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

Рабочая программа дисциплины
ЗАЩИТА ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.06**
Трудоемкость в зачетных единицах:	**4 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**4 семестр - 12 часов;**
Практические занятия	**4 семестр - 8 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**4 семестр - 2 часа;**
Самостоятельная работа	**4 семестр - 121,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Тестирование**	
Промежуточная аттестация:	
Экзамен	**4 семестр - 0,5 часа;**

Москва 2024

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	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

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: получение систематизированных теоретических знаний о базовых принципах и методах построения систем защиты информации в киберфизических системах, в том числе и на объектах энергетики РФ; освоение типовых методов построения систем защиты от базовых угроз, изучение основ теории информационной безопасности, ознакомление с проблематикой защиты информации в киберфизических системах на современном этапе развития информационных технологий.

Задачи дисциплины

- Сформировать представление об основных положениях теории информационной безопасности, методологии защиты информационных коммуникаций, овладеть основными понятиями – угрозы, уязвимости и риски в информационной безопасности.;
- Изучить свойства технологических процессов с точки зрения защиты информации, обрабатываемой в киберфизических системах.;
- Изучить свойства технологических процессов с точки зрения защиты информации, обрабатываемой в киберфизических системах.;
- Дать характеристику проблематики защиты информации киберфизических систем на современном этапе развития информационных технологий, определить основные направления и перспективы развития направления..

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	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..
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$_{ПК-1}$ 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 киберфизической системы..

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Киберфизические системы и интернет вещей (далее – ОПОП), направления подготовки 11.04.01 Радиотехника, уровень образования: высшее образование - магистратура.

Базируется на уровне высшего образования (бакалавриат, специалитет).

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Основные положения, термины и определения кибербезопасности индустриальных систем.	22	4	4	-	2	-	-	-	-	-	16	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Общие понятия о защите информации. Нормативная база." подготовка к выполнению заданий на практических занятиях ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Общие понятия о защите информации. Нормативная база." ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Общие понятия о защите информации. Нормативная база." ***Изучение материалов литературных источников:*** [1], 10-64 [2], 45-60 [4], 385-390 [5], 10-35
1.1	Основные понятия кибербезопасности индустриальных систем.	11		2	-	1	-	-	-	-	-	8	-	
1.2	Оценка безопасности киберфизических систем.	11		2	-	1	-	-	-	-	-	8	-	
2	Основные методы защиты информации от базовых угроз в киберфизической системе.	56		4	-	4	-	-	-	-	-	48	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Каналы утечки информации" ***Подготовка к практическим занятиям:***

2.1	Концепции, методы и средства применения кибероружия.	15		2	-	1	-	-	-	-	-	12	-	Изучение материала по разделу "Каналы утечки информации" подготовка к выполнению заданий на практических занятиях ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Каналы утечки информации" ***Изучение материалов литературных источников:*** [1], 65-140 [3], 43-56 [5], 40-75
2.2	Типовые угрозы и уязвимости в системах киберзащиты.	14		1	-	1	-	-	-	-	-	12	-	
2.3	Методы выявления программных уязвимостей.	14		1	-	1	-	-	-	-	-	12	-	
2.4	Обеспечение кибербезопасности конечных точек систем информационной инфраструктуры организации.	13		-	-	1	-	-	-	-	-	12	-	
3	Управление информационной безопасностью в киберфизических системах.	30		4	-	2	-	-	-	-	-	24	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Средства защиты информации." ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Средства защиты информации." подготовка к выполнению заданий на практических занятиях ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Средства защиты информации." ***Изучение материалов литературных источников:*** [1], 141-560 [3], 123-147
3.1	Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур.	15		2	-	1	-	-	-	-	-	12	-	
3.2	Основные направления обеспечения кибербезопасности.	15		2	-	1	-	-	-	-	-	12	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**12**	**-**	**8**	**-**	**2**	**-**	**-**	**0.5**	**88**	**33.5**	
	Итого за семестр	**144.0**		**12**	**-**	**8**	**2**		**-**		**0.5**	**121.5**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Основные положения, термины и определения кибербезопасности индустриальных систем.

