

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ  
РЕСПУБЛИКИ ТАДЖИКИСТАН  
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»**

«Утверждаю»  
Декан юридического факультета  
д.ю.н., профессор Хамроев Ш.С.

« 18 » 06 2024 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ**

Направление подготовки - 40.04.01 «Юриспруденция»

Программа подготовки – Уголовно-криминологическая основа  
следственной деятельности

Форма подготовки – очная

Уровень подготовки - магистратура

**ДУШАНБЕ 2024**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 40.04.01 «Юриспруденция», утвержденного приказом Министерства науки и высшего образования РФ от 25.11.2020 г. №1451.

При разработке рабочей программы учитываются

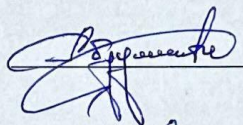
- требования работодателей;
- содержание программ дисциплин, изучаемых на предыдущих и последующих этапах обучения;
- новейшие достижения в данной предметной области.

Рабочая программа обсуждена на заседании кафедры «Уголовное право», протокол № 11 от «22» 06 2024 г.

Рабочая программа утверждена УМС юридического факультета, протокол № 11 от «28» 06 2024 г.

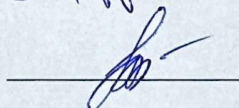
Рабочая программа утверждена Ученым советом юридического факультета, протокол № 11 от «28» 06 2024 г.

Заведующая кафедрой,  
д.ю.н., доцент



Абдуллаева Р.А.

Зам. председателя  
УМС факультета



Смоктый М.Е.

Разработчик:  
к.ю.н., доцент



Абдуллаев Н.С.

Разработчик от организации:  
Судья района Шохмансур г. Душанбе  
к.ю.н., ст. преподаватель



Муродзода А.А.

## 1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

### 1.1. Цели изучения дисциплины:

Целями освоения дисциплины «Особенности противодействия киберпреступности» является формирование знаний понятия, сущности, видов киберпреступности, а также его предупреждения.

### 1.2. Задачи изучения дисциплины

Для достижения данной цели обозначаются и решаются следующие задачи:

- сформировать у обучающихся теоретические знания основных знаний о понятии и видах киберпреступности;
- способствовать приобретению навыков анализа криминологической характеристики киберпреступности;
- раскрыть методологические подходы в практическом применении механизмов и инструментов борьбы с ним;
- сформировать основные компетенции обучающихся в сфере проблем противодействия киберпреступности.

### 1.3. В результате изучения данной дисциплины у обучающихся формируются следующие компетенции (элементы компетенций)

#### а) универсальные (УК):

Код компетенции	Содержание компетенции	Перечень планируемых результатов обучения по дисциплине (индикаторы достижения компетенций)	Вид оценочных средств
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий	<b>ИУК-1.1.</b> Демонстрирует основные методы критического анализа, методологию системного подхода. <b>ИУК-1.2.</b> Выявляет проблемные ситуации, используя методы анализа, синтеза и абстрактного мышления; осуществляет поиск решений проблемных ситуаций на основе действий, эксперимента и опыта; <b>ИУК-1.3.</b> Владеет технологиями выхода из проблемных ситуаций, навыками выработки стратегии действий; навыками критического анализа.	выступление на семинарах, защита рефератов, доклад, эссе  дискуссия, выступление на семинарах, защита рефератов  выступление на семинарах, защита рефератов, доклад, эссе
УК-3	Способен организовать и руководить работой команды, выработывая командную стратегию для достижения поставленной цели	<b>ИУК-3.1.</b> Анализирует общие формы организации деятельности коллектива; психологию межличностных отношений в группах разного возраста; основы стратегического планирования <b>ИУК-3.2.</b> Способен создавать в коллективе психологически безопасную доброжелательную среду; учитывать в своей социальной и профессиональной деятельности интересы коллег <b>ИУК-3.3.</b> Владеет навыками постановки цели в условиях командной работы; способами управления командной работой в решении поставленных задач;	выступление на семинарах, защита рефератов, доклад, эссе  дискуссия, выступление на семинарах, защита рефератов  выступление на семинарах, защита рефератов, доклад, эссе

