Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 11.04.01 Радиотехника

Наименование образовательной программы: Киберфизические системы и интернет вещей

Уровень образования: высшее образование - магистратура

Форма обучения: Очно-заочная

Оценочные материалы
по дисциплине
Защита информации

Москва
2023

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Крутских В.В. Идентификатор: R49539849-KrutskikhVV-f1575360	В.В. Крутских

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Стрелков Н.О. Идентификатор: R784cde94-StrelkovNO-f448f943	Н.О. Стрелков
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Шалимова Е.В. Идентификатор: Rf4bb1f0c-ShalimovaYV-f267ebd6	Е.В. Шалимова

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. УК-1 способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

ИД-3 Вырабатывает стратегию решения поставленной задачи

2. ПК-1 Способен определять цели, осуществлять постановку задач проектирования и эксплуатации, подготавливать технические задания на выполнение проектных и эксплуатационных работ по созданию устройств сбора данных и управления инфраструктурой

ИД-1 Знает структурные схемы и устройство радиотехнических узлов и систем различного функционального назначения

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. Тест по темам 1.1 и 1.2 (Тестирование)
2. Тест по темам 2.1 и 2.2 (Тестирование)
3. Тест по темам 2.3 и 2.4 (Тестирование)
4. Тест по темам 3.1 и 3.2 (Тестирование)

БРС дисциплины

4 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	5	11	14	15
Основные положения, термины и определения кибербезопасности индустриальных систем.					
Основные понятия кибербезопасности индустриальных систем.		+			
Оценка безопасности киберфизических систем.		+			
Основные методы защиты информации от базовых угроз в киберфизической системе.					
Концепции, методы и средства применения кибероружия.			+	+	
Типовые угрозы и уязвимости в системах киберзащиты.			+	+	
Методы выявления программных уязвимостей.			+	+	

Обеспечение кибербезопасности конечных точек систем информационной инфраструктуры организации.		+	+	
Управление информационной безопасностью в киберфизических системах.				
Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур.				+
Основные направления обеспечения кибербезопасности.				+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
УК-1	ИД-З$_{УК-1}$ Вырабатывает стратегию решения поставленной задачи	Знать: принципы и методы построения комплексных систем защиты информации киберфизических систем Уметь: применять современные методики анализа процессов управления в учебном процессе.	Тест по темам 2.1 и 2.2 (Тестирование) Тест по темам 3.1 и 3.2 (Тестирование)
ПК-1	ИД-1$_{ПК-1}$ Знает структурные схемы и устройство радиотехнических узлов и систем различного функционального назначения	Знать: проблематику систем защиты информации киберфизических систем направления и перспективы развития систем защиты информации киберфизических систем Уметь: обосновано выбирать стратегию управления рисками информационной безопасности	Тест по темам 1.1 и 1.2 (Тестирование) Тест по темам 2.3 и 2.4 (Тестирование) Тест по темам 3.1 и 3.2 (Тестирование)

		киберфизической системы.	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Тест по темам 1.1 и 1.2

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Необходимо ответить на вопросы теста.

Краткое содержание задания:
Необходимо ответить на вопросы теста.

Контрольные вопросы/задания:

Знать: проблематику систем защиты информации киберфизических систем	1.Специфика оценки информационной безопасности киберфизических систем. 2.Подходы к информационной безопасности киберфизических систем.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-2. Тест по темам 2.1 и 2.2

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Необходимо ответить на вопросы теста.

Краткое содержание задания:
Необходимо ответить на вопросы теста.

Контрольные вопросы/задания:

Знать: принципы и методы	1.Уязвимости программного обеспечения

построения комплексных систем защиты информации киберфизических систем	информационных систем. 2.Проблемы идентификации исполнителей и заказчиков кибератак.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-3. Тест по темам 2.3 и 2.4

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Необходимо ответить на вопросы теста.

Краткое содержание задания:
Необходимо ответить на вопросы теста.

Контрольные вопросы/задания:

Знать: направления и перспективы развития систем защиты информации киберфизических систем	1.Виды и порядок проведения сертификационных испытаний. 2.Мероприятия по устранению уязвимостей в критических информационных системах.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-4. Тест по темам 3.1 и 3.2

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Необходимо ответить на вопросы теста.

Краткое содержание задания:
Необходимо ответить на вопросы теста.

