

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ  
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»  
(ФГБОУ ВО «ЛГПУ»)

Институт физико-математического образования, информационных и  
обслуживающих технологий  
Кафедра безопасности жизнедеятельности и охраны труда

УТВЕРЖДАЮ

Директор Института физико-  
математического образования,  
информационных и обслуживающих  
технологий



Е. Е. Горбенко  
«13» декабря 2023 г.

Приложение к рабочей программе учебной дисциплины

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**  
для проведения текущего контроля и промежуточной аттестации  
обучающихся по дисциплине  
«Информационная безопасность государства и гражданская оборона»

По направлению подготовки – 44.03.04 Профессиональное обучение  
(по отраслям)

Профиль подготовки – Безопасность жизнедеятельности и охрана труда

Квалификация выпускника – бакалавр

Форма обучения – очная

Курс – 2

Разработчик:

заведующий кафедрой БЖД и ОТ  
ФГБОУ ВО «ЛГПУ»

Корнеева Анжелика Николаевна

Заведующий кафедрой БЖД и ОТ  
А.Н. Корнеева

Протокол

от «04» декабря 2023 г. № 6

Луганск, 2023

## 1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

### 1.1. Перечень компетенций, формируемых в процессе освоения основной образовательной программы

Процесс освоения дисциплины направлен на овладение следующими компетенциями:

УК-8 – способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций.

ПК-5 – готов к деятельности по обеспечению безопасности образовательного учреждения, способен применять современные методы и средства индивидуальной и коллективной защиты для организации безопасности обучающихся и сотрудников.

### 1.2. Этапы формирования компетенций и средства оценивания уровня их сформированности

Этапы формирования компетенций	Компетенции	Контрольно-оценочные средства / способ оценивания
Концепция информационной безопасности	УК-8 ПК-5	Выполнение практических заданий. Тестирование.
Информация как объект защиты	УК-8 ПК-5	Устный опрос. Выполнение практических заданий, выступление с презентацией.
Основные угрозы информационной безопасности России	УК-8	Выполнение практических заданий и их защита. Подготовка презентации.
Стратегия информационной безопасности РФ	УК-8 ПК-5	Выполнение практических заданий и их защита. Устный опрос.
Основные доктрины главных видов национальной безопасности	УК-8 ПК-5	Составление ментальной карты.
Гражданская оборона	УК-8	Выполнение практических заданий и их защита. Устный опрос.
Промежуточная аттестация	УК-8 ПК-5	Зачет (устный)

### 1.3. Описание показателей формирования компетенций

Код компетенции	Планируемые результаты обучения (показатели)
УК-8	<b>знать:</b> основные теоретические положения курса; законодательные и нормативно-правовые акты в области безопасности и охране труда, механизмы защиты человека от опасных и вредных факторов, правила оказания первой помощи в чрезвычайных ситуациях; <b>уметь:</b> предпринимать профилактические меры для снижения уровня опасностей и их последствий, проводить мероприятия по защите населения от негативных воздействий чрезвычайных ситуаций; <b>владеть:</b> навыками оказания первой помощи пострадавшим и себе;

	навыками выбора методов защиты от опасностей, требований к безопасности в сфере профессиональной деятельности.
ПК-5	<p><b>знать:</b> основные понятия и термины дисциплины и основы информационной безопасности, принципы межличностных отношений в многонациональном государстве;</p> <p><b>уметь:</b> объяснить национальные интересы и приоритеты России в современной геополитической ситуации, корректно выражать свои мысли и доводы в рамках предмета и будущей профессиональной деятельности;</p> <p><b>владеть:</b> навыками анализа современной политической ситуации, навыками отбора конкретной информации из различных источников, основными компетенциями в сфере информационной безопасности РФ.</p>

#### 1.4. Критерии оценивания компетенций на разных этапах их формирования

##### Система оценивания учебных достижений магистрантов очной формы обучения

Вид учебной работы	Количество баллов	
	4 семестр	
Практические занятия	40	
Самостоятельная работа (составление ментальной карты, подготовка выступления с презентацией)	30	
Зачетная работа	30	
<b>Итого:</b>	<b>100</b>	

##### Накопительная система оценивания по 100-балльной шкале

Четырехбалльная система оценивания экзамена	100-балльная шкала	Буквенная шкала, соответствующая 100-балльной шкале	Система оценивания зачета
Отлично	90–100	А – отлично – теоретическое содержание курса освоено полностью, без пробелов; необходимые практические навыки работы с освоенным материалом сформированы; все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	Зачтено
Хорошо	83–89	В – очень хорошо – теоретическое содержание курса освоено полностью, без пробелов; необходимые практические навыки работы с освоенным материалом в основном сформированы; все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному	
Хорошо	75–82	С – хорошо – теоретическое содержание курса	

		освоено полностью; некоторые практические навыки работы с освоенным материалом сформированы недостаточно; все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	
Удовлетворительно	<b>63–74</b>	<b>D</b> – удовлетворительно – теоретическое содержание дисциплины освоено частично, но пробелы не носят существенного характера; необходимые практические навыки работы с освоенным материалом в основном сформированы; большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, содержат ошибки	
Удовлетворительно	<b>50–62</b>	<b>E</b> – посредственно – теоретическое содержание курса освоено частично; некоторые практические навыки работы не сформированы, многие предусмотренные программой обучения учебные задания не выполнены либо качество выполнения некоторых из них оценено числом баллов, близким к минимальному	
Неудовлетворительно	<b>21–49</b>	<b>FX</b> – неудовлетворительно – теоретическое содержание курса освоено частично; необходимые практические навыки работы не сформированы; большинство предусмотренных программой обучения учебных заданий не выполнено либо качество их выполнения оценено числом баллов, близким к минимальному; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий	Не зачтено
Неудовлетворительно	<b>0–20</b>	<b>F</b> – неудовлетворительно – теоретическое содержание курса не освоено; необходимые практические навыки работы не сформированы; все выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к какому-либо значимому повышению качества выполнения учебных заданий	