#### б) профессиональных (ПК):

ПК-1	Способность организовывать и реализовать уголовно - правовую и криминологическую деятельности, связанные с проведением исследования личности преступника, квалификации деяния, следственной	<b>ИПК-1.1.</b> Способен воспринимать знание в области уголовно-криминологической, следственной деятельности по выявлению, расследованию, пресечению и раскрытию и преступлений и иных правонарушений; <b>ИПК-1.1.</b> Способен воспринимать знание в области уголовно-криминологической, следственной деятельности по выявлению, расследованию, пресечению и раскрытию и преступлений и иных правонарушений; <b>ИПК-1.3.</b> Способен применять навыки определения последовательности	выступление на семинарах, защита рефератов, доклад, эссе  дискуссия, выступление на семинарах, защита рефератов
------	---	--	---



деятельности с целью расследования и раскрытия преступлений	проведения следственных деятельности для выявления, пресечения, расследования и раскрытия различных видов преступлений и основе анализа следственной ситуации досудебного производства.	выступление на семинарах, защита рефератов, доклад, эссе
---	---	--

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

### 2.1. Цикл (раздел) ОПОП, к которому относится данная дисциплина

Дисциплина «Особенности противодействия киберпреступности» представляет собой дисциплину вариативной части профессионального цикла дисциплин (Б1.В.14). Дисциплина «Особенности противодействия киберпреступности» является комплексной междисциплинарной отраслью науки. Она рассматривает проблемы предупреждения киберпреступности в современный период и является составной частью уголовного права и криминологии.

Приобретенные в ходе изучения дисциплины «Особенности противодействия киберпреступности» теоретические знания должны быть закреплены при прохождении производственной практики.

2.2.

Таблица 1.\*

	Название дисциплины	Семестр	Место дисциплины в структуре ОПОП
1.	<i>Философия права</i>	2	<i>Б1.О.01</i>
2.	<i>История политических и правовых учений</i>	2	<i>Б1.О.06</i>
3.	<i>История и методология юридической науки</i>	1	<i>Б1.О.05</i>
4.	<i>Сравнительное правоведение</i>	2	<i>Б1.О.08</i>
5.	<i>Актуальные проблемы уголовного права</i>	3	<i>Б1.О.09</i>
6.	<i>Квалификация преступлений: вопросы теории и практики</i>	3	<i>Б1.В.07</i>
7.	<i>Уголовное право зарубежных стран</i>	3	<i>Б1.В.ДВ.03.01</i>
8.	<i>Организованная преступность: нац. и транснац. аспекты</i>	3	<i>Б1.В.04</i>
9.	<i>Терроризм и экстремизм в современном обществе</i>	3	<i>Б1.В.06</i>

## 3. СТРУКТУРА И СОДЕРЖАНИЕ КУРСА

Объем дисциплины на очном отделении составляет 3 зачетные единицы, всего 72 часа, из которых: лекции – 6 час., практические занятия – 10 час., всего часов аудиторной нагрузки 16 час., в том числе в интерактивной форме – часов, лабораторные работы - 0 час., КСР 8 час., самостоятельная работа – 26 час.

Зачет – 3 семестр

### 3.1 Структура и содержание теоретической части курса

№ п/п		Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Литература
		Лек.	Пр.	СРС	КСР	
<b>Семестр 3</b>						
1.	<p><b>Тема 1. Понятие и сущность киберпреступности.</b> Киберпреступности и экстремистская деятельность. Правовое определение понятия «киберпреступности» и «экстремистская деятельность».</p> <p><b>Практическое занятие.</b> Виды и формы киберпреступности. Характеристика нормативно-правовых актов в области противодействия киберпреступности. Причины и условия киберпреступности.</p>	2	2	2	-	1 (с.7-25). 3 (с.6-13)

