

МИНОБРНАУКИ РОССИИ



**Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)**

**ИСТОРИКО-АРХИВНЫЙ ИНСТИТУТ
ФАКУЛЬТЕТ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ, ПОЛИТОЛОГИИ И
ЗАРУБЕЖНОГО РЕГИОНОВЕДЕНИЯ**

Кафедра зарубежного регионоведения и внешней политики

**КИБЕРТЕРРОРИЗМ В XXI ВЕКЕ КАК РЕГИОНАЛЬНАЯ
И ГЛОБАЛЬНАЯ УГРОЗА**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Направление подготовки: 41.04.01 «Зарубежное регионоведение»
Направленность (профиль): «Страны и регионы мира в мировой политике и
международном бизнесе»**

**Уровень квалификации выпускника - магистр
Форма обучения - очная**

**РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов**

Москва 2024

**КИБЕРТЕРРОРИЗМ В XXI ВЕКЕ
КАК РЕГИОНАЛЬНАЯ И ГЛОБАЛЬНАЯ УГРОЗА**

Составитель:

д.ю.н., профессор В.В.Алешин

УТВЕРЖДЕНО

Протокол заседания кафедры международной
безопасности

№ 5 от 05.03 2024 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1 Цель и задачи дисциплины

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

1.3. Место дисциплины в структуре образовательной программы

2. Структура дисциплины

3. Содержание дисциплины

4. Образовательные технологии

5. Оценка планируемых результатов обучения

5.1. Система оценивания

5.2. Критерии выставления оценок

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

7. Материально-техническое обеспечение дисциплины

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

9. Методические материалы

9.1. Планы практических (семинарских, лабораторных) занятий

9.2. Методические рекомендации по подготовке письменных работ

9.3. Иные материалы

Приложения

Приложение 1. Аннотация дисциплины

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Дисциплина «Кибертерроризм в XX веке как региональная и глобальная угроза» является частью профессионального цикла дисциплин подготовки студентов по направлению подготовки магистратуры 41.04.01 «Зарубежное регионоведение», направленность «Страны и регионы мира в мировой политике и бизнесе». Дисциплина реализуется на факультете международных отношений, политологии и зарубежного регионоведения ИАИ РГГУ кафедрой международной безопасности.

Цель дисциплины – формирование у студентов целостных знаний о современном кибертерроризме, современных террористических вызовах и угрозах, их взаимосвязи с проблемами безопасности в условиях динамично меняющегося мира.

Задачи дисциплины:

- приобретение студентами необходимых знаний, умений и навыков по анализу причин и условий, способствующих проявлению и росту экстремизма и кибертерроризма в 21 веке;
- привитие аналитических навыков по оценке современных кибертеррористических угроз;
- овладение студентами базовыми знаниями по контр кибертеррористическим мерам в странах изучаемого региона;
- формирование представления об особенностях противодействия современному кибертерроризму с позиций межкультурного диалога в регионе и в мире в целом;
- развитие у студентов навыков работы с основными источниками и литературой по тематике, связанной с проблемами противодействия современному международному кибертерроризму;
- развитие у студентов навыков работы с интернет-сайтами, посвященными изучаемой тематике;
- достижение творческого осмысления изучаемого материала, на основе полученных знаний, выработка студентами собственного личностного видения процессов, наиболее характерных явлений, развивающихся в глобальном международном пространстве при оценке современного кибертерроризма;
- овладение студентами умением применять полученные теоретические знания для анализа текущих проблем национальной безопасности России и международной безопасности.

1.2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
УК- 5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1. Находит и использует необходимую для саморазвития и взаимодействия с другими людьми информацию о культурных особенностях	Знать: различные типы культур в регионах мира Уметь: учитывать разнообразие культур в процессе межкультурного взаимодействия Владеть: навыками анализа разнообразия культур в процессе межкультурного взаимодействия

