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
МАТЕМАТИЧЕСКИЕ МОДЕЛИ РИСКОВ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.05.02.01**
Трудоемкость в зачетных единицах:	**2 семестр - 3;**
Часов (всего) по учебному плану:	**108 часов**
Лекции	**2 семестр - 16 часов;**
Практические занятия	**2 семестр - 32 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**2 семестр - 59,7 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Отчет** **Деловая игра**	
Промежуточная аттестация:	
Зачет с оценкой	**2 семестр - 0,3 часа;**

Москва 2021

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
(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: освоение профессиональных компетенций по моделированию угроз, оценке и анализу рисков информационной безопасности с использованием различных современных методик управления рисками информационной безопасности

Задачи дисциплины

- изучение ключевых понятий "неопределенность" и "риск", различных аспектов усиления неопределенности и полезности риска в современных условиях хозяйствования;
- изучение критериев классификации рисков и видов рисков в соответствии с выделенными критериями;;
- изучение теоретических основ исследования рисков;
- изучение традиционных и современных методов исследования рисков, методов количественной оценки рисков;
- ознакомление с основными аксиомами и элементами современной теорией рисков и существующими концепциями риска;
- практическое изучение порядка проведения исследования рисков информационной безопасности;
- практическое изучение порядка определения ценности информации и критериев выбора в рисковых ситуациях и принятия управленческих решений, а также методы моделирования этих рисковых ситуаций и обоснования решений.

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-1 Оценивание уровня безопасности компьютерных систем и сетей	ПК-1.З$_{ПК-1}$ Проводит анализ безопасности компьютерных систем	знать: - фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества; - угрозы информационной безопасности объектов. уметь: - анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества; - проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента.

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 3 зачетных единицы, 108 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	Моделирование угроз информационной безопасности	24	2	8	-	8	-	-	-	-	-	8	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Моделирование угроз информационной безопасности" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к деловой игры ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Моделирование угроз информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Моделирование угроз информационной безопасности" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Моделирование угроз информационной
1.1	Термины и определения: угроза, риск, моделирование угроз, оценка, оценивание и анализ рисков.	12		4	-	4	-	-	-	-	-	4	-	
1.2	Моделирование угроз информационной безопасности.	12		4	-	4	-	-	-	-	-	4	-	

														безопасности" ***Изучение материалов литературных источников:*** [2], 1-84
2	Управление рисками информационной безопасности	66		8	-	24	-	-	-	-	-	34	-	***Изучение материалов литературных источников:*** [1], 1-106 [3], 5-25
2.1	Управление рисками в концепции стандарта NIST.	11		1	-	4	-	-	-	-	-	6	-	
2.2	Управление рисками в концепции стандарта BS 7799-3.	11		1	-	4	-	-	-	-	-	6	-	
2.3	Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005.	12		2	-	4	-	-	-	-	-	6	-	
2.4	Многофакторные модели рисков.	16		2	-	6	-	-	-	-	-	8	-	
2.5	Моделирование рисков информационной безопасности на примере модели филиала АКБ.	16		2	-	6	-	-	-	-	-	8	-	
	Зачет с оценкой	18.0		-	-	-	-	-	-	-	0.3	-	17.7	
	Всего за семестр	**108.0**		**16**	**-**	**32**	**-**	**-**	**-**	**-**	**0.3**	**42**	**17.7**	
	Итого за семестр	**108.0**		**16**	**-**	**32**	**-**		**-**		**0.3**	**59.7**		

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. Моделирование угроз информационной безопасности

1.1. Термины и определения: угроза, риск, моделирование угроз, оценка, оценивание и анализ рисков.

Цели и задачи курса. Структура дисциплины и требования к результатам изучения курса. История развития методик управления рисками в различных концепциях создания систем информационной безопасности..

1.2. Моделирование угроз информационной безопасности.

Цели и задачи моделирования угроз информационной безопасности. Различные подходы к формализованному описанию угроз информационной безопасности. Базовая модель угроз: достоинства и недостатки. Современные подходы к моделированию угроз на основе вербального (описательного), параметрического и когнитивного моделирования. Достоинства и недостатки этих подходов к моделированию угроз..

2. Управление рисками информационной безопасности

2.1. Управление рисками в концепции стандарта NIST.

Концепция управления рисками в стандарте США NIST 800-30 «Руководство по управлению информационными рисками ИТ-систем». Девять этапов методологии оценки рисков: характеристика системы, идентификация угроз, идентификация уязвимостей, анализ мероприятий защиты, определение вероятностей использования уязвимостей, анализ воздействия, определение рисков, рекомендации по мероприятиям защиты, разработка итоговых документов..

2.2. Управление рисками в концепции стандарта BS 7799-3.

Концепция управления рисками в британском стандарте BS-7799-3. Четыре фазы управления рисками: оценка рисков, включающая анализ и вычисление рисков; обработка риска — выбор и реализация мер и средств безопасности; контроль рисков путем мониторинга, тестирования, анализа механизмов безопасности, а также аудита системы; оптимизация рисков путем модификации и обновления правил, мер и средств безопасности. Достоинства и недостатки стандарта. Другие концепции управления рисками: COBIT, CORBA и др..

2.3. Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005.

Назначение стандарта. Область действия стандарта и его применимость. Основные этапы процесса менеджмента риска информационной безопасности: установление контекста, оценка риска, обработка риска, принятие риска, коммуникация риска, мониторинг и переоценка риска информационной безопасности. Особенности стандарта и процессный подход к оценке рисков. Сущность и содержание процессного подхода к оценке рисков. Достоинства и недостатки стандарта. Возможные направления его развития..

2.4. Многофакторные модели рисков.

Концепция многофакторных моделей рисков, позволяющая учитывать кроме основных и дополнительные факторы, а также соотношения между ними. Понятие «стратегия управления» рисками. Методика анализа рисков с использованием многофакторных 5 моделей. Задачи, решаемые с использованием многофакторных моделей управления рисками. Имитационное моделирование на основе многофакторных моделей. Основные этапы процесса менеджмента риска информационной безопасности: установление контекста,

оценка риска, обработка риска, принятие риска, коммуникация риска, мониторинг и переоценка риска информационной безопасности. Оценка погрешностей моделирования. Методика анализа рисков с использованием многофакторных моделей. Имитационное моделирование на основе многофакторных моделей. Оценка погрешностей моделирования..

2.5. Моделирование рисков информационной безопасности на примере модели филиала АКБ.

Постановка деловой игры. Анализ исходных данных и результатов аудита информационной безопасности. Анализ бизнес-процессов модели хозяйствующего субъекта. Классификация и оценка ценности информационных активов организации. Моделирование угроз информационной безопасности. Оценка и моделирование рисков при различных стратегиях управления ими. Разработка плана управления рисками. Обоснование предлагаемых решений управления рисками..

3.3. Темы практических занятий

1. 1.Анализ различных подходов к формализованному описанию угроз информационной безопасности;
2. 2.Порядок разработки методики моделирования угроз в стандарте IDEF0;
3. 3.Моделирование рисков информационной безопасности на примере модели филиала АКБ;
4. 4.Анализ исходных данных и результатов аудита информационной безопасности;
5. 5.Разработка плана управления рисками.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Моделирование угроз информационной безопасности"
2. Обсуждение материалов по кейсам раздела "Управление рисками информационной безопасности"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Моделирование угроз информационной безопасности"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Управление рисками информационной безопасности"

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	
Знать:				
угрозы информационной безопасности объектов	ПК-1.З$_{ПК-1}$	+		Отчет/Коллоквиум 1 Отчет/Коллоквиум 2
фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	ПК-1.З$_{ПК-1}$		+	Деловая игра/Контрольное задание 1. Контрольное задание 2 Деловая игра/Контрольное задание 3
Уметь:				
проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента	ПК-1.З$_{ПК-1}$		+	Отчет/Коллоквиум 2 Деловая игра/Контрольное задание 1. Контрольное задание 2 Деловая игра/Контрольное задание 3
анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	ПК-1.З$_{ПК-1}$	+		Отчет/Коллоквиум 1

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

4.1. Текущий контроль успеваемости

2 семестр

Форма реализации: Проверка задания

1. Коллоквиум 1 (Отчет)
2. Коллоквиум 2 (Отчет)
3. Контрольное задание 1. Контрольное задание 2 (Деловая игра)
4. Контрольное задание 3 (Деловая игра)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №2)

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и зачетной / экзаменационной составляющих.

В диплом выставляется оценка за 2 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Управление событиями информационной безопасности : учебное пособие / А. С. Минзов, О. Р. Баронов, С. А. Минзов, П. А. Осипов, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ" ; ред. А. Ю. Невский . – Москва : ВНИИгеосистем, 2020 . – 110 с. - Для студентов бакалавриата, магистратуры, аспирантов и преподавателей, занимающихся вопросами создания эффективных систем управления кибербезопасностью . - ISBN 978-5-8481-0244-4 .;
2. Минзов, А. С. Методология применения терминов и определений в сфере информационной, экономической и комплексной безопасности бизнеса : учебно-методическое пособие / А. С. Минзов, Л. М. Кунбутаев, Нац. исслед. ун-т "МЭИ", Ин-т безопасности бизнеса МЭИ (ТУ) . – М. : ВНИИгеосистем, 2011 . – 84 с. - ISBN 978-5-8481-0083-9 .;
3. Нестеров С. А.- "Анализ и управление рисками в информационных системах на базе операционных систем Microsoft", (2-е изд.), Издательство: "ИНТУИТ", Москва, 2016 - (250 с.)
https://e.lanbook.com/book/100566.

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. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных Web of Science** - http://webofscience.com/
5. **База данных Scopus** - http://www.scopus.com
6. **Национальная электронная библиотека** - https://rusneb.ru/
7. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
8. **База данных диссертаций ProQuest Dissertations and Theses Global** - https://search.proquest.com/pqdtglobal/index
9. **Журнал Science** - https://www.sciencemag.org/
10. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
11. **Портал открытых данных Российской Федерации** - https://data.gov.ru
12. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
13. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
14. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
15. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
16. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com
17. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
18. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
19. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
20. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru
21. **Официальный сайт Министерства науки и высшего образования Российской Федерации** - https://minobrnauki.gov.ru
22. **Официальный сайт Федеральной службы по надзору в сфере образования и науки** - https://obrnadzor
23. **Федеральный портал "Российское образование"** - http://www.edu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	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	М-508, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая

промежуточной аттестации	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
	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	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

Математические модели рисков

(название дисциплины)

2 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:
КМ-1 Коллоквиум 1 (Отчет)
КМ-2 Коллоквиум 2 (Отчет)
КМ-3 Контрольное задание 1. Контрольное задание 2 (Деловая игра)
КМ-4 Контрольное задание 3 (Деловая игра)

Вид промежуточной аттестации – Зачет с оценкой.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Моделирование угроз информационной безопасности					
1.1	Термины и определения: угроза, риск, моделирование угроз, оценка, оценивание и анализ рисков.		+	+		
1.2	Моделирование угроз информационной безопасности.		+	+		
2	Управление рисками информационной безопасности					
2.1	Управление рисками в концепции стандарта NIST.			+	+	+
2.2	Управление рисками в концепции стандарта BS 7799-3.			+	+	+
2.3	Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005.			+	+	+
2.4	Многофакторные модели рисков.			+	+	+
2.5	Моделирование рисков информационной безопасности на примере модели филиала АКБ.			+	+	+
Вес КМ, %:			25	25	25	25