2.	<p><b>Тема 2. Информационная безопасность и компьютерный терроризм.</b>  Понятие информационной безопасности.  Понятие и классификация компьютерного терроризма.  <b>Практическое занятие.</b>  Проблемы применения норм УК РФ и РТ об ответственности за информационную безопасность. Современное состояние уголовной политики в сфере противодействия компьютерному терроризму. Проблемы совершенствования норм об ответственности за преступления в сфере информационной безопасности.</p>	2	2	2	-	2 (с.10-13) 2 (с.13-17)
3.	<p><b>Тема 3. Киберпреступность как новая форма терроризма.</b>  Современное состояние и динамика киберпреступности.  <b>Практическое занятие.</b>  Проблемы детерминации киберпреступности. Причинный комплекс киберпреступности.</p>	2	2	2	-	2 (с.10-13)2 (с.13-17)
4.	<p><b>Тема 4. Компьютерная преступность и обеспечение безопасности информации.</b>  <b>КСР</b>  Характеристика нормативно-правовых актов в области противодействия киберпреступности. Определение и сущность современного киберпреступности. Причины и условия современного киберпреступности.</p>	-	-	4	2	3 (с.30-45)
5.	<p><b>Тема 5. Правовые аспекты противодействия высокотехнологичному киберпреступностию.</b>  <b>Практическое занятие</b>  Совершенствование уголовно-правовых мер противодействия с проявлениями киберпреступности. Совершенствование правоприменительной практики в сфере противодействия киберпреступности.  <b>КСР</b>  Кибертерроризм и киберпреступность: понятие и виды</p>	-	-	4	2	4 (с.58-62)
6.	<p><b>Тема 6. Специфика борьбы с преступлениями в сфере компьютерных системах и сетях</b>  <b>Практическое занятие</b>  Специфика борьбы с преступлениями в сфере компьютерных системах и сетях. Основные направления борьбы с высокотехнологичному преступлению. Деятельность правоохранительных органов по борьбе с кибертерроризмом и киберпреступности.  <b>КСР</b>  Предупреждения органами внутренних дел киберпреступности.</p>	-	2	4	2	4 (с.31-58)
7	<p><b>Тема 7. Правовые аспекты противодействия высокотехнологичному киберпреступности.</b>  Перспективы совершенствования права в условиях нарастания кибертеррористической угрозы.  <b>КСР</b>  Право безопасности: проблемы развития</p>	-	-	4	2	

	информационно-электронных систем. Перспективы совершенствования права в условиях нарастания кибертеррористической угрозы.					
8	<b>Тема 8. Законодательные акты в сфере противодействия киберпреступности КСР</b> <b>Законодательные акты в сфере противодействия киберпреступности</b> Совершенствование нормативно-правовых актов в области противодействия киберпреступности ФЗ «О противодействии экстремистской деятельности» и Закона РТ «О противодействии экстремизму» «О борьбе с терроризму» и их значение для теории и практики противодействия с киберпреступности.	-	-	4	2	
<b>Всего: 50 час.</b>		<b>6</b>	<b>10</b>	<b>26</b>	<b>8</b>	

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

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Особенности противодействия киберпреступности» включает в себя:

1. план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
2. характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;
3. требования к представлению и оформлению результатов самостоятельной работы;
4. критерии оценки выполнения самостоятельной работы.

##### **4.1. План-график выполнения самостоятельной работы**

<b>№ п/п</b>	<b>Объем самостоятельной работы в часах</b>	<b>Тема самостоятельной работы</b>	<b>Форма и вид самостоятельной работы</b>	<b>Форма контроля</b>
<b>Семестр 3</b>				
<b>1.</b>	<b>2</b>	<b>Тема 1. Понятие и сущность киберэкстремизма.</b>	Изучение рекомендованной литературы, нормативного материала, разъяснений Пленума Верховного Суда РФ, решение задач из сборника	Устный опрос, проверка решения задач из сборника
<b>2.</b>	<b>2</b>	<b>Тема 2. Информационная безопасность и компьютерный терроризм.</b>	Изучение рекомендованной литературы, нормативного материала, разъяснений Пленума Верховного Суда РФ, решение задач из сборника	Устный опрос, проверка решения задач из сборника
<b>3.</b>	<b>2</b>	<b>Тема 3. Киберэкстремизм как новая форма терроризма.</b>	Изучение рекомендованной литературы, нормативного материала, разъяснений Пленума Верховного Суда РФ,	Устный опрос, проверка решения задач из сборника

