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
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: 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)

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. ПК-1 Оценивание уровня безопасности компьютерных систем и сетей
   ПК-1.3 Проводит анализ безопасности компьютерных систем

и включает:

для текущего контроля успеваемости:

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)

БРС дисциплины

2 семестр

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.		+	+		
Моделирование угроз информационной безопасности.		+	+		
Управление рисками информационной безопасности					
Управление рисками в концепции стандарта NIST.			+	+	+
Управление рисками в концепции стандарта BS 7799-3.			+	+	+
Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005.			+	+	+
Многофакторные модели рисков.			+	+	+
Моделирование рисков информационной безопасности на примере модели филиала АКБ.			+	+	+
	Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

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
ПК-1	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,	Коллоквиум 1 (Отчет) Коллоквиум 2 (Отчет) Контрольное задание 1. Контрольное задание 2 (Деловая игра) Контрольное задание 3 (Деловая игра)

		технических и программных средств обработки результатов эксперимента	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Коллоквиум 1

Формы реализации: Проверка задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Задания 1 для индивидуального выполнения. Условия проведения Учебная группа. Используемые технические и программные средства: Компьютер с ОС Linux, Windows. Встроенное программное обеспечение

Краткое содержание задания:

Коллоквиум 1. Анализ различных подходов к формализованному описанию угроз информационной безопасности
Цель задания: На основе методических документов ФСТЭК и стандартов ГОСТ Р ИСО/МЭК 27000+ изучить рекомендованные подходы к формализованному описанию угроз информационной безопасности.
Пример задания.
1) Формализованное описание угроз ИСПДн в концепции ФСТЭК.
2) Классификация угроз по среде их возникновения в руководящих документах ФСТЭК.

Контрольное задание 1. Деловая игра. Моделирование рисков информационной безопасности на примере модели филиала АКБ.
Пример задания: При выполнении этого этапа определить сначала цель (цели) управления рисками, а затем исходя из этого, определить основные критерии, области и границы применения и методики обработки рисков.
1. Определить цели управления рисками.
2. Определить основные критерии оценки рисков.
Активы для каждого студента определяются по вариантам.
Вариант 1:
1. Предлагаемые активы:
1) Банковский платежный технологический процесс, включающий все виды платежей в бумажной и электронной формах. Выполняется в расчетно-кассовом отделении (относится к банковской тайне).
2) Банковский технологический процесс по обслуживанию физических лиц (депозиты, кредиты).
9) Банковское делопроизводство (внешнее и внутреннее) включает обычную почту, внутреннюю и внешнюю электронную почту для сотрудников в соответствии с их должностными полномочиями. Ответственный – заместитель управляющего банка.
20) Антивирусное ПО (инсталляции и установленное ПО).
24) Система видеонаблюдения (видеокамеры и регистраторы).
32) Информационные базы и информационные архивы, являющиеся результатом финансовой, экономической и управленческой деятельности банка (в бумажном и электронном формах). Имеют статус «банковская тайна», размещаются в кабинете управляющего банком.
34) Сертификаты, лицензии и другие документы, сгенерированные банком самостоятельно и полученные им для использования от других организаций (например ЦБ и пр.). Размещаются в кабинете управляющего банка в сейфе.

40) В кабинете управляющего банка проводятся совещания, которые могут содержать конфиденциальную информацию – банковскую и коммерческую тайну.

Контрольные вопросы/задания:

Знать: угрозы информационной безопасности объектов	1.Какие фундаментальные проблемы для информационной безопасности существуют в условиях становления современного информационного общества? 2.Какие прикладные проблемы для информационной безопасности существуют в условиях становления современного информационного общества?
Уметь: анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	1.Как проводить экспериментальные исследования защищенности объектов с применением современных математических методов? 2.Как проводить экспериментальные исследования защищенности объектов с применением современных технических и программных средств обработки результатов эксперимента?

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. Коллоквиум 2

Формы реализации: Проверка задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Коллоквиум 2 для индивидуального выполнения. Условия проведения Учебная группа. Используемые технические и программные средства: Компьютер с ОС Linux, Windows. Встроенное программное обеспечение

Краткое содержание задания:
Коллоквиум 2. Порядок разработки методики моделирования угроз в стандарте IDEF0.
Цель задания: Провести моделирование процессов СМИБ по стандарту ГОСТ Р ИСО/МЭК 27001-2006. Форма моделирования выбирается из варианта задания. Все подпроцессы должны быть с необходимыми пояснениями для работы.
Пример задания:
Вариант 1:

1) Составить алгоритм для п. 4.2.1 e) ГОСТ Р ИСО/МЭК 27001-2006.
2) Составить интеллектуальную карту для п. 4.2.1 a) ГОСТ Р ИСО/МЭК 27001-2006.
3) Составить IDEF0 для п. 4.2.1 b) ГОСТ Р ИСО/МЭК 27001-2006.

