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 ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

(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)

1. Паспорт оценочных средств

Направление подготовки (специальность): 10.03.01 Информационная безопасность

Дисциплина: Основы информационного противоборства

№ п/п	Контролируемые разделы (темы) дисциплины	Наименование оценочного средства
1.	Тема 2. Информационная безопасность Российской Федерации и проблемы ее обеспечения в условиях межгосударственного противоборства	Письменный экспресс-опрос на семинаре (практическом занятии) с выставлением оценок в балльной системе
2.	Тема 4. Основы информационного противоборства как системы специальных мер обеспечения информационной безопасности	
3.	Тема 5. Особенности информационно-психологического воздействия и защиты от него личности и общества	
4.	Тема 8. Работа руководителя по организации информационного противоборства	
5.	Тема 9. Методика принятия решения руководителем учреждения (предприятия) на ведение информационного противоборства в конкурентной борьбе	

Виды контроля по периодам обучения

2.1 Материалы для проведения текущего контроля.

Наименование оценочного средства (в соответствии с паспортом фонда оценочных средств) Контрольные вопросы. Контрольные задачи

Перечень контрольных вопросов:

1. Сущность, содержание и принципы непрямых действий как методологической основы информационно противоборства.

2. Основы классификации и содержание способов непрямых действий как методологической основы информационно противоборства.

3. Формы и приемы непрямых действий как методологической основы информационного противоборства.

4. Универсальная взаимосвязь видов, объектов и средств борьбы и направленность информационного воздействия.

5. Направления развития концепций и содержания информационного противоборства.

6. Сущность, цели и задачи информационного противоборства.

7. Пути достижения информационного превосходства в информационной сфере.

8. Пути достижения информационного превосходства в информационно-психологической сфере.

9. Пути достижения информационного превосходства в информационно-технической сфере.

10. Сущность и содержание информационно-психологического воздействия и средства воздействия.

11. Сущность, содержание и средства информационно-технического воздействия.

12. Сущность, содержание и приемы защиты от воздействия на информацию.

13. Сущность, содержание и приемы защиты от информационно-технического воздействия.

14. Сущность, содержание и приемы защиты от информационно-психологического воздействия.

15. Содержание понятия об информационном оружии.

16. Мишени информационно-психологического воздействия на социальные объекты.

17. Определение психологической манипуляции, ее признаки и основы противодействия.

18. Основные приемы защиты личности
от информационно-психологического воздействия.

19. Содержание алгоритма информационно-психологической самозащиты личности.

20. Сущность и содержание нейролингвистического программирования.

21. Репрезентативные системы личности и ключи доступа для подстройки.

22. Условия формирования угроз информационной безопасности через СМИ и рекламу.

23. Основные приемы психологического воздействия на личность через СМИ и рекламу.

24. Реклама: типы, виды коммуникативных функций, искажений и манипулятивные приемы.

25. Роль органов управления в формировании условий обеспечения информационной безопасности при взаимодействии со СМИ и в рекламной деятельности.

26. Формы работы со СМИ и задачи пресс-службы в обеспечении информационной безопасности предприятия.

27. Направления обеспечения информационной безопасности в ходе публикаторской и рекламно-выставочной деятельности.

28. Сущность и задачи управления в информационном противоборстве и содержание организации управления.

29. Рефлексивное управление противником в ходе информационного противоборства.

30. Этапы, методы и методики оценки информационной обстановки.

31. Содержание аналитической технологии, применяемой при оценке информационной обстановки.

32. Основы аналитической декомпозиции объектов и отношений в информационной сфере.

33. Содержание работы органа управления по организации информационного противоборства.

34. Содержание способа информационного противоборства в решении на информационное противоборство.

Задание № 1. Современные международные противоречия и национальная безопасность Российской Федерации. Угрозы информационной безопасности и пути их нейтрализации.

Вопрос № 1. Цель, значение и основные тезисы соглашения о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности от 28 мая 2012 года № 856-р.

