Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Обязательная**
№ дисциплины по учебному плану:	**Б1.О.05**
Трудоемкость в зачетных единицах:	**3 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**3 семестр - 32 часа;**
Практические занятия	**3 семестр - 48 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**3 семестр - 2 часа;**
Самостоятельная работа	**3 семестр - 97,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Отчет**	
Промежуточная аттестация:	
Экзамен	**3 семестр - 0,5 часа;**

Москва 2023

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Капгер И.В. Идентификатор: R5d33df1e-KapgerIV-059b09ee	И.В. Капгер
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
(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: приобретение необходимых теоретических знаний и практических навыков по созданию и эксплуатации защищенных информационных систем

Задачи дисциплины

- изучение методов анализа защищенности информационных систем;
- освоение способов выбора и настройки программно-аппаратных средств защиты информационных систем;
- приобретение навыков построения и использования инфраструктуры открытых ключей в защищенных информационных системах.

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**
ОПК-1 способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИД-1$_{ОПК-1}$ Самостоятельно осваивает и адаптирует к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты	знать: - каналы распространения вредоносных программ, способы предупреждения заражения вредоносными программами и методы их обнаружения; - угрозы информационной безопасности при подключении информационной системы к глобальной компьютерной сети; - формальные модели, лежащие в основе защищенных информационных систем. уметь: - выбирать методы защиты информации при ее передаче по открытым компьютерным сетям; - проводить анализ информационных систем с точки зрения обеспечения их защищенности; - использовать формальные модели построения защищенных информационных систем; - применять методы и программно-аппаратные средства защиты информационных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Управление информационной безопасностью (далее – ОПОП), направления подготовки 10.04.01 Информационная безопасность, уровень образования: высшее образование - магистратура.

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	Модели и критерии оценки защищенных информационных систем	14	3	4	-	2	-	-	-	-	-	8	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Модели и критерии оценки защищенных информационных систем" подготовка к выполнению заданий на практических занятиях ***Подготовка к контрольной работе:*** Изучение материалов по разделу Модели и критерии оценки защищенных информационных систем и подготовка к контрольной работе ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Модели и критерии оценки защищенных информационных систем" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Модели и
1.1	Определение защищенной информационной системы (ИС), критерии оценки защищенности ИС.	14		4	-	2	-	-	-	-	-	8	-	

														критерии оценки защищенных информационных систем" ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Модели и критерии оценки защищенных информационных систем" ***Изучение материалов литературных источников:*** [1], 1-352 [4], 1-88 [5], 6-40
2	Программно-аппаратные средства защищенных информационных систем	66		14	-	24	-	-	-	-	-	28	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Программно-аппаратные средства защищенных информационных систем"
2.1	Классификация программно-аппаратных средств защиты ИС.	66		14	-	24	-	-	-	-	-	28	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Программно-аппаратные средства защищенных информационных систем" подготовка к выполнению заданий на практических занятиях ***Подготовка к контрольной работе:*** Изучение материалов по разделу Программно-аппаратные средства защищенных информационных систем и подготовка к контрольной работе ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Программно-аппаратные средства защищенных информационных систем" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по

														представленным письменным работам. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Программно-аппаратные средства защищенных информационных систем" ***Изучение материалов литературных источников:*** [3], 50-87
3	Инфраструктура открытых ключей в защищенных информационных системах	64		14	-	22	-	-	-	-	-	28	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Инфраструктура открытых ключей в защищенных информационных системах" ***Подготовка к аудиторным занятиям:***
3.1	Принципы аутентификации на основе модели «рукопожатия»	64		14	-	22	-	-	-	-	-	28	-	Проработка лекции, выполнение и подготовка к защите лаб. работы ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Инфраструктура открытых ключей в защищенных информационных системах" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Инфраструктура открытых ключей в защищенных информационных системах" подготовка к выполнению заданий на практических занятиях ***Подготовка к контрольной работе:*** Изучение материалов по разделу Инфраструктура открытых ключей в защищенных информационных системах и подготовка к контрольной работе ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе

														"Инфраструктура открытых ключей в защищенных информационных системах" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Изучение материалов литературных источников:*** [2], 1-227
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**180.0**		**32**	**-**	**48**	**-**	**2**	**-**	**-**	**0.5**	**64**	**33.5**	
	Итого за семестр	**180.0**		**32**	**-**	**48**	**2**		**-**		**0.5**	**97.5**		

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. Модели и критерии оценки защищенных информационных систем

1.1. Определение защищенной информационной системы (ИС), критерии оценки защищенности ИС.