1.1. Основные понятия кибербезопасности индустриальных систем.

Цифровая трансформация производства. Новые угрозы безопасности. Безопасная среда функционирования информационных систем. Оценка текущего состояния киберфизической системы. Оценка способности системы сопротивляться деструктивным воздействиям..

1.2. Оценка безопасности киберфизических систем.

Киберпространство – новый виток эволюции IT систем. Понятие киберфизического объекта. Систематизация киберфизических систем. Проблема информационной безопасности киберфизических систем. Специфика оценки информационной безопасности киберфизических систем. Подходы к информационной безопасности киберфизических систем. Общая схема оценки информационной безопасности различных классов киберфизических систем..

2. Основные методы защиты информации от базовых угроз в киберфизической системе.

2.1. Концепции, методы и средства применения кибероружия.

Методологические принципы классификации кибероружия. Проблемы идентификации исполнителей и заказчиков кибератак. Основные проблемы решения задачи идентификации источника кибератаки..

2.2. Типовые угрозы и уязвимости в системах киберзащиты.

Угрозы и уязвимости в микросхемах. Угрозы и уязвимости в криптографических алгоритмах (стандартах). Преднамеренные уязвимости в шифровальном оборудовании. Уязвимости программного обеспечения информационных систем. Уязвимости в автомобилях. Уязвимости бортового оборудования воздушных судов и робототехнических комплексов..

2.3. Методы выявления программных уязвимостей.

Виды и порядок проведения сертификационных испытаний. Тестирование безопасности кода. Типовая статистика выявления уязвимостей в программном обеспечении. Мероприятия по устранению уязвимостей в критических информационных системах..

2.4. Обеспечение кибербезопасности конечных точек систем информационной инфраструктуры организации.

Тенденции развития киберугроз, направленных на конечные точки инфраструктурных систем. Тенденция роста бесфайловых атак. Рост ущерба от атак на конечные точки. Мировой рынок EDR-решений. Основные платформы Endpoint Detection and Response..

3. Управление информационной безопасностью в киберфизических системах.

3.1. Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур.

Тенденции развития и особенности цифровизации промышленных инфраструктур. Оценка рисков безопасности в энергетических системах. Стандарты и методы обеспечения кибербезопасности в электроэнергетических структурах..

3.2. Основные направления обеспечения кибербезопасности.

Концепции и сценарии «цветного противостояния». Имитация целевых атак как оценка безопасности. Охота за угрозами как «проактивный метод» киберзащиты. Стандартные инструменты для организации проактивного поиска..

3.3. Темы практических занятий

1. 8. Протокол Modbus;
2. 7. Системы автоматического контроля и сбора информации –SCADA;
3. 6. Уязвимости киберфизических беспилотных авиационных систем;
4. 5. Поиск угроз и уязвимостей киберфизических систем. Нейтрализация угроз безопасности и устранение уязвимостей защиты объектов киберфизических систем;
5. 4. Особенности экспериментального тестирования защищенности киберфизических систем. Общий порядок экспериментального тестирования защищенности киберфизических систем;
6. 3. Основные алгоритмы (пути) внедрения «зараженных» микросхем в технические объекты киберфизических систем;
7. 2. Современные технологии контроля безопасности в микроэлектронике;
8. 1. Основы проектирования кибербезопасной электронной аппаратуры для АСУТП критических инфраструктур.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)			Оценочное средство (тип и наименование)
		1	2	3	
Знать:					
принципы и методы построения комплексных систем защиты информации киберфизических систем	ИД-З$_{УК-1}$		+		Тестирование/Тест по темам 2.1 и 2.2
направления и перспективы развития систем защиты информации киберфизических систем	ИД-1$_{ПК-1}$		+		Тестирование/Тест по темам 2.3 и 2.4
проблематику систем защиты информации киберфизических систем	ИД-1$_{ПК-1}$	+			Тестирование/Тест по темам 1.1 и 1.2
Уметь:					
применять современные методики анализа процессов управления в учебном процессе.	ИД-З$_{УК-1}$	+	+		Тестирование/Тест по темам 3.1 и 3.2
обосновано выбирать стратегию управления рисками информационной безопасности киберфизической системы.	ИД-1$_{ПК-1}$			+	Тестирование/Тест по темам 3.1 и 3.2

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

4 семестр

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)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №4)

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.