			решение задач из сборника	
4.	4	<b>Тема 4. Компьютерная преступность и обеспечение безопасности информации в ОВД.</b>	Изучение рекомендованной литературы, нормативного материала, разъяснений Пленума Верховного Суда РФ, решение задач из сборника	Устный опрос, проверка решения задач из сборника
5.	4	<b>Тема 5. Правовые аспекты противодействия высокотехнологичному киберэкстремизму.</b>	Изучение рекомендованной литературы, нормативного материала, разъяснений Пленума Верховного Суда РФ, решение задач из сборника	Устный опрос, проверка решения задач из сборника
6.	4	<b>Тема 6. Специфика борьбы с преступлениями в сфере компьютерных системах и сетях.</b>	Изучение рекомендованной литературы, нормативного материала, разъяснений Пленума Верховного Суда РФ, решение задач из сборника	Устный опрос, проверка решения задач из сборника
7.	4	<b>Тема 7. Правовые аспекты противодействия высокотехнологичному киберэкстремизму.</b>	Изучение рекомендованной литературы, нормативного материала, решение задач из сборника	Устный опрос, проверка решения задач из сборника
8.	4	<b>Тема 8. Законодательные акты в сфере противодействия киберпреступности</b>	Изучение рекомендованной литературы, нормативного материала, решение задач из сборника	Устный опрос, проверка решения задач из сборника
<b>Всего: 26 час.</b>				

#### **4.2. Характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению**

Важной составной частью учебного процесса являются семинарские и практические занятия.

Семинарские занятия проводятся главным образом для научно-теоретического обобщения литературных источников и помогают студентам глубже усвоить учебный материал, приобрести навыки творческой работы над документами и первоисточниками.

Планы семинарских занятий, их тематика, рекомендуемая литература, цель и задачи ее изучения сообщаются преподавателем на вводных занятиях или в методических указаниях по данной дисциплине.

Прежде чем приступить к изучению темы, необходимо прокомментировать основные вопросы плана семинара. Такой подход преподавателя помогает студентам быстро находить нужный материал к каждому из вопросов, не задерживаясь на второстепенном.

Начиная подготовку к семинарскому занятию, необходимо, прежде всего, указать студентам страницы в конспекте лекций, разделы учебников и учебных пособий, чтобы они получили общее представление о месте и значении темы в изучаемом курсе. Затем следует рекомендовать им поработать с дополнительной литературой, сделать записи по

рекомендованным источникам.

Подготовка к семинарскому занятию включает 2 этапа:

1й – организационный этап;

2й - закрепление и углубление теоретических знаний.

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

- уяснение задания на самостоятельную работу;

- подбор рекомендованной литературы;

- составление плана работы, в котором определяются основные пункты предстоящей подготовки.

Составление плана дисциплинирует и повышает организованность в работе.

Второй этап включает непосредственную подготовку студента к занятию. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале.

Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам.

В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретает практика в изложении и разъяснении полученных знаний, развивается речь.

При необходимости следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В начале занятия студенты под руководством преподавателя более глубоко осмысливают теоретические положения по теме занятия, раскрывают и объясняют основные положения публичного выступления. В процессе творческого обсуждения и дискуссии вырабатываются умения и навыки использовать приобретенные знания для различного рода ораторской деятельности.

Записи имеют первостепенное значение для самостоятельной работы студентов. Они помогают понять построение изучаемого материала, выделить основные положения, проследить их логику и тем самым проникнуть в творческую лабораторию автора.

