МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
Государственное образовательное учреждение высшего образования Московской области
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ОБЛАСТНОЙ УНИВЕРСИТЕТ
(МГОУ)
Факультет безопасности жизнедеятельности

Кафедра социальной безопасности

Согласовано управлением организации и контроля качества образовательной деятельности
«24» марта 2022 г.
Начальник управления _____
/ Р.В. Самолетов /

Одобрено учебно-методическим советом
Протокол «24» марта 2022 г. № 23
Председатель _____
/ М.А. Миненкова /

Рабочая программа дисциплины
Защита критически важной инфраструктуры

Направление подготовки
05.04.06 Экология и природопользование

Программа подготовки:
Экологическая безопасность

Квалификация
Магистр

Форма обучения
Очная

Согласовано учебно-методической комиссией факультета безопасности жизнедеятельности
Протокол «03» 03 2022 г. № 7
Председатель УМКом _____
/ Е.М. Приорова /

Рекомендовано кафедрой социальной безопасности
Протокол от «03» 02 2022 г. № 7
Зав. кафедрой _____
/ Е.М. Приорова /

Мытищи
2022

Автор-составитель:

Приорова Елена Михайловна кандидат биологических наук, доцент

Рабочая программа дисциплины «Защита критически важной инфраструктуры» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 05.04.06 Экология и природопользование, утвержденного приказом Минобрнауки России от 07.08.2020 г. № 897.

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

Год начала подготовки (по учебному плану) 2022

Содержание

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

1.1. Цель и задачи дисциплины

Целью преподавания дисциплины «Защита критически важной инфраструктуры» является формирование у обучающихся представление о возможных источниках угрозы, изучение основных понятий, методологии и практических приемов обеспечения безопасности объектов критической инфраструктуры.

Задачи дисциплины:

– изучение основных понятий и технологий обеспечения безопасности объектов критической информационной инфраструктуры;

– получение знаний и навыков защиты объектов критической инфраструктуры;

– изучение нормативно-правовых актов, регулирующих вопросы создания, эксплуатации и защиты объектов критически важной инфраструктуры;

– приобретение обучаемыми необходимого объема знаний в области организации работы по защите объектов критической инфраструктуры;

– формирование у обучаемых целостного представления о внедрении системного подхода к решению задач обеспечения информационной безопасности.

1.2. Планируемые результаты обучения

В результате освоения данной дисциплины у обучающихся формируются следующие компетенции:

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

СПК-3.Способен осуществлять организацию и управление научно-исследовательскими и научно-производственными и экспертно-аналитическими работами с использованием углубленных знаний в области управления природопользованием.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

Дисциплина «Защита критически важной инфраструктуры» является базовой для освоения дисциплин «Система защиты и спасения при стихийных бедствиях», «Управление рисками стихийных бедствий», «Защита населения и территорий при стихийных бедствиях».

3. ОБЪЁМ И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Объем дисциплины

Показатель объема дисциплины	Количество часов
Объем дисциплины в зачетных единицах	6
Объем дисциплины в часах	216[1]
Контактная работа:	14,3[2]
Лекции	8[3]
Практические занятия	4[4]
Контактные часы на промежуточную аттестацию	2,3[5]

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

Экзамен	0,3[6]
Предэкзаменационная консультация	2[7]
Самостоятельная работа	192[8]
Контроль	9,7[9]

Форма промежуточной аттестации: экзамен в 3 семестре.