В диплом выставляется оценка за 4 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Кибербезопасность цифровой индустрии : теория и практика функциональной устойчивости к кибератакам / Д. П. Зегжда, Е. Б. Александрова, М. О. Калинин, [и др.] ; ред. Д. П. Зегжда . – Москва : Горячая Линия-Телеком, 2020 . – 560 с. - Авторы указаны на обороте тит. л. - ISBN 978-5-9912-0827-7 .;
2. Родичев, Ю. А. Информационная безопасность: нормативно-правовые аспекты : учебное пособие для вузов по специальностям 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем" / Ю. А. Родичев . – СПб. : Питер, 2008 . – 272 с. – (Учебное пособие) . - ISBN 978-5-388-00069-9 .;
3. Васильев, В. И. Интеллектуальные системы защиты информации : учебное пособие для вузов по специализациям специальности "Комплексное обеспечение информационной безопасности автоматизированных систем" / В. И. Васильев . – 2-е изд., испр . – М. : Машиностроение, 2013 . – 172 с. – (Для вузов) . - ISBN 978-5-94275-667-3 .;
4. Ли П.- "Архитектура интернета вещей", Издательство: "ДМК Пресс", Москва, 2019 - (454 с.)
https://e.lanbook.com/book/112923;
5. А. А. Титов- "Инженерно-техническая защита информации", Издательство: "Томский государственный университет систем управления и радиоэлектроники", Томск, 2010 - (195 с.)
https://biblioclub.ru/index.php?page=book&id=208567.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Видеоконференции (Майнд, Сберджаз, ВК и др);
3. Scilab;
4. Python;
5. Libre Office;
6. ОС Debian.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Е-802/2, Учебная лаборатория Радиоизмерений и медицинской электроники	стол, стул, вешалка для одежды, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер, верстак электротехнический , стенд учебный
Учебные аудитории для проведения практических занятий, КР и КП	Е-802/2, Учебная лаборатория Радиоизмерений и медицинской электроники	стол, стул, вешалка для одежды, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер, верстак электротехнический , стенд учебный
Учебные аудитории для проведения промежуточной аттестации	Е-802/2, Учебная лаборатория Радиоизмерений и медицинской электроники	стол, стул, вешалка для одежды, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер, верстак электротехнический , стенд учебный
Помещения для самостоятельной работы	НТБ-201, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	Е-815, Преподавательская	стол, стул, шкаф, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер
Помещения для хранения оборудования и учебного инвентаря	Е-802/4, Склад инвентаря и оборудования	стеллаж, стол, стул, шкаф, шкаф для документов, сервер

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Защита информации

(название дисциплины)

4 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 Тест по темам 1.1 и 1.2 (Тестирование)
КМ-2 Тест по темам 2.1 и 2.2 (Тестирование)
КМ-3 Тест по темам 2.3 и 2.4 (Тестирование)
КМ-4 Тест по темам 3.1 и 3.2 (Тестирование)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	5	11	14	15
1	Основные положения, термины и определения кибербезопасности индустриальных систем.					
1.1	Основные понятия кибербезопасности индустриальных систем.		+			+
1.2	Оценка безопасности киберфизических систем.		+			
2	Основные методы защиты информации от базовых угроз в киберфизической системе.					
2.1	Концепции, методы и средства применения кибероружия.			+	+	+
2.2	Типовые угрозы и уязвимости в системах киберзащиты.			+	+	
2.3	Методы выявления программных уязвимостей.			+	+	
2.4	Обеспечение кибербезопасности конечных точек систем информационной инфраструктуры организации.			+	+	
3	Управление информационной безопасностью в киберфизических системах.					
3.1	Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур.					+
3.2	Основные направления обеспечения кибербезопасности.					+
		Вес КМ, %:	25	25	25	25