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

ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра «Уголовное право»

«УТВЕРЖДАЮ»
Зав. кафедрой уголовного права
д.ю.н. доцент Абдуллаева Р.А.
_____
«18» _____ 2024г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

По учебной дисциплине
«Особенности противодействия киберпреступности»
Направления подготовки – **40.04.01 «Юриспруденция»**
Программа подготовки – **«Уголовно-криминологическая основа следственной деятельности»**
Форма подготовки – **очная**
Уровень подготовки – **магистратура**

ДУШАНБЕ – 2024

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Особенности противодействия киберпреступности»

№ п/п	Контролируемые разделы, темы,	Формируемые компетенции	Оценочные средства		
			Индикаторы достижения компетенции	Другие оценочные средства	
				Кол-во экз-ных билетов	Вид
1	Тема 1. Понятие и сущность киберэкстремизма.	УК-1 УК-3 ПК-1	**ИУК-1.1.** Демонстрирует основные методы критического анализа, методологию системного подхода. **ИУК-1.2.** Выявляет проблемные ситуации, используя методы анализа, синтеза и абстрактного мышления; осуществляет поиск решений проблемных ситуаций на основе действий, эксперимента и опыта; **ИУК-1.3.** Владеет технологиями выхода из проблемных ситуаций, навыками выработки стратегии действий; навыками критического анализа.	2	Тестирование ,выступление на семинарах, защита рефератов
2	Тема 2. Информационная безопасность и компьютерный терроризм.	УК-1 УК-3 ПК-1	**ИУК-3.1.** Анализирует общие формы организации деятельности коллектива; психологию межличностных отношений в группах разного возраста; основы стратегического планирования работы коллектива для достижения поставленной цели; **ИУК-3.2.** Способен создавать в коллективе психологически безопасную доброжелательную среду; предвидеть результаты (последствия) как личных, так и коллективных действий; планировать командную работу, распределять поручения и делегировать полномочия членам команды; **ИУК-3.3.** Владеет навыками постановки цели в условиях командой работы; способами управления командной работой в решении поставленных задач; навыками преодоления возникающих в коллективе разногласий, споров и конфликтов на основе учета интересов всех сторон.	2	Тестирование ,выступление на семинарах, защита рефератов
3.	Тема 3. Киберэкстремизм как новая форма терроризма.	УК-1 УК-3 ПК-1	**ИПК-1.1.** Способен воспринимать знание в области уголовно-криминологической, следственной деятельности по выявлению, расследованию, пресечению и раскрытию и преступлений и иных правонарушений; **ИПК-1.2.** Способен планировать выявление, пресечение, расследование и раскрытие преступлений и иных правонарушений, разрабатывать алгоритм и совершать необходимые уголовно-криминологические, уголовно-процессуальные действия, связанные с выявлением, пресечением, расследованием и раскрытием преступлений и правонарушений. **ИПК-1.3.** Способен применять навыки определения последовательности проведения следственных деятельности	1	Тестирование ,выступление на семинарах, защита рефератов, докладов

			для выявления, пресечения, расследования и раскрытия различных видов преступлений и основе анализа следственной ситуации досудебного производства.		
4.	Тема 4. Компьютерная преступность и обеспечение безопасности информации в ОВД.	УК-1 УК-3 ПК-1	ИУК-1.1.;ИУК-1.2.;ИУК-1.3. ИУК-3.1.;ИУК-3.2;ИУК-3.3. ИПК-1.1.;ИПК-1.2.;ИПК-1.3.	1	Тестирование, выступление на семинарах, защита рефератов
5.	Тема 5. Правовые аспекты противодействия высокотехнологичному киберэкстремизму.	УК-1 УК-3 ПК-1	ИУК-1.1.;ИУК-1.2.;ИУК-1.3. ИУК-3.1.;ИУК-3.2;ИУК-3.3. ИПК-1.1.;ИПК-1.2.;ИПК-1.3.	2	Тестирование выступление на семинарах, защита рефератов, докладов
6.	Тема 6. Специфика борьбы с преступлениями в сфере компьютерных системах и сетях.	УК-1 УК-3 ПК-1	ИУК-1.1.;ИУК-1.2.;ИУК-1.3. ИУК-3.1.;ИУК-3.2;ИУК-3.3. ИПК-1.1.;ИПК-1.2.;ИПК-1.3.	2	тестирование, выступление на семинарах, защита рефератов
7.	Тема 7. Правовые аспекты противодействия высокотехнологичному киберэкстремизму.	УК-1 УК-3 ПК-1	ИУК-1.1.;ИУК-1.2.;ИУК-1.3. ИУК-3.1.;ИУК-3.2;ИУК-3.3. ИПК-1.1.;ИПК-1.2.;ИПК-1.3.	1	тестирование, выступление на семинарах, защита рефератов, докладов
8.	Тема 8. Законодательные акты в сфере противодействия киберпреступности	УК-1 УК-3 ПК-1	ИУК-1.1.;ИУК-1.2.;ИУК-1.3. ИУК-3.1.;ИУК-3.2;ИУК-3.3. ИПК-1.1.;ИПК-1.2.;ИПК-1.3.	1	тестирование, выступление на семинарах, защита рефератов
Всего:				**16**	