3.2.Содержание дисциплины

по очной форме обучения

Наименование разделов (тем) дисциплины с кратким содержанием	Количество часов	
	Лекции	Практические занятия
Тема 1. Объекты критической инфраструктуры: Категорирование объектов критической информационной инфраструктуры: Реестр значимых объектов критической информационной инфраструктуры	2	
Тема 2. Основы информационной безопасности на объектах критической инфраструктуры: Понятие информационной безопасности на объектах критической инфраструктуры. Основные составляющие. Наиболее распространенные угрозы информационной безопасности и её составляющие	4	4
Тема 3. Технологии обеспечения безопасности объектов критической инфраструктуры: Права и обязанности субъектов критической инфраструктуры; Система безопасности значимого объекта критической инфраструктуры; требования по обеспечению безопасности значимых объектов критической инфраструктуры	2	
Итого	8[10]	4[11]

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Темы для самостоятельного изучения	Изучаемые вопросы	Кол-во часов	Формы самостоятельной работы	Методические обеспечения	Формы отчетности
Основные понятия и общеметодологи ческие принципы теории информационно й безопасности	1. Основные понятия информационной безопасности 2. Классификация угроз. 3. Классификация средств защиты информации. 4. Методы и средства организационно- правовой защиты информации. 6.Методы и средства инженерно- технической защиты. Программные и	96	Самостоятельное теоретическое исследование проблемы, работа с учебной литературой, интернет-источниками	Учебно-методическое обеспечение дисциплины	Тест. Доклад

[6] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[7] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[8] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[9] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[10] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.
[11] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

	программно- аппаратные методы и средства обеспечения информационной безопасности				
Обеспечения информационно й безопасности компьютерных систем	1. Методы и средства обеспечения информационной безопасности компьютерных систем. 2.Компьютерная система как объект информационной безопасности. 3.Общая характеристика способов и средств защиты информации 4. Механизмы защиты информации в автоматизированных системах. 5.Содержание сервисов безопасности программно-технического уровня. 6.Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит	96	Самостоятельное теоретическое исследование проблемы, работа с учебной литературой, интернет-источниками	Учебно-методическое обеспечение дисциплины	Реферат
Итого		192[12]			

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

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

Код и наименование компетенции	Этапы формирования
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	1. Работа на учебных занятиях. 2. Самостоятельная работа
СПК-3. Способен осуществлять организацию и управление научно-исследовательскими и научно производственными и экспертно- аналитическими работами с использованием углубленных знаний в области управления	1. Работа на учебных занятиях. 2. Самостоятельная работа

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

Оцениваемые компетенции	Уровень сформированности	Этап формирования	Описание показателей	Критерии оценивания	Шкала оценивания
УК-3	Пороговый	1.Работа на учебных занятиях. 2. Самостоятельная работа	Знать: Основные технологии защиты критически важной инфраструктуры. Уметь: Вырабатывать стратегию сотрудничества	Устный опрос, доклад, тестирование	Шкала оценивания устного опроса Шкала

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

			и на ее основе организует отбор членов команды для достижения поставленной цели в сфере защиты критически важной инфраструктуры		оценивания доклада Шкала оценивания тестирования
	Продвинутый	1.Работа на учебных занятиях. 2. Самостоятельная работа	Знать: Технологии обеспечения безопасности объектов критической, требования по обеспечению безопасности значимых объектов критической инфраструктуры. Уметь: Вырабатывать стратегию сотрудничества и на ее основе организует отбор членов команды для достижения поставленной цели в сфере защиты критически важной инфраструктуры Разрешать конфликты и противоречия при деловом общении на основе учета интересов всех сторон; организует дискуссии по заданной теме и обсуждение	Устный опрос, тестирование, доклад, реферат	Шкала оценивания устного опроса Шкала оценивания тестирования Шкала оценивания доклад Шкала оценивания реферата
СПК-3	Пороговый	1.Работа на учебных занятиях. 2. Самостоятельная работа	Знать: Основные проблемы защиты критически важной инфраструктуры. Уметь: Проводить оценку защитного потенциала критически важных объектов	Устный опрос, доклад	Шкала оценивания устного опроса Шкала оценивания доклада
	Продвинутый	1.Работа на учебных занятиях. 2. Самостоятельная работа	Знать: Основные проблемы защиты критически важной инфраструктуры, практические рекомендации по защите критических важных объектов. Уметь: Проводить оценку защитного потенциала критически важных объектов. Выявить и диагностировать проблемы защиты критически важной инфраструктуры Владеть: навыками решения задачи профессиональной деятельности в области защиты критически важных объектов	Устный опрос, тестирование, доклад, реферат	Шкала оценивания устного опроса Шкала оценивания тестирования Шкала оценивания доклад Шкала оценивания реферата

