Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 11.03.01 Радиотехника

Наименование образовательной программы: Беспроводные технологии и интернет вещей

Уровень образования: высшее образование - бакалавриат

Форма обучения: Заочная

Оценочные материалы
по дисциплине
Защита информации

Москва
2025

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Власкин Д.Н. Идентификатор: R563fb3df-VlaskinDN-4d4341df	Д.Н. Власкин

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Крутских В.В. Идентификатор: R49539849-KrutskikhVV-f1575360	В.В. Крутских
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Шалимова Е.В. Идентификатор: Rf4bb1f0c-ShalimovaYV-f267ebd6	Е.В. Шалимова

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-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности

ИД-1 Знает современные принципы поиска, хранения, обработки, анализа и представления в требуемом виде информации

ИД-2 Соблюдает требования информационной безопасности при использовании современных информационных технологий и программного обеспечения

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. Инженерно-техническое обеспечение системы информационной безопасности (Тестирование)
2. Информационная безопасность и защита информации, основы системы информационной безопасности (Тестирование)
3. Организационно-правовое, кадровое и финансово-экономическое обеспечение системы информационной безопасности (Тестирование)
4. Программно-аппаратное обеспечение системы информационной безопасности (Тестирование)

Форма реализации: Письменная работа

1. Информационная безопасность и защита информации (Доклад)

БРС дисциплины

4 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Информационная безопасность и защита информации (Доклад)

КМ-2 Информационная безопасность и защита информации, основы системы информационной безопасности (Тестирование)

КМ-3 Организационно-правовое, кадровое и финансово-экономическое обеспечение системы информационной безопасности (Тестирование)

КМ-4 Инженерно-техническое обеспечение системы информационной безопасности (Тестирование)

КМ-5 Программно-аппаратное обеспечение системы информационной безопасности (Тестирование)

Вид промежуточной аттестации – Экзамен.

Раздел дисциплины	Веса контрольных мероприятий, %					
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5
	Срок КМ:	3	6	9	12	15
Информационная безопасность и защита информации						
Сущность информации		+				
Конфиденциальная информация. Угрозы информации. Каналы утечки информации		+				
Основы системы информационной безопасности						
Структура системы информационной безопасности			+			
Основы системы обеспечения информационной безопасности			+			
Организационно-правовое, кадровое и финансово-экономическое обеспечение системы информационной безопасности						
Организационно-правовое обеспечение системы информационной безопасности				+		
Кадровое обеспечение системы информационной безопасности. Финансово-экономическое обеспечение системы информационной безопасности				+		
Инженерно-техническое обеспечение системы информационной безопасности						
Структура инженерно-техническое обеспечение системы информационной безопасности					+	
Средства защиты компьютерной информации от утечки и несанкционированного доступа					+	
Программно-аппаратное обеспечение системы информационной безопасности						
Программная защита информации						+
Программно-аппаратная защита информации						+
	Вес КМ:	20	20	20	20	20

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-3	ИД-1$_{ОПК-3}$ Знает современные принципы поиска, хранения, обработки, анализа и представления в требуемом виде информации	Знать: информационные ресурсы, подлежащие защите, а также основные угрозы и риски информационной безопасности объекта защиты основные законодательные и нормативные документы, определяющие организацию и функционирование системы защиты информации	КМ-2 Информационная безопасность и защита информации, основы системы информационной безопасности (Тестирование) КМ-4 Инженерно-техническое обеспечение системы информационной безопасности (Тестирование)
ОПК-3	ИД-2$_{ОПК-3}$ Соблюдает требования информационной безопасности при использовании современных информационных технологий и программного обеспечения	Знать: мероприятия обеспечения защиты информации средства и систему обеспечения защиты информации Уметь: классифицировать основные угрозы безопасности информации	КМ-1 Информационная безопасность и защита информации (Доклад) КМ-3 Организационно-правовое, кадровое и финансово-экономическое обеспечение системы информационной безопасности (Тестирование) КМ-5 Программно-аппаратное обеспечение системы информационной безопасности (Тестирование)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Информационная безопасность и защита информации

Формы реализации: Письменная работа
Тип контрольного мероприятия: Доклад
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Выполненное задание отправляется в СДО "Прометей" в рамках функционала "Письменная работа".

