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
Основы управления информационной безопасностью

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-5 способностью использовать нормативные правовые акты в профессиональной деятельности

2. ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

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

4. ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

5. ОК-8 способностью к самоорганизации и самообразованию

и включает:

для текущего контроля успеваемости:

Форма реализации: Защита задания
1. КМ-3 (Деловая игра)

Форма реализации: Смешанная форма
1. КМ-1 (Коллоквиум)
2. КМ-2 (Коллоквиум)

БРС дисциплины

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %			
	Индекс КМ:	КМ-1	КМ-2	КМ-3
	Срок КМ:	4	8	13
Введение в курс. Термины и определения. Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-				

2008			
Введение в курс. Термины и определения	+		
Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008	+	+	
Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)			
Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)		+	
Разработка СМИБ на примере АКБ (деловая ситуация)			
Разработка СМИБ на примере АКБ (деловая ситуация)			+
Вес КМ:	30	35	35

$Общая часть/Для промежуточной аттестации$

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-5	ОПК-5(Компетенция)	Знать: основные нормативные документы по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ	КМ-1 (Коллоквиум)
ОПК-7	ОПК-7(Компетенция)	Знать: основные понятия, термины, определения в сфере управления информационной безопасностью в бизнес-процессах Уметь: использовать полученные в процессе обучения знания для проведения анализа состояния объектов и систем на соответствие требованиям стандартов по	КМ-1 (Коллоквиум) КМ-2 (Коллоквиум)

		информационной безопасности определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
ПК-10	ПК-10(Компетенция)	Уметь: использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации	КМ-3 (Деловая игра)
ПК-13	ПК-13(Компетенция)	Знать: методы управления СМИБ на основе методик управления рисками	КМ-2 (Коллоквиум)
ОК-8	ОК-8(Компетенция)	Знать: содержание процессов самоорганизации и самообразования, их особенности и технологии реализации, исходя из	КМ-3 (Деловая игра)

		целей совершенствования Индивидуальный устный опрос, письменный опрос, тестирование в профессиональной деятельности	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. КМ-1

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Условия проведения: Учебная группа. Продолжительность: 4 учебных часа.

Краткое содержание задания:

1. Описать определение термина, и пояснить механизмы его проявления или реализации. Каждому студенту задаются вопросы не менее чем по 5 терминам.
2. 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.

Контрольные вопросы/задания:

Знать: основные нормативные документы по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ	1.Назовите основные методы управления СМИБ на основе методик управления рисками 2.Назовите специфические методы управления СМИБ на основе методик управления рисками
Знать: основные понятия, термины, определения в сфере управления информационной безопасностью в бизнес-процессах	1.Какие основные термины используются в сфере управления информационной безопасностью в бизнес-процессах? 2.Приведите дефиниции основных терминов в сфере управления информационной безопасностью в бизнес-процессах
Уметь: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	1.Определите, с позиции какого руководящего стандарта применяются выбранные термины для управления информационной безопасностью в банковской сфере 2.Определите, с позиции какого руководящего стандарта применяются выбранные термины для управления информационной безопасностью в маркетинговой сфере 3.Определите использованные методы управления СМИБ на основе методик управления рисками для представленной организации 4.Проведите сопоставление использованных методов управления СМИБ на основе методик управления рисками для представленной 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

КМ-2. КМ-2

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 35
Процедура проведения контрольного мероприятия: Условия проведения: Учебная группа. Продолжительность: 4 учебных часа.

Краткое содержание задания:
1. На основе стандартов ГОСТ Р ИСО/МЭК 27000+ изучить рекомендованные формы составления документов СМИБ.
2. На основе стандарта ГОСТ Р ИСО/МЭК 27002-2012 изучить рекомендованные меры и средства контроля и управления при создании СМИБ.