Шкала оценивания доклада

Баллы	Критерии оценивания
6-10	Подготовленный доклад свидетельствует о проведенном самостоятельном исследовании с привлечением различных источников информации; логично, связно и полно раскрывается тема; заключение содержит логично вытекающие из содержания выводы; правильно (уместно и достаточно) используются разнообразные средства речи
4-5	Подготовленный доклад свидетельствует о проведенном самостоятельном исследовании с привлечением двух-трех источников информации; логично, связно и полно раскрывается тема; заключение содержит логично вытекающие из содержания выводы; правильно (уместно и достаточно) используются разнообразные средства речи
3	Подготовленный доклад свидетельствует о проведенном исследовании с привлечением одного источника информации; тема раскрыта не полностью; логичный вывод не сделан
2	Тема доклада не раскрыта полностью
1	Содержание доклада не соответствует выбранной теме

Шкала оценивания реферата

Баллы	Критерии оценивания
8-10	Работа сдана в указанные сроки, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, логично изложена собственная позиция, сформулированы выводы, раскрыта тема реферата, выдержан объем, соблюдены требования к внешнему оформлению
5-7	Основные требования к реферату выполнены, но при этом допущены недочеты, например: имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, объем реферата выдержан более чем на 50%, имеются упущения в оформлении.
3-4	Тема не раскрыта, обнаруживается существенное непонимание проблемы, допущены грубейшие ошибки в оформление работы
0	Реферат студентом не представлен

Шкала оценивания тестирования

Баллы	Критерии оценивания
10	Из заданий теста студент выполнил как минимум 90%
7	Из заданий теста студент выполнил как минимум 80%
6	Из заданий теста студент выполнил 70%
5	Из заданий теста студент выполнил 60%
4	Из заданий теста студент выполнил 50%
3	Из заданий теста студент выполнил 40%
0-2	Из заданий теста студент выполнил менее 40%

Шкала оценивания устного опроса

Баллы	Критерии оценивания
7-10	Ответ полный, логичный
0	Ответ не соответствует вопросу

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

Примерный перечень вопросов выносимых на практические занятия

1. Перенос деятельности критически важного объекта в безопасный район
2. Мероприятия по совершенствованию системы технической и физической защищенности критически важных объектов
3. Ресурсное обеспечение защищенности.
4. Подготовка системы информации и управления.
5. Подготовка локальной системы оповещения на критически важном объекте.
6. Подготовка аппарата управления к действиям при угрозе возникновения и возникновении ЧС, в том числе и при совершении диверсионно террористических актов.
7. Информационная безопасность и информационное противоборство.
8. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности
9. Назначение формальных моделей безопасности.
10. Политика безопасности. Монитор безопасности обращений.
11. Дискреционная и мандатная модели безопасности. Формальные модели управления доступом.
12. Пресечение разглашения конфиденциальной информации.
13. Противодействие несанкционированному доступу к источникам конфиденциальной информации.
14. Способы несанкционированного доступа. Возможности типичных систем управления безопасностью.

Примерная тематика докладов

1. Организация управления и контроля при выполнении мероприятий по повышению защищенности объекта.
2. Способы защиты информации.
3. Общая характеристика защитных действий.
4. Пресечение разглашения конфиденциальной информации.
5. Противодействие несанкционированному доступу к источникам конфиденциальной информации.
6. Способы несанкционированного доступа.
7. Возможности типичных систем управления безопасностью.
8. Основные понятия и общеметодологические принципы теории информационной безопасности.
9. Методы и средства обеспечения информационной безопасности компьютерных систем
10. Информационная безопасность и информационное противоборство.
11. Составные части и методы информационного противоборства.
12. Информационное оружие, его классификация и возможности.
13. Условия удовлетворяющие СЗИ.
14. Основные требования систем защиты информации.

