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

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Защита информации в киберфизических системах

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Рыжиков С.С. Идентификатор: R6eeae99e-RyzhikovSS-b1299f04	С.С. Рыжиков
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

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. ПК-3 Способен администрировать средства защиты информации в компьютерных системах и сетях

ПК-3.2 Администрирует программно-аппаратные средства защиты информации в компьютерных сетях

и включает:

для текущего контроля успеваемости:

Форма реализации: Устная форма

1. Контрольный опрос № 1 по темам 1 и 2 (Перекрестный опрос)
2. Контрольный опрос № 2 по темам 3 и 4 (Перекрестный опрос)
3. Контрольный опрос № 3 по темам 5 и 6 (Перекрестный опрос)
4. Контрольный опрос № 4 по темам 7 и 8 (Перекрестный опрос)

БРС дисциплины

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	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
ПК-3	ПК-3.2$_{ПК-3}$ Администрирует программно-аппаратные средства защиты информации в компьютерных сетях	Знать: Принципы и методы построения комплексных систем защиты информации киберфизических систем. Проблематику систем защиты информации киберфизических систем. Направления и перспективы развития систем защиты информации киберфизических систем. Уметь: Обосновано выбирать стратегию управления рисками информационной безопасности киберфизической системы. Применять современные методики анализа процессов управления в учебном процессе.	Контрольный опрос № 1 по темам 1 и 2 (Перекрестный опрос) Контрольный опрос № 2 по темам 3 и 4 (Перекрестный опрос) Контрольный опрос № 3 по темам 5 и 6 (Перекрестный опрос) Контрольный опрос № 4 по темам 7 и 8 (Перекрестный опрос)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольный опрос № 1 по темам 1 и 2

Формы реализации: Устная форма
Тип контрольного мероприятия: Перекрестный опрос
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Устный контрольный опрос группы по пройденным темам с выставлением оценок.

Краткое содержание задания:
Опрос

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 ответ прозвучал в полном объеме

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется при частично неполном ответе

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется при в основном верном ответе

КМ-2. Контрольный опрос № 2 по темам 3 и 4

Формы реализации: Устная форма
Тип контрольного мероприятия: Перекрестный опрос
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Устный контрольный опрос группы по пройденным темам с выставлением оценок.

Краткое содержание задания:
Опрос

Контрольные вопросы/задания:

Знать: Принципы и методы построения комплексных систем защиты информации киберфизических систем.	1.Уязвимости программного обеспечения 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 ответ прозвучал в полном объеме

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется при частично неполном ответе

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется при в основном верном ответе

КМ-3. Контрольный опрос № 3 по темам 5 и 6

Формы реализации: Устная форма
Тип контрольного мероприятия: Перекрестный опрос
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Устный контрольный опрос группы по пройденным темам с выставлением оценок.

Краткое содержание задания:
Опрос

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 ответ прозвучал в полном объеме

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется при частично неполном ответе

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется при в основном верном ответе

КМ-4. Контрольный опрос № 4 по темам 7 и 8

Формы реализации: Устная форма
Тип контрольного мероприятия: Перекрестный опрос

Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Устный контрольный опрос группы по пройденным темам с выставлением оценок.

Краткое содержание задания:
Опрос

Контрольные вопросы/задания:

Уметь: Обосновано выбирать стратегию управления рисками информационной безопасности киберфизической системы.	1.Стандартные инструменты для организации проактивного поиска.
Уметь: Применять современные методики анализа процессов управления в учебном процессе.	1.Оценивать 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 ответ прозвучал в полном объеме

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется при частично неполном ответе

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется при в основном верном ответе

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ МЭИ	**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1** Кафедра *Безопасности и информационных технологий* Дисциплина «Защита информации в киберфизических системах»	*Утверждаю:* *Зав. каф. БИТ* *А.Ю.Невский* Протокол № от 2021 года .
1. Основные задачи SIEM. 2. Интерфейсы ввода/вывода киберфизических систем. Доцент, к.т.н. С.С. Рыжиков		

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: ПК-3.2$_{ПК-3}$ Администрирует программно-аппаратные средства защиты информации в компьютерных сетях

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.
11.Проблемы выбора аппаратного обеспечения для реализации компонентов киберфизических систем.
12.Датчики и актуаторы в киберфизических системах: виды и назначение.
13.Виды беспроводных сетей, применяемых для создания компонентов киберфизических систем.
14.Роль облачных вычислений в Интернете вещей и киберфизических системах.
15.Основные проблемы использования облачных вычислений при реализации киберфизических систем.
16.Простой анализ данных в киберфизических системах.

17.Этапы модельного проектирования киберфизических систем.
18.Классификация, принцип действия и области применения измерительных устройств в составе киберфизических систем.
19.Классификация, принцип действия и области применения исполнительных устройств киберфизических систем.
20.Интерфейсы ввода/вывода киберфизических систем.

Материалы для проверки остаточных знаний

1.Детализированный алгоритм типовой кибератаки:
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:
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
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.

4.Особенности автономных адаптивных систем кибервоздействий
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.

5.Факторы, способствующие успешному проведению удаленных сетевых атак:
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).

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

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 (проводимого по билетам).