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: Безопасность компьютерных систем

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-6 способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ИД-2 Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты

ИД-3 Организует технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

2. ОПК-10 способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

ИД-2 Принимает участие в формировании, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации

3. ОПК-12 способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

ИД-1 Проводит анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвует в проведении технико-экономического обоснования соответствующих проектных решений

и включает:

для текущего контроля успеваемости:

Форма реализации: Выполнение задания

1. Задание 2. Моделирование процессов управления СМИБ в стандарте IDEF0 (Отчет)
2. Задание 3. Моделирование процессов управления рисками в различных концепциях (Отчет)

Форма реализации: Защита задания

1. Контрольные задания 1-6. Деловая игра (Деловая игра)

Форма реализации: Письменная работа

1. Задание 1. Термины и определения стандарта ГОСТ ИСО/МЭК 27000 (Отчет)

БРС дисциплины

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Вводный раздел					
Введение в курс. Термины и определения		+			
Система менеджмента					
Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008			+		
Управление информационной безопасностью					
Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)			+	+	
Разработка системы менеджмента информационной безопасности					
Разработка СМИБ на примере АКБ (деловая игра)				+	+
	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
ОПК-6	ИД-2$_{ОПК-6}$ Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты	Знать: современные концепции управления информационной безопасностью принципы оправления на основе цикла Дёменга-Шухарта Уметь: моделировать системы управления информационной безопасностью	Задание 2. Моделирование процессов управления СМИБ в стандарте IDEF0 (Отчет) Задание 3. Моделирование процессов управления рисками в различных концепциях (Отчет)
ОПК-6	ИД-3$_{ОПК-6}$ Организует технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по	Знать: требования нормативных документов по формированию политики информационной безопасности Уметь: выполнять процессы разработки основных планирующих документов и политик безопасности	Задание 2. Моделирование процессов управления СМИБ в стандарте IDEF0 (Отчет) Контрольные задания 1-6. Деловая игра (Деловая игра)

	техническому и экспортному контролю		
ОПК-10	ИД-2$_{ОПК-10}$ Принимает участие в формировании, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации	Знать: требования нормативных документов ФСТЭК и ФСБ по организации и построении систем защиты информации ограниченного доступа Уметь: выполнять комплекс мер по обеспечению информационной безопасности	Задание 1. Термины и определения стандарта ГОСТ ИСО/МЭК 27000 (Отчет) Задание 3. Моделирование процессов управления рисками в различных концепциях (Отчет)
ОПК-12	ИД-1$_{ОПК-12}$ Проводит анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвует в проведении технико-экономического обоснования соответствующих проектных решений	Знать: технологии сбора исходных данных для проектирования СМИБ методы технико-экономического обоснования проектов по информационной безопасности с использованием моделей рисков Уметь: моделировать риски информационной безопасности на основе анализа и классификации активов, уязвимостей и угроз	Задание 2. Моделирование процессов управления СМИБ в стандарте IDEF0 (Отчет) Задание 3. Моделирование процессов управления рисками в различных концепциях (Отчет) Контрольные задания 1-6. Деловая игра (Деловая игра)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Задание 1. Термины и определения стандарта ГОСТ ИСО/МЭК 27000

Формы реализации: Письменная работа
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Место проведения: учебная аудитория Условия проведения: Учебная группа: 1 человек. Продолжительность: 1 учебный час. Используемые технические и программные средства: Компьютер с ОС Windows. Встроенное программное обеспечение

Краткое содержание задания:
Описать определение термина, и пояснить механизмы его проявления или реализации по варианту, соответствующему номеру в списке группы. Каждому студенту необходимо дать определение по 5 терминам.

Контрольные вопросы/задания:

Знать: требования нормативных документов ФСТЭК и ФСБ по организации и построении систем защиты информации ограниченного доступа	1.Назовите современные концепции управления информационной безопасностью 2.Охарактеризуйте концепцию Дёминга-Шухарта

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
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. Задание 2. Моделирование процессов управления СМИБ в стандарте IDEF0

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Место проведения: учебная аудитория Условия проведения: Учебная группа: 1 человек. 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 27001-2006. Форма моделирования выбирается из варианта задания. Все подпроцессы должны быть с необходимыми пояснениями для работы

Контрольные вопросы/задания:

Знать: принципы оправления на основе цикла Дёменга-Шухарта	1.Перечислите принципы управления на основе цикла Дёменга-Шухарта
Знать: методы технико-экономического обоснования проектов по информационной безопасности с использованием моделей рисков	1.Охарактеризуйте основные ступени цикла Дёминга-Шухарта
Уметь: моделировать системы управления информационной безопасностью	1.Выделите в планирующем документе основные требования к процессу управления информационной безопасностью
Уметь: выполнять процессы разработки основных планирующих документов и политик безопасности	1.Выделите в политике информационной безопасности базовые разделы основного документа

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
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. Задание 3. Моделирование процессов управления рисками в различных концепциях

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Место проведения: учебная аудитория Условия проведения: Учебная группа: 1 человек. Продолжительность: 2 учебных часа. Используемые технические и программные средства: Компьютер с ОС Windows. Встроенное программное обеспечение

Краткое содержание задания:

На основе стандарта ГОСТ Р ИСО/МЭК 27002-2012 изучить рекомендованные меры и средства контроля и управления при создании СМИБ.