Контрольные вопросы/задания:

Знать: методы управления СМИБ на основе методик управления рисками	1.Назовите основные нормативные документы ФСТЭК по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ 2.Назовите основные ГОСТы по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ 3.Проанализируйте содержание процессов самоорганизации и самообразования, исходя из целей совершенствования профессиональной деятельности 4.Проанализируйте особенности и технологии реализации процессов самоорганизации и самообразования, исходя из целей совершенствования профессиональной деятельности
Уметь: использовать полученные в процессе обучения знания для проведения анализа состояния объектов и систем на соответствие требованиям стандартов по информационной безопасности	1.Определите, какие нормативные документы ФСТЭК были использованы при создании и управлении системой менеджмента информационной безопасности предложенной организации 2.Определите, какие ГОСТы были использованы при создании и управлении системой менеджмента информационной безопасности предложенной организации

	3.Определите, какие технологии использовались при создании и управлении системой менеджмента информационной безопасности предложенной организации 4.Определите содержание процессов, использованных при создании и управлении системой менеджмента 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

КМ-3. КМ-3

Формы реализации: Защита задания
Тип контрольного мероприятия: Деловая игра
Вес контрольного мероприятия в БРС: 35
Процедура проведения контрольного мероприятия: Деловая ситуация выполняется в форме отдельных функционально завершенных работ в определенной последовательности. 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. Условия проведения: Учебная группа: 1 человек. Продолжительность: 24 учебных часов.

Краткое содержание задания:
Создать СМИБ для АКБ. Содержание 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.

Контрольные вопросы/задания:

Знать: содержание процессов самоорганизации и самообразования, их особенности и технологии реализации, исходя из целей совершенствования Индивидуальный устный опрос, письменный опрос, тестирование	1.Какие требования стандарты предъявляют к СМИБ? 2.Какие методы используются для анализа процессов для определения ценности информационных активов организации? 3.Какие методы используются для моделирования актуальных угроз организации? 4.Какие информационные ресурсы подлежат

в профессиональной деятельности	обязательной защите в организации?
Уметь: использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации	1.Определите состояние объектов и систем предложенной организации на соответствие требованиям стандартов по информационной безопасности 2.Предложите методы анализа процессов для определения ценности информационных активов для предложенной организации 3.Какие методы моделирования актуальных угроз использованы при создании СМИБ предложенной организации? 4.Определите возможные пути реализации угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования 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

7 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ МЭИ	**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1** Кафедра *Безопасности и информационных технологий* Дисциплина «Основы управления информационной безопасностью»	*Утверждаю:* *Зав. каф. БИТ* *А.Ю.Невский* Протокол № от 20__ года
1. Какие в настоящее время существуют подходы к созданию систем информационной безопасности в РФ? Дайте краткую характеристику и принципиальные отличия. 2. Состав и содержание политики физической безопасности и защиты от окружающей среды. Профессор, д.т.н. А.Минзов		

Процедура проведения

Экзамен проводится в письменной форме по билетам согласно программе экзамена

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

1. Компетенция/Индикатор: ОПК-5(Компетенция)

Вопросы, задания

1.Особенности организации защиты информации в концепции Cobit 5.0 по сравнению с ГОСТ Р ИСО/МЭК 27001.

2.Как классифицируются документы, разрабатываемые в концепциях стандарта ГОСТ Р ИСО/МЭК 27001,27002, 27005?

3.Модель уязвимостей в концепции ГОСТ Р ИСО/МЭК 27002.

4.Какие методы определения опасности рисков рекомендуются в ГОСТ Р ИСО/МЭК 27005?

Материалы для проверки остаточных знаний

1.Какие меры и средства с точки зрения законодательства являются ключевыми мерами и средствами контроля и управления для организации?

Ответы:

a защита данных и конфиденциальность персональных данных
b защита документов организации
c права на интеллектуальную собственность
d физическая защита активов
e Кадровая политика
f применение криптографии

Верный ответ: abc

2. Компетенция/Индикатор: ОПК-7(Компетенция)