Ведение записей способствует превращению чтения в активный процесс, мобилизует, наряду со зрительной, и моторную память. Следует помнить: у студента, систематически ведущего записи, создается свой индивидуальный фонд подсобных материалов для быстрого повторения прочитанного, для мобилизации накопленных знаний. Особенно важны и полезны записи тогда, когда в них находят отражение мысли, возникшие при самостоятельной работе.

Важно развивать у студентов умение сопоставлять источники, продумывать изучаемый материал.

Большое значение имеет совершенствование навыков конспектирования у студентов.

Преподаватель может рекомендовать студентам следующие основные формы записи:

план (простой и развернутый), выписки, тезисы.

Результаты конспектирования могут быть представлены в различных формах.

План – это схема прочитанного материала, краткий (или подробный) перечень вопросов, отражающих структуру и последовательность материала. Подробно составленный план вполне заменяет конспект.

Конспект – это систематизированное, логичное изложение материала источника.

Различаются четыре типа конспектов:

□ *План-конспект* – это развернутый детализированный план, в котором достаточно подробные записи приводятся по тем пунктам плана, которые нуждаются в пояснении.

□ *Текстуальный конспект* – это воспроизведение наиболее важных положений и фактов источника.

□ *Свободный конспект* – это четко и кратко сформулированные (изложенные) основные положения в результате глубокого осмысливания материала. В нем могут присутствовать



выписки, цитаты, тезисы; часть материала может быть представлена планом.

□ *Тематический конспект* – составляется на основе изучения ряда источников и дает более или менее исчерпывающий ответ по какой-то схеме (вопросу).

Ввиду трудоемкости подготовки к семинару преподавателю следует предложить студентам алгоритм действий, рекомендовать еще раз внимательно прочитать записи лекций и уже готовый конспект по теме семинара, тщательно продумать свое устное выступление.

На семинаре каждый его участник должен быть готовым к выступлению по всем поставленным в плане вопросам, проявлять максимальную активность при их рассмотрении. Выступление должно строиться свободно, убедительно и аргументировано.

Преподаватель следит, чтобы выступление не сводилось к репродуктивному уровню (простому воспроизведению текста), не допускается и простое чтение конспекта.

Необходимо, чтобы выступающий проявлял собственное отношение к тому, о чем он говорит, высказывал свое личное мнение, понимание, обосновывал его и мог сделать правильные выводы из сказанного. При этом студент может обращаться к записям конспекта и лекций, непосредственно к первоисточникам, использовать знание художественной литературы и искусства, факты и наблюдения современной жизни и т. д.

Вокруг такого выступления могут разгореться споры, дискуссии, к участию в которых должен стремиться каждый. Преподавателю необходимо внимательно и критически слушать, подмечать особенное в суждениях студентов, улавливать недостатки и ошибки, корректировать их знания, и, если нужно, выступить в роли рефери. При этом обратить внимание на то, что еще не было сказано, или поддержать и развить интересную мысль, высказанную выступающим студентом.

В заключение преподаватель, как руководитель семинара, подводит итоги семинара.

Он может (выборочно) проверить конспекты студентов и, если потребуется, внести в них исправления и дополнения.

#### **4.3. Требования к представлению и оформлению результатов самостоятельной работы**

Объем контрольной работы – 16-20 страниц. Она должна быть выполнена от руки, грамотно, с соблюдением следующих требований: страницы должны быть пронумерованы и иметь поля для замечаний рецензента; в конце работы необходимо привести список использованных нормативных материалов и литературы (с указанием автора, название работы, места и года издания), поставить дату и подпись.

#### **4.4. Критерии оценки выполнения самостоятельной работы**

*Критериями* оценок результатов внеаудиторной самостоятельной работы магистранта являются:

- уровень освоения магистрантами учебного материала.
- умение магистранта использовать теоретические знания при выполнении практических задач.
- обоснованность и четкость изложения ответа.