Перечень оценочных средств

№ п/п	Наименование оценочного средства	Характеристика оценочного средства	Представление оценочного средства в ФОС
Устные оценочные средства			
1.	Собеседование Устный опрос Дискуссия Коллоквиум Круглый стол	Средство контроля, организованное как специальная беседа преподавателя со студентами на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний студента по определённому разделу, теме, проблеме.	Вопросы по темам, разделам
2.	Доклад Собеседование	Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определённой темы.	Темы докладов, сообщений
Письменные оценочные средства			
1.	Эссе	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определённой темы, где автор раскрывает суть исследуемой темы, приводит различные точки зрения, а также собственные взгляды на неё.	Темы рефератов, эссе
2.	Тест Задачи	Система проверки умений применять полученные знания для решения задач определённого типа по теме или разделу.	Вопросы по темам, вопросы задач

МОУ ВО «Российско-Таджикский (Славянский) университет»
Кафедра уголовного права

ТЕМЫ ЭССЕ
(рефератов, докладов)
по дисциплине «Особенности противодействия киберпреступности»
Темы рефератов:

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.

Темы рефератов:

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.

Критерии оценки:
Оценка «зачтено» выставляется магистранту, если **присутствует:**
- актуальность темы исследования;
- соответствие содержания теме;
- глубина проработки материала;
- правильность и полнота разработки поставленных вопросов;
- значимость выводов для дальнейшей практической деятельности;

- правильность и полнота использования литературы;
- соответствие оформления реферата стандарту;
- качество сообщения и ответов на вопросы при защите реферата.

К примеру, объем реферата может колебаться в пределах 15-20 печатных страниц. Основные разделы: оглавление (план), введение, основное содержание, заключение, список литературы.

Текст реферата должен содержать следующие разделы:

- титульный лист с указанием: названия ВУЗа, кафедры, темы реферата, ФИО автора и ФИО научного руководителя.
- введение, актуальность темы.
- основной раздел.
- заключение (анализ результатов литературного поиска); выводы.
- библиографическое описание, в том числе и интернет-источников.
- список литературных источников должен иметь не менее 10 библиографических названий, включая сетевые ресурсы.

Текстовая часть реферата оформляется на листе следующего формата:

- отступ сверху – 2 см; отступ слева – 3 см; отступ справа – 1,5 см; отступ снизу – 2,5 см;
- шрифт текста: Times New Roman, высота шрифта – 14, пробел – 1,5;
- нумерация страниц – снизу листа. На первой странице номер не ставится.

Реферат должен быть выполнен грамотно с соблюдением культуры изложения. Обязательно должны иметься ссылки на используемую литературу, включая периодическую литературу за последние 5 лет.

Доклад – вид самостоятельной научно-исследовательской работы, где обучающийся раскрывает суть исследуемой проблемы; приводит различные точки зрения, а также собственные взгляды на нее.

Этапы работы над докладом:

- подбор и изучение основных источников по теме (как и при написании реферата рекомендуется использовать не менее 8 - 10 источников);
- составление библиографии;
- обработка и систематизация материала, подготовка выводов и обобщений.
- разработка плана доклада.
- написание;
- публичное выступление с результатами исследования.

Если магистрант готовить доклад, то самостоятельная работа по их написанию может проходить в следующей последовательности.

1. Нужно проконсультироваться у преподавателя по содержанию предстоящего доклада (выступления), списку литературы, которую лучше использовать для их подготовки. Подобрать рекомендованную литературу.
2. Необходимо изучить литературу, сгруппировать материал и составить подробный план доклада (выступления).
3. Следует написать полный текст доклада (выступления). Для того чтобы доклад получился интересным и имел успех, в нем следует учесть:

а) теоретическое содержание рассматриваемых вопросов и их связь с практикой профессиональной деятельности;

б) логику и аргументы высказываемых суждений и предложений, их остроту и актуальность;

в) конкретные примеры из сферы профессиональной или учебной деятельности;

г) обобщающие выводы по всему содержанию сделанного доклада с выходом на будущую профессию.

Для выступления с докладом магистранту отводится 10 – 12 минут, поэтому все содержание доклада должно быть не более 7-10 страниц рукописного текста. Для выступления с сообщением обычно отводится 5-7 минут. Соблюдение регламента времени является обязательным условием.

