

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Наумова Наталия Александровна

Должность: Ректор

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Дата подписания: 21.11.2025 09:37:11

Федеральное государственное автономное образовательное учреждение высшего образования

Уникальный программный ключ: 6b5279da4e034bfff679172803da5b78959c692

«ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОСВЕЩЕНИЯ»

(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОСВЕЩЕНИЯ)

Юридический факультет

Кафедра уголовного права, уголовного процесса и криминалистики

Согласовано

и.о. декана юридического факультета  
«25» марта 2025 г.

/ Узденов Ш.Ш./

### **Рабочая программа дисциплины**

Актуальные проблемы квалификации и расследования преступлений в  
сфере высоких технологий

#### **Направление подготовки**

40.04.01 Юриспруденция

#### **Программа подготовки:**

Юрист в уголовном судопроизводстве

#### **Квалификация**

Магистр

#### **Форма обучения**

Очная

Согласовано учебно-методической комиссией  
юридического факультета

Протокол от «24» марта 2025 г. № 8

Председатель УМК

/ Софинская Е.Д. /

Рекомендовано кафедрой уголовного  
права, уголовного процесса и  
криминалистики

Протокол от «07» марта 2025 г. № 7

Заведующий кафедрой

/ Москалев М.А. /

Москва  
2025

Автор-составитель:  
Кандидат юридических наук, доцент  
Колесова А.С.

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

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

Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

Год начала подготовки (по учебному плану) 2025.

## СОДЕРЖАНИЕ

1.	Планируемые результаты обучения	3
2.	Место дисциплины в структуре образовательной программы	3
3.	Объем и содержание дисциплины	4
4.	Учебно-методическое обеспечение самостоятельной работы обучающихся	8
5.	Фонд оценочных средств для проведения текущей и промежуточной аттестации по дисциплине	17
6.	Учебно-методическое и ресурсное обеспечение дисциплины	29
7.	Методические указания по освоению дисциплины	30
8.	Информационные технологии для осуществления образовательного процесса по дисциплине	30
9.	Материально-техническое обеспечение дисциплины	30

## **1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ**

### **1.1 Цель и задачи дисциплины**

**Цель освоения дисциплины:** формирование у студентов твердых знаний о правовых основаниях и содержании актуальных проблем квалификации и расследования преступлений в сфере высоких технологий.

**Задачи дисциплины:**

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

### **1.2 Планируемые результаты обучения**

В результате освоения данной дисциплины у обучающихся формируются следующие компетенции:

**УК-3.** Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.

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

## **2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

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

Знания и навыки, приобретенные студентами при изучении дисциплины «Актуальные проблемы квалификации и расследования преступлений в сфере высоких технологий», имеют тесные связи с такими дисциплинами как: «Актуальные проблемы уголовного права, криминологии и уголовно-исполнительного права», «Национальная безопасность и основные направления устойчивого развития Российской Федерации» и др.

При изучении дисциплины «Актуальные проблемы квалификации и расследования преступлений в сфере высоких технологий» студентам необходимо опираться на знания, полученные, прежде всего, при изучении дисциплины «Философия научного познания».

## **3. ОБЪЕМ И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ**

### **3.1 Объем дисциплины**

Показатель объема дисциплины	Форма обучения
	Очная
Объем дисциплины в зачетных единицах	2

Объем дисциплины в часах	72 (20) <sup>1</sup>
Контактная работа	28,2 (20) <sup>2</sup>
Лекции	12 (12) <sup>3</sup>
Практические занятия	16 (8) <sup>4</sup>
Контактные часы на промежуточную аттестацию:	0,2
Зачет	0,2
Самостоятельная работа	36
Контроль	7,8

Формы промежуточной аттестации: зачет в 4 семестре.