	и традициях различных социальных групп.	
ПК-2 Способен анализировать современные политико-экономические тенденции на уровне страны или региона с учетом исторической ретроспективы.	ПК-2.1. Самостоятельно подбирает необходимый методологический инструментарий для аналитических работ разной сложности, посвященных регион специализации.	<p>Знать: основные направления и школы научных исследований в области изучения конфликтологии ;</p> <p>Хронологию международных конфликтов после окончания Второй мировой войны; взаимосвязи глобальных, макрорегиональных, национально-государственных, региональных и локальных политико-культурных, социально-экономических и общественно-политических явлений и процессов.</p> <p>Уметь моделировать и оценивать глобальные, макрорегиональные, национально-государственные, региональные и локальные политико-культурные, социально-экономические и общественно-политические процессы в области международных конфликтов и национальных интересов России.</p> <p>Владеть навыком прогнозирования глобальных, макрорегиональных, национально-государственных, региональных и локальных политико-культурных, социально-экономических и общественно-политических процессов в области международной безопасности; способностью профессионально грамотно анализировать и пояснять позиции Российской Федерации по основным международным проблемам и конфликтам</p>

<p>ПК-3 Способен применять на практике основы исторических, политологических и социологических концепций и методов, принимать участие в планировании и проведении полевого исследования в стране или регионе специализации</p>	<p>ПК-3.1. Самостоятельно анализирует классические и современные теории и концепции общественно-политического развития стран(ы) профильного региона в контексте глобального, макрорегионального, национально-государственного, регионального и локального уровней.</p>	<p>Знать: теории и методы международно-политических исследований; принципы формулирования задач научного исследования кибертерроризма. Уметь: соотносить задачи научного исследования с имеющимися в современной международных отношения с теориями и методами и мировым опытом борьбы с кибертерроризмом; вести поиск релевантной исследовательским задачам информационной и международной безопасности, Владеть: - опытом решения задач научных исследований с помощью свободно выбираемых теорий и методов, информационных технологий с использованием мирового опыта, составления плана и программы научного исследования кибертерроризма.</p>
--	--	---

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Кибертерроризм в XX веке как региональная и глобальная угроза» является частью профессионального цикла дисциплин подготовки студентов по направлению подготовки магистратуры 41.04.01 «Зарубежное регионоведение», направленность «Страны и регионы мира в мировой политике и бизнесе». Дисциплина реализуется на факультете международных отношений и зарубежного регионоведения ИАИ РГГУ кафедрой международной безопасности.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения таких дисциплин, как: «Кросс-региональный анализ», «Интеграционные и дезинтеграционные процессы в регионах мира», «Европейский союз как международный актор», «Внешняя политика США: региональные и глобальные аспекты», прохождения научно-исследовательской практики.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Ближний Восток в эпоху турбулентности», «Особенности политического и социально-экономического развития США в XXI веке», «Политические и социально-экономические трансформации в странах Европы», «Типология современных региональных конфликтов», , прохождения преддипломной практики.

2. Структура дисциплины

Общая трудоемкость освоения дисциплины составляет 3 зач.ед. 108 ак.ч.

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
3	Лекции	18

3	Семинары	12
Всего:		30

Объем дисциплины в форме самостоятельной работы обучающихся составляет 60 академических часов, контроль - 18 ак. ч.

3. Содержание дисциплины

<i>№</i>	<i>Наименование раздела дисциплины</i>	<i>Содержание</i>
<i>1</i>	Теоретические основы терроризма и экстремизма. Терроризм как проблема современности.	Экстремизм и причины его возникновения. Сущность и содержание экстремизма как идеологии и конкретной политической практики. Экстремизм как выражение крайних взглядов и установок определенных социальных сил. Характеристика понятий «экстремизм», «политический экстремизм», «религиозный экстремизм» и «религиозно-политический экстремизм». Анализ причинно-следственных связей экстремизма, его функций в системе общественных отношений, объективные и субъективные причины возникновения экстремизма. Специфика религиозно-политического экстремизма. Связь экстремизма с терроризмом как крайним проявлением экстремистской деятельности. Проблемы проявления религиозно-политического экстремизма во внутри- и межконфессиональных отношениях. Виды терроризма: государственный, международный, организационно-групповой, индивидуальный, революционный, криминальный (уголовный), информационный, идеологический. Виды террористических актов: диверсия, похищение, покушение и убийство, ограбление (экспроприация), захват зданий, вооруженное нападение, кибертерроризм.
<i>2</i>	Кибертерроризм как продукт глобализации. Интернет как сфера распространения идеологии терроризма.	Глобальное развитие информационных технологий. Двойственность роли информационно-коммуникационных технологий. Злоупотребление высокими технологиями как фактор возникновения кибертерроризма. Сущность понятий кибертерроризма. Общая характеристика и отличительные черты от терроризма вообще. Противодействие кибертерроризму как важная государственная задача по обеспечению информационной безопасности гражданского населения.
<i>3</i>	Законодательное противодействие распространению террористических материалов в Интернете и кибертерроризма.	Международное законодательство. Международные стандарты в области предупреждения преступлений в информационно-коммуникационной сфере. Конгрессы ООН по предупреждению преступности и обращению с правонарушителями. Конвенция Совета Европы «О