4. Магистранту рекомендуется продумать методику чтения доклада. Лучше если магистрант будет свободно владеть материалом и излагать доклад доходчивым разговорным языком, поддерживать контакт с аудиторией. При возможности следует применять технические средства, наглядные пособия (например, подготовить доклад с презентацией или раздаточным материалом), использовать яркие примеры.

Важно потренироваться в чтении доклада. Если есть возможность, то записать свое выступление на видео - или аудионоситель. Просмотр, прослушивание сделанной записи позволят увидеть и

устранить недостатки: неправильное произношение слов, несоответствующий темп речи, ошибки в ударении, неинтересные или непонятные места, продолжительность доклада и т.п.
Критерии оценки:
- актуальность темы;
- соответствие содержания теме;
- глубина проработки материала;
- грамотность и полнота использования источников;
- соответствие оформления доклада требованиям.
- оценка «не зачтено» выставляется магистранту в случае, если он не ориентируется в теме подготовленного реферата, доклада, эссе.

Составитель _____ Абдуллаев Н.С.

«____»_____2024 г.

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

МОУ ВО «Российско-Таджикский» (Славянский) университет»
Кафедра уголовного права.

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.
10. Киберпреступности и экстремистская деятельность.
11. Виды и формы киберпреступности
12. Характеристика нормативно-правовых актов в области противодействия киберпреступности
13. Причины и условия киберпреступности
14. Понятие информационной безопасности.
15. Понятие и классификация компьютерного терроризма.
16. Проблемы детерминации киберпреступности.
17. Причинный комплекс киберпреступности.
18. Кибертерроризм и киберпреступность: понятие и виды
19. Предупреждения органами внутренних дел киберпреступности.
20. **Законодательные акты в сфере противодействия киберпреступности**
21. Перспективы совершенствования права в условиях нарастания кибертеррористической угрозы.
22. Понятие и сущность киберэкстремизма.

Критерии оценки:

Максимальное количество баллов, указанное по каждому виду задания, магистрант получает, если:

- обстоятельно с достаточной полнотой излагает соответствующую тему;
- даёт правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания магистрантом данного материала.

70~89% от максимального количества баллов магистрант получает, если:

- неполно (не менее 70% от полного), но правильно изложено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- даёт правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания магистрантом данного материала.

50~69% от максимального количества баллов магистрант получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.
- 49% и менее от максимального количества баллов магистрант получает, если:
- неполно (менее 50% от полного) изложено задание;

- при изложении были допущены существенные ошибки.

В "0" баллов преподаватель вправе оценить выполненное магистрантом задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель магистранта. Рейтинговый показатель магистранта влияет на выставление итоговой оценки по результатам изучения дисциплины.

Составитель _____ Абдуллаев Н.С.

«____» _____ 2024 г.

КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ КОНТРОЛЯ ОСТАТОЧНЫХ ЗНАНИЙ ПО ДИСЦИПЛИНЕ (ДЛЯ АТТЕСТАЦИИ ПО ТРЕБОВАНИЮ)

1. Понятие и принципы информационной безопасности
2. Внешние и внутренние угрозы информационной безопасности.
3. Государственно-правовые меры обеспечения информационной безопасности.
4. Научно-технические меры обеспечения информационной безопасности.
5. Специальные меры обеспечения информационной безопасности.
6. Организационные меры обеспечения информационной безопасности.
7. Правовое понятие информации. Классификация охраняемой законом информации.
8. Виды охраняемой законом информации.
9. Законодательство Российской Федерации об информации, информационных технологиях и защите информации.
10. Общая характеристика преступлений в сфере компьютерной информации.
11. Неправомерный доступ к компьютерной информации.
12. Создание, использование и распространение вредоносных компьютерных программ
13. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
14. Уголовно-правовая защита тайны частной жизни (личная, семейная тайна, тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, тайна усыновления).
15. Уголовно-правовая защита коммерческой, банковской, налоговой тайны.
16. Уголовно-правовая защита государственной тайны.
17. Уголовно-правовая защита интеллектуальной собственности.
18. Правовая защита персональных данных.
19. Общая характеристика зарубежного законодательства по защите информации.
20. Международные конвенции, соглашения и иные официальные документы
21. Состояние, структура, динамика, тенденции преступности в сфере высоких информационных технологий в современной России.
22. Актуальные проблемы противодействия преступности в сфере высоких информационных технологий в современной России.
23. Приоритетные направления предупреждения преступности в сфере высоких информационных технологий.

Критерии оценки:

Оценка зачета	**Критерии**
Зачтено	Оценка «зачтено» выставляется магистранту, если он знает материал, грамотно и по существу излагает его, не допуская существенных неточностей. В ответе могут быть допущены неточности или незначительные ошибки, исправленные магистрантом в ходе ответа на дополнительные вопросы преподавателя.
Незачтено	Оценка «не зачтено» выставляется магистранту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

Составитель _____ Абдуллаев Н.С.

«____» _____ 2024 г.