Контрольные вопросы/задания:

Знать: современные концепции управления информационной безопасностью	1.Перечислите требования нормативных документов ФСТЭК по организации и построении систем защиты информации ограниченного доступа 2.Перечислите требования нормативных документов ФСБ по организации и построении систем защиты информации ограниченного доступа
Знать: технологии сбора исходных данных для проектирования СМИБ	1.Назовите требования нормативных документов по формированию политики информационной безопасности
Уметь: выполнять комплекс мер по обеспечению информационной безопасности	1.Определите основной комплекс мер по обеспечению информационной безопасности для предложенной организации

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
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. Контрольные задания 1-6. Деловая игра

Формы реализации: Защита задания
Тип контрольного мероприятия: Деловая игра
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Место проведения: учебная аудитория 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:

Знать: требования нормативных документов по формированию политики информационной безопасности	1.Охарактеризуйте технологии сбора исходных данных для проектирования СМИБ 2.Раскройте методы технико-экономического обоснования проектов по информационной безопасности с использованием моделей рисков
Уметь: моделировать риски информационной безопасности на основе анализа и классификации активов, уязвимостей и угроз	1.Смоделируйте риски информационной безопасности на основе анализа и классификации активов, уязвимостей и угроз

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
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. Что включает в себя концепция СМИБ? С какой целью она разрабатывается? 3. Какие критерии управления рисками используются? 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: ИД-2$_{ОПК-6}$ Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты

Вопросы, задания

1.Как оценить стоимость информационных активов?
2.Как оценить ущерб от реализации угроз информационной безопасности?
3.Как оценить возможность реализации уязвимости информационной системы?
4.Как оценить меру затрат на создание СМИБ?
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.

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. Компетенция/Индикатор: ИД-3$_{ОПК-6}$ Организует технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Вопросы, задания

1.Методы учета связей между рисками по угрозам, уязвимостям, активам и мерам защиты. Выявления агрегатов рисков.
2.Понятие стратегии управления рисками. Анализ стратегий.
3.Как выбирать метод обработки рисков? Какие при этом используются правила?
4.Политика менеджмента коммуникаций и работ.
5.Политика управления доступом.
6.Политика защиты персональных данных.
7.Политика защиты коммерческой тайны.
8.Политика защиты банковской тайны.

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

3. Компетенция/Индикатор: ИД-2$_{ОПК-10}$ Принимает участие в формировании, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации

Вопросы, задания

1.Политика аудита ИБ.
2.Политика распределения ролей персонала.
3.Политика обучения персонала.
4.Политика повышения осведомленности персонала.
5.Сущность концепции защиты информации на основе цикла Деминга –Шухарта.
6.Модель уязвимостей в концепции ГОСТ Р ИСО/МЭК 27002.
7.Многофакторная модель управления рисками информационной безопасности: назначение, решаемые задачи, стратегии рисков и последовательность работы.

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

4. Компетенция/Индикатор: ИД-1$_{ОПК-12}$ Проводит анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвует в проведении технико-экономического обоснования соответствующих проектных решений

Вопросы, задания

1.Понятие риск информационной безопасности. Составляющие риска. С какой целью используется управление СМИБ на основе рисков?
2.Обработка рисков: виды обработки и правила выбора процессов обработки.
3.Аксиомы и правила, используемые при моделировании рисков.
4.Алгоритм моделирования рисков информационной безопасности.
5.С какой целью устанавливается контекст организации при моделировании рисков ?
6.Какие критерии управления рисками используются?
7.Какие методы определения опасности рисков рекомендуются в ГОСТ Р ИСО/МЭК 27005?
8.Почему при защите персональных данных не используются модели рисков?

Материалы для проверки остаточных знаний

1.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

2.Что включают в себя вопросы электронной торговли?

Ответы:

a) планирование СМИБ электронной торговли.
b) аутентификацию субъектов электронной торговли..
c) авторизацию субъектов электронной торговли.
d) расследование инцидентов.
e) информирование партнеров об условиях их авторизации.
f) создание механизмов неотказуемости сделок.
g) защиту от мошенничества при оплате.

Верный ответ: abce

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.