Контрольные вопросы/задания:

Уметь: применять современные методики анализа процессов управления в учебном процессе.	1.Оцените стандартные инструменты для организации проактивного поиска.
Уметь: обосновано выбирать стратегию управления рисками информационной безопасности киберфизической системы.	1.Оцените риски безопасности в энергетических системах.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1. Основные задачи SIEM.
2. Интерфейсы ввода/вывода киберфизических систем.

Процедура проведения

Экзамен проводится в письменной форме по билетам согласно программе экзамена.

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-З$_{УК-1}$ Вырабатывает стратегию решения поставленной задачи

Вопросы, задания

1.Определение и архитектура киберфизической системы.
2.Концепция «Индустрия 4.0». Описание, основные задачи.
3.Понятие и характерные признаки киберугрозы.
4.Оценка безопасности киберфизических систем.
5.Схема управления киберфизической системой.
6.Основные направления обеспечения кибербезопасности.
7.Основные цели и задачи SIEM.
8.Особенности цифрового управления промышленными инфраструктурами.
9.Основные угрозы безопасности цифрового производства.
10.Индустриальные киберфизические системы: особенности и текущее состояние.

Материалы для проверки остаточных знаний

1.Особенности автономных адаптивных систем кибервоздействий

Ответы:

Необходим полный исчерпывающий ответ.

Верный ответ: - Независимость от связи с оператором. - Является экспертной системой, опирающейся на базу знаний об объекте воздействия. - Имеет модульную схему построения, позволяющую комбинировать различные способы воздействия на целевую систему и при необходимости способность изменять себя в зависимости от внешних факторов.

2.Факторы, способствующие успешному проведению удаленных сетевых атак:

Ответы:

Необходим полный исчерпывающий ответ.

Верный ответ: - несвоевременное отслеживание и выполнение рекомендаций специалистов по защите и анализу случаев вторжения для ликвидации эксплойтов и ошибок в программном обеспечении; - открытость информационной системы, свободный доступ к информации по организации сетевого взаимодействия, способам защиты, применяемым в системе; - наличие ошибок в операционных системах, прикладном программном обеспечении, протоколах сетевого обмена; - разнородность используемых версий программного обеспечения и операционных

систем; - ошибки конфигурирования систем и средств защиты; - «экономия» на средствах и системах обеспечения безопасности (или игнорирование их).

2. Компетенция/Индикатор: ИД-1$_{ПК-1}$ Знает структурные схемы и устройство радиотехнических узлов и систем различного функционального назначения

Вопросы, задания

1.Проблемы выбора аппаратного обеспечения для реализации компонентов киберфизических систем.
2.Датчики и актуаторы в киберфизических системах: виды и назначение.
3.Виды беспроводных сетей, применяемых для создания компонентов киберфизических систем.
4.Роль облачных вычислений в Интернете вещей и киберфизических системах.
5.Основные проблемы использования облачных вычислений при реализации киберфизических систем.
6.Простой анализ данных в киберфизических системах.
7.Этапы модельного проектирования киберфизических систем.
8.Классификация, принцип действия и области применения измерительных устройств в составе киберфизических систем.
9.Классификация, принцип действия и области применения исполнительных устройств киберфизических систем.
10.Интерфейсы ввода/вывода киберфизических систем.

Материалы для проверки остаточных знаний

1.Детализированный алгоритм типовой кибератаки:
Ответы:
Необходим полный исчерпывающий ответ.
Верный ответ: - идентификация доменных имен и связанных с ними сетей; - опрос службы доменных имен (DNS); - разведка сети с целью определения их топологии и потенциальных путей доступа; - определение конкретных целей и задач; - получение доступа к объекту; - расширение полномочий; - кража информации.
2.Классификация кибервоздействия по категориям:
Ответы:
Необходим полный исчерпывающий ответ.
Верный ответ: - по виду (одиночные и групповые), - по типу (пассивные и активные), - по характеру поражающих свойств (высокочастотные и комплексные), - по цели использования (атакующие, оборонительные и обеспечивающие), - по способу реализации (алгоритмические, программные, аппаратные, физические).
3.Особенности адаптивных кибервоздействий с внешним управлением
Ответы:
Необходим полный исчерпывающий ответ.
Верный ответ: - Целью являются системы и комплексы, действующие по однозначно установленным законам и алгоритмам. - Воздействие может быть описано как информационная система, состоящая из четырех блоков: проникновения; сбора информации; связи и управления; модернизации. - Данному воздействию существенный недостаток - потребность в действующем канале связи.

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

Оценка: 2

Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.