Методология анализа защищенности ИС. Надежность механизмов защиты ИС. Основные угрозы информационной безопасности при подключении ИС к сети Интернет..

2. Программно-аппаратные средства защищенных информационных систем

2.1. Классификация программно-аппаратных средств защиты ИС.

Принцип работы и классификация межсетевых экранов. Фильтрующие маршрутизаторы. Шлюзы сеансового и прикладного уровня. Настройка и использование межсетевых экранов.Сканеры уязвимостей информационных систем. Системы обнаружения атак. Системы контроля содержимого. Системы защиты от утечек данных (DLP-системы). Примеры DLP-систем. Вредоносные программы, их признаки и классификация. Каналы распространения и предупреждение заражения вредоносными программами. Методы обнаружения и удаления вредоносных программ..

3. Инфраструктура открытых ключей в защищенных информационных системах

3.1. Принципы аутентификации на основе модели «рукопожатия»

Построение системы аутентификации на основе аппаратных и программных генераторов одноразовых паролей. Использование непрямой аутентификации. Использование асимметричной криптографии в системах аутентификации. Управление сертификатами открытых ключей. Структура и разновидности сертификатов. Элементы инфраструктуры открытых ключей (PKI). Архитектура PKI. Отзыв сертификатов, его причины и стратегии. Списки отозванных сертификатов, их структура и виды. Распространение сертификатов и списков отозванных сертификатов. Управление жизненным циклом сертификатов. Способы хранения личных (закрытых) ключей. Управление доступом к устройству с личным ключом. Хранение личных ключей на сервере..

3.3. Темы практических занятий

1. Модели и критерии оценки защищенности информационных систем.;
2. Выполнение практического задания №1 «Межсетевые экраны».;
3. Программно-аппаратные средства защиты информационных систем.;
4. Защита отчета о выполнении практического задания №1.;
5. Методы выбора, настройки и использования межсетевых кранов.;
6. Выполнение практического задания №2 «Сканеры уязвимостей информационных систем.;
7. Анализ защищенности информационных систем с использованием сканеров уязвимостей;
8. Защита отчета о выполнении практического задания №2.;
9. Использование систем защиты от утечек данных в информационных системах.;
10. Выполнение практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ».;
11. Элементы и архитектура удостоверяющих центров в инфраструктуре открытых ключей.;
12. Защита отчета о выполнении практического задания №3.;
13. Управление распространением и жизненным циклом сертификатов открытых ключей в защищенных информационных системах.;

14. Выполнение практического задания №4 «Системы защиты от утечек данных и контроля содержимого.;
15. Способы хранения личных ключей пользователей в инфраструктуре открытых ключей.;
16. Защита отчета о выполнении практического задания №4..

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Модели и критерии оценки защищенных информационных систем"
2. Обсуждение материалов по кейсам раздела "Программно-аппаратные средства защищенных информационных систем"
3. Обсуждение материалов по кейсам раздела "Инфраструктура открытых ключей в защищенных информационных системах"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Модели и критерии оценки защищенных информационных систем"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Программно-аппаратные средства защищенных информационных систем"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Инфраструктура открытых ключей в защищенных информационных 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:					
формальные модели, лежащие в основе защищенных информационных систем	ИД-1$_{ОПК-1}$	+			Отчет/Защита практического задания №2 «Сканеры уязвимостей».Тест №1 «Модели защищенных информационных систем. Выбор программно-аппаратных средств защиты в информационных системах»
угрозы информационной безопасности при подключении информационной системы к глобальной компьютерной сети	ИД-1$_{ОПК-1}$		+		Отчет/Защита практического задания №2 «Сканеры уязвимостей».Тест №1 «Модели защищенных информационных систем. Выбор программно-аппаратных средств защиты в информационных системах»
каналы распространения вредоносных программ, способы предупреждения заражения вредоносными программами и методы их обнаружения	ИД-1$_{ОПК-1}$		+		Отчет/Защита практического задания №4 «Системы защиты от утечек данных и контроля содержимого». Тест №2 «Методы построения и использования инфраструктуры открытых ключей»
Уметь:					
применять методы и программно-аппаратные средства защиты информационных систем	ИД-1$_{ОПК-1}$		+	+	Отчет/Защита практического задания №1 «Межсетевые экраны»
использовать формальные модели построения защищенных информационных систем	ИД-1$_{ОПК-1}$			+	Отчет/Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ»
проводить анализ информационных систем с точки зрения обеспечения их защищенности	ИД-1$_{ОПК-1}$	+	+	+	Отчет/Защита практического задания №4 «Системы защиты от утечек данных и контроля содержимого». Тест №2 «Методы построения и использования инфраструктуры открытых ключей»
выбирать методы защиты информации при ее передаче по открытым компьютерным сетям	ИД-1$_{ОПК-1}$		+	+	Отчет/Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ»

