мошенничество с использованием компьютерных технологий.

26. Состояние преступности в сфере компьютерной информации в РФ.

27. Качественная характеристика преступности компьютерной информации в РФ.

28. Ответственность за несанкционированное проникновение к охраняемой законом компьютерной информации с неосторожной формой вины.

29. Формы сотрудничества стран СНГ в сфере борьбы с компьютерными преступлениями.

30. Выбор стратегии борьбы с преступлениями в сфере информационных технологий: понятие и общая характеристика.

31. Условия успешности реализации выбранной стратегии (постоянная и планомерная работа, взаимодействие правоохранительных органов).

32. Общая характеристика системы правоохранительных органов России, осуществляющих борьбу с преступлениями в сфере информационных технологий.

33. Какие отделы выделяются в системе правоохранительных органов зарубежных государств, осуществляющих борьбу с компьютерными преступлениями.

34. Роль кадрового и технического обучения в деятельности правоохранительных органов России, осуществляющих борьбу с преступлениями в сфере информационных технологий.

35. Ст. 272 УК РФ. Неправомерный доступ к компьютерной информации: общая характеристика.

36. Ст. 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ: общая характеристика.

37. Ст. 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: общая характеристика.

38. Кибертерроризм в России: его свойства и особенности.

39. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности.

40. Ответственность за киберпреступления.

41. Общая характеристика преступления ст. 159.6 УК РФ.

42. Криминологическая характеристика лиц, совершающих деяния, предусмотренные статьей 159.6 УК РФ.

43. Цели и задачи уголовной политики в сфере противодействия компьютерной преступности.

44. Правовая основа противодействия компьютерной преступности.

45. Программы обеспечения информационной безопасности.

5.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Шкала оценивания контрольной работы

Уровень оценивания	Критерии оценивания	Баллы
Контрольная работа	Свободное владение материалом. Полное усвоение сути проблемы, чёткое грамотное изложение текста. Задание выполнено верно.	81-100
	Достаточное усвоение материала. Суть проблемы в основном, усвоена; материал не содержит грубых ошибок; основные положения изложены и, в основном, осмыслены. Задание выполнено, однако допущены несущественные ошибки.	61-80
	Поверхностное усвоение материала. Суть проблемы изложена нечётко; в использованном материале встречаются ошибки; основные положения изложены и, в основном, осмыслены. Задание выполнено с допущением нескольких ошибок.	41-60
	Неудовлетворительное усвоение материала. Суть проблемы изложена плохо; в использовании материале встречаются грубые ошибки; основные результаты изложены и осмыслены плохо. Задание не выполнено или выполнено неверно.	0-40

Итоговая шкала выставления оценки по контрольной работе

Количество баллов	Оценка по традиционной шкале
41-100	Зачтено
0-40	Не зачтено

Шкала оценивания экзамена

Критерии оценивания	Баллы
Полные и точные ответы на два вопроса билета. Свободное владение основными терминами и понятиями курса; последовательное и логичное изложение материала курса; законченные выводы и обобщения по теме вопросов; исчерпывающие ответы на вопросы.	20-30
Ответы на вопросы билета носят преимущественно описательный характер. Знание основных терминов и понятий курса; последовательное изложение материала курса; недостаточно полные ответы на вопросы.	13-19
Дан ответ только на один вопрос билета. Удовлетворительное знание основных терминов и понятий курса; недостаточно последовательное изложение материала курса.	2-12
Ответ, не соответствующий вышеуказанным критериям выставления оценок.	0-1

Итоговая шкала оценивания результатов освоения модуля

Итоговая оценка по модулю выставляется по приведенной ниже шкале. При выставлении итоговой оценки преподавателем учитывается работа обучающегося в течение освоения модуля, а также оценка по промежуточной аттестации.

Количество баллов	Оценка по традиционной шкале
81-100	Отлично
61-80	Хорошо
41-60	Удовлетворительно
0-40	Неудовлетворительно

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ МОДУЛЯ

6.1. Основная литература:

1. Бегишев И.Р. Преступления в сфере обращения цифровой информации: монография. Казань: Изд-во «Познание» Казанского инновационного университета, 2020. – 300 с.URL: file:///C:/Users/Lopat/Downloads/cifrovaya-informaciya-begishev-bikeev.pdf

2. Корабельников С.М. Преступления в сфере информационной безопасности: учебное пособие для вузов. Москва: Издательство Юрайт, 2022. 111 с. URL: https://urait.ru/book/prestupleniya-v-sfere-informacionnoy-bezopasnosti-448295

3. Криминология: учебник для бакалавриата, специалитета и магистратуры / под общ. ред. О. С. Капинус. 2-е изд., пер. и доп. Москва: Издательство Юрайт, 2019. – 1132 с.URL: https://urait.ru/book/kriminologiya-428579

4. Преступления против общественной безопасности и общественного порядка : учебник для вузов / ответственные редакторы А. В. Наумов, А. Г. Кибальник. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 158 с. — (Высшее образование). — ISBN 978-5-534-18589-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590565

5. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов / ответственные редакторы С. В. Зуев, В. Б. Вехов. Москва: Издательство Юрайт, 2021. 243 с. URL: https://urait.ru/bcode/467208

6. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебник для вузов / ответственные редакторы С. В. Зуев, В. Б. Вехов. — Москва : Издательство Юрайт, 2026. — 243 с. — (Высшее образование). — ISBN 978-5-534-

13898-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/index.php/bcode/588521