Краткое содержание задания:
Контрольная точка направлена на проверку знаний по защите информации. Доклад должен раскрыть суть задания. Объем доклада – до 20 печатных листов. Объем презентации – до 15 слайдов. Доклад и презентация должны быть оформлены в соответствии с требованиями

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: мероприятия обеспечения защиты информации	1.Уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных 2.Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры 3.Угрозы аппаратных средств для безопасности информации 4.Акустическое излучение информативного речевого сигнала 5.Требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: оценка "отлично" выставляется, если задание выполнено верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: оценка "хорошо" выставляется, если задание выполнено верно с незначительными ошибками, выбрано верное направление решения

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: оценка "удовлетворительно" выставляется, если задание выполнено преимущественно верно, допущены ошибки при выборе направления решения

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: оценка "неудовлетворительно" выставляется, если не выполнены критерии для оценки "удовлетворительно"

КМ-2. Информационная безопасность и защита информации, основы системы информационной безопасности

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Решение тестов в объеме 30 вопросов в течение 60 мин. на компьютере в СДО "Прометей".

Краткое содержание задания:
Контрольная точка направлена на проверку знаний по защите информации

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: основные законодательные и нормативные документы, определяющие организацию и функционирование системы защиты информации	1.Что понимают под объектами защиты информации? 1. Объекты организации 2. Информационный процесс 3. Носитель информации 4. 1, 3 5. 2, 3 6. 1, 3 Ответ: 5 2.Безопасность информации – состояние защищенности информации, при котором обеспечены ее? 1. Оперативность 2. Целостность 3. Достоверность 4. Доступность 5. Конфиденциальность 6. 2, 4, 5 7. 1, 3, 5 Ответ: 6 3.Что из перечисленного не относится к задачам СИБ? 1. Предупреждение появления угроз 2. Обнаружение появившихся угроз 3. Обнаружение воздействия угроз 4. Стабилизация обнаруженных угроз 5. Ликвидация последствий воздействия угроз Ответ: 4 4.Способы защиты информации не включают? 1. Защиту информации от разведки (иностранной разведки) 2. Защиту информации от

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
	санкционированного доступа 3. Защиту информации от непреднамеренного воздействия 4. Защиту информации от утечки 5. Защиту информации от разглашения, защита информации от несанкционированного доступа 6. Защиту информации от преднамеренного воздействия Ответ: 2 5.Какая из перечисленных подсистем не относится к СОИБ? 1. Кадровое обеспечение 2. Инженерно-техническое обеспечение 3. Информационное обеспечение 4. Аудит ИБ 5. Программно-аппаратного обеспечения 6. Организационно-правовое обеспечение Ответ: 3

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: оценка "отлично" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: оценка "хорошо" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: оценка "удовлетворительно" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: оценка "неудовлетворительно" выставляется, если задание выполнено ниже порогового уровня, установленного шкалой

КМ-3. Организационно-правовое, кадровое и финансово-экономическое обеспечение системы информационной безопасности

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Решение тестов в объеме 30 вопросов в течение 60 мин. на компьютере в СДО «Прометей».

Краткое содержание задания:

Контрольная точка направлена на проверку знаний по организационно-правовом, кадровом и финансово-экономическом обеспечение системы информационной безопасности

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: средства и систему обеспечения защиты информации	1.Что не относится к Кодексу профессиональной этики специалиста в области информационной безопасности? 1. Обеспечение объективной и качественной работы 2. Обеспечение конфиденциальности информации 3. Развитие собственных компетенций 4. Обеспечение прозрачности своей работы и результатов 5. Обеспечение спортивного образа жизни 6. Повышение осведомленности других специалистов 7. Ориентир на «лучшие этики» Ответ: 5 2.К мероприятиям организации режима и охраны относится? 1. Обеспечение контрольных функций организации; 2. Устранение внутренних угроз ИБ 3. Создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа 4. Устранение внешних угроз ИБ 5. Определение мер ответственности за нарушения ИБ 6. Защиту информации от преднамеренного воздействия Ответ: 3 3.К задачам ФЭО СИБ относится: 1. Экономическая защита организации 2. Анализ и оценка эффективности затрат на информационную безопасность 3. Руководство и управление расчетами неблагоприятного исхода рисков 4. Финансовое обеспечение активов организации 5. Защита информации о финансовой деятельности организации 6. Предотвращение разглашения финансовой информации Ответ: 2 4.Одной из задач обучения кадров является? 1. Определить меры ответственности за нарушения ИБ 2. Создать благоприятные межличностные отношения 3. Защитить информацию от непреднамеренного воздействия 4. Определить должностных лиц, ответственных за информационную безопасность 5. Создать нормативные документы обеспечения ИБ 6. Предотвратить утечку информации по причине