Контрольные вопросы/задания:

Знать: угрозы информационной безопасности объектов	1.Какие существуют природные угрозы информационной безопасности объектов? 2.Какие существуют антропогенные угрозы информационной безопасности объектов? 3.Какие существуют техногенные угрозы информационной безопасности объектов?
Уметь: проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента	1.Проанализируйте фундаментальные проблемы информационной безопасности в условиях становления современного информационного общества на примере выбранной организации 2.Проанализируйте прикладные проблемы информационной безопасности в условиях становления современного информационного общества

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. Контрольное задание 1. Контрольное задание 2

Формы реализации: Проверка задания
Тип контрольного мероприятия: Деловая игра
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольное задание 1,2 для индивидуального выполнения. Условия проведения Учебная группа 1 человек. Используемые технические и программные средства: Компьютер с ОС Linux, Windows. Встроенное программное обеспечение

Краткое содержание задания:
Контрольное задание 1. Деловая игра. Моделирование рисков информационной безопасности на примере модели филиала АКБ.
Пример задания: При выполнении этого этапа определить сначала цель (цели) управления рисками, а затем исходя из этого, определить основные критерии, области и границы применения и методики обработки рисков.
1. Определить цели управления рисками.

2. Определить основные критерии оценки рисков.
Активы для каждого студента определяются по вариантам.
Вариант 1:
1. Предлагаемые активы:
1) Банковский платежный технологический процесс, включающий все виды платежей в бумажной и электронной формах. Выполняется в расчетно-кассовом отделении (относится к банковской тайне).
2) Банковский технологический процесс по обслуживанию физических лиц (депозиты, кредиты).
9) Банковское делопроизводство (внешнее и внутреннее) включает обычную почту, внутреннюю и внешнюю электронную почту для сотрудников в соответствии с их должностными полномочиями. Ответственный – заместитель управляющего банка.
20) Антивирусное ПО (инсталляции и установленное ПО).
24) Система видеонаблюдения (видеокамеры и регистраторы).
32) Информационные базы и информационные архивы, являющиеся результатом финансовой, экономической и управленческой деятельности банка (в бумажном и электронном формах). Имеют статус «банковская тайна», размещаются в кабинете управляющего банком.
34) Сертификаты, лицензии и другие документы, сгенерированные банком самостоятельно и полученные им для использования от других организаций (например ЦБ и пр.). Размещаются в кабинете управляющего банка в сейфе.
40) В кабинете управляющего банка проводятся совещания, которые могут содержать конфиденциальную информацию – банковскую и коммерческую тайну.

Контрольное задание 2. Деловая игра. Анализ исходных данных и результатов аудита информационной безопасности.
Пример задания. На основе результатов аудита разработать частную политику информационной безопасности. При разработки политики необходимо использовать исходные данные деловой игры, требования по содержанию политики, приведенные в стандарте ГОСТ Р ИСО/МЭК 27002 и материалы пособия по СМИБ.
Вариант 1:
1. Предлагаемые активы:
1) Банковский платежный технологический процесс, включающий все виды платежей в бумажной и электронной формах. Выполняется в расчетно-кассовом отделении (относится к банковской тайне).
2) Банковский технологический процесс по обслуживанию физических лиц (депозиты, кредиты).
9) Банковское делопроизводство (внешнее и внутреннее) включает обычную почту, внутреннюю и внешнюю электронную почту для сотрудников в соответствии с их должностными полномочиями. Ответственный – заместитель управляющего банка.
20) Антивирусное ПО (инсталляции и установленное ПО).
24) Система видеонаблюдения (видеокамеры и регистраторы).
32) Информационные базы и информационные архивы, являющиеся результатом финансовой, экономической и управленческой деятельности банка (в бумажном и электронном формах). Имеют статус «банковская тайна», размещаются в кабинете управляющего банком.
34) Сертификаты, лицензии и другие документы, сгенерированные банком самостоятельно и полученные им для использования от других организаций (например ЦБ и пр.). Размещаются в кабинете управляющего банка в сейфе.
40) В кабинете управляющего банка проводятся совещания, которые могут содержать конфиденциальную информацию – банковскую и коммерческую тайну.
2. Разработать политику управления рисками информационной безопасности.