		киберпреступности» ETS № 185 от 23 ноября 2001 г. Международный опыт противодействия терроризму в сфере информационно-коммуникационных технологий. Российское законодательство. Закон РФ «О средствах массовой информации» от 27 декабря 1991 года. Федеральный закон «О противодействии терроризму» от 6 марта 2006 года.
4	Экстремизм и кибертерроризм как угрозы национальной безопасности России.	Экстремизм как угроза национальной безопасности и целостности Российской Федерации. Рост проявлений экстремизма в современной России. Виды экстремизма: националистический, политический, религиозный, экологический, экономический. Специфика молодежного экстремизма. Политические, экономические, социальные, культурно-цивилизационные и идеологические причины возрастания террористических и кибертеррористических угроз в современной России.
5	Международный кибертерроризм и опыт противодействия терроризму	Международный кибертерроризм как вызов безопасности мирового сообщества. межгосударственное сотрудничество и его роль в борьбе с кибертерроризмом. Роль ООН в выработке и реализации стандартов в сфере предупреждения и пресечения кибертерроризма. Глобальная контртеррористическая стратегия ООН и других международных организаций.

4. Образовательные и информационные технологии

Для проведения занятий лекционного типа по дисциплине применяются такие образовательные технологии как интерактивные лекции, проблемное обучение. Для проведения занятий семинарского типа используются групповые дискуссии, анализ ситуаций и решений кейсов.

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов
----------------	-------------------------

	За одну работу	Всего
Текущий контроль:		
- опрос	5 баллов	30 баллов
- письменная работа (реферат)	30 баллов	30 баллов
Промежуточная аттестация		40 баллов
Ответ на контрольные вопросы		
Итого за семестр		100 баллов
Экзамен		

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
82-68/ С	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	«неудовлетворительно»/ не зачтено	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Контрольные вопросы для опроса на семинаре

1. Понятие экстремизма и терроризма. Виды терроризма.
2. Психология террориста. Проблема экстремизма и терроризма.
3. Виды экстремизма: националистический, политический, религиозный, экологический, экономический.
4. Кибертеррористические акты на территории постсоветской России.
5. Международный кибер терроризм как вызов безопасности мирового сообщества.
6. Кибертерроризм как продукт глобализации.
7. Интернет как сфера распространения идеологии терроризма.
8. Глобальное развитие информационных технологий.
9. Двойственность роли информационно-коммуникационных технологий. Злоупотребление высокими технологиями как фактор возникновения кибертерроризма.
10. Сущность понятий кибертерроризма.
11. Социально важные функции Интернета: коммуникативная, интегрирующая, актуализирующая, геополитическая, социальная.
12. Противодействие кибертерроризму как важная государственная задача по обеспечению информационной безопасности гражданского населения.
13. Законодательное противодействие распространению террористических материалов в Интернете и кибертерроризма.
14. Международные стандарты в области предупреждения преступлений в информационно-коммуникационной сфере.
15. Международный опыт противодействия терроризму в сфере информационно-коммуникационных технологий.
16. Экстремизм и кибертерроризм как угрозы национальной безопасности России.
17. Экстремизм как угроза национальной безопасности и целостности Российской Федерации.
18. Международный кибертерроризм и опыт противодействия терроризму.
19. Международный кибертерроризм как вызов безопасности мирового сообщества. Межгосударственное сотрудничество и его роль в борьбе с кибертерроризмом.
20. Роль ООН в выработке и реализации стандартов в сфере предупреждения и пресечения кибертерроризма.
21. Глобальная контртеррористическая стратегия ООН и других международных организаций.

Критерии оценки опроса

оценка «неудовлетворительно» (0-2 балла) ставится в том случае, если знание материала носит фрагментарный характер, наличие грубых ошибок в ответе;

оценка «удовлетворительно» (3 балла) выставляется, если материал освоен частично, допущено не более двух-трех недочетов;

оценка «хорошо» (4 балла) выставляется в том случае, если материал освоен почти полностью, допущено не более одного-двух недочетов, но обучающийся смог бы их исправить самостоятельно;

оценка «отлично» (5 баллов) выставляется студенту, если материал освоен полностью, ответ построен по собственному плану.