6.2 Дополнительная литература

1. Боровиков, В. Б. Уголовное право. Особенная часть : учебник для вузов / В. Б. Боровиков, А. А. Смердов ; под редакцией В. Б. Боровикова. — 8-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 532 с. — (Высшее образование). — ISBN 978-5-534-20397-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/600456

2. Воронин Ю.А. Преступления в сфере обращения цифровой информации и их детерминанты // Виктимология. – 2020. – № 1 (23). – С. 74–80. URL: https://elibrary.ru/item.asp?id=42768187

3. Грачева Ю.В. Уголовно-правовые риски в сфере цифровых технологий: проблемы и предложения // Lex russica (Русский закон). – 2020. – № 1 (158). – С. 145-159. URL: https://elibrary.ru/item.asp?id=42335041

3. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: монография. – Москва: Юрлитинформ, 2018. – 312 с. URL: https://elibrary.ru/item.asp?id=30081476

4. Зуев, С. В. Организация расследования преступлений : учебник для вузов / С. В. Зуев, В. А. Задорожная, О. В. Овчинникова. — Москва : Издательство Юрайт, 2026. — 231 с. — (Высшее образование). — ISBN 978-5-534-17632-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589351

5. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2026. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588094

6. Мосечкин И.Н. Искусственный интеллект в уголовном праве: перспективы совершенствования охраны и регулирования: монография. – Киров: Вятский государственный университет, 2020. – 111 с. URL:https://elibrary.ru/item.asp?id=42968607

7. Поляков И.В. Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики // Проблемы правоохранительной деятельности. – 2020. – № 4. – С. 21-25. URL: https://elibrary.ru/item.asp?id=44449876

8. Электронные доказательства в уголовном судопроизводстве : учебник для вузов / ответственный редактор С. В. Зуев. — Москва : Издательство Юрайт, 2026. — 193 с. — (Высшее образование). — ISBN 978-5-534-13286-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588277

9. Цифровая криминалистика : учебник для вузов / под редакцией В. Б. Вехова, С. В. Зуева. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 485 с. — (Высшее образование). — ISBN 978-5-534-21152-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581669

10. Уголовное право зарубежных стран. Особенная часть : учебник для вузов / ответственный редактор Н. Е. Крылова. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 522 с. — (Высшее образование). — ISBN 978-5-534-18041-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580422

6.3 Ресурсы информационно-телекоммуникационной сети «Интернет»

1. Российская Государственная библиотека http://www.rsl.ru
2. Федеральный правовой портал Юридическая Россия http:// law.edu.ru/
3. Банк данных «Библиотека копий официальных публикаций правовых актов» http://lib.ksrf.ru/
4. Правотека http://www.pravoteka.ru/

5. Киберленинка. Cyberleninka.ru
6. Библиотека юридической литературы http://pravo.eup.ru/
7. Классика Российского права http://civil.consultant.ru
8. Библиотека юриста http://www.lawbook.by.ru
9. Журнал Юрист http://www.jurist.by/
10. Верховный Суд России http://www.vsrf.ru/
11. Обзоры нового законодательства, комментарии законов различных отраслей права, правовая энциклопедия. http://empire.list.ru/law/
12. Официальный сайт Следственного комитета Российской Федерации http://www.sledcom.ru
13. Официальный сайт Генеральной прокуратуры Российской Федерации. http://genproc.gov.ru
14. Официальный сайт Министерства Внутренних дел Российской Федерации https://мвд.рф
15. Электронно-библиотечная система Лань https://e.lanbook.com
16. ООО «Электронное издательство Юрайт» https://urait.ru

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ МОДУЛЯ

1. Методические рекомендации по подготовке к практическим занятиям.
2. Методические рекомендации по организации самостоятельной работы по дисциплинам.

8. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО МОДУЛЮ

Лицензионное программное обеспечение:

Microsoft Windows
Microsoft Office
Kaspersky Endpoint Security

Информационные справочные системы:

Система «КонсультантПлюс»

Профессиональные базы данных:

fgosvo.ru – Портал Федеральных государственных образовательных стандартов высшего образования

pravo.gov.ru – Официальный интернет-портал правовой информации

www.edu.ru – Федеральный портал Российское образование

Свободно распространяемое программное обеспечение, в том числе отечественного производства:

ОМС Плеер (для воспроизведения Электронных Учебных Модулей)
7-zip
Google Chrome

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ МОДУЛЯ

Материально-техническое обеспечение модуля включает в себя:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения: комплект учебной мебели, доска, технические средства обучения (проектор подвесной, компьютер стационарный - моноблок);

- помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой, подключенной к сети Интернет, обеспеченные доступом к электронной информационно-образовательной среде Университета. Персональные компьютеры с подключением к сети Интернет и обеспечением доступа к электронным библиотекам и в электронную информационно-образовательную среду Университета. Доска. Программное обеспечение: Лицензионное программное обеспечение: Зарубежное: Microsoft Windows,

Microsoft Office Отечественное: Kaspersky Endpoint Security Свободно распространяемое программное обеспечение: Зарубежное: Google Chrome, 7-zip Отечественное: ОМС Плеер (для воспроизведения Электронных Учебных Модулей) Информационные справочные системы: система «КонсультантПлюс» Профессиональные базы данных: fgosvo.ru pravo.gov.ru;

- помещение для самостоятельной работы для инвалидов и лиц с ограниченными возможностями здоровья, оснащенное компьютерной техникой, подключенной к сети Интернет, обеспечено доступом к электронно-образовательной среде Университета, Комплект учебной мебели, персональные компьютеры с подключением к сети Интернет и обеспечением доступа к электронным библиотекам и в электронную информационно-образовательную среду Университета, доска, проектор подвесной.