### 3.2 Содержание дисциплины

Наименование разделов (тем) дисциплины	Кол-во часов	
	Лекции	Практические занятия
<b>Тема 1. Преступления в сфере высоких технологий - новый вид преступных посягательств в уголовном законодательстве Российской Федерации</b> 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.	2	4 (4) <sup>5</sup>
<b>Тема 2. Информационные отношения как объект уголовно-правовой охраны</b> 1. Понятие родового объекта преступных посягательств в сфере высоких технологий. 2. Понятие предмета компьютерного преступления. 3. Понятие и виды преступлений в сфере высоких технологий.	2	2 (2) <sup>6</sup>

<sup>1</sup> Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

<sup>2</sup> Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

<sup>3</sup> Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

<sup>4</sup> Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

<sup>5</sup> Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

<sup>6</sup> Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

<p><b>Тема 3. Виды и способы совершения преступлений в сфере высоких технологий</b></p> <p>1. Многообразие способов совершения преступлений в сфере высоких технологий.</p> <p>2. Классификация способов совершения компьютерных преступлений по законодательству России.</p> <p>3. Сложность в квалификации деяний, совершенных в сфере высоких технологий.</p> <p>4. Перечень смежных составов, предусматривающих неправомерное обращение с информацией по уголовному кодексу Российской Федерации.</p> <p>5. Проблема ответственности за компьютерное мошенничество.</p>	2	2 (2) <sup>7</sup>
<p><b>Тема 4. Вопросы уголовной ответственности за неправомерный доступ к компьютерной информации.</b></p> <p>1. Характеристика объективных признаков составов преступлений.</p> <p>2. Понятие охраняемой законом компьютерной информации.</p> <p>3. Понятие «вируса» и «вредоносной» компьютерной программы.</p> <p>4. Характеристика субъективных признаков составов преступлений.</p> <p>5. Совершение неправомерного доступа к компьютерной информации по неосторожности.</p> <p>6. Особенности субъекта преступлений.</p>	2	4
<p><b>Тема 5. Типология личности компьютерного преступника</b></p> <p>1. Особенности субъектов компьютерных преступлений.</p> <p>2. Классификация субъектов компьютерных преступлений.</p> <p>3. Личностный аспект субъекта компьютерного преступления.</p> <p>4. Основные характеристики личности компьютерного преступника.</p>	2	2
<p><b>Тема 6. Мировой опыт правового регулирования предупреждения преступности в сфере высоких технологий</b></p> <p>1. Международное сотрудничество как форма борьбы с преступностью в сфере высоких технологий.</p> <p>2. Понятие, задачи и средства комплексного контроля над преступностью в сфере высоких технологий.</p> <p>3. Международный опыт борьбы с преступлениями в сфере высоких технологий.</p> <p>4. Опыт правового регулирования общественных отношений в сфере высоких технологий в Российской Федерации.</p>	2	2

<sup>7</sup> Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

<b>Итого</b>	<b>12 (12)<sup>8</sup></b>	<b>16 (8)<sup>9</sup></b>
--------------	----------------------------	---------------------------

#### **4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ**

<b>Темы для самостоятельного изучения</b>	<b>Изучаемые вопросы</b>	<b>Кол-во часов</b>	<b>Формы самостоятельной работы</b>	<b>Методическое обеспечение</b>	<b>Формы отчетности</b>
Тема 1. Преступления в сфере высоких технологий - 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	Работа с литературой, ресурсами Интернет, ответы на вопросы	Учебно-методическое и ресурсное обеспечение дисциплины	Опрос на практических занятиях

<sup>8</sup> Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

<sup>9</sup> Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

Тема 2. Информационные отношения как объект уголовно-правовой охраны	1. Понятие родового объекта преступных посягательств в сфере высоких технологий. 2. Понятие предмета компьютерного преступления. 3. Понятие и виды преступлений в сфере высоких технологий.	6	Работа с литературой, ресурсами Интернет, ответы на вопросы	Учебно-методическое и ресурсное обеспечение дисциплины	Опрос на практических занятиях
Тема 3. Виды и способы совершения преступлений в сфере высоких технологий	1. Многообразие способов совершения преступлений в сфере высоких технологий. 2. Классификация способов совершения компьютерных преступлений по законодательству России. 3. Сложность в квалификации деяний, совершенных в сфере высоких технологий. 4. Перечень смежных составов, предусматривающих неправомерное обращение с информацией по уголовному кодексу Российской Федерации. 5. Проблема ответственности за компьютерное мошенничество.	6	Работа с литературой, ресурсами Интернет, ответы на вопросы	Учебно-методическое и ресурсное обеспечение дисциплины	Опрос на практических занятиях
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	6	Работа с литературой, ресурсами Интернет, ответы на вопросы	Учебно-методическое и ресурсное обеспечение дисциплины	Опрос на практических занятиях