## **2. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА**

### **2.1. Оценочные средства текущего контроля (типовые)**

#### **Вопросы для устного опроса:**

1. В чём заключаются интересы государства в информационной сфере?
2. В чём заключаются интересы общества в информационной сфере?
3. В чём заключаются интересы личности в информационной сфере?
4. В чём заключаются национальные интересы РФ в информационной сфере?
5. Какие существуют виды угроз информационной безопасности РФ?
6. Перечислите внешние источники угроз информационной безопасности РФ.
7. Перечислите внутренние источники угроз информационной безопасности РФ.
8. Покажите на примерах значение информационной безопасности в обеспечении национальной безопасности государства.
9. Какие нормативные акты обеспечивают информационную безопасность на территории РФ?
10. Какие международные нормативные акты в сфере защиты информации вы знаете?
11. В чём заключается суть государственной политики обеспечения информационной безопасности?
12. Назовите основные функции системы обеспечения информационной безопасности.
13. Из каких элементов состоит Государственная система защиты информации?
14. Почему русский язык рассматривается как объект национальной информационной безопасности?
15. Какие существуют угрозы русскому языку?
16. Как связана речь человека с его мышлением?

#### **Темы для подготовки сообщений и рефератов:**

1. Информация с ограниченным доступом. Понятие, виды и нормативная база.
2. Виды угроз информационной безопасности РФ.
3. Правовые вопросы обеспечения информационной безопасности государства.
4. Система информационной безопасности в Российской Федерации.
5. Обеспечение информационной безопасности в Российской Федерации.
6. Гражданская защита зарубежных стран.
7. Защита населения при радиоактивном загрязнении.

8. Защита населения при химическом загрязнении. Устойчивость работы субъектов хозяйствования (СХ) в ЧС.

## **2.2. Оценочные средства для промежуточной аттестации (зачет устный)**

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Экономическая информация как товар и объект безопасности.
6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
7. Персональные данные и их защита.
8. Информационные угрозы, их виды и причины возникновения.
9. Информационные угрозы для государства.
10. Информационные угрозы для компании.
11. Информационные угрозы для личности (физического лица).
12. Действия и события, нарушающие информационную безопасность.
13. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
14. Способы воздействия информационных угроз на объекты.
15. Внешние и внутренние субъекты информационных угроз.
16. Компьютерные преступления и их классификация.
17. Исторические аспекты компьютерных преступлений и современность.
18. Субъекты и причины совершения компьютерных преступлений.
19. Вредоносные программы, их виды.
20. История компьютерных вирусов и современность.
21. Государственное регулирование информационной безопасности.
22. Деятельность международных организаций в сфере информационной безопасности.
23. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.
24. Доктрина информационной безопасности России.
25. Уголовно-правовой контроль над компьютерной преступностью в России.
26. Федеральные законы по ИБ в РФ.

27. Политика безопасности и ее принципы.
28. Фрагментарный и системный подход к защите информации.
29. Методы и средства защиты информации.
30. Организационное обеспечение ИБ.
31. Организация конфиденциального делопроизводства.
32. Комплекс организационно-технических мероприятий по обеспечению защиты информации.
33. Инженерно-техническое обеспечение компьютерной безопасности.
34. Организационно-правовой статус службы безопасности.
35. Защита информации в Интернете.
36. Электронная почта и ее защита.
37. Защита от компьютерных вирусов.
38. «Больные» мобильники и их «лечение».
39. Популярные антивирусные программы и их классификация.
40. Организация системы защиты информации экономических объектов.
41. Криптографические методы защиты информации.
42. Этапы построения системы защиты информации.
43. Оценка эффективности инвестиций в информационную безопасность.
44. План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.
45. Управление информационной безопасностью на государственном уровне.
46. Аудит ИБ автоматизированных банковских систем.
47. Электронная коммерция и ее защита.
48. Менеджмент и аудит информационной безопасности на уровне предприятия.
49. Информационная безопасность предпринимательской деятельности.
50. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов.
51. Организация гражданской обороны (ГО) в современных условиях.
52. Основные положения международного права по защите человека.
53. Гражданская защита зарубежных стран.
54. Основные законодательные и нормативно-правовые акты по ГО в РФ.
55. Государственная система органов исполнительной власти по вопросам предупреждения и реагирования на чрезвычайные ситуации (ЧС) в Луганской Народной Республике.

56. Организация ГЗ в учебных заведениях.
57. Чрезвычайные ситуации (ЧС).
58. Основные определения и классификация ЧС.
59. ЧС техногенного характера.
60. ЧС природного характера.
61. ЧС экологического характера.
62. ЧС военного времени.
63. Организация оповещения населения в ЧС.
64. Защита населения и территорий при ЧС.
65. Организация защиты населения в ЧС, основные принципы и способы защиты населения и территорий в ЧС техногенного и природного характера.
66. Защита населения при радиоактивном загрязнении.
67. Защита населения при химическом загрязнении. Устойчивость работы субъектов хозяйствования (СХ) в ЧС.
68. Сущность и факторы, влияющие на устойчивость работы СХ.
69. Оценка устойчивости СХ к воздействию поражающих факторов.
70. Пути и способы повышения устойчивости работы СХ.