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 УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(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)

ЭКЗАМЕН.

Список вопросов для экзамена по дисциплине

1 вопрос

1. Формирование политики управления инцидентами ИБ. Основное содержание политики управления инцидентами ИБ
2. Создание группы реагирования на инциденты ИБ. Цель создания. Роли группы реагирования на инциденты ИБ
3. Подготовка к обработке инцидентов ИБ. Классификация инцидентов ИБ по значимости
4. Обеспечение осведомленности и обучение управлению инцидентами. Цель осведомления об управлении инцидентами ИБ. Цель обучения управлению инцидентами ИБ
5. Тестирование системы управления инцидентами ИБ
6. Первичная оценка событий ИБ. Цель проведения первичной оценки. Последовательность действий при проведении первичной оценки
7. Вторичная оценка инцидента ИБ. Цель проведения вторичной оценки. Последовательность действий при проведении вторичной оценки
8. Сдерживание, устранение инцидента ИБ и восстановление после него
9. Формирование и хранение свидетельств инцидентов ИБ
10. Определение инцидента неавторизованного доступа. Цели инцидента неавторизованного доступа
11. Определение инцидента отказа в обслуживании. Цели инцидента отказа в обслуживании. Примеры инцидентов отказа в обслуживании
12. Определение инцидента сбора информации. Цели инцидента сбора информации
13. Определение инцидента внедрения вредоносного кода. Средства реализации инцидента внедрения вредоносного кода. Цели инцидента
14. Определение инцидента несоответствующего использования. Примеры инцидентов несоответствующего использования
15. Стратегии управления непрерывностью функционирования АС для помещений и технологий
16. Стратегии управления непрерывностью функционирования АС для данных. Стратегии управления непрерывностью функционирования АС для поставщиков
17. Стратегии управления непрерывностью функционирования АС для компьютеров
18. Стратегии управления непрерывностью функционирования АС для серверов

19. Стратегии управления непрерывностью функционирования АС для локальной сети

2 вопрос

1. Привести пример формы сообщения «Отчет о событии ИБ» сотрудника, обнаружившего нештатную ситуацию, имеющую отношение к ИБ
2. Привести пример формы сообщения «Отчет об инциденте ИБ» сотрудника ГРИИБ, проводившего первичную оценку событий ИБ
3. Привести пример матрицы для определения значимости инцидентов неавторизованного доступа
4. Определить предвестники и указатели инцидентов неавторизованного доступа
5. Определить меры по сдерживанию, устранению инцидентов неавторизованного доступа и восстановлению после них
6. Привести пример матрицы для определения значимости инцидентов отказа в обслуживании
7. Определить предвестники и указатели инцидентов отказа в обслуживании
8. Определить меры по сдерживанию, устранению инцидентов отказа в обслуживании и восстановлению после них
9. Привести пример матрицы для определения значимости инцидентов сбора информации
10. Определить предвестники и указатели инцидентов сбора информации
11. Определить меры по сдерживанию, устранению инцидентов сбора информации и восстановлению после них
12. Привести пример матрицы для определения значимости инцидентов внедрения вредоносного кода
13. Определить предвестники и указатели инцидентов внедрения вредоносного кода
14. Определить меры по сдерживанию, устранению инцидентов внедрения вредоносного кода и восстановлению после них
15. Привести пример матрицы для определения значимости инцидентов несоответствующего использования
16. Определить предвестники и указатели инцидентов несоответствующего использования. Определить меры по сдерживанию, устранению инцидентов несоответствующего использования и восстановлению после них

3 вопрос

1. Построить возможные сценарии инцидента неавторизованного доступа
2. Построить возможные сценарии инцидента отказа в обслуживании
3. Построить возможные сценарии инцидента внедрения вредоносного кода
4. Построить возможные сценарии инцидента сбора информации
5. Построить возможные сценарии инцидента несоответствующего использования

Пример билета.

1. Тестирование системы управления инцидентами ИБ
2. Определить меры по сдерживанию, устранению инцидентов внедрения вредоносного кода и восстановлению после них
3. Построить возможные сценарии инцидента внедрения вредоносного кода