	доступа к компьютерной информации по неосторожности. 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.	6	Работа с литературой, ресурсами Интернет, ответы на вопросы	Учебно-методическое и ресурсное обеспечение дисциплины	Опрос на практических занятиях
Тема 6. Мировой опыт правового регулирования предупреждения преступности в сфере высоких технологий	1. Международное сотрудничество как форма борьбы с преступностью в сфере высоких технологий. 2. Понятие, задачи и средства комплексного контроля над преступностью в сфере высоких технологий. 3. Международный опыт борьбы с преступлениями в сфере высоких технологий. 4. Опыт правового регулирования общественных отношений в сфере высоких технологий в Российской Федерации.	6	Работа с литературой, ресурсами Интернет, ответы на вопросы	Учебно-методическое и ресурсное обеспечение дисциплины	Опрос на практических занятиях
<b>ИТОГО</b>		<b>36</b>			

## **5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ**

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

Код и наименование компетенции	Этапы формирования
<b>УК-3.</b> Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	1. Работа на учебных занятиях. 2. Самостоятельная работа.
<b>СПК-4.</b> 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.

## 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
УК-3	Пороговый	1.Работа на учебных занятиях. 2.Самостоятельная работа.	<b>Знать:</b> принципы формирования команд, методы эффективного руководства коллективами, основные теории лидерства и стили руководства. <b>Уметь:</b> разрабатывать план групповых и организационных коммуникаций при подготовке и выполнении проекта, формулировать задачи для достижения поставленной цели и распределять полномочия членам команды, разрабатывать командную стратегию, организовывать и координировать работу, конструктивно преодолевать возникающие разногласия и конфликты.	Опрос	Шкала оценивания опроса
	Продвинутый	1.Работа на учебных занятиях. 2.Самостоятельная работа.	<b>Знать:</b> принципы формирования команд, методы эффективного руководства коллективами, основные теории лидерства и стили руководства. <b>Уметь:</b> разрабатывать план групповых и организационных коммуникаций при подготовке и выполнении проекта, формулировать задачи для достижения поставленной цели и распределять полномочия членам команды, разрабатывать командную стратегию, организовывать и	Опрос, реферат	Шкала оценивания опроса Шкала оценивания реферата

			<p>координировать работу, конструктивно преодолевать возникающие разногласия и конфликты.</p> <p><b>Владеть:</b> навыками анализа, проектирования и организации межличностных, групповых и организационных коммуникаций в команде для достижения поставленной цели, методами организации и управления коллективом.</p>		
<b>СПК-4</b>	Пороговый	1.Работа на учебных занятиях. 2.Самостоятельная работа.	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- законодательство в сфере в сфере высоких технологий;</li> <li>- систему и принципы построения и функционирования отношений, складывающихся в сфере высоких технологий;</li> <li>- основные научные подходы к пониманию права и дискуссионные проблемы современной юридической науки и правоприменительной практики по вопросам преступлений в сфере высоких технологий.</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- консультировать по вопросам законодательства по отношениям в сфере высоких технологий;</li> <li>- давать квалифицированные разъяснения и заключения по вопросам применения действующих правовых норм по вопросам преступлений в сфере высоких технологий.</li> </ul>	Опрос	Шкала оценивания опроса
	Продвинутый	1.Работа на учебных занятиях. 2.Самостоятельная работа.	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- законодательство в сфере в сфере высоких технологий;</li> <li>- систему и принципы построения и функционирования отношений, складывающихся в сфере высоких технологий;</li> <li>- основные научные подходы к пониманию права и дискуссионные проблемы современной юридической науки и</li> </ul>	Опрос, реферат	Шкала оценивания опроса Шкала оценивания реферата

