

**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
Менеджмент информационной безопасности в организации**

**Москва
2022**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

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

(подпись)

А.С. Минзов

(расшифровка
подписи)

СОГЛАСОВАНО:

Руководитель
образовательной
программы

(должность, ученая степень, ученое
звание)

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

(подпись)

А.С. Минзов

(расшифровка
подписи)

Заведующий
выпускающей кафедры

(должность, ученая степень, ученое
звание)

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

(подпись)

А.Ю.

Невский

(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-1.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. Защита результатов выполнения индивидуального задания «Анализ рекомендованных мер и средств контроля при создании системы СМИБ (ГОСТ 27001, 27002)» (Домашнее задание)
2. Контрольное задание №2 «Моделирование процессов менеджмента информационной безопасности». Тест 1: Перечень и основное содержание документов СМИБ организации (Контрольная работа)

Форма реализации: Письменная работа

1. Контрольная работа 1: Менеджмент информационной безопасности в британских стандартах BS 7799 (Контрольная работа)
2. Тест 2: Моделирование информационных рисков организации (Тестирование)

БРС дисциплины

1 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Требования отечественных и международных стандартов к организации системы менеджмента информационной безопасности (СМИБ)					
Системы менеджмента информационной безопасности.	+	+	+	+	
Управление рисками информационной безопасности в различных концепциях					
Менеджмент рисков информационной безопасности. Концепция управления рисками на основе ГОСТ Р ИСО/МЭК 27005.	+	+	+	+	
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-1.2 _{ПК-1} Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	<p>Знать:</p> <p>перечень и содержание основных нормативных документов по менеджменту информационной безопасности и при организации СМИБ</p> <p>теорию управления информационной безопасностью организаций и бизнес-процессов</p> <p>Уметь:</p> <p>проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов</p>	<p>Контрольная работа 1: Менеджмент информационной безопасности в британских стандартах BS 7799 (Контрольная работа)</p> <p>Контрольное задание №2 «Моделирование процессов менеджмента информационной безопасности». Тест 1: Перечень и основное содержание документов СМИБ организации (Контрольная работа)</p> <p>Тест 2: Моделирование информационных рисков организации (Тестирование)</p> <p>Защита результатов выполнения индивидуального задания «Анализ рекомендованных мер и средств контроля при создании системы СМИБ (ГОСТ 27001, 27002)» (Домашнее задание)</p>

		использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации применять методы оценки и анализа рисков информационной безопасности организации и создавать документы по управлению СМИБ	
--	--	--	--

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольная работа 1: Менеджмент информационной безопасности в британских стандартах BS 7799

Формы реализации: Письменная работа

Тип контрольного мероприятия: Контрольная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: 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. Отчет включает ответы на 5 вопросов. При анализе уделить внимание тем тер-минам, которые в разных стандартах сформулированы по-разному.

Краткое содержание задания:

Дать определение термина и пояснить механизмы его проявления или реализации по варианту, соответствующему номеру в списке группы.

Контрольные вопросы/задания:

Знать: перечень и содержание основных нормативных документов по менеджменту информационной безопасности и при организации СМИБ	1.Цели внедрения СМИБ 2.Меры и средства контроля и управления (синонимы)
Знать: теорию управления информационной безопасностью организаций и бизнес-процессов	1.Управление инцидентом ИБ
Уметь: использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации	1.Конфиденциальность
Уметь: применять методы оценки и анализа рисков информационной безопасности организации и создавать документы по управлению СМИБ	1.ГОСТ 27003 назначение и область применения
Уметь: проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	1.Принципы СМИБ

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. Контрольное задание №2 «Моделирование процессов менеджмента информационной безопасности». Тест 1: Перечень и основное содержание документов СМИБ организации

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Контрольная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Провести моделирование процессов СМИБ. Варианты задания приведены в таблице 1. Результаты представить в форме отчета в электронной форме в виртуальном университете (<http://bc.mpei.ru>). Уровень агрегации процессов выполнить таким образом, чтобы описание модели процессов размещалось с необходимыми комментариями на листе формата А4.