### **5. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

#### **5.1 Основная литература**

1. Козаченко, И. Я. Уголовное право. Общая часть [Текст]: учебник для бакалавриата и специалитета / И. Я. Козаченко, Г. П. Новоселов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 373 с.
2. Уголовное право в 2 т. Том 2. Особенная часть [Электронный ресурс]: учебник для академического бакалавриата / А. В. Наумов [и др.]; ответственный редактор А. В. Наумов, А. Г. Кибальник. — 5-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2019. — 499 с. — URL: <https://biblio-online.ru/>
3. Сверчков, В. В. Уголовное право. Общая и особенная части [Текст]: учебник для академического бакалавриата / В. В. Сверчков. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 603 с.
4. **Степанов, Олег Анатольевич.** Противодействие кибертерроризму в цифровую эпоху [Текст : Электронный ресурс] : монография / О. А. Степанов. - Электрон. дан.col. - Москва : Юрайт, 2024. - 103 с. - (Актуальные монографии). - Режим доступа: <https://urait.ru/bcode/543303>

#### **5.2 Дополнительная литература**

1. Номоконов В.А., Тропина Т.Л. Терроризм с помощью Интернета // Терроризм в России и проблемы системного реагирования. – М.: Российская криминологическая ассоциация, 2008. – 192 с.
2. 2.Комментарий к Уголовному кодексу Республики Таджикистан /под. ред. Х.Х. Шарипова. – Душанбе: Глобус, 2006 – 880 с.
3. Кошечев В.Ю.Учебно-методическое пособие по дисциплине Уголовное право (Особенная часть). Душанбе. РТСУ. 2015. 161 с.
4. 4.Действующее международное право. (в двух томах). М., 2002.
5. 5.Международное публичное право. Сборник документов: в 2 ч. Ч. I / сост. и авт. вступ. статьи К. А. Бекяшев, Д. К. Бекяшев. – М.: ТК Велби, Изд-во Проспект, 2006. – 1408 с.
6. 6.Международное публичное право. Сборник документов: в 2 ч. Ч. II / сост. и авт. вступ. статьи К. А. Бекяшев, Д. К. Бекяшев. – М.: ТК Велби, Изд-во Проспект, 2006. – 1456 с.

### **5.3 Нормативно-правовые материалы (по мере необходимости)**

1. Конституция Российской Федерации. – М., 20.12.2017//Электронный ресурс constitutionrf.ru
2. Конституция Республики Таджикистан.- Издательство ИРФОН, Душанбе, 2016
3. Уголовный кодекс Российской Федерации/ Электронный ресурс www.consultant.ru – М., 2017.
4. Уголовный кодекс Республики Таджикистан. – Душанбе., Ахбори Маджлиси Оли РТ 24.02.2017.
5. Уголовно – процессуальный кодекс Российской Федерации. – М., 2013.
6. Кодекс исполнения уголовных наказаний Республики Таджикистан. – Душанбе., 2014.
7. Об охране здоровья граждан: Федеральный закон РФ от 21 ноября 2011г. // Российская газета. – 2011. – 23 ноября.
8. О предупреждении распространения в Российской Федерации заболевания, вызываемого вирусом иммунодефицита человека (ВИЧ-инфекции): Федеральный закон РФ от 30 марта 1995 г. // Российская газета. – 1995. – 12 апреля.
9. О трансплантации органов и (или) тканей человека: Федеральный закон РФ от 22 декабря 1992 г. (в ред. ФЗ от 29 ноября 2007г. № 279 ФЗ) // Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1993 г. – № 2. – Ст. 62.
10. О психиатрической помощи и гарантиях прав граждан при её оказании: закон Российской Федерации от 2 июля 1992 г. // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1992. – 20 авг.
11. О персональных данных: Федеральный закон РФ от 27 июля 2006 г. // Российская газета. – 2006. – 29 июля.
12. О средствах массовой информации: Федеральный закон РФ от 27 декабря 1991 г. // Российская газета. – 1992. – 8 января.
13. Об информации, информационных технологиях и о защите информации: Федеральный закон РФ от 27 июля 2006 г. // Российская газета. – 2006. – 29 июля.
14. О собраниях, митингах, демонстрациях, шествиях и пикетированиях: Федеральный закон РФ от 19 июня 2004 г. (в ред. ФЗ от 8 июля 2012г.) // Российская газета. – 2004. – 22 июня.
15. О свободе совести и о религиозных объединениях: Федеральный закон РФ от 26 сентября 1997г. (в ред. ФЗ от 1 июля 2011г.) // Российская газета. – 1997. – 1 октября.
16. Об оперативно-розыскной деятельности: Федеральный закон РФ от 12 августа 1995 г. (в ред. ФЗ от 29 ноября 2012г.) // Российская газета. –1995. – 18 августа.
17. Семейный кодекс Российской Федерации. – М., 2013.
18. Об основных гарантиях прав ребенка в Российской Федерации: Федеральный закон РФ от 24 июля 1998 г. (в ред. ФЗ от 21 июля 2011г.) // Российская газета. – 1998. – 5 августа.
19. Гражданский кодекс Российской Федерации. – М., 2013.
20. Налоговый кодекс Российской Федерации. – М., 2013.
21. Таможенный кодекс Российской Федерации. – М., 2013.
22. Земельный кодекс Российской Федерации. – М., 2013.