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
	небрежности Ответ: 6 5.К составляющим затрат на обеспечение СИБ не относится? 1. Структурирование затрат на предупредительные мероприятия 2. Структурирование затрат на Политику СИБ 3. Структурирование затрат на контроль СИБ 4. Структурирование внутренних затрат на компенсацию нарушений политики СИБ 5. Структурирование внешних затрат на компенсацию нарушений политики СИБ Ответ: 2

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: оценка "отлично" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: оценка "хорошо" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: оценка "удовлетворительно" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: оценка "неудовлетворительно" выставляется, если задание выполнено ниже порогового уровня, установленного шкалой

КМ-4. Инженерно-техническое обеспечение системы информационной безопасности

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Технология проверки связана с выполнением контрольного теста по изученной теме. Тестирование проводится с использованием СДО "Прометей". К тестированию допускается пользователь, изучивший материалы, авторизованный уникальным логином и паролем.

Краткое содержание задания:
Контрольная точка направлена на проверку знаний по инженерно-техническому обеспечению систем информационной безопасности

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: информационные ресурсы, подлежащие защите, а также основные угрозы и риски информационной безопасности объекта защиты	1.К методам защиты информации средствами инженерно-технического обеспечения СИБ относится? 1. Защита информации от преднамеренного воздействия 2. Защита информации от появившихся угроз 3. Предотвращение нарушения целостности информации 4. Скрытие достоверной информации, посредством информационного и энергетического срытия 5. Предотвращение доступности информации 6. Защита информации от воздействия угроз Ответ: 4 2.К контактным извещателям (датчикам) не относятся? 1. Вибрационные 2. Ударноконтактные 3. Электроконтактные 4. Магнитоконтактные 5. Обрывные Ответ: 1 3.К подсистеме предупреждения угроз инженерно-технической защиты территорий и помещений относятся? 1. Средства методов физического поиска каналов утечки информации 2. Средства контроля и управления доступом 3. Средства обнаружения радиоизлучений закладных устройств 4. Инженерные средства физической защиты 5. 1, 3 6. 1, 4 7. 2, 4 Ответ: 7 4.Что не относится к способам гарантированного уничтожения информации? 1. Размагничивание носителя 2. Шифрование данных 3. Захоронение носителя установленным порядком 4. Химическое уничтожение носителя 5. Перезапись данных по специальному алгоритму

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
	6. Механическое уничтожение носителя 7. Термическое уничтожение носителя Ответ: 3 5.К средствам поиска каналов утечки информации за счет ПЭМИН не относятся? 1. Обнаружители диктофонов 2. Анализаторы спектра 3. Генераторы шума 4. Селективные микровольтметры 5. Специальные измерительные комплексы для проведения измерений уровней ЭМИ Ответ: 3

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: оценка "отлично" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: оценка "хорошо" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: оценка "удовлетворительно" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: оценка "неудовлетворительно" выставляется, если задание выполнено ниже порогового уровня, установленного шкалой

КМ-5. Программно-аппаратное обеспечение системы информационной безопасности

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Технология проверки связана с выполнением контрольного теста по изученной теме. Тестирование проводится с использованием СДО "Прометей". К тестированию допускается пользователь, изучивший материалы, авторизованный уникальным логином и паролем.