Вопрос № 2. Европейская конвенция о киберпреступности от 23 ноября 2001 г. и проблема ее ратификации Российской Федерацией. Российский проект Конвенции ООН «Об обеспечении международной информационной безопасности».

Вопрос № 3. Доктрина информационной безопасности Российской Федерации об информационном противоборстве.

Вопросы для самоконтроля:

1. Система и методы обеспечения информационной безопасности Российской Федерации.

2. Сущность, цели и задачи обеспечения информационной безопасности Российской Федерации.

3. Методика создания системы обеспечения информационной безопасности.

Проблемные вопросы:

1. Проблема ратификации Российской федерацией Европейской конвенции о киберпреступности от 23 ноября 2001 г.

2. Противодействие угрозам непрямых действий в политической, экономической и социальной сферах.

Задание № 2. Угрозы информационных воздействий на личность, общество и государство. Развитие существующих концепций информационного противоборства по взглядам руководства ведущих государств.

Вопрос № 1. Информационная сфера. Понятие об источниках и направленности информационных воздействий. Информационные объекты и цели информационного воздействия.

Вопрос № 2. Топология социотехнического информационного объекта.

Вопрос № 3. Факторы угроз информационной безопасности. Угрозы информационной безопасности социотехническим объектам и системам управления.

Вопрос № 4. Сущность и содержание информационного превосходства.

Вопросы для самоконтроля:

1. Понятие о системе конфликтных взаимодействий информационных объектов противоборствующих сторон.

2. Угрозы структурам информационного объекта.

3. Угрозы программам информационного объекта.

4. Угрозы ресурсам информационного объекта.

Проблемные вопросы:

1. Развитие теории информационных воздействий на социотехнические объекты и разработка методов их нейтрализации.

2. Важность информационных объектов и ее мониторинг.

Задание № 3. Сущность и содержание специальных методов обеспечения информационной безопасности.

Вопрос № 1. Способы информационного противоборства как системы специальных методов обеспечения информационной безопасности.

Вопрос № 2. Приемы информационных воздействий.

Вопрос № 3. Силы, средства и приемы защиты личности от информационно-психологического воздействия.

Вопрос № 4. Силы, средства и приемы защиты объектов информационной инфраструктуры от информационно-технических воздействий.

Вопросы для самоконтроля:

1. Цели и задачи информационного противоборства.

2. Психологические приемы защиты личности от информационных воздействий.

3. Приемы защиты объектов информационной инфраструктуры от информационно-технических воздействий.

4. Средства защиты от информационно-технического воздействия.

Проблемные вопросы:

1. Эффективность защиты объектов информационной инфраструктуры от информационно-технических воздействий.

2. Эффективность защиты личности от информационных воздействий.

Задание № 4. Оценка информационной обстановки в интересах выработки специальных способов обеспечения информационной безопасности.

Вопрос № 1. Методы сбора и систематизации информации об уровне информационной безопасности.

Вопрос № 2. Аналитическое выявление угроз информационной безопасности.

Вопросы для самоконтроля:

1. Оценка достоверности сведений.

2. Виды и методы системного анализа угроз информационной безопасности.

3. Виды и методы морфологического анализа угроз информационной безопасности.

Проблемные вопросы:

1. Применение аналитических методов в ходе оценки информационной обстановки в условиях ее изменчивости и неопределенности.

2. Субъективность оценки и снижение ее влияния в интересах достижения достоверности.

Задание № 5. Алгоритмы работа руководителя предприятия по применению специальных методов обеспечения информационной безопасности.

Вопрос № 1. Содержание решения и планирование

Вопрос № 2. Силы и средства, постановка задач и непосредственное руководство их действиями.

Вопросы для самоконтроля:

1. Алгоритм работы руководителя при разработке и в ходе применения специальных методов обеспечения информационной безопасности

2. Методы обеспечения информационной безопасности и их влияние на работу руководителя.

Проблемные вопросы:

1. Контроль действий сил и средств, оценка их результативности.

2. Совершенствование непосредственного руководства силами и средствами.