Вопросы, задания

1.Перечислите последовательность организации защиты информации в государственных информационных системах.
2.Перечислите последовательность организации защиты информации в негосударственных информационных системах.
3.Состав и содержание политики физической безопасности и защиты от окружающей среды.
4.Как оценить стоимость информационных активов?
5.Какие существуют методы вычисления интегральных метрик оценки рисков?
6.Как провести описание сценариев инцидентов информационной безопасности? Как и где использовать эти сценарии?
7.Методы моделирования плана обработки рисков и выстраивания их приоритетов по уровню опасности на основе стратегий управления рисками и их анализа.
8.Методы учета связей между рисками по угрозам, уязвимостям, активам и мерам защиты. Выявления агрегатов рисков.
9.Понятие стратегии управления рисками. Анализ стратегий.
10.Как выбирать метод обработки рисков? Какие при этом используются правила?
11.Многофакторная модель управления рисками информационной безопасности: назначение, решаемые задачи, стратегии рисков и последовательность работы.
12.Понятие риск информационной безопасности. Составляющие риска. С какой целью используется управление СМИБ на основе рисков?
13.Обработка рисков: виды обработки и правила выбора процессов обработки.
14.Аксиомы и правила, используемые при моделировании рисков.
15.С какой целью устанавливается контекст организации при моделировании рисков?
16.Какие критерии управления рисками используются?

Материалы для проверки остаточных знаний

1.На какие активы в организации может распространяться владение активами?
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: abcd
2.Что подразумевает принцип "необходимого знания" в отношении зон безопасности?
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: abd

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

Вопросы, задания

1.Назначение и краткое содержание политики СМИБ.

2.Что включает в себя концепция СМИБ? С какой целью она разрабатывается?
3.Назначение и краткое содержание политики СИБ. Как разделяются 2 политики СИБ и СМИБ?
4.Состав и содержание политики соответствия.
5.Как оценить меру затрат на создание СМИБ?

Материалы для проверки остаточных знаний

1.Какие требования должны в себя включать роли и обязанности в области безопасности?

Ответы:

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.
f информирования о событиях или потенциальных событиях, связанных с безопасностью, или других рисках безопасности для организации.

Верный ответ: a

4. Компетенция/Индикатор: ПК-13(Компетенция)

Вопросы, задания

1.Какие в настоящее время существуют подходы к созданию систем информационной безопасности в РФ? Дайте краткую характеристику и принципиальные отличия.
2.Как оценить ущерб от реализации угроз информационной безопасности?
3.Как оценить возможность реализации уязвимости информационной системы?
4.Сущность концепции защиты информации на основе цикла Деминга –Шухарта.
5.Алгоритм моделирования рисков информационной безопасности.

Материалы для проверки остаточных знаний

1.Что включает в себя политика ИБ?

Ответы:

a определения информационной безопасности, ее общих целей и сферы действия, а также упоминания значения безопасности как инструмента, обеспечивающего возможность совместного использования информации
b изложения намерений руководства
c подхода к установлению мер и средств контроля и управления
d краткого разъяснения наиболее существенных для организации политик безопасности, принципов, стандартов и требований соответствия
e наличие осведомленности персонала
f учебные фильмы по функциям персонала

Верный ответ: abcd

5. Компетенция/Индикатор: ОК-8(Компетенция)

Вопросы, задания

1.Состав и содержание политики непрерывности бизнеса.
2.Состав и содержание политики приобретения, разработки и эксплуатации информационных систем.
3.Состав и содержание политики безопасности, связанная с персоналом.

4.Состав и содержание политики расследования инцидентов.
5.Состав и содержание политики безопасности услуг электронной торговли.
6.Политика менеджмента коммуникаций и работ.
7.Политика управления доступом.
8.Политика защиты персональных данных.
9.Политика защиты коммерческой тайны.
10.Политика защиты банковской тайны.
11.Политика аудита ИБ.
12.Политика распределения ролей персонала.
13.Политика обучения персонала.
14.Политика повышения осведомленности персонала.
15.Почему при защите персональных данных не используются модели рисков?

Материалы для проверки остаточных знаний

1.Что не включают обязанности руководства по отношению к ИБ?

Ответы:

a обеспечение уверенности в том, что цели информационной безопасности определены, соответствуют требованиям организации и включены в соответствующие процессы;
b обеспечение ресурсами, необходимыми для информационной безопасности
c обеспечение уверенности в том, что персонал осознает значимость системы менеджмента ИБ.
d обеспечение четкого управления и очевидной поддержки менеджмента в отношении инициатив, связанных с безопасностью
e Обеспечение осведомленности персонала о политике ИБ
f Финансирование СМИБ
g Обеспечение профессиональными кадрами

Верный ответ: abcd

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.