Приложение к рабочей программе дисциплины (практики)

Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» (РУДН)

Факультет искусственного интеллекта

(наименование основного учебного подразделения)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ)

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/ специальности)

Освоение дисциплины (практики) ведется в рамках реализации основной профессиональной образовательной программы (ОП ВО, профиль/ специализация):

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(направленность (профиль) ОП ВО)

Москва, 2025

1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

Материалы для проведения контроля:

1. Наименование оценочного средства (в соответствии с паспортом фонда оценочных средств): Доклад на семинарском занятии

2. Перечень вопросов (заданий)

Тематика доклада с презентацией:

1. Угрозы информационной безопасности Российской Федерации.
5. Внешние и внутренние источники угроз информационной безопасности государства.
6. Проблемы региональной информационной безопасности.
7. Информационное оружие, его классификация и возможности.
8. Методы нарушения конфиденциальности, целостности и доступности информации.
9. Правовые, организационно-технические и экономические методы обеспечения инфор-мационной безопасности.
10. Компьютерная система как объект информационной безопасности.
11. Особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну.
12. Анализ современных подходов к построению систем защиты информации.
13. Общая характеристика средств видеонаблюдения и обнаружения оптических прибо-ров.
14. Основные виды диктофонов и подавителей диктофонов.
15. Политика использования паролей в организации.
16. Политика использования алгоритмов шифрования в организации.
17. Примеры угроз ИБ.
18. Примеры уязвимостей объектов ИБ.
19. Аспекты ИБ в управлении непрерывностью бизнеса.
20. Инструментальные средства управления рисками ИБ.
21. Учет вопросов ИБ при работе с персоналом.

2.2 Материалы для проведения аттестации:

1 семестр.

1. Вид аттестации: экзамен.
2. Форма проведения: устный опрос.
3. Перечень тем, вопросов, практических заданий, выносимых на экзамен:

1. Понятие информационной безопасности.
2. Цели обеспечения информационной безопасности.
3. Основные задачи, решаемые при обеспечении информационной безопасности.
4. Состояние информационной безопасности Российской Федерации.
5. Основные положения государственной политики обеспечения

информационной безопас-ности Российской Федерации.

6. Доктрина информационной безопасности Российской Федерации. Система обеспечения информационной безопасности.

7. Особенности обеспечения информационной безопасности в России

8. Законодательство Российской Федерации в области информационной безопасности.

9. Защиты государственной тайны и конфиденциальной информации

10. Конституционные гарантии прав граждан на информацию и механизм их реализации.

11. Понятие и виды защищаемой информации по законодательству Российской Федерации.

12. Защита интеллектуальной собственности средствами патентного и авторского права.

13. Модели оценки ценности информации.

14. Классификация и общий анализ угроз безопасности информации.

15. Причины, виды, каналы утечки и искажения информации.

16. Основные методы реализации угроз информационной безопасности: методы нарушения конфиденциальности, целостности и доступности информации.

17. Информационная безопасность в условиях функционирования глобальных сетей.

18. Понятие компьютерного вируса.

19. История появления компьютерных вирусов и факторы, влияющие на их распространение.

20. Компьютерная преступность.

21. Сущность и перечень организационных мер по защите информации.

22. Структура и задачи подразделения по защите информации.

23. Сущность инженерно-технических мер по защите информации.

24. Информационная безопасность в системе национальной безопасности Российской Феде-рации

25. Понятие защиты информации и виды защиты информации.

26. Национальная безопасность. Основы и значение.

27. Экономическая безопасность. Основы и значение.

28. Виды безопасности и сферы жизнедеятельности личности, общества и государства: эко-номическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.

29. Виды защищаемой информации. Основные понятия и принципы информационной без-опасности.

30. Роль информационной безопасности в обеспечении национальной безопасности государ-ства

31. Интересы личности в информационной сфере.

32. Интересы общества в информационной сфере.

33. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

34. Направления обеспечения информационной безопасности государства. Проблемы регио-нальной информационной безопасности.

35. Правовая основа обеспечения информационной безопасности.

36. Суть обеспечения безопасности компьютерных сетей. Понятие и виды

информации.

37. Основные положения Доктрины информационной безопасности Российской Федерации.

38. Государственная политика обеспечения информационной безопасности Российской Фе-дерации.

39. Специфика обеспечения информационной безопасности в правоохранительных органах.

40. Угрозы информационной безопасности.

41. Задача обеспечения информационной безопасности как составная часть борьбы с пре-ступностью.

42. Виды каналов утечки информации.

43. Способы несанкционированного доступа к автоматизированным системам.

44. Основные принципы и направления защиты автоматизированных систем от несанкциони-рованного доступа.

45. Угрозы безопасности информации, обрабатываемой в автоматизированных системах.

46. Основные положения Федерального закона «Об информации, информационных техноло-гиях и о защите информации».

47. Объективные факторы, представляющие угрозу безопасности информации.

48. Субъективные факторы, представляющие угрозу безопасности информации.

49. Методы ограничения доступа к информации.

50. Защита информации, составляющей государственную тайну.

51. Виды и правовые источники конфиденциальной информации.

52. Основные способы защиты информации.

53. Организационные меры по защите информации.

54. Технические мероприятия по защите информации.

55. Виды технических средств защиты информации.

56. Актуальность обеспечения сохранности информации на электронных носителях.

57. Особенности затрат на обеспечение информационной безопасности предприятия

58. Единовременные затраты - значение и составляющие, влияние на ИБ

59. Систематические затраты – значение и составляющие, влияние на ИБ на обслуживание системы информационной безопасности Конституционные

Критерии и показатели оценки

Критерии	**Оценка**			
	«отлично»	**«хорошо»**	**«удовлетвори-тельно»**	**«неудовлетвори-тельно»**

1.Знание теоретических основ информационной безопасности.	Студент демонстрирует глубокое знание теоретических основ и принципов, базовых понятий, которые используются при обеспечении информационной безопасностью.	Студент достаточно хорошо владеет знаниями теоретических основ и принципов, базовых понятий, которые используются при обеспечении информационной безопасностью.	Студент затрудняется с изложением теории, поверхностно ориентируется в базовых понятиях, которые используются при обеспечении информационной безопасностью.	Студент не понимает поставленной проблемы, не знает теоретических основ и принципов основ информационной безопасностью.
2. Умение иллюстрировать теоретические знания на конкретных практических примерах.	Студент уверенно иллюстрирует теоретические положения обоснованными примерами.	Студент иллюстрирует ответ немногочисленными конкретными примерами, испытывая затруднения при их подборе.	Студент может подкрепить теоретические положения примерами только после наводящих вопросов, допуская при этом ошибки.	Студент демонстрирует неумение проиллюстрировать теоретические положения практическими примерами.
3. Владение профессиональной терминологией.	Студент демонстрирует свободное владение понятийным аппаратом и умение быть корректным в употреблении терминологией.	Студент достаточно хорошо владеет профессиональной терминологией, в случае ошибки в употреблении термина способен исправить ее сам.	Студент слабо владеет профессиональной терминологией, допускает неточности в интерпретации понятий и определений в данной предметной области.	Студент не владеет профессиональной терминологией и не разбирается в понятийном аппарате дисциплины.