		<p>правоприменительной практики по вопросам преступлений в сфере высоких технологий.</p> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- консультировать по вопросам законодательства по отношениям в сфере высоких технологий;</li> <li>- давать квалифицированные разъяснения и заключения по вопросам применения действующих правовых норм по вопросам преступлений в сфере высоких технологий.</li> </ul> <p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>- навыками разработки и представления собственных вариантов правовых решений в конкретной ситуации или исходя из заданных (поставленных) условий;</li> <li>- 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;</li> <li>- навыками систематизации источников, принципов и нормы права для квалифицированного их применения.</li> </ul>		
--	--	---	--	--

#### Шкала оценивания опроса

Критерии оценивания	Баллы
Содержание ответа соответствует поставленному вопросу (заданию), полностью раскрывает цели и задачи, сформулированные в вопросе; изложение материала отличается логичностью и смысловой завершенностью, студент показал хорошее владение материалом, умение четко, аргументировано и корректно отвечать на поставленные вопросы, отстаивать собственную точку зрения.	4-5
Содержание ответа недостаточно полно соответствует поставленному вопросу, не раскрыты полностью цели и задачи, сформулированные в вопросе; изложение материала не отличается логичностью и нет смысловой завершенности сказанного, студент показал достаточно уверенное владение материалом, не показал умение четко, аргументировано и корректно отвечать на поставленные вопросы, отстаивать собственную точку зрения.	2-3

Содержание ответа не отражает особенности проблематики заданного вопроса, – содержание ответа не полностью соответствует обозначенной теме, не учитываются новейшие достижения историографии темы, студент показал неуверенное владение материалом, неумение отстаивать собственную позицию и отвечать на вопросы.	1
Ответ не имеет логичной структуры, содержание ответа в основном не соответствует теме, студент показал неуверенное владение материалом, неумение формулировать собственную позицию.	0

### Шкала оценивания реферата

Критерии оценивания	Баллы
Содержание соответствует поставленным цели и задачам, изложение материала отличается логичностью и смысловой завершенностью, студент показал владение материалом, умение четко, аргументировано и корректно отвечать на поставленные вопросы, отстаивать собственную точку зрения.	8-10
Содержание недостаточно полно соответствует поставленным цели и задачам исследования, работа выполнена на недостаточно широкой базе источников и не учитывает новейшие достижения, изложение материала носит преимущественно описательный характер, студент показал достаточно уверенное владение материалом, однако недостаточное умение четко, аргументировано и корректно отвечать на поставленные вопросы и отстаивать собственную точку зрения.	5-7
Содержание не отражает особенности проблематики избранной темы, – содержание работы не полностью соответствует поставленным задачам, база источников является фрагментарной и не позволяет качественно решить все поставленные в работе задачи, работа не учитывает новейшие достижения историографии темы, студент показал неуверенное владение материалом, неумение отстаивать собственную позицию и отвечать на вопросы.	2-4
Работа не имеет логичной структуры, содержание работы в основном не соответствует теме, база источников исследования является недостаточной для решения поставленных задач, студент показал неуверенное владение материалом, неумение формулировать собственную позицию.	0-1

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

#### Примеры вопросов для проведения опроса

1. Ретроспектива создания первых счетных машин и их модификация в современные компьютеры.
2. Международный опыт противодействия преступлениям в сфере высоких технологий.