Примерная тематика рефератов

1. Оценка защищенности критически важного объекта.
2. Мероприятия по повышению уровня защищенности критически важного объекта.

3. Направления обеспечения информационной безопасности (организационная защита).

4. Направления обеспечения информационной безопасности (инженерно-техническая защиты.

5. Правовой режим конфиденциальной информации. Персональные данные.

6. Правовой режим конфиденциальной информации. Сведения, составляющие тайну следствия и судопроизводства. Служебная тайна.

7. Правовой режим конфиденциальной информации. Сведения, связанные с профессиональной деятельностью.

8. Формальные модели безопасности автоматизированных систем.

9. Основные цели и задачи информационного противоборства.

10. Основные положения системы защиты информации.

11. Концептуальная модель информационной безопасности.

12. Угрозы конфиденциальной информации.

13. Защита информации, обрабатываемой в автоматизированных системах от технических разведок. Классификация и возможности технических разведок

Примерные вопросы для устного опроса

1. Понятия катастрофоустойчивости, живучести и отказоустойчивости.
2. Информационные системы.
3. Виды, архитектура, субъекты и объекты взаимодействия.
4. Модель катастрофических воздействий.
5. Моделирование и прогноз природных и техногенных катастроф.
6. Уровни катастрофоустойчивости.
7. Показатели и критерии функционирования катастрофоустойчивой информационной системы.
8. Живучесть информационных систем.
9. Отказоустойчивость и надежность.
10. Разработка моделей оценки живучести ИС.
11. Модели и показатели функционирования катастрофоустойчивых ИС.
12. Модель оценки информационной системы с позиции доступности.
13. Модель оценки информационной системы по уровням катастрофоустойчивости.
14. Модель оценки информационной системы с позиции живучести.
15. Оценка эффективности катастрофоустойчивых решений.
16. Структурный анализ катастрофоустойчивой ИС.
17. Методы обеспечения катастрофоустойчивости ИС.
18. Методика создания катастрофоустойчивой информационной системы.
19. Классификация методов обеспечения катастрофоустойчивости.
20. Стратегии резервирования.
21. Кластеризация
22. Избыточные структуры
23. Резервные центры обработки данных.
24. Выбор варианта катастрофоустойчивой конструкции центра обработки информации.
25. Выбор стратегии восстановления в катастрофоустойчивой системе.
26. Разработка модели оценки доступности информации в катастрофоустойчивых системах.
27. Исследование готовности и доступности ИС.
28. Исследование уровней катастрофоустойчивости на моделях типовых ИС.
29. Моделирование дестабилизирующих воздействий и их последствий на ИС.
30. Разработка модели оценки катастрофоустойчивых решений.

Примерные варианты тестирования

1. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется:

1. актуальностью информации;
2. доступностью;
3. качеством информации;
4. целостностью.

2. Согласно «Оранжевой книге» минимальную защиту имеет группа критериев:

1. C
2. A
3. B
4. D

3. Организационные требования к системе защиты

1. управленческие и идентификационные
2. административные и аппаратурные
3. административные и процедурные
4. аппаратурные и физические

4. Основу политики безопасности составляет

1. программное обеспечение
2. управление риском
3. способ управления доступом
4. выбор каналов связи

5. Соответствие средств безопасности решаемым задачам характеризует

1. эффективность
2. корректность
3. адекватность
4. унификация

6. С точки зрения ФСТЭК основной задачей средств безопасности является обеспечение сохранности информации

