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)

МЕЖДУНАРОДНЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ И КИБЕРТЕРРОРИЗМУ

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/ специальности)

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

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(направленность (профиль) ОП ВО)

Москва, 2025

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

Паспорт оценочных средств

Направление подготовки: 10.04.01 «Информационная безопасность» (программа подготовки магистра)

Дисциплина: «Международное сотрудничество в обеспечении информационной безопасности»

№ п/п	Контролируемые разделы (темы) дисциплины	Наименование оценочного средства
1	Информационно-телекоммуникационные технологии на современном этапе развития общества и их влияние на развитие международного сотрудничества	Письменный экспресс-опрос на семинаре с выставлением оценок в балльной системе
2	Международное сотрудничество в условиях глобальной информационной революции в условиях ее влияния на политику и социум	
3	Влияние угроз международной информационной безопасности на международное сотрудничество Российской Федерации	
4	Основы государственной политики Российской Федерации в области обеспечения международной информационной безопасности и ее реализация в международном сотрудничестве в рамках ООН, ЮНЕСКО, БРИКС и СНГ	
5	Реализация государственной политики Российской Федерации в области международной информационной безопасности в работе ОБСЕ, Совета Европы и профильных площадок АТР	
6	Проблемные аспекты международного сотрудничества в ходе реализации альтернативных подходов США, ЕС и НАТО к обеспечению международной информационной безопасности	

Типовые контрольные вопросы и задания для проведения промежуточной аттестации:

Контрольные вопросы.

1. Отношения межгосударственных противоречий и участники мировой политики как субъекты и объекты обеспечения информационной безопасности
2. Сущность, цель и задачи, принципы, средства, методы и способы обеспечения международной безопасности
3. Модели международной безопасности в зависимости от количества субъектов и характера отношений между участниками
4. Особенности изменения условий международной безопасности
5. Актуальные угрозы международной безопасности

6. Сущность, характер и проблематика глобальной безопасности

7. Сущность международной информационной безопасности и масштабы оценки информационной обстановки в зависимости от уровня управления и масштаба обобщения информации

8. Непрямые действия в международных отношениях и угрозы международной информационной безопасности

9. Мишени деструктивных воздействий на международное сообщество

10. Философские концепции постиндустриализма и глобального информационного общества

11. Внутреннее и внешнее, объективность и субъективность в философской концепции информационного общества

12. Характеристики информационного общества и закономерности воздействия информации на общество

13. Окинавская хартия глобального информационного общества 2000 г. о вхождении в него государств и реализации его экономических, социальных и культурных преимуществ

14. Окинавская хартия глобального информационного общества 2000 г. о преодолении электронно-цифрового разрыва и содействии всеобщему участию

15. Окинавская хартия глобального информационного общества 2000 г. о дальнейшем развитии и приоритетных областях информационного общества

16. Опасность и безопасность в информационной обстановке внешнеполитической сферы деятельности России

17. Деструктивные действия и угрозы информационного воздействия на Россию как объект международной безопасности

18. Сущность, цель, задачи и субъекты обеспечения международной информационной безопасности

19. Основные информационные угрозы России во внешнеполитической сфере ее деятельности и национальные интересы в соответствии с положениями Доктрины информационной безопасности РФ 2016 г.

20. Характеристики информационного общества, отражаемые Окинавской хартией глобального информационного общества 2000 г.

21. Структура Окинавской хартии глобального информационного общества 2000 г. Окинавская хартия о вхождении государств в информационное общество.

22. Сущность и Соглашения о сотрудничестве государств - участников СНГ в области обеспечения информационной безопасности и его основные положения.

23. Проблемы принятия международных конвенций по информационной безопасности. Предложения РФ в области совершенствования международной информационной безопасности.

24. «Стратегия обеспечения национальной безопасности РФ до 2020 г.» об информационной безопасности.

25. Доктрина информационной безопасности РФ о национальных интересах России в информационной сфере и составляющих их достижения.

Практические задания для проведения промежуточной аттестации

1. Осуществить анализ тенденций изменения условий безопасности международного сотрудничества в информационной сфере с реализацией предложений по обеспечению безопасности ГА ООН в 2010-19 гг.

2. Провести анализ актуальных угроз международной информационной безопасности в связи со сложностями интеграции предложений Российской Федерации в практику деятельности по обеспечению кибербезопасности США и ЕС.

3. Разработать основные положения Концепции информационной безопасности совместного предприятия в контексте требований Доктрины информационной безопасности Российской Федерации 2016 г. в части касающейся национальных интересов России в

информационной сфере и основных информационных угроз путем их трансформации применительно к специализации предприятия и масштабам его деятельности.