Краткое содержание задания:

Провести моделирование процессов СМИБ (ГОСТ Р ИСО/МЭК 27001-2006 г., приказов ФСТЭК №17, 21 и пост. Правит. 1119) по одной из предложенных форм: IDEF0, алгоритм или Интеллектуальная карта (ИК).

Контрольные вопросы/задания:

Знать: перечень и содержание основных нормативных документов по менеджменту информационной безопасности и при организации СМИБ	1.4.2.3 (IDEF0) 2.4.2.3 (алгоритм)
Знать: теорию управления информационной безопасностью организаций и бизнес-процессов	1.5 (IDEF0)
Уметь: использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации	1.Пр-з ФСТЭК №21 (Пост.Прав.1119) (алгоритм)
Уметь: применять методы оценки и анализа рисков информационной безопасности организации и создавать документы по управлению	1.Пр-з ФСТЭК №21 (Пост.Прав.1119) (IDEF0)

СМИБ	
Уметь: проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	1.Пр-з ФСТЭК №17 (IDEF0)

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. Тест 2: Моделирование информационных рисков организации

Формы реализации: Письменная работа

Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Тестирование

Краткое содержание задания:

Тестирование. Необходимо выбрать верный вариант ответа на вопрос.

Контрольные вопросы/задания:

Знать: перечень и содержание основных нормативных документов по менеджменту информационной безопасности и при организации СМИБ	<p>1.Роли и обязанности в области безопасности должны включать в себя требования в отношении:</p> <ul style="list-style-type: none"> a) реализации и действия в соответствии с политиками информационной безопасности организации; b) защиты активов от несанкционированного доступа, разглашения сведений, модификации, разрушений или вмешательства; c) выполнения определенных процессов или деятельности, связанных с безопасностью; d) обеспечения уверенности в том, что на индивидуума возлагается ответственность за предпринимаемые действия; e) создание системы осведомленности сотрудников.
--	--

	<p>f) информирования о событиях или потенциальных событиях, связанных с безопасностью, или других рисках безопасности для организации.</p>
<p>Знать: теорию управления информационной безопасностью организаций и бизнес-процессов</p>	<p>1. Управление производительностью информационных систем проводится с целью:</p> <p>a) Прогнозирования производительности оборудования исходя будущих целей обработки информации.</p> <p>b) Оптимизация производительности информационных систем.</p> <p>c) Разработки требований к производительности оборудования по обработке информации.</p> <p>2. Основной принцип размещения средств обработки информации:</p> <p>a) Минимизация занимаемой площади.</p> <p>b) Минимизация рисков просмотра информации неавторизованными лицами.</p> <p>c) Исключение воровства.</p> <p>d) Выполнение требований ФСТЭК.</p>
<p>Уметь: использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации</p>	<p>1. Порядок увольнения сотрудников включает следующие этапы:</p> <p>a) Информирование о прекращении обязанностей с соответствующим правовым обеспечением.</p> <p>b) Возврат сотрудником активов.</p> <p>c) Оформление увольняемым сотрудником документов с передачей компетенций.</p> <p>d) Аннулирование прав доступа.</p> <p>e) Подписание соглашения о нераспространении конфиденциальной информации.</p> <p>f) Удаление персональных данных увольняемого.</p>
<p>Уметь: применять методы оценки и анализа рисков информационной безопасности организации и создавать документы по управлению СМИБ</p>	<p>1. Круг обязанностей каждого руководителя определяется границами :</p> <p>a) активов и процессов;</p> <p>b) наличием ответственных за каждый актив;</p> <p>c) наличием документов по управлению;</p> <p>d) наличием полномочий и уровней обязанностей.</p>
<p>Уметь: проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов</p>	<p>1. Защита активов, включает:</p> <p>a) процедуры защиты активов организации, в том числе информацию и программное обеспечение, а также менеджмент известных уязвимостей;</p> <p>b) процедуры для определения компрометации активов, например вследствие потери или модификации данных;</p> <p>c) целостность;</p> <p>d) ограничения на копирование и разглашение информации;</p>

	е) процедуры доступности; ф) процедуры резервирования.
--	---

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. Защита результатов выполнения индивидуального задания «Анализ рекомендованных мер и средств контроля при создании системы СМИБ (ГОСТ 27001, 27002)»

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Домашнее задание

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: На основе стандарта 27002 изучить рекомендованные меры и средства контроля и управления при создании СМИБ. Результаты представить в форме интеллектуальных карт с необходимыми детальными пояснениями (MS visio или Mind Maple Lite).

