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: Организация и технология защиты информации

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Математические модели рисков

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

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: 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)

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. ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач

2. ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

и включает:

для текущего контроля успеваемости:

Форма реализации: Смешанная форма

1. Деловая игра (Деловая игра)
2. Практическое задание 1 (Семинар)
3. Практическое задание 2 (Семинар)
4. Практическое задание 3 (Семинар)
5. Практическое задание 4 (Семинар)
6. Практическое задание 5 (Семинар)
7. Практическое задание 6 (Семинар)

БРС дисциплины

5 семестр

Раздел дисциплины	Веса контрольных мероприятий, %						
	Индекс КМ:	КМ-1	КМ-1	КМ-2	КМ-2	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	4	8	8	8	12	15
Термины и определения. Цели и задачи курса. Моделирование угроз информационной безопасности							
Введение. Термины и определения. Цели и задачи курса. Структура дисциплины и требования к результатам изучения курса	+	+					
Моделирование угроз информационной безопасности	+	+					
Управление рисками в концепциях отечественных и зарубежных стандартов							
Управление рисками в концепции стандарта NIST			+	+	+		
Управление рисками в концепции стандарта BS 7799-3			+	+	+		

Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005			+	+	+		
Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005. Многофакторные модели рисков							
Многофакторные модели рисков						+	
Моделирование рисков информационной безопасности на примере модели филиала АКБ							
Моделирование рисков информационной безопасности на примере модели филиала АКБ							+
Вес КМ:	10	10	10	10	10	20	30

$Общая часть/Для промежуточной аттестации$

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
ОПК-2	ОПК-2(Компетенция)	Знать: требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины основы анализа и синтеза систем информационной безопасности на основе отдельных подсистем и структурных элементов Уметь: выполнять работы по компьютерному моделированию и проектированию отдельных элементов систем информационной безопасности на основе управления рисками	Практическое задание 1 (Семинар) Практическое задание 2 (Семинар) Практическое задание 3 (Семинар) Практическое задание 4 (Семинар) Практическое задание 5 (Семинар) Практическое задание 6 (Семинар)
ПК-10	ПК-10(Компетенция)	Уметь: проводить анализ информационной безопасности объектов и систем с использованием	Деловая игра (Деловая игра)

		отечественных и зарубежных стандартов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Практическое задание 2

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Условия проведения: Учебная группа. Продолжительность: 2 учебных часа. Используемые технические и программные средства: Компьютер с ОС Windows. Встроенное программное обеспечение

Краткое содержание задания:
На основе методических документов ФСТЭК и стандартов ГОСТ Р ИСО/МЭК 27000+ изучить рекомендованные подходы к формализованному описанию угроз информационной безопасности в стандарте IDEF0.

Контрольные вопросы/задания:

Знать: основы анализа и синтеза систем информационной безопасности на основе отдельных подсистем и структурных элементов	1.Какие требования к моделированию угроз предъявляются в методических документах ФСТЭК? 2.Какие требования к моделированию угроз предъявляются в стандартах ГОСТ Р ИСО/МЭК 27000+?

Описание шкалы оценивания:

Оценка: 5
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
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
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-1. Практическое задание 1

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Условия проведения: Учебная группа. Продолжительность: 2 учебных часа. Используемые технические и программные средства: Компьютер с ОС Windows. Встроенное программное обеспечение

Краткое содержание задания:
Дать определение термина, и пояснить механизмы его реализации по варианту, соответствующему номеру в списке группы. Каждому студенту необходимо дать

определение по 5 терминам. Результаты оформляются в виде отчета по заданию в формате .doc, включающему титульный лист (наименование университета, института, кафедры), номер и наименование задания, фамилия имя и отчество студента. Следующие листы включают ответы на 5 вопросов. При анализе уделить внимание тем терминам, которые в разных стандартах сформулированы по-разному. На занятии быть готовым изложить содержание своей работы.

Контрольные вопросы/задания:

Знать: основы анализа и синтеза систем информационной безопасности на основе отдельных подсистем и структурных элементов	1.Перечислите содержание основных терминов, используемых для описания основ анализа систем информационной безопасности 2.Раскройте дефиниции основных терминов, используемых для описания основ анализа систем информационной безопасности

Описание шкалы оценивания:

Оценка: 5
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
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
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-2. Практическое задание 5

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Условия проведения: Учебная группа. Продолжительность: 2 учебных часа. Используемые технические и программные средства: Компьютер с ОС Windows. Встроенное программное обеспечение

Краткое содержание задания:
Провести моделирование процессов СМИБ по стандарту ГОСТ Р ИСО/МЭК 27005. Форма моделирования выбирается из варианта задания. Все подпроцессы должны быть с необходимыми пояснениями для работы.