Краткое содержание задания:
Контрольная точка направлена на проверку знаний по программно-аппаратном обеспечении системы информационной безопасности

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Уметь: классифицировать основные угрозы безопасности информации	1.Продемонстрируйте комплексную систему обеспечения безопасности беспроводных сетей 2.Составьте и обоснуйте перечень средств контроля состояния проводных сетей 3.Рассмотрите применение возможностей VPN

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: оценка "отлично" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: оценка "хорошо" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: оценка "удовлетворительно" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: оценка "неудовлетворительно" выставляется, если задание выполнено ниже порогового уровня, установленного шкалой

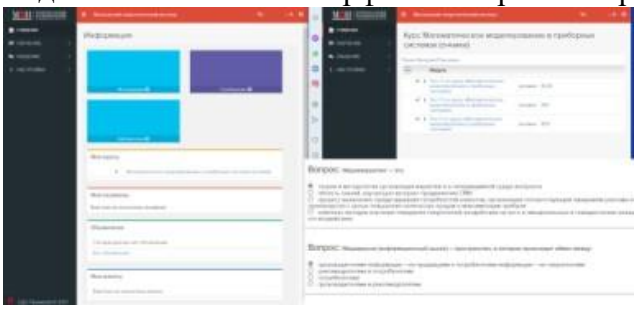
СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

Вид билета связан с интерфейсом сервиса "Прометей"



Процедура проведения

Форма проведения экзамена – письменный экзамен на основе тестирования
В тесте встречаются вопросы следующих типов:
1. с одним вариантом ответа (в вопросах «один из многих», система сравнивает ответ слушателя с правильным ответом и автоматически выставляет за него назначенный балл)
2. с выбором нескольких вариантов ответов (в вопросах «многие из многих» система оценивает каждый ответ отдельно; есть возможность разрешить слушателю получить за вопрос 0,75 балла, если он выберет 3 правильных ответа из 4)
3. на соответствие слушатель должен привести в соответствие левую и правую часть ответа (в вопросах «соответствие» система оценивает каждый ответ отдельно; можно разрешить слушателю получить за вопрос 0,75 балла, если он выберет 3 правильных ответа из 4)
4. развернутый ответ, вводится вручную в специально отведенное поле (ручная оценка преподавателем)

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

1. Компетенция/Индикатор: ИД-1$_{ОПК-3}$ Знает современные принципы поиска, хранения, обработки, анализа и представления в требуемом виде информации

Вопросы, задания

1.К подсистеме обнаружения технических каналов утечки информации системы обнаружения и защиты технических каналов утечки информации относятся?
2.Одной из целей организационно-правового обеспечения защиты информации является?
3.Что не относится к стратегии управления рисками?
4.К контактным извещателям (датчикам) не относятся?
5.Не относится к способам защиты информации при применении программно-аппаратных и аппаратных межсетевых экранов?

Материалы для проверки остаточных знаний

1.Что не относится к стратегии управления рисками?

Ответы:

1. Принятие риска

2. Уклонение от риска
3. Отражение риска
4. Изменение характера риска
5. Уменьшение риска

Верный ответ: 3

2. К контактным извещателям (датчикам) не относятся?

Ответы:

1. Вибрационные
2. Ударноконтактные
3. Электроконтактные
4. Магнитоконтактные
5. Обрывные

Верный ответ: 1

3.Не относится к способам защиты информации при применении программно-аппаратных и аппаратных межсетевых экранов?

Ответы:

1. Защищенные VPN сети
2. Зашумление сети
3. Журналирование
4. Контроль доступа
5. Фильтрация портов
6. Ограничение/фильтрация содержания

Верный ответ: 2

4.С какого мероприятия необходимо начинать работу по обеспечению функционирования СИБ?

Ответы:

1. Организации кадровой работы
2. Изучения правовых основ обеспечения ИБ
3. Введением комплекса ограничительных мер
4. Определение перечня источников конфиденциальной информации
5. Применения комплекса мер инженерно-технических защиты

Верный ответ: 2

5.К подсистеме предупреждения угроз инженерно-технической защиты территорий и помещений относятся?