4. Разработать модель обеспечения информационной безопасности в сфере международного сотрудничества в связи с реальным характером и проблематикой обеспечения глобальной безопасности.

5. Разработать предложения по дальнейшей реализации соглашений, подписанных под Окинавской хартией глобального информационного общества 2000 г., в соответствии с реалиями международного сотрудничества 2019 г.

6. Провести сравнительный анализ понятий, предмета, системы, принципов и субъектов международного информационного права и правовой системы Российской Федерации в области информационной безопасности

7. Провести анализ результатов международного сотрудничества в информационной сфере в 2010-19 гг.

8. Провести анализ содержания Европейской конвенции о киберпреступности в интересах информационной безопасности Российской Федерации и развития междунаодного сотрудничества.

9. Разработать концептуальные аспекты обеспечения кибербезопасности и противодействия киберпреступности исходя из Ваших представлений о содержании проблемы обеспечения информационной безопасности Вашего предприятия.

10. Разработать Ваши предложения в развитие межгосударственных практик борьбы с кибертерроризмом и обеспечения кибербезопасности.

11. Сравнить положения базовых международных стандартов обеспечения информационной безопасности ISO/IEC 27001 и ISO/IEC 27002 с положениями отечественных стандартов в области обеспечения информационной безопасности.

12. Проанализировать и обобщить требования «Концепции внешней политики РФ», «Стратегии обеспечения национальной безопасности РФ до 2020 г.» в части обеспечения информационной безопасности и положения Доктрины информационной безопасности Российской Федерации 2016 г.

13. Провести сравнительный анализ содержания базовых понятий «опасность», «информационная безопасность», «угроза», «управление информационной безопасностью», «менеджмент информационной безопасности», «обеспечение информационной безопасности», «защита информации», «риск», «ущерб», применяемых в отечественных и иностранных нормативных источниках.

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

Оценивание знаний студентов по дисциплине «Международное сотрудничество в обеспечении информационной безопасности» осуществляется в ходе текущего контроля успеваемости и промежуточной аттестации в соответствии с балльно-рейтинговой системой.

Оценка знаний студентов включает:

1. Оценку работы студента в течение семестра – до 60 баллов.
2. Оценка знаний студента на промежуточной аттестации – до 40 баллов.

Промежуточная аттестация предусмотрена в форме экзамена, который проводится в виде устного собеседования по контрольным вопросам. Предлагается два теоретических вопроса.

Важнейшими критериями оценки знаний и умений являются:

– степень усвоения учебной программы;

– содержание ответа на контрольные вопросы: логичность и доказательность изложения;

– степень творчества и самостоятельности в раскрытии поставленных вопросов.

Содержание текущего контроля успеваемости.

Выполнение мероприятий учебной работы	**Удельный вес в баллах**	**Количество мероприятий**	**Всего баллов**
Работа на лекциях	до 1,3	7	до 9,0
Работа на семинарских и практических занятиях	до 3,0	7	до 21,0
		Итого:	**до 30,0**

Оценка знаний на экзамене.

	Удельный вес одного вопроса в баллах	**Количество вопросов**	**Всего баллов**
Ответ на экзамене	до 10,0	2	до 20,0
		Итого:	**до 50,0**

Критерии оценивания ответов на вопросы экзамена.

Для получения 9-10 баллов за ответ на один вопрос студент должен:

1. Исчерпывающе владеть терминологическим аппаратом по теме, ее метаязыком; видеть системные связи объекта с общим контекстом дисциплины и смежными вопросами.

2. Иметь системное представление об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Владеть методикой анализа объекта, видеть связь теоретических аспектов темы с прикладными исследованиями.

4. Уметь выстраивать связные научные формулировки ответа с опорой на базовые понятия и категории; проявлять необходимую степень самостоятельности в представлении темы в ее внутренней логике.

Для получения 6-8 баллов студент должен:

1. В достаточной мере владеть терминологическим аппаратом по теме; видеть системные связи объекта со смежными вопросами.

2. Иметь общее представление об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Владеть основными принципами методики анализа объекта, видеть связь теоретических аспектов темы с прикладными исследованиями.

4. Уметь выстраивать связные научные формулировки с опорой на базовые понятия и категории; проявлять необходимую степень самостоятельности в представлении темы в ее внутренней логике.

Менее 6 баллов выставляется студенту в том случае, если он:

1. Не владеет терминологическим аппаратом по теме.

2. Не имеет представлений об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Не владеет принципами анализа объекта.

4. Не умеет выстраивать связные научные формулировки.