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 автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

Рабочая программа дисциплины
ЗАЩИТА ИНФОРМАЦИИ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.05**
Трудоемкость в зачетных единицах:	**8 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**8 семестр - 16 часов;**
Практические занятия	**8 семестр - 20 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**8 семестр - 2 часа;**
Самостоятельная работа	**8 семестр - 141,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Перекрестный опрос**	
Промежуточная аттестация:	
Экзамен	**8 семестр - 0,5 часа;**

Москва 2023

ПРОГРАММУ СОСТАВИЛ:

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)

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.;
- Дать понятие о комплексной защите информации 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
ПК-3 Способен администрировать средства защиты информации в компьютерных системах и сетях	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..

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность автоматизированных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

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 5 зачетных единиц, 180 часов.

№ 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.	36	8	4	-	4	-	-	-	-	-	28	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Основные положения, термины и определения кибербезопасности индустриальных систем." ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка к контрольной работе:*** Изучение материалов по разделу Основные положения, термины и определения кибербезопасности индустриальных систем. и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Основные положения, термины и определения кибербезопасности индустриальных систем." подготовка к выполнению заданий на практических занятиях
1.1	Основные понятия кибербезопасности индустриальных систем.	18		2	-	2	-	-	-	-	-	14	-	
1.2	Оценка безопасности киберфизических систем.	18		2	-	2	-	-	-	-	-	14	-	

														Самостоятельное изучение теоретического материала: Изучение дополнительного материала по разделу "Основные положения, термины и определения кибербезопасности индустриальных систем." ***Изучение материалов литературных источников:*** [1], 28-33
2	Основные методы защиты информации от базовых угроз в киберфизической системе.	72		8	-	10	-	-	-	-	-	54	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Основные методы защиты информации от базовых угроз в киберфизической системе." ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к контрольной работе:*** Изучение материалов по разделу Основные методы защиты информации от базовых угроз в киберфизической системе. и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Основные методы защиты информации от базовых угроз в киберфизической системе." подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Основные методы защиты информации от базовых угроз в киберфизической системе." ***Изучение материалов литературных источников:*** [1], 10-20 [2], 25-35
2.1	Концепции, методы и средства применения кибероружия.	16		2	-	2	-	-	-	-	-	12	-	
2.2	Типовые угрозы и уязвимости в системах киберзащиты.	18		2	-	2	-	-	-	-	-	14	-	
2.3	Методы выявления программных уязвимостей.	18		2	-	2	-	-	-	-	-	14	-	
2.4	Обеспечение кибербезопасности конечных точек систем информационной инфраструктуры организации.	20		2	-	4	-	-	-	-	-	14	-	
3	Управление информационной безопасностью в	36		4	-	6	-	-	-	-	-	26	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Управление информационной

	киберфизических системах.													безопасностью в киберфизических системах."
3.1	Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур.	16		2	-	2	-	-	-	-	-	12	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка к контрольной работе:*** Изучение материалов по разделу Управление информационной безопасностью в киберфизических системах. и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Управление информационной безопасностью в киберфизических системах." подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Управление информационной безопасностью в киберфизических системах." ***Изучение материалов литературных источников:*** [1], 61-65
3.2	Основные направления обеспечения кибербезопасности.	20		2	-	4	-	-	-	-	-	14	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**180.0**		**16**	**-**	**20**	**-**	**2**	**-**	**-**	**0.5**	**108**	**33.5**	
	Итого за семестр	**180.0**		**16**	**-**	**20**	**2**		**-**		**0.5**	**141.5**		

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

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Основные положения, термины и определения кибербезопасности индустриальных систем."
2. Обсуждение материалов по кейсам раздела "Основные методы защиты информации от базовых угроз в киберфизической системе."
3. Обсуждение материалов по кейсам раздела "Управление информационной безопасностью в киберфизических системах."

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основные положения, термины и определения кибербезопасности индустриальных систем."
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основные методы защиты информации от базовых угроз в киберфизической системе."
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Управление информационной безопасностью в киберфизических системах."

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:					
Направления и перспективы развития систем защиты информации киберфизических систем.	ПК-3.2$_{ПК-3}$		+		Перекрестный опрос/Контрольный опрос № 3 по темам 5 и 6
Проблематику систем защиты информации киберфизических систем.	ПК-3.2$_{ПК-3}$	+			Перекрестный опрос/Контрольный опрос № 1 по темам 1 и 2
Принципы и методы построения комплексных систем защиты информации киберфизических систем.	ПК-3.2$_{ПК-3}$		+		Перекрестный опрос/Контрольный опрос № 2 по темам 3 и 4
Уметь:					
Применять современные методики анализа процессов управления в учебном процессе.	ПК-3.2$_{ПК-3}$			+	Перекрестный опрос/Контрольный опрос № 4 по темам 7 и 8
Обосновано выбирать стратегию управления рисками информационной безопасности киберфизической системы.	ПК-3.2$_{ПК-3}$			+	Перекрестный опрос/Контрольный опрос № 4 по темам 7 и 8

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

4.1. Текущий контроль успеваемости

8 семестр

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)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №8)

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).

В диплом выставляется оценка за 8 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. А. Д. Фефилов- "Методы и средства защиты информации в сетях", Издательство: "Лаборатория книги", Москва, 2011 - (105 с.) https://biblioclub.ru/index.php?page=book&id=140796.

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. **ЭБС Лань** - https://e.lanbook.com/
2. **База данных Web of Science** - http://webofscience.com/
3. **База данных Scopus** - http://www.scopus.com
4. **Национальная электронная библиотека** - https://rusneb.ru/
5. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php

6. **Портал открытых данных Российской Федерации** - https://data.gov.ru
7. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
8. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
9. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
10. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
11. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com
12. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
13. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
14. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
Учебные аудитории для проведения практических занятий, КР и КП	М-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	М-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	М-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Защита информации в киберфизических системах

(название дисциплины)

8 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 Контрольный опрос № 1 по темам 1 и 2 (Перекрестный опрос)
КМ-2 Контрольный опрос № 2 по темам 3 и 4 (Перекрестный опрос)
КМ-3 Контрольный опрос № 3 по темам 5 и 6 (Перекрестный опрос)
КМ-4 Контрольный опрос № 4 по темам 7 и 8 (Перекрестный опрос)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	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