Баллы суммируются

Максимум – 30 баллов

Темы письменной работы (реферат):

1. Причины, условия и формы проявления терроризма и кибертерроризма.
2. Сущность терроризма и кибертерроризма.
3. Виды кибертеррористических актов.
4. Влияние глобализации на рост экстремизма и кибертерроризма.
5. Транснациональный характер экстремизма и кибертерроризма.
6. Пропаганда экстремизма и терроризма в сети Интернет.
7. Экстремизм и кибертерроризм как угроза безопасности России.
8. Теоретико-правовые основы противодействия кибертерроризму.
9. Опыт противодействия кибертерроризму в Европе.
10. Опыт противодействия кибертерроризму в США.
11. Деятельность правоохранительных органов Российской Федерации по противодействию кибертерроризму на современном этапе.
12. Международное законодательство в борьбе с кибертерроризмом.
13. Понятие кибертерроризма. Виды кибертерроризма.
14. Виды экстремизма: националистический, политический, религиозный, экологический, экономический, информационный.
15. Специфика экстремизма и кибертерроризма.
16. Политические, экономические, социальные, культурно-цивилизационные и идеологические причины террористических и кибертеррористических угроз.
17. Международный кибертерроризм как вызов безопасности мирового сообщества.
18. Межгосударственное сотрудничество в борьбе с кибертерроризмом.
19. Роль ООН в выработке и реализации стандартов в сфере предупреждения и пресечения кибертерроризма.
20. Глобальная контртеррористическая стратегия ООН и ее задачи.
21. Международные контртеррористические операции в области кибертерроризма.
22. Модели построения кибертеррористических структур
23. Особенности кибертеррористических актов в России в XXI в..
24. Опыт и проблемы противодействия кибер терроризму зарубежных стран(на примере государства) .
25. Принципы борьбы с киберроризмом в международно-правовых документах.
26. Законы Российской Федерации по борьбе с экстремизмом и кибертерроризмом.
27. Институты России в борьбе с кибертерроризмом.
28. Проблема кибертерроризма в Европе.
29. Кибертеррористические акты в США. Законодательные акты по борьбе с кибертерроризмом.

Критерии оценки письменной работы (реферат)

оценка «отлично» (30-25 баллов) выставляется студенту, если он дал исчерпывающие ответы на задания; текст хорошо и логично структурирован, написан хорошим научным языком, грамотно;

оценка «хорошо» (24-16) баллов) выставляется в том случае, если даны довольно полные ответы на задания, но допущены неточности, есть отдельные ошибки; нарушена структура текста;

оценка «удовлетворительно» (15-9 баллов) ставится, если ответы на задания неполные, есть ошибки; написано небрежно, нет хорошей структуры текста;

оценка «неудовлетворительно» (0-9) баллов) ставится в том случае, если либо фактически не выполнены задания, либо нет демонстрации общей эрудиции и знаний лекционного материала.

Максимум – 30 баллов

Контрольные вопросы для итоговой аттестации

1. Виды экстремизма: националистический, политический, религиозный, экологический, экономический.
2. Кибертеррористические акты на территории постсоветской России.
3. Международный кибер терроризм как вызов безопасности мирового сообщества.
4. Кибертерроризм как продукт глобализации.
5. Интернет как сфера распространения идеологии терроризма.
6. Глобальное развитие информационных технологий.
7. Двойственность роли информационно-коммуникационных технологий. Злоупотребление высокими технологиями как фактор возникновения кибертерроризма.
8. Сущность понятий кибертерроризма.
9. Социально важные функции Интернета: коммуникативная, интегрирующая, актуализирующая, геополитическая, социальная.
10. Противодействие кибертерроризму как важная государственная задача по обеспечению информационной безопасности гражданского населения.
11. Законодательное противодействие распространению террористических материалов в Интернете и кибертерроризма.
12. Экстремизм как угроза национальной безопасности и целостности Российской Федерации.
13. Международный кибертерроризм и опыт противодействия терроризму
14. Международный кибертерроризм как вызов безопасности мирового сообщества. Межгосударственное сотрудничество и его роль в борьбе с кибертерроризмом.
15. Роль ООН в выработке и реализации стандартов в сфере предупреждения и пресечения кибертерроризма.
16. Глобальная контртеррористическая стратегия ООН и других международных организаций.

Критерии оценки ответа

оценка «отлично» (35-40 баллов) выставляется студенту, если он дал исчерпывающие ответы на задания; ответы хорошо и логично структурированы, изложены хорошим научным языком, грамотно;

оценка «хорошо» (25-35 баллов) выставляется в том случае, если даны довольно полные ответы на задания, но допущены неточности, есть отдельные ошибки; нарушена структура ответа;

оценка «удовлетворительно» (10-25 баллов) ставится, если ответы на задания неполные, есть ошибки; написано небрежно, нет хорошей структуры ответа;

оценка «неудовлетворительно» (1-10 баллов) ставится в том случае, если либо фактически не выполнены задания, либо нет демонстрации общей эрудиции и знаний лекционного материала.

Максимум – 40 баллов

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Основная литература

Учебная

1. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1167736>
2. Информационное общество и международные отношения: Учебник / Болгов Р.В., Васильева Н.А., Виноградова С.М. - СПб:СПбГУ, 2014. - 384 с.: ISBN 978-5-288-05510-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/941412>
3. Кафтан, В. В. Противодействие терроризму : учебное пособие для бакалавриата и магистратуры / В. В. Кафтан. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 261 с. — (Высшее образование). — ISBN 978-5-534-00322-2. — URL : <https://urait.ru/book/protivodeystvie-terrorizmu-433075>
4. Красинский, В. В. Кто есть кто в международном терроризме : справочник / В.В. Красинский, В.В. Машко. — Москва : ИНФРА-М, 2020. — 128 с. — www.dx.doi.org/10.12737/textbook_5acf296dbf4dd8.80181407. - ISBN 978-5-16-014191-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1042598>
5. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху: О. А. Степанов. — Москва : Издательство Юрайт, 2020. — 103 с. — (Актуальные монографии). — ISBN 978-5-534-12775-1. — URL : <https://urait.ru/bcode/448300>
6. Овчинский, В. С. Криминология цифрового мира : учебник для магистратуры / В. С. Овчинский. - Москва : Норма : ИНФРА-М, 2018. -352 с. - ISBN 978-5-16-106320-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/948179>
7. Овчинский, В. С. Основы борьбы с киберпреступностью и кибертерроризмом : хрестоматия / сост. В. С. Овчинский. — Москва : Норма, 2020. — 528 с. - ISBN 978-5-91768-814-5. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1047117>

Дополнительная литература

1. Акопов, Г. Л. Политика и Интернет: Монография / Г.Л. Акопов. - Москва : НИЦ ИНФРА-М, 2014. - 202 с. (Научная мысль; Политология). ISBN 978-5-16-009930-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/462249>
2. Бабурин, С. Н. Стратегия национальной безопасности России: теоретико-методологические аспекты : монография / С.Н. Бабурин, М.И. Дзалиев, А.Д. Урсул.

- Москва : Магистр : ИНФРА-М, 2018. — 512 с. - ISBN 978-5-9776-0224-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/926476>
3. Демидов, О. Глобальное управление Интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества: Научно-популярное / Демидов О. - М.: Альпина Паблишер, 2016. - 198 с.: ISBN 978-5-9614-5820-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1002128>
 4. Информационное противодействие угрозам терроризма в глобальном мире: Монография / Поликарпов В.С., Котенко В.В., Поликарпова Е.В. - Таганрог: Южный федеральный университет, 2016. - 204 с.: ISBN 978-5-9275-2310-8. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/999>
 5. Красинский, В. В. Международная террористическая организация «Исламское государство»: история, современность : монография / В.В. Красинский, В.В. Машко. — Москва : ИНФРА-М, 2018. — 108 с. — (Научная мысль). — www.dx.doi.org/10.12737/monography_58edd04b5a9c70.03011442. - ISBN 978-5-16-105741-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/920285>
 - Лабуш, Н. С. Медиатизация экстремальных форм политического процесса : война, революция, терроризм : учебное пособие / Н. С. Лабуш, А. С. Пую. - СПб : Изд-во С.-Петерб. ун-та, 2019. - 340 с. - ISBN 978-5-288-05944-5. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/1080921>
 6. Овчинский, В. С. Интерпол против терроризма: Сборник международных документов / Министерство Внутренних Дел РФ; Сост. В.С. Овчинский. - Москва : ИНФРА-М, 2012. - 810 с. ISBN 978-5-16-003474-4. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/323701>
 7. Овчинский, В. С. Международно-правовые основы борьбы с терроризмом: Сборник документов / Сост. В.С. Овчинский. - Москва : ИНФРА-М, 2003. - 480 с. (Высшее образование). ISBN 5-16-001527-2. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/63797>
 8. Понкин, И. В. Неклассические войны : монография / И.В. Понкин. — Москва : ИНФРА-М, 2019. — 87 с. — (Научная мысль). — www.dx.doi.org/10.12737/monography_5c06232de7a053.62136867. - ISBN 978-5-16-107051-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/989823> (дата обращения: 14.09.2020)
 9. Соснин, В. А. Психология современного терроризма : учебное пособие / В.А. Соснин. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2020. — 160 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-103961-8. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/1082921>
 10. Соснин, В.А. Современный терроризм: социально-психологический анализ : монография / В.А. Соснин, Т.А. Нестик. - Москва : Институт психологии РАН, 2008. - 240 с. - ISBN 978-5-9270-0137-8. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/1059119>
 11. Терроризм и организованная преступность: монография / С.А. Солодовников [и др.] ; под ред. С .А. Солодовникова. — 2-е изд., перераб. и доп. — М. : ЮНИТИ-ДАНА: Закон и право, 2017. — 247 с. - ISBN 978-5-238-01749-5. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/1028773>
 12. Шариков, П. А. Проблемы информационной безопасности в полицентричном мире / П.А. Шариков. - М.: Весь Мир, 2015. - 320 с. ISBN 978-5-7777-0601-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/>
 13. Харрис, Ш. Кибервойн@: Пятый театр военных действий / Харрис Ш.; Пер. с англ. Лазарева Д. - Москва : Альпина нон-фикшн, 2016. - 390 с. ISBN 978-5-91671-495-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/697989>

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Электронная библиотека диссертаций Российской государственной библиотеки - <http://diss.rsl.ru> (только из отдела «Электронная библиотека» ГУУ)

Электронно-библиотечная система «BOOK.RU»- <http://book.ru>

EBSCO – универсальная база данных зарубежных полнотекстовых научных журналов по всем областям знаний - <http://search.epnet.com>

Научные материалы широкого диапазона академических дисциплин издательства Scientific&AcademicPublishing (SAP), США - <http://www.sapub.org>

База данных междисциплинарного характера, включает научные журналы по гуманитарным, социальным наукам (всего 26 дисциплин) - www.jstor.org/

Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Национальная электронная библиотека (НЭБ) www.rusneb.ru

ELibrary.ru Научная электронная библиотека www.elibrary.ru

Электронная библиотека Grebennikon.ru www.grebennikon.ru

Cambridge University Press

ProQuest Dissertation & Theses Global

SAGE Journals

Taylor and Francis

JSTOR

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины используются: компьютерный класс с возможностью презентации в системе «Power Point» с лицензионным программным обеспечением с доступом в Интернет.

1. Windows
2. Microsoft Office
3. Adobe Master Collection
4. AutoCAD
5. Archicad
6. SPSS Statistics
7. ОС «Альт Образование»
8. Visual Studio
9. Adobe Creative Cloud

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины «Современный международный терроризм» используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
 - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
 - в форме аудиофайла.

- для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа;
 - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
 - устройством для сканирования и чтения с камерой SARA CE;
 - дисплеем Брайля PAC Mate 20;
 - принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:
 - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;

- акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - передвижными, регулируемые эргономическими партами СИ-1;
 - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий (12ч.)

Итогом практических занятий является закрепление и прочное усвоение материалов прослушанного лекционного курса. На этапе подготовки семинара доминирует самостоятельная работа учащихся с учебной литературой и другими дидактическими средствами над серией поставленных вопросов, проблем и задач. В процессе семинара идут активное обсуждение, дискуссии и выступления учащихся, под руководством педагога делаются обобщающие выводы и заключения.

Тема 1. Теоретические основы терроризма и экстремизма. Терроризм как проблема современности. (2 ч.)

Вопросы для обсуждения и докладов

1. Причины, условия и формы проявления экстремизма и терроризма.
2. Сущность экстремизма и терроризма.
3. Виды терроризма и террористических актов.
4. Международный экстремизм и терроризм.
5. Терроризм как крайняя форма проявления экстремизма.

Контрольные вопросы

1. В чем заключается смысл терроризма.
2. В чем заключается смысл экстремизма.
3. Приведите примеры террористических и экстремистских проявлений.

Тема 2. Кибертерроризм как продукт глобализации.

Интернет как сфера распространения идеологии терроризма. – 2 ч.

Вопросы для обсуждения

1. Глобальное развитие информационных технологий.
2. Двойственность роли информационно-коммуникационных технологий. Злоупотребление высокими технологиями как фактор возникновения кибертерроризма.
3. Сущность понятий кибертерроризма. Общая характеристика и отличительные черты от терроризма вообще.
4. Противодействие кибертерроризму как важная задача по обеспечению информационной безопасности государства и гражданского населения.

Тема 3 Законодательное противодействие распространению террористических материалов в Интернете и кибертерроризма. – 2 ч.

Вопросы для обсуждения

1. Международное законодательство. Международные стандарты в области предупреждения преступлений в информационно-коммуникационной сфере.
2. Конгрессы ООН по предупреждению преступности и обращению с правонарушителями.
3. Конвенция Совета Европы «О киберпреступности» ETS № 185 от 23 ноября 2001 г.

4. Международный опыт противодействия терроризму в сфере информационно-коммуникационных технологий.
5. Российское законодательство. Закон РФ «О средствах массовой информации» от 27 декабря 1991 г. Федеральный закон «О противодействии терроризму» от 6 марта 2006 г.

Тема 4. Экстремизм и кибертерроризм как угрозы национальной безопасности России. – 2 ч.

Вопросы для обсуждения

1. Экстремизм как угроза национальной безопасности и целостности Российской Федерации. Виды экстремизма: националистический, политический, религиозный, экологический, экономический.
2. Кибертерроризм в России: внутри политические и внешне политические аспекты
3. Кибертерроризм в экономической и финансовой сферах России
4. Политические, экономические, социальные, культурно-цивилизационные и идеологические причины возрастания кибертеррористических угроз в современной России.

Тема 5. Международный кибертерроризм и опыт противодействия терроризму – 2 ч.

Вопросы для обсуждения

1. Международный кибертерроризм как вызов безопасности мирового сообщества. Межгосударственное сотрудничество и его роль в борьбе с кибертерроризмом.
2. Роль ООН в выработке и реализации стандартов в сфере предупреждения и пресечения кибертерроризма.
3. Глобальная контр террористическая стратегия ООН и других международных организаций.
4. Опыт зарубежных стран в борьбе с кибертерроризмом

9.2 Методические указания по освоению дисциплины.

Самостоятельная работа нацелена на расширение теоретических и фактических знаний, когнитивных и практических умений на основе поиска и анализа информации, а также изучения студентами теоретической базы курса при подготовке к семинарским занятиям, к промежуточной и итоговой письменной аттестации.

Самостоятельная работа может выполняться студентом в читальном зале библиотеки, в компьютерных классах, а также в домашних условиях.

Наряду с обсуждением основных вопросов планов семинарских занятий, изучением основных и дополнительных источников и литературы по темам семинарских занятий, каждому студенту следует выступить с докладом по выбранной теме.

Для выступления на занятии студенту отводится 10-12 минут. Поэтому в своем выступлении по избранной теме нужно изложить основные позиции и выводы. После заслушивания доклада продолжается общая дискуссия на семинаре по вопросам плана занятия. Активность участия в дискуссии – один из важных критериев аттестации по итогам семинарских занятий.

9.3 Методические рекомендации по подготовке письменных работ

Требования к выполнению письменной работы (реферат):

- рефераты выполняются в часы, отведенные для самостоятельных занятий,
- студенты, не написавшие рефераты, выполняют их в установленное преподавателем сроки по заданию преподавателя,
- рефераты должны раскрывать заданные преподавателем темы, базируясь на литературе, приведенной в РПД.

Реферат (эссе) по выбранной теме рекомендуется готовить объемом 12 стр. Его структура включает следующие разделы: введение, с постановкой проблемы, обзором использованных источников и литературы по теме. Основной текст разбивается, как правило, на 2 части. Он должен содержать анализ главных проблем и мнения автора, его мысли, идеи. В конце реферата следует заключение (1 – 2 стр.) с основными выводами по теме. В работе должен содержаться список используемых источников и литературы (не менее 5-7). Оформление должно соответствовать требованиям ГОСТов.

Аннотация

Дисциплина «Кибертерроризм в XX веке как региональная и глобальная угроза» является частью профессионального цикла дисциплин подготовки студентов по направлению подготовки магистратуры 41.04.01 «Зарубежное регионоведение», направленность «Страны и регионы мира в мировой политике и бизнесе». Дисциплина реализуется на факультете международных отношений, политологии и зарубежного регионоведения ИАИ РГГУ кафедрой международной безопасности.

Цель дисциплины – формирование у студентов целостных знаний о современном кибертерроризме, современных террористических вызовах и угрозах, их взаимосвязи с проблемами безопасности в условиях динамично меняющегося мира.

Задачи дисциплины:

- приобретение студентами необходимых знаний, умений и навыков по анализу причин и условий, способствующих проявлению и росту экстремизма и кибертерроризма в 21 веке;
- привитие аналитических навыков по оценке современных кибертеррористических угроз;
- овладение студентами базовыми знаниями по контр кибертеррористическим мерам в странах изучаемого региона;
- формирование представления об особенностях противодействия современному кибертерроризму с позиций межкультурного диалога в регионе и в мире в целом;
- развитие у студентов навыков работы с основными источниками и литературой по тематике, связанной с проблемами противодействия современному международному кибертерроризму;
- развитие у студентов навыков работы с интернет-сайтами, посвященными изучаемой тематике;
- достижение творческого осмысления изучаемого материала, на основе полученных знаний, выработка студентами собственного личностного видения процессов, наиболее характерных явлений, развивающихся в глобальном международном пространстве при оценке современного кибертерроризма;
- овладение студентами умением применять полученные теоретические знания для анализа текущих проблем национальной безопасности России и международной безопасности.

В результате освоения дисциплины обучающиеся должны:

Знать:

- основные понятия дисциплины «Кибертерроризм в 21 веке как глобальная и региональная угроза» особенности международного кибертерроризма, включая условия и причины его появления и развития.
- взаимосвязи глобальных, макрорегиональных, национально-государственных, региональных и локальных политико-культурных, социально-экономических и общественно-политических явлений и процессов в области кибертерроризма
- возможные угрозы национальной безопасности России со стороны террористических движений и угроз кибертерроризма
- типовое содержание основных профессиональных и дополнительных образовательных программ в области методологии исследования причин кибертерроризма.
- предпосылки возникновения, особенности формирования, ключевые этапы и характерные черты современных кибертеррористических организаций; основные механизмы и политические технологии противодействия экстремизму и кибертерроризму

- теории и методы международно-политических исследований; принципы формулирования задач научного исследования кибертерроризма.

- правовые основы обеспечения безопасности РФ и нормативно-правовую базу противодействия экстремизму и кибертерроризму.

Уметь:

- составлять предложения и рекомендации по противодействию кибертерроризму для органов государственной власти, негосударственных политических и общественных организаций

- моделировать и оценивать глобальные, макрорегиональные, национально-государственные, региональные и локальные политико-культурные, социально-экономические и общественно-политические процессы в области кибертерроризма и мировой политики с применением методов теоретического и эмпирического исследования и прикладного характера

- анализировать наличие и рост экстремизма и кибертерроризма в регионе, выявлять причины и условия существования террористической угрозы.

- реализовывать основные профессиональные и дополнительные образовательные программы в области теоретических исследований кибертерроризма в международных отношениях.

- ориентироваться в современной государственной, региональной и международной системе противодействия кибертерроризму.

- соотносить задачи научного исследования с имеющимися в современной международных отношениях с теориями и методами и мировым опытом борьбы с кибертерроризмом;

Владеть:

- алгоритмом разрешения ситуаций в областях повышенной политической напряженности с использованием знаний и методов межкультурной коммуникации в борьбе с кибертерроризмом.

- способностью к обобщению, анализу, восприятию политической информации по проблемам кибертерроризма.

- навыком прогнозирования глобальных, национально-государственных процессов и борьбы с кибертерроризмом

- знанием составления и оформления нормативно-правовых документов в сфере противодействия кибертеррористической угрозе.