Контрольные вопросы/задания:

Знать: фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	1.Какие фундаментальные проблемы для информационной безопасности в условиях становления современного информационного общества применимы для предлагаемой организации? 2.Какие прикладные проблемы для информационной безопасности в условиях становления современного информационного общества применимы для предлагаемой организации?
Уметь: проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента	1.Как для предложенной организации провести экспериментальные исследования защищенности объектов с применением современных математических методов? 2.Как для предложенной организации провести экспериментальные исследования защищенности объектов с применением современных технических и программно-аппаратных методов?

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. Контрольное задание 3

Формы реализации: Проверка задания
Тип контрольного мероприятия: Деловая игра
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольное задание 3 для индивидуального выполнения. Условия проведения Учебная группа 1 человек. Используемые технические и программные средства: Компьютер с ОС Linux, Windows. Встроенное программное обеспечение

Краткое содержание задания:
Контрольное задание 3. Деловая игра. Разработка плана управления рисками
Этап 5. Моделирование плана обработки рисков и защита проекта.
Цель задания: разработать план обработки риска.
Пример задания: Провести моделирование плана обработки рисков с соответствии с предложенной таблицей. Результаты представляются в форме отчета.

Таблица

ПЛАН ОБРАБОТКИ РИСКОВ
<Наименование организации>
<Год>

№ риска	**Угрозы (код)**	**Уязвимости (код)**	**Активы (код)**	**Оценка ущерба**	**Возможность реализации риска**	**Способ обработки риска**	**Меры обработки риска**	**Остаточный риск**	**Затраты на обработку**	**Ответственный за обработку риска**
	{Из табл. П9] }	*{Из табл. П9] }*	*{Из табл. П9] }*	*{Из табл. П9] }*	*{Из табл. П9] }*	*{Снижение, сохранение, предотвращение или перенос}*	*{Кратко описываются меры или их код}*	*{Описывается в терминах высокий, средний, удовлетвор. }*	*{Имеют конкретное денежное выражение }*	*{Фам. и инициалы}*

Ознакомлены:_____ <Фамилия и инициалы>
{План обработки рисков составляется в сгруппированном по общим уязвимостям и угрозам виде. После этого риски упорядочиваются по оценкам ущерба. План утверждается руководителем организации и является основанием для его финансирования. }

Контрольные вопросы/задания:

Знать: фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	1.Какие природные угрозы информационной безопасности актуальны для предложенной организации? 2.Какие антропогенные угрозы информационной безопасности актуальны для предложенной организации? 3.Какие техногенные угрозы информационной безопасности актуальны для предложенной организации?
Уметь: проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента	1.Выделите основные проблемы в области СМИБ для предложенной организации 2.Классифицируйте основные риски информационной безопасности предложенной организации

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

2 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. Уязвимость: определение, параметры представления. 2. Понятие «стратегия управления» рисками. 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: ПК-1.З$_{ПК-1}$ Проводит анализ безопасности компьютерных систем

Вопросы, задания

1.Риск: определение, параметры для его определения и описания.
2.Угроза: определение, параметры угрозы.
3.Уязвимость: определение, параметры представления.
4.В какой последовательности проводится оценка риска?
5.Как выбирается способ обработки рисков?
6.Агрегат риска: назначение, как вычисляется.
7.Актив: параметры описания.
8.Для чего выполняется процесс «установление контекста»?
9.Для чего предусмотрен возврат на «установление контекста» после процесса «оценка риска»?
10.Для чего предусмотрен возврат на «установление контекста» после процесса «обработка риска»?
11.Чем заканчивается обработка риска?
12.Поясните процесс «коммуникация риска».
13.Поясните процесс «мониторинг риска».
14.Что представляет собой план осведомленности риска.
15.Для чего разрабатывается положение о применимости?
16.Проводится ли полная обработка рисков повторно при возврате на контекст риска после первой и второй точкой принятия решений?
17.В каких единицах измеряются риски?
18.Какие вы знаете базы данных угроз?

19.Какие вы знаете базы данных уязвимостей?
20.Почему нет баз данных рисков?
21.Агрегат риска: назначение, форма представления и как вычисляется.
22.Что нам дает процесс моделирования рисков?
23.Как создается перечень мер и средств контроля и управления?
24.Почему измерения параметров риска проводятся в форме принадлежности к классам?
25.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.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

3.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.