Краткое содержание задания:

Защита результатов выполнения индивидуального задания.

Контрольные вопросы/задания:

Знать: перечень и содержание основных нормативных документов по менеджменту информационной безопасности и при организации СМИБ	1.Менеджмент коммуникаций
Знать: теорию управления информационной безопасностью организаций и бизнес-процессов	1.Организационные аспекты информационной безопасности 2.Безопасность, связанная с персоналом
Уметь: использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации	1.Менеджмент инцидентов информационной безопасности
Уметь: применять методы оценки и анализа рисков информационной безопасности организации и создавать	1.Обращение с носителями информации

документы по управлению СМИБ	
Уметь: проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	1.Планирование и приемка систем

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

1 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: ПК-1.2_{ПК-1} Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей

Вопросы, задания

1. Системы менеджмента информационной безопасности.
2. Концепции управления информационной безопасностью, анализ различных подходов к управлению информационной безопасностью.
3. Менеджмент информационной безопасности в британских стандартах BS 7799.
4. Система менеджмента информационной безопасности в концепции стандарта ГОСТ Р ИСО/МЭК 27000.
5. Управление информационной безопасностью на основе подходов документов INIL и COBIT 5.0.
6. Формализация документов СМИБ.
7. Менеджмент рисков информационной безопасности.
8. Концепция управления рисками на основе ГОСТ Р ИСО/МЭК 27005.
9. Модели рисков.
10. Многофакторные модели рисков.
11. Концепция управления информационными рисками на основе документов INIL и COBIT 5.0.
12. Инвентаризация информационных активов организации.
13. Разработка модели и моделирование рисков информационной безопасности организации.
14. Управление информационной безопасностью организации на основе информации моделирования информационных рисков.

Материалы для проверки остаточных знаний

1. Владение может распространяться на:

Ответы:

- a) процесс бизнеса;
- b) определенный набор деятельностей;
- c) прикладные программы;
- d) определенное множество данных;
- e) операционные системы;
- f) офисные приложения;
- g) базы знаний.

Верный ответ: a, b, c, d

2. Политика ИБ включает:

Ответы:

- a) Цели и задачи СМИБ.
- b) Концепция СМИБ.

- c) Частные политики.
- d) Ответственных за организацию СМИБ.
- e) Лист изменений.

Верный ответ: a, b, d, e

3.Порядок увольнения сотрудников включает следующие этапы:

Ответы:

- a) Информирование о прекращении обязанностей с соответствующим правовым обеспечением.
- b) Возврат сотрудником активов.
- c) Оформление увольняемым сотрудником документов с передачей компетенций.
- d) Аннулирование прав доступа.
- e) Подписание соглашения о нераспространении конфиденциальной информации.
- f) Удаление персональных данных увольняемого.

Верный ответ: a, b, c, d, e

4.Принцип "необходимого знания" в отношении зон безопасности подразумевает:

Ответы:

- a) Отсутствие возможности получения информации о целях и технологиях её обработки.
- b) Запрещение использования фото и видео записывающего оборудования.
- c) Контроль за действиями персонала.
- d) Отсутствие информационных материалов, раскрывающих конфиденциальную информацию.
- e) Наличие документации.

Верный ответ: a, b, c

5.Резервирование информации включает решение следующих вопросов:

Ответы:

- a) необходимо определить количество копий, формы их хранения и обновления;
- b) шифрование копий;
- c) тестирование копий;
- d) обеспечение физической защиты;
- e) 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: a, c, d, f, g

6.Управление производительностью информационных систем проводится с целью:

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: a, b

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 по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»