Контрольные вопросы/задания:

Знать: требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины	1.Какие требования к моделям управления рисками информационной безопасности предъявляются в стандарте ГОСТ Р ИСО/МЭК 27005? 2.Какие методики оценки рисков предлагаются в стандарте ГОСТ Р ИСО/МЭК 27005?

Описание шкалы оценивания:

Оценка: 5
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
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
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-2. Практическое задание 4

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Условия проведения: Учебная группа. Продолжительность: 2 учебных часа. Используемые технические и программные средства: Компьютер с ОС Windows. Встроенное программное обеспечение

Краткое содержание задания:
Разработать методику управления рисками BS 7799. Форма представления методики выбирается из варианта задания. Все подпроцессы должны быть с необходимыми пояснениями для работы.

Контрольные вопросы/задания:

Знать: требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины	1.Какие требования к моделям управления рисками информационной безопасности предъявляются в британском стандарте BS-7799-3? 2.Какие этапы методологии оценки рисков существуют в британском стандарте BS-7799-3?

Описание шкалы оценивания:

Оценка: 5
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
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
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-2. Практическое задание 3

Формы реализации: Смешанная форма

Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Условия проведения: Учебная группа. Продолжительность: 2 учебных часа. Используемые технические и программные средства: Компьютер с ОС Windows. Встроенное программное обеспечение

Краткое содержание задания:
Разработать методику управления рисками NIST. Форма представления методики выбирается из варианта задания. Все подпроцессы должны быть с необходимыми пояснениями для работы.

Контрольные вопросы/задания:

Знать: требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины	1.Какие требования к моделям управления рисками информационной безопасности предъявляются в стандарте США NIST 800-30? 2.Какие этапы методологии оценки рисков существуют в стандарте США NIST 800-30?

Описание шкалы оценивания:

Оценка: 5
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
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
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-3. Практическое задание 6

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Условия проведения: Учебная группа. Продолжительность: 2 учебных часа. Используемые технические и программные средства: Компьютер с ОС Windows. Встроенное программное обеспечение

Краткое содержание задания:
Провести моделирование процессов СМИБ по многофакторным моделям. Форма моделирования выбирается из варианта задания. Все подпроцессы должны быть с необходимыми пояснениями для работы

Контрольные вопросы/задания:

Уметь: выполнять работы по компьютерному моделированию и проектированию отдельных элементов систем	1.Представьте вариант моделирования отдельных элементов информационной безопасности на основе моделирования рисков предложенного объекта 2.Представьте вариант проектирования отдельных

информационной безопасности на основе управления рисками	элементов информационной безопасности на основе моделирования рисков предложенного объекта

Описание шкалы оценивания:

Оценка: 5
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
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
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-4. Деловая игра

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Деловая игра
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Условия проведения: Учебная группа: 1 человек. Продолжительность: 20 учебных часов. Используемые технические и программные средства: Компьютер с ОС Windows. Встроенное программное обеспечение

Краткое содержание задания:
Деловая ситуация выполняется в форме отдельных функционально завершенных работ в определенной последовательности. Содержание этих работ определяется концепцией создаваемой системой защиты информации для АКБ *«X-trim Bank».*Для АКБ была использована модель защиты на основе требований стандарта ГОСТ ИСО/МЭК 27001-2006 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.
Для защиты необходимо выполнить все этапы по настоящему заданию и подготовить презентацию.

Контрольные вопросы/задания:

Уметь: проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью	1.Проведите анализ информационной безопасности рассматриваемого объектов с использованием отечественных и зарубежных стандартов, предложите две меры по совершенствованию системы управления информационной безопасностью объекта 2.Проведите моделирование предложенных отдельных элементов систем информационной безопасности рассматриваемого объекта на основе управления рисками 3.Выделите цель управления информационной безопасностью предложенного объекта 4.Проведите анализ информационной безопасности

	предложенного объекта с использованием отечественных и зарубежных стандартов

Описание шкалы оценивания:

Оценка: 5
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
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
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5 семестр

Форма промежуточной аттестации: Зачет с оценкой

Пример билета

НИУ МЭИ	**БИЛЕТ № 1** Кафедра *Безопасности и информационных технологий* Дисциплина «Математические модели рисков»	*Утверждаю:* *Зав. каф. БИТ* *А.Ю.Невский* Протокол № от 20__ года
1. В какой последовательности проводится оценка риска? 2. Методика анализа рисков с использованием многофакторных моделей. Профессор, д.т.н. А.Минзов		