### **5.4 Перечень ресурсов информационно-телекоммуникационной сети Интернет**

1. ЭБС Юрайт.
2. ЭБС bibliorossica.com.
3. <http://www.consultant.ru/> - Справочно-правовая система «Консультант Плюс»;
4. <http://www.alleng.ru/edu/jurispr.htm> - Учебные материалы по юриспруденции;
5. [allpravo.ru](http://allpravo.ru) - сайт "Право России";
1. [law.pp.ru](http://law.pp.ru) - "Юридический факультет", конституции, законодательство;

6. tarasei.narod.ru - "Все о праве", правовая библиотека (учебники, пособия, лекции); "Все юридические ресурсы Интернета";
7. orgrave.ru - Юридический портал "Правопорядок": статьи, новости, судебная практика;
8. yurclub.ru - ЮрКлуб - виртуальный клуб юристов;
9. interlaw.dax.ru - Студенту – юристу;
10. <http://www.pravobazis.ru/osaite.php> - «Право как основа...»;
11. <http://www.preiskurant.ru/> - Справочник "Preiskurant";
12. <http://www.twirpx.com/> - Электронная библиотека twirpx.com.

#### **5.4. Перечень информационных технологий и программного обеспечения**

1. Адлия
2. Гарант
3. 3.Консультант Плюс
4. Электронная библиотека

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

Содержание методических указаний может включать:

1. рекомендации по планированию и организации времени, отведенного на изучение дисциплины;
2. рекомендации по работе с литературой;
3. разъяснения по работе с электронным учебным курсом, по выполнению домашних заданий.

Если по дисциплине изданы методические указания (рекомендации), здесь необходимо поместить их перечень со всеми выходными данными, а сами пособия либо приложить к РПД в печатном (изданном) виде, либо поместить в электронном виде в приложении к РПД (Приложение 3). Если изданных методических указаний по дисциплине нет, в приложение выносить ничего не нужно, все методические указания помещаются в данном разделе РПД.

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

В образовательном процессе используются:

- учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (учебная мебель, ноутбук, мультимедийный проектор, интерактивная доска/экран, меловая доска, трибуна);

- помещения для самостоятельной работы (оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронно-образовательную среду университета);

- помещения для хранения и профилактического обслуживания учебного оборудования.

В Университете созданы специальные условия обучающихся с ограниченными возможностями здоровья - специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания организаций и другие условия, без которых невозможно или затруднено освоение дисциплины обучающимися с ограниченными возможностями здоровья.

Обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература, а также обеспечивается:

наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;

присутствие ассистента, оказывающего обучающемуся необходимую помощь;

обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проёмов, лифтов).