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

4.1. Текущий контроль успеваемости

3 семестр

Форма реализации: Письменная работа

1. Защита практического задания №1 «Межсетевые экраны» (Отчет)
2. Защита практического задания №2 «Сканеры уязвимостей».Тест №1 «Модели защищенных информационных систем. Выбор программно-аппаратных средств защиты в информационных системах» (Отчет)
3. Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ» (Отчет)
4. Защита практического задания №4 «Системы защиты от утечек данных и контроля содержимого». Тест №2 «Методы построения и использования инфраструктуры открытых ключей» (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №3)

В диплом выставляется оценка за 3 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлению "Информационная безопасность" / П. Б. Хорев . – 2-е изд., испр. и доп . – М. : Форум : ИНФРА-М, 2017 . – 352 с. – (Высшее образование) . - ISBN 978-5-00091-004-7 .;
2. Бабаш, А. В. Информационная безопасность. История защиты информации в России / А. В. Бабаш, Е. К. Баранова, Д. А. Ларин . – М. : КДУ, 2013 . – 736 с. - ISBN 978-5-98227-928-6 .;
3. Грушо, А. А. Теоретические основы компьютерной безопасности : учебное пособие для вузов по специальности 090100 "Информационная безопасность" / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина . – М. : АКАДЕМИЯ, 2009 . – 272 с. – (Высшее профессиональное образование) . - ISBN 978-5-7695-4242-8 .;
4. Хорев, П. Б. Криптографические протоколы : учебное пособие по курсу "Криптографические методы защиты информации" по направлению 01.03.02 "Прикладная математика и информатика" / П. Б. Хорев, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ") . – М. : Изд-во МЭИ, 2019 . – 88 с. - ISBN 978-5-7046-2162-1 . http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=10969;
5. Бахаров Л. Е.- "Информационная безопасность и защита информации (разделы криптография и стеганография)", Издательство: "МИСИС", Москва, 2019 - (59 с.) https://e.lanbook.com/book/116907.

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 Росфинмониторинга** - http://www.fedsfm.ru/opendata
9. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com
10. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
11. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
12. **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-301, Учебная аудитория	стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска маркерная, кондиционер
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для	НТБ-303,	стол компьютерный, стул, стол

самостоятельной работы	Компьютерный читальный зал	письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	К-301, Учебная аудитория	стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска маркерная, кондиционер
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

Защищенные информационные системы

(название дисциплины)

3 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:

КМ-1 Защита практического задания №1 «Межсетевые экраны» (Отчет)

КМ-2 Защита практического задания №2 «Сканеры уязвимостей».Тест №1 «Модели защищенных информационных систем. Выбор программно-аппаратных средств защиты в информационных системах» (Отчет)

КМ-3 Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ» (Отчет)

КМ-4 Защита практического задания №4 «Системы защиты от утечек данных и контроля содержимого». Тест №2 «Методы построения и использования инфраструктуры открытых ключей» (Отчет)

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	Модели и критерии оценки защищенных информационных систем					
1.1	Определение защищенной информационной системы (ИС), критерии оценки защищенности ИС.			+		+
2	Программно-аппаратные средства защищенных информационных систем					
2.1	Классификация программно-аппаратных средств защиты ИС.		+	+	+	+
3	Инфраструктура открытых ключей в защищенных информационных системах					
3.1	Принципы аутентификации на основе модели «рукопожатия»		+		+	+
		Вес КМ, %:	20	25	20	35