Процедура проведения

Зачёт проводится в письменной форме по билетам согласно программе зачёта

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

1. Компетенция/Индикатор: ОПК-2(Компетенция)

Вопросы, задания

1.Риск: определение, параметры для его определения и описания.
2.Угроза: определение, параметры угрозы.
3.Уязвимость: определение, параметры представления.
4.Цели и задачи моделирования угроз информационной безопасности.
5.Различные подходы к формализованному описанию угроз информационной безопасности.
6.Базовая модель угроз ФСТЭК: достоинства и недостатки.
7.Современные подходы к моделированию угроз на основе вербального (описательного), параметрического и когнитивного моделирования: достоинства и недостатки.
8.Агрегат риска: назначение, как вычисляется в стандарте США NIST 800-30.
9.Девять этапов методологии оценки рисков в стандарте США NIST 800-30.
10.Агрегат риска: назначение, как вычисляется в британском стандарте BS-7799-3.
11.Четыре фазы управления рисками в британском стандарте BS-7799-3.
12.Концепции управления рисками: COBIT, CORBA и др.
13.Актив: параметры описания в ГОСТ 27005.
14.Концепция многофакторных моделей рисков, позволяющая учитывать кроме основных и дополнительные факторы, а также соотношения между ними.
15.Понятие «стратегия управления» рисками.
16.Методика анализа рисков с использованием многофакторных моделей.
17.Поясните процесс «коммуникация риска».
18.Поясните процесс «мониторинг риска».
19.Что представляет собой план осведомленности риска.
20.Какие вы знаете базы данных угроз?

21.Агрегат риска: назначение, форма представления и как вычисляется.

Материалы для проверки остаточных знаний

1.С какой целью проводится управление производительностью информационных систем?

Ответы:

a прогнозирования производительности оборудования исходя будущих целей обработки информации

b оптимизация производительности информационных систем

c разработки требований к производительности оборудования по обработки информации

Верный ответ: ac

2. Компетенция/Индикатор: ПК-10(Компетенция)

Вопросы, задания

1.В какой последовательности проводится оценка риска?

2.Как выбирается способ обработки рисков в стандарте США NIST 800-30?

3.Как выбирается способ обработки рисков в британском стандарте BS-7799-3?

4.Для чего выполняется процесс «установление контекста» по стандарту ГОСТ 27005?

5.Для чего предусмотрен возврат на «установление контекста» после процесса «оценка риска» по стандарту ГОСТ 27005?

6.Для чего предусмотрен возврат на «установление контекста» после процесса «обработка риска» по стандарту ГОСТ 27005?

7.Какие задачи решаются решаемые с использованием многофакторных моделей управления рисками?

8.Как проводится имитационное моделирование на основе многофакторных моделей?

9.Как проводится оценка погрешностей моделирования?

10.Чем заканчивается обработка риска?

11.Для чего разрабатывается положение о применимости?

12.Проводится ли полная обработка рисков повторно при возврате на контекст риска после первой и второй точкой принятия решений?

13.В каких единицах измеряются риски?

14.Какие вы знаете базы данных уязвимостей?

15.Почему нет баз данных рисков?

16.Что нам дает процесс моделирования рисков?

17.Как создается перечень мер и средств контроля и управления?

18.Почему измерения параметров риска проводятся в форме принадлежности к классам?

19.Опишите коротко схему обработки рисков.

Материалы для проверки остаточных знаний

1.Решение каких вопросов включает резервирование?

Ответы:

a необходимо определить количество копий, формы их хранения и обновления;

b шифрование копий;

c тестирование копий;

d обеспечение физической защиты;

t централизованное хранение;

f объем (т.е. полное или выборочное резервирование) и частота резервирования должны отражать требования бизнеса организации, требования к безопасности затрагиваемой информации и критичность информации для непрерывной работы организации;

g аудит резервных копий

Верный ответ: abcdf

2.Чем не обеспечивается безопасность при использовании мобильных программ?

Ответы:

a логически изолированной средой;

b блокированием любого несанкционированного использования мобильной программы;

c не блокированием приема мобильной программы;

d обеспечением уверенности в отсутствии мобильной программы;

e контроле ресурсов доступных мобильной программе;

f применением криптографических мер и средств контроля и управления для однозначной аутентификации мобильной программы.

Верный ответ: cd

II. Описание шкалы оценивания

Оценка: 5

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

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

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

III. Правила выставления итоговой оценки по курсу

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