### **8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ**

## **МАГИСТРАНТОВ**

*Форма итоговой аттестации (зачет).*

В качестве оценочных средств контроля знаний применяются:

- написание эссе по дисциплине
- контрольные задания и вопросы для промежуточного контроля знаний по дисциплине (для зачета – промежуточная аттестация)
- контрольные вопросы для контроля остаточных знаний по дисциплине (для аттестации по требованию)

**КОНТРОЛЬНЫЕ ВОПРОСЫ  
ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ЗНАНИЙ  
ПО ДИСЦИПЛИНЕ «ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ»  
(ДЛЯ ТЕКУЩЕЙ АТТЕСТАЦИИ И КОНТРОЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ)**

**Тематика контрольных работ по дисциплине  
«Особенности противодействия киберпреступности»**

1. Информационная безопасность и компьютерный терроризм методологические проблемы информационной безопасности.
2. Вопросы федеральной службы безопасности Российской Федерации.
3. Киберпреступность как новая форма терроризма
4. Европейская конвенция о пресечении терроризма от 27.01.1977.
5. Концепция противодействия терроризму в Российской Федерации.
6. Компьютерная преступность и обеспечение безопасности информации в ОВД.
7. Информационно-телекоммуникационная среда как новая сфера преступных посягательств.
8. Терроризм с помощью Интернета.
9. Кибертеррористический факт или воображение.
10. Защита информации в компьютерных системах и сетях.
11. Кибертерроризм как одна из разновидностей киберпреступности: понятие и виды.
12. Актуальные проблемы противодействия кибертерроризму.
13. Международные правовые аспекты противодействия высокотехнологичному терроризму.
14. Перспективы совершенствования права в условиях нарастания кибертеррористической угрозы.
15. Право безопасности: проблемы развития информационно-электронных систем.
16. Проблема обеспечения общественной безопасности в условиях создания «электронного государства».
17. Теоретико-правовые основы безопасного функционирования и развития информационно-электронных систем.
18. Интернет и терроризм: прежние цели — новые средства.
19. Киберпреступность и кибертерроризм.
20. Криминализация электронных посягательств.
21. Оценка риска кибертерроризма, кибервойн и других киберугроз.

**КОНТРОЛЬНЫЕ ЗАДАНИЯ И ВОПРОСЫ  
ДЛЯ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ЗНАНИЙ  
ПО ДИСЦИПЛИНЕ «ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ»  
(ДЛЯ ЗАЧЕТА – ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ)**

1. Кибертеррористический факт или воображение.
2. Защита информации в компьютерных системах и сетях.
3. Кибертерроризм как одна из разновидностей киберпреступности: понятие и виды.
4. Актуальные проблемы противодействия кибертерроризму.
5. Международные правовые аспекты противодействия высокотехнологичному терроризму.
6. Перспективы совершенствования права в условиях нарастания кибертеррористической угрозы.
7. Право безопасности: проблемы развития информационно-электронных систем.
8. Проблема обеспечения общественной безопасности в условиях создания «электронного государства».
9. Теоретико-правовые основы безопасного функционирования и развития информационно-электронных систем.
10. Интернет и терроризм: прежние цели — новые средства.
11. Киберпреступность и кибертерроризм.
12. Криминализация электронных посягательств.
13. Оценка риска кибертерроризма, кибервойн и других киберугроз.



**КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ КОНТРОЛЯ ОСТАТОЧНЫХ  
ЗНАНИЙ ПО ДИСЦИПЛИНЕ «ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ  
КИБЕРПРЕСТУПНОСТИ» (ДЛЯ АТТЕСТАЦИИ ПО ТРЕБОВАНИЮ)**

1. Вопросы федеральной службы безопасности Российской Федерации.
2. Европейская конвенция о пресечении терроризма от 27.01.1977.
3. Защита информации в компьютерных системах и сетях
4. Информационная безопасность и компьютерный терроризм методологические проблемы информационной безопасности.
5. Информационно-телекоммуникационная среда как новая сфера преступных посягательств.
6. Кибертерроризм как новая форма терроризма
7. Кибертеррористический факт или воображение.
8. Компьютерная преступность и обеспечение безопасности информации в ОВД.
9. Концепция противодействия терроризму в Российской Федерации.