1. защиты от НСД
2. простоты реализации
3. надежности функционирования

7. Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне

1. E5
2. E7
3. E4
4. E6

8. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это

1. аудит
2. аутентификация
3. авторизация
4. идентификация

0. Соответствие средств безопасности решаемым задачам характеризует

1. эффективность
2. корректность
3. адекватность
4. унификация

10. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется

1. системой защиты

2. стандартом безопасности
3. профилем безопасности
4. профилем защиты
11. Организационные требования к системе защиты
1. управленческие и идентификационные
2. административные и аппаратурные
3. административные и процедурные
4. аппаратурные и физические
12. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности
1. Лендвера
2. С полным перекрытием
3. Белла-ЛаПадула
4. На основе анализа угроз
14. Из перечисленного услуга защиты целостности доступна на уровнях:
1. сетевом;
2. транспортном;
3. сеансовом;
4. канальном;
5. прикладном;
6. физическом

Примерный перечень вопросов к экзамену

1. Основные требования к методам и средствам технической защиты информации на критически важных объектах.
2. Системы мониторинга средств защиты информации.
3. Работоспособность средств защиты информации, функционирующих на критически важных объектах.
4. Технические средства организации дистанционного управления.
5 Основные понятия о радио мониторинге.
6. Понятия «информационная безопасность» и «защита информации».
7. Основные положения системы защиты информации.
8. Условия удовлетворяющие СЗИ.
9. Основные требования систем защиты информации
10. Концептуальная модель информационной безопасности.
11. Угрозы конфиденциальной информации.
12. Действия, приводящие к неправомерному овладению конфиденциальной информацией. Направления обеспечения информационной безопасности (правовая защита).
13. Страховая и лицензионная защита информации.
14. Направления обеспечения информационной безопасности (организационная защита). 15. Направления обеспечения информационной безопасности (инженерно-техническая защита).
16 Основные понятия о радиомониторинге. Обнаружение радиопередатчиков, простых и шумоподобных.
17. Основные представления о нелинейной локации, дальность обнаружения. Ложные срабатывания.
18.Общая характеристика критически важного объекта.

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

Основными формами текущего контроля являются устные опросы, подготовка рефератов, докладов, выполнение тестирования.

Студент должен показать, что известно по этому поводу в науке, какие вопросы еще не освещены. Одним из условий, обеспечивающих успех практических занятий, является совокупность определенных конкретных требований к докладам студентов. Эти требования должны быть достаточно четкими и в то же время не настолько регламентированными, чтобы сковывать творческую мысль, насаждать схематизм.

Перечень требований к выступлению студента:

– связь выступления с предшествующей темой или вопросом;

– раскрытие сущности проблемы;

– методологическое значение для научной, профессиональной и практической деятельности.

Проверка уровня усвоения материала студентом производится на практических занятиях после изучения отдельных тем дисциплины посредством устного опроса.

Доклад – средство, позволяющее проводить самостоятельный поиск материалов по заданной теме, реферировать и анализировать их, и доносить полученную информацию до окружающих. Доклад готовится по одной из проблем, находящихся в пределах обсуждаемой темы

Важнейшие требования к выступлениям студентов – самостоятельность в подборе фактического материала и аналитическом отношении к нему, умение рассматривать примеры и факты во взаимосвязи и взаимообусловленности, отбирать наиболее существенные из них.

Приводимые студентом примеры и факты должны быть существенными, по возможности перекликаться с программой подготовки. Примеры из области наук, близких к программе подготовки студента, из сферы познания. Выступление студента должно соответствовать требованиям логики. Четкое вычленение излагаемой проблемы, ее точная формулировка, неукоснительная последовательность аргументации именно данной проблемы, без неоправданных отступлений от нее в процессе обоснования, безусловная доказательность, непротиворечивость и полнота аргументации, правильное и содержательное использование понятий и терминов.