3. Основные этапы межгосударственного сотрудничества в борьбе с преступностью в сфере высоких технологий.
4. Проблема создания эталонной схемы закона об уголовной ответственности за совершение компьютерных преступлений Organization for Economic Cooperation and Development.
5. Классификация компьютерных преступлений, предложенная экспертами ООН.
6. Категория объекта в современной уголовно – правовой теории.
7. Понятие информации в различных аспектах.
8. Понятие компьютерного преступления и преступления в сфере высоких технологий.
9. Характеристика точек зрения на понятие «компьютерное преступление».
10. Компьютерное преступление как вид информационного преступления, посягающего на информационные отношения.
11. Основные классификации способов совершения преступлений в сфере высоких технологий.
12. Способы совершения компьютерных преступлений по уголовному законодательству некоторых государств-участников СНГ.
13. Понятие охраняемой законом компьютерной информации.
14. Совершение неправомерного доступа к компьютерной информации по неосторожности.
15. Особенности субъекта преступлений в сфере высоких технологий.
16. Сущность уголовно-правового запрета, установленного собственником на доступ к компьютерной информации.
17. Виды охраняемой законом информации.

### **Примеры тем для реферата**

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 высоких технологий
5. Особенности законодательной конструкции составов преступлений в сфере робототехники
6. Характеристика основных групп способов совершения преступлений в сфере высоких технологий
7. Зарубежный опыт классификации способов совершения преступлений в сфере высоких технологий
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

### **Примерный перечень вопросов для зачета**

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 высоких технологий.

5. Особенности законодательной конструкции составов преступлений в сфере робототехники.
6. Характеристика основных групп способов совершения преступлений в сфере высоких технологий.
7. Зарубежный опыт классификации способов совершения преступлений в сфере высоких технологий.
8. Ответственность за несанкционированное проникновение к охраняемой законом компьютерной информации с неосторожной формой вины.
9. Внутренние пользователи: опасность изнутри компаний.
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 окончного 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 высоких технологий.
25. Правовое регулирование ответственности за мошенничество с использованием компьютерных технологий.
26. Состояние преступности в сфере компьютерной информации в РФ.
27. Качественная характеристика преступности высоких технологий в РФ

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

**Шкала оценивания зачета**

<b>Критерии оценивания</b>	<b>Баллы</b>
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.	15-20
Ответы на вопросы билета носят преимущественно описательный характер. Знание основных терминов и понятий курса; последовательное изложение материала курса; недостаточно полные ответы на вопросы.	9-14

Критерии оценивания	Баллы
Дан ответ только на один вопрос билета. Удовлетворительное знание основных терминов и понятий курса; недостаточно последовательное изложение материала курса.	2-8
Ответ, не соответствующий вышеуказанным критериям выставления оценок.	0-1

### **Итоговая шкала оценивания результатов освоения дисциплины**

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

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

## **6. УЧЕБНО-МЕТОДИЧЕСКОЕ И РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **6.1 Основная литература:**

1. 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>
2. Бегищев 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>
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. 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>

### **6.2. Дополнительная литература:**

1. 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>
2. 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. 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>
5. 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>

## **6.3 Ресурсы информационно-телекоммуникационной сети «Интернет»**

- 1) <http://www.ksrf.ru>
- 2) [www.arbitr.ru](http://www.arbitr.ru)
- 3) <http://www.vsrif.ru>

Электронно-библиотечная система Лань <https://e.lanbook.com>

ООО «Электронное издательство Юрайт» <https://urait.ru>

## **7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ**

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 ДИСЦИПЛИНЕ**

### **Лицензионное программное обеспечение:**

Microsoft Windows

Microsoft Office

Kaspersky Endpoint Security

### **Информационные справочные системы:**

Система ГАРАНТ

Система «КонсультантПлюс»

Профессиональные базы данных

[fgosvo.ru – Портал Федеральных государственных образовательных стандартов высшего образования](http://fgosvo.ru)

[pravo.gov.ru - Официальный интернет-портал правовой информации](http://pravo.gov.ru)

[www.edu.ru – Федеральный портал Российской образования](http://www.edu.ru)

Свободно распространяемое программное обеспечение, в том числе отечественного производства

ОМС Плеер (для воспроизведения Электронных Учебных Модулей)

7-zip

Google Chrome

## **9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Материально-техническое обеспечение дисциплины включает в себя:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения: учебной мебелью, доской, демонстрационным оборудованием, персональными компьютерами, проектором;

- помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключением к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде.