

**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

**Оценочные материалы
по дисциплине
Математические модели рисков**

**Москва
2024**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Минзов А.С.
	Идентификатор	R17801759-MinzovAS-e8de8907

А.С. Минзов

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

Заведующий
выпускающей кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

А.Ю.
Невский

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. РПК-1 Способен активно участвовать в управлении функционированием системы обеспечения информационной безопасности (СОИБ) организации на основе современных положений СМИБ

ИД-2 Проводит анализ безопасности компьютерных систем

и включает:

для текущего контроля успеваемости:

Форма реализации: Защита задания

1. Коллоквиум № 1 Контрольное задание № 1 (Коллоквиум)
2. Коллоквиум №2 (Коллоквиум)

Форма реализации: Компьютерное задание

1. Контрольная задание №3 (Деловая игра)

Форма реализации: Письменная работа

1. Контрольная задание №2 (Контрольная работа)

БРС дисциплины

2 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Коллоквиум № 1 Контрольное задание № 1 (Коллоквиум)

КМ-2 Коллоквиум №2 (Коллоквиум)

КМ-3 Контрольная задание №2 (Контрольная работа)

КМ-4 Контрольная задание №3 (Деловая игра)

Вид промежуточной аттестации – Зачет с оценкой.

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Моделирование угроз информационной безопасности					
Термины и определения: угроза, риск, моделирование угроз, оценка, оценивание и анализ рисков		+	+	+	+

Управление рисками информационной безопасности				
Управление рисками в концепции стандарта	+	+	+	+
Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005	+	+	+	+
Многофакторные модели рисков	+	+	+	+
Вес КМ:	25	25	25	25

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
РПК-1	ИД-2 _{РПК-1} Проводит анализ безопасности компьютерных систем	Знать: фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества угрозы информационной безопасности объектов Уметь: проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента анализировать фундаментальные и прикладные проблемы информационной	КМ-1 Коллоквиум № 1 Контрольное задание № 1 (Коллоквиум) КМ-2 Коллоквиум №2 (Коллоквиум) КМ-3 Контрольная задание №2 (Контрольная работа) КМ-4 Контрольная задание №3 (Деловая игра)

		безопасности в условиях становления современного информационного общества	
--	--	--	--

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Коллоквиум № 1 Контрольное задание № 1

Формы реализации: Защита задания

Тип контрольного мероприятия: Коллоквиум

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Занятие проводится в форме дискуссионного обсуждения.

Краткое содержание задания:

Обсуждение вопросов по заданной тематике

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: угрозы информационной безопасности объектов	1.Цели внедрения СМИБ
Знать: фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	1.Процессный подход к СМИБ 2.Цикл Деминга (почему используется этот подход к управлению)
Уметь: анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	1.Критические факторы успешного внедрения СМИБ
Уметь: проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента	1.Принципы внедрения СМИБ

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-2. Коллоквиум №2

Формы реализации: Защита задания

Тип контрольного мероприятия: Коллоквиум

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Занятие проводится в форме дискуссионного обсуждения.

Краткое содержание задания:

Обсуждение вопросов по заданной тематике

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: угрозы информационной безопасности объектов	1. Обработка риска 2. Коммуникация риска
Знать: фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	1. Оценка риска
Уметь: анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	1. Сравнение риска
Уметь: проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента	1. Критерии риска

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-3. Контрольная задание №2

Формы реализации: Письменная работа

Тип контрольного мероприятия: Контрольная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Необходимо дать полные ответы на вопросы или раскрыть содержание терминов (ответить на 3 вопроса или термина).

Краткое содержание задания:

Ответить на вопросы или раскрыть содержание терминов

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: угрозы информационной безопасности объектов	1.Как определять угрозы при известных уязвимостях и ценностях активов?
Знать: фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	1.Модель взаимосвязанных угроз: ограничения и возможности 2.Параметрическая комплексная модель угроз
Уметь: анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	1.Как описываются угрозы в государственных информационных системах? 2.Почему умышленные угрозы связаны с уязвимостями активов и их ценностью?
Уметь: проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента	1.Модель взаимосвязанных угроз: ограничения и возможности

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто, выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-4. Контрольная задание №3

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Деловая игра

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Деловая ситуация выполняется в форме отдельных функционально завершенных работ, выполняемых в определенной последовательности. Содержание этих работ определяется концепцией создаваемой системой защиты информации. В нашем случае была использована модель защиты на основе требований стандарта ГОСТ ИСО/МЭК 27001-2012 г. По каждому этапу результаты работы

представляются в форме таблиц, графиков и диаграмм. В результате их анализа делаются выводы, позволяющие обратить внимание на основные и наиболее важные для последующих работ значения анализируемых показателей.

Краткое содержание задания:

Моделирование рисков информационной безопасности

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: угрозы информационной безопасности объектов	1.Как распределяются угрозы по уязвимости активов и их ценности? 2.Как распределяются риски по вариантам обработки и ценности активов?
Знать: фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	1.Как распределяется ответственность персонала по активам?
Уметь: анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	1.Как распределяются риски по степени влияния на бизнес-процессы?
Уметь: проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента	1.Как распределяются активы по ценности? 2.Как распределяются угрозы по вероятности и возможному ущербу?

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2 семестр

Форма промежуточной аттестации: Зачет с оценкой

Процедура проведения

Зачет проводится в устной форме по билетам согласно программе зачета

1. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-2_{РПК-1} Проводит анализ безопасности компьютерных систем

Вопросы, задания

1. Применение методик моделирования угроз на примере модели хозяйствующего субъекта
2. Разработка методики моделирования угроз в стандарте IDEF0
3. Разработка методики управления рисками NIST в стандарте IDEF0
4. Разработка методики управления рисками BS 7799 в стандарте IDEF0
5. Разработка методики управления рисками по ГОСТ 27005 в стандарте IDEF0
6. Разработка методики управления рисками многофакторных моделей в стандарте IDEF0
7. Разработка пяти этапов управления рисками на модели хозяйствующего субъекта с методиками, шаблонами и примерами выполнения в электронном виде
8. Моделирование рисков информационной безопасности на примере модели филиала АКБ
9. Анализ исходных данных и результатов аудита информационной безопасности
10. Анализ бизнес-процессов модели хозяйствующего субъекта
11. Разработка плана управления рисками
12. Обоснование предлагаемых решений управления рисками

Материалы для проверки остаточных знаний

1. Управление риском – это:
Ответы:
а. отказ от рискованного проекта;
б. комплекс мер, направленных на снижение вероятности реализации риска;
в. комплекс мер, направленных на компенсацию, снижение, перенесение, принятие риска или уход от него.
Верный ответ: в
2. Риск – это:
Ответы:
а. неблагоприятное событие, влекущее за собой убыток;
б. все предпосылки, могущие негативно повлиять на достижение стратегических целей в течение строго определенного временного промежутка;
в. вероятность провала программы продаж.
Верный ответ: б
3. Что их перечисленного не относится к видам производственных рисков?
Ответы:
а. изменение конъюнктуры рынка
б. усиление конкуренции
в. форс-мажор

г. амортизация производственного оборудования

Верный ответ: г

4. Методы управления рисками, предполагающие исключение рисков ситуации из бизнеса, носят название:

Ответы:

- а. методы диссипации риска
- б. методы компенсации риска
- в. методы уклонения от риска
- г. методы локализации риска

Верный ответ: в

II. Описание шкалы оценивания

Оценка: 5 («отлично»)

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 («хорошо»)

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 («удовлетворительно»)

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

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

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».