Как и любая другая форма подготовки к контролю знаний, тестирование имеет ряд особенностей, знание которых помогает успешно выполнить тест. Можно дать следующие методические рекомендации:

– Прежде всего, следует внимательно изучить структуру теста, оценить объем времени, выделяемого на данный тест, увидеть, какого типа задания в нем содержатся. Это поможет настроиться на работу.

– Лучше начинать отвечать на те вопросы, в правильности решения которых нет сомнений, пока, не останавливаясь на тех, которые могут вызвать долгие раздумья. Это позволит успокоиться и сосредоточиться на выполнении более трудных вопросов.

– Очень важно всегда внимательно читать задания до конца, не пытаясь понять условия «, по первым словам,» или выполнив подобные задания в предыдущих тестированиях. Такая спешка нередко приводит к досадным ошибкам в самых легких вопросах.

– Если вы не знаете ответа на вопрос или не уверены в правильности, следует пропустить его и отметить, чтобы потом к нему вернуться.

– Думать только о текущем задании. Как правило, задания в тестах не связаны друг с другом непосредственно, поэтому необходимо концентрироваться на данном вопросе и находить решения, подходящие именно к нему. Кроме того, выполнение этой рекомендации даст еще один психологический эффект – позволит забыть о неудаче в ответе на предыдущий вопрос, если таковая имела место.

– Многие задания можно быстрее решить, если не искать сразу правильный вариант ответа, а последовательно исключать те, которые явно не подходят. Метод исключения позволяет в итоге сконцентрировать внимание на одном-двух вероятных вариантах.

– Рассчитывать выполнение заданий нужно всегда так, чтобы осталось время на проверку и доработку (примерно 1/3-1/4 запланированного времени).

– Процесс угадывания правильных ответов желательно свести к минимуму.

Реферат – письменная работа по одному из актуальных вопросов в рамках дисциплины. Цель подготовки реферата – обобщение различных научных идей, концепций, точек зрения по наиболее важным изучаемым проблемам на основе самостоятельного анализа монографических работ и учебной литературы.

Обучающемуся предоставляется право самостоятельно выбрать тему реферата из списка рекомендованных тем приведенных в рабочей программе дисциплины. Не допускается в одной группе написания двух и более рефератов по одной теме.

Подготовка реферата должна осуществляться в соответствии с планом, текст должен иметь органическое внутреннее единство, строгую логику изложения, смысловую завершенность.

Реферат должен состоять из введения, где дается план изложения, объект и предмет исследования, задачи и цели. Затем в реферате идет основная часть, состоящая из трех разделов. В первом дается теоретический обзор, во втором аналитический материал, в третьи результаты исследования. В заключении реферата результаты исследования сопоставляются с поставленными целями и задачами.

Во введении (максимум 3-4 страницы) раскрывается актуальность темы, излагаются основные точки зрения, формируются цель и задачи исследования. В основной части раскрывается содержание понятий и положений, вытекающих из анализа изученной литературы и результатов эмпирических исследований. В заключении подводятся итоги авторского исследования в соответствии с выдвинутыми задачами, делаются самостоятельные выводы и обобщения. Объем реферата должен составлять 10-15 страниц машинописного (компьютерного) текста.

В ходе освоения дисциплины студенту необходимо посещать все занятия, подготовить один доклад, один реферат, пройти тестирование, а также активно участвовать в устных опросах на практических занятиях.

Тестирование имеет ряд особенностей, знание которых помогает успешно выполнить тест. Можно дать следующие методические рекомендации:

– Прежде всего, следует внимательно изучить структуру теста, оценить объем времени, выделяемого на данный тест, увидеть, какого типа задания в нем содержатся. Это поможет настроиться на работу.

– Лучше начинать отвечать на те вопросы, в правильности решения которых нет сомнений, пока, не останавливаясь на тех, которые могут вызвать долгие раздумья. Это позволит успокоиться и сосредоточиться на выполнении более трудных вопросов.

– Очень важно всегда внимательно читать задания до конца, не пытаясь понять условия «по первым словам,» или выполнив подобные задания в предыдущих тестированиях. Такая спешка нередко приводит к досадным ошибкам в самых легких вопросах.

– Если вы не знаете ответа на вопрос или не уверены в правильности, следует пропустить его и отметить, чтобы потом к нему вернуться.

– Думать только о текущем задании. Как правило, задания в тестах не связаны друг с другом непосредственно, поэтому необходимо концентрироваться на данном вопросе и находить решения, подходящие именно к нему. Кроме того, выполнение этой рекомендации даст еще один психологический эффект – позволит забыть о неудаче в ответе на предыдущий вопрос, если таковая имела место.

– Многие задания можно быстрее решить, если не искать сразу правильный вариант ответа, а последовательно исключать те, которые явно не подходят. Метод исключения позволяет в итоге сконцентрировать внимание на одном-двух вероятных вариантах.

– Рассчитывать выполнение заданий нужно всегда так, чтобы осталось время на проверку и доработку (примерно 1/3-1/4 запланированного времени).

–Процесс угадывания правильных ответов желательно свести к минимуму.

Шкала оценивания экзамена

Баллы	Критерии оценивания
25-30	Студент демонстрирует сформированные и систематические знания; успешное и систематическое умение; успешное и систематическое применение навыков в соответствии с планируемыми результатами освоения дисциплины, свободно владеет теоретическими понятиями дисциплины; проявляет системность знаний учебного материала и способность устанавливать связи между теоретическими понятиями; умеет делать перенос теоретических знаний в практическую область применения, понимает значение приобретенных знаний для будущей профессии, проявляет творческие способности в понимании, изложении и использовании учебно-программного материала
15-24	Студент владеет теоретическими знаниями, достаточно свободно и оперирует ими; успешно выполняет предусмотренные в программе задания, осуществляет частичный перенос теоретических знаний в прикладную область; проявляет незначительные нарушения в установлении взаимосвязи между теоретическими понятиями; в целом успешное, но сопровождающееся отдельными ошибками применение навыков в соответствии с планируемыми результатами освоения дисциплины
9-14	Студент демонстрирует неполные знания; в целом успешные, но не систематические умения; в целом успешное, но не систематическое применение навыков в соответствии с планируемыми результатами освоения дисциплины, отсутствует интеграция знаний
0-8	Студент демонстрирует ответ, не соответствующий теоретическому вопросу. Нет ответов на вопросы, или ответы неточные (неопределенные).

Итоговая шкала по дисциплине

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

Баллы, полученные магистрантом по текущему контролю и промежуточной аттестации	Оценка в традиционной системе
81-100	Отлично
61-80	Хорошо
41-60	Удовлетворительно
0-40	Неудовлетворительно

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Основная литература

1. Александров А.А. Анализ и управление техногенными и природными рисками: учебник / А.А. Александров, В.И. Ларионов, С.П. Сущев. – Москва: Издательство МГТУ им. Н.Э. Баумана, 2019. – 357 с. – Текст: электронный. – URL: https://www.studentlibrary.ru/book /ISBN9785703851081.html.

2. Горелов Н.А. Управление человеческими учебник и практикум для вузов / Н.А. Горелов, Москва: Юрайт, 2021. – 270 с. – Текст: электронный. – URL: https://urait.ru/bcode/470091.

3. Кован С.Е. Антикризисный консалтинг: учеб. пособие для магистратуры. – М.: Кнорус, 2020. – 226с. – Текст: непосредственный.

3. Кочеткова А.И. Антикризисное управление. Инструментарий: учебник и практикум для вузов/ А.И. Кочеткова, П.Н.К очетков. – Москва: Юрайт, 2021. – 440 с. – Текст: электронный. — URL: https://urait.ru/bcode/470354

6.2. Дополнительная литература

1. Зубрев Н.И. Системы защиты среды обитания: учебник для вузов / Н.И. Зубрев, И. Ю. Крошечкина, М.В. Устинова. – М.: Кнорус, 2020. – 382 с.

2. Кислов А.В. Климатология : учебник / А.В. Кислов, Г.В. Суркова. – 3-е изд. – Москва: ИНФРА-М, 2018. – 324 с. – Текст: электронный. – Режим доступа: https://znanium.com/bookread2.php?book=961449

3. Косенкова С.В. Управление качеством окружающей среды: учебное пособие. – Волгоград: Волгоградский государственный аграрный университет, 2017. – 152 с. – Текст: электронный. – Режим доступа: https://znanium.com/bookread2.php?book=1007879.

4. Организация защиты населения и территорий от чрезвычайных ситуаций. Защитные сооружения: учебное пособие / сост. С.Д. Николенко, С.А. Сазонова, Е.А. Сушко. – Москва: АйПиАр Медиа, 2021. – 105 с. – Текст : электронный. – URL: https://www.iprbookshop.ru/108315.html.

5. Прудников С.П. Защита населения и территорий от чрезвычайных ситуаций: учебник / С.П. Прудников, О.В. Шереметова, О.А. Скрыпниченко. – 2-е изд. – Минск РИПО, 2020. – 256 с. – Текст: электронный. – URL: https://www.iprbookshop.ru/100383.html.

6. Пушкарь В.С. Экология: учебник / В.С. Пушкарь, Л.В. Якименко. – Москва: ИНФРА-М, 2018. – 397 с. – Текст: https://znanium.com/bookread2.php?book=972302.

7. Юртушкин В.И. Чрезвычайные ситуации: защита населения и территорий: учеб. пособие для вузов. – 3-е изд. – М. Кнорус, 2019. – 366с. – Текст: непосредственный.

6.3. Ресурсы информационно-телекоммуникационной сети «Интернет»

1. Программа ООН по окружающей среде UNEP http://www.unep.net.

2. Сайт Министерств РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий. http://www.mchs.gov.ru.

3. Программы по охране природы (марш парков, лесная программа и др.). Электронные и печатные публикации, журналы. Ссылки на всемирные и европейские экологические организации. http://biodiversity.ru

4. Российская Программа Всемирного фонда дикой природы (WWF). Развитие системы ООПТ, охрана редких животных и растений, сохранение лесов, устойчивое http://www.wwf.ru – лесопользование, поддержка экологического образования и др.

5 Фонд содействия исследованиям проблем безопасности [Электронный ресурс]. – URL: http://www.naukaxxi.ru

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Методические рекомендации по организации самостоятельной работы студентов.

2. Методические рекомендации по подготовке к практическим занятиям.

8. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Лицензионное программное обеспечение:

Microsoft Windows.

Microsoft Office.

Kaspersky Endpoint Security.

Информационные справочные системы:

Система ГАРАНТ.

Система «КонсультантПлюс» .

Профессиональные базы данных:

fgosvo.ru – Портал Федеральных государственных образовательных стандартов высшего образования.

pravo.gov.ru – Официальный интернет-портал правовой информации www.edu.ru – Федеральный портал Российское образование.

Свободно распространяемое программное обеспечение, в том числе отечественного производства.

ОМС Плеер (для воспроизведения Электронных Учебных Модулей).

7-zip.

Google Chrome.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины включает в себя:

– учебные аудитории для проведения занятий лекционного и семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные учебной мебелью, доской, демонстрационным оборудованием;

– помещения для самостоятельной работы, укомплектованные учебной мебелью, персональными компьютерами с подключением к сети Интернет и обеспечением доступа к электронным библиотекам и в электронную информационно-образовательную среду МГОУ;

– помещения для хранения и профилактического обслуживания учебного оборудования, укомплектованные мебелью (шкафы/стеллажи), наборами демонстрационного оборудования и учебно-наглядными пособиями.