Ответы:

1. Средства методов физического поиска каналов утечки информации
2. Средства контроля и управления доступом
3. Средства обнаружения радиоизлучений закладных устройств
4. Инженерные средства физической защиты
5. 1, 3
6. 1, 4
7. 2, 4

Верный ответ: 7

2. Компетенция/Индикатор: ИД-2$_{ОПК-3}$ Соблюдает требования информационной безопасности при использовании современных информационных технологий и программного обеспечения

Вопросы, задания

1.С какого мероприятия необходимо начинать работу по обеспечению функционирования СИБ?

2.Средства защиты информации – это совокупность правовых, организационных, технических и других решений, предназначенных для защиты?
3.К подсистеме предупреждения угроз инженерно-технической защиты территорий и помещений относятся?
4.Не относится к задачам организационно-правового обеспечения СИБ?
5.По виду охраняемой зоны (виду защиты) к извещателям (датчикам) не относятся?
6.Какие угрозы не относятся к природе возникновения?
7.Способы защиты информации не включают?

Материалы для проверки остаточных знаний

1.Средства защиты информации – это совокупность правовых, организационных, технических и других решений, предназначенных для защиты?

Ответы:

1. Информационной системы организации
2. Информации от непреднамеренного воздействия
3. Информационно-телекоммуникационных сетей
4. Автоматизированной системы управления
5. Информационных ресурсов от внутренних и внешних воздействий
6. Системы контроля и управления доступом

Верный ответ: 5

2.Не относится к задачам организационно-правового обеспечения СИБ?

Ответы:

1. Обеспечение контроля функционирования организации
2. Формирование и проведение политики информационной безопасности организации (предприятия)
3. Разработка нормативно-правовых актов, регламентирующих отношения в информационной сфере
4. Организация мероприятий обеспечения СИБ
5. 1, 2, 3
6. 2, 3, 4

Верный ответ: 1

3.По виду охраняемой зоны (виду защиты) к извещателям (датчикам) не относятся?

Ответы:

1. Поверхностные средства
2. Контактные средства
3. Объемные средства
4. Линейные средства
5. Точечные средства

Верный ответ: 2

4.Какие угрозы не относятся к природе возникновения?

Ответы:

1. Непреднамеренные
2. Естественные
3. Искусственные
4. Техногенные угрозы

Верный ответ: 1

5. Какое отношение характеризует область снижения величины риска ИБ при увеличении затрат на обеспечение ИБ?

Ответы:

1. $\delta R/\delta S \geq 0$
2. $\delta R/\delta S = 0$

3. $\delta R/\delta S > 0$
4. $\delta R/\delta S < 0$
5. $\delta R/\delta S \leq 0$

Верный ответ: 4

6.Что понимают под объектами защиты информации?

Ответы:

1. Объекты организации
2. Информационный процесс
3. Носитель информации
4. 1, 3
5. 2, 3
6. 1, 3

Верный ответ: 5

7.Обеспечение информационной безопасности организации – это деятельность, направленная на?

Ответы:

1. Устранение внутренних угроз ИБ
2. Устранение внешних угроз ИБ
3. Минимизацию ущерба от угроз
4. 1-3
5. 1-2
6. 2-3

Верный ответ: 4

8.Безопасность информации – состояние защищенности информации, при котором обеспечены ее?

Ответы:

1. Оперативность
2. Целостность
3. Достоверность
4. Доступность
5. Конфиденциальность
6. 2, 4, 5
7. 1, 3, 5

Верный ответ: 6

9.Выполнение каких функции должна обеспечивать нормативно-правовая база СОИБ?

Ответы:

1. Определение мер ответственности за нарушения ИБ
2. Создание благоприятных межличностных отношений
3. Определение системы органов и должностных лиц, ответственных за информационную безопасность
4. Создание нормативных документов обеспечения ИБ
5. Определение величины риска ИБ
6. 1, 3, 4
7. 1, 2, 4, 5

Верный ответ: 6

10.Что не относится к категориям цели Политики информационной безопасности?

Ответы:

1. Доступность
2. Аутентификация
3. Авторизация
4. Целостность

5. Конфиденциальность
6. Аудит безопасности

Верный ответ: 1

II. Описание шкалы оценивания

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: оценка "отлично" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: оценка "хорошо" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: оценка "удовлетворительно" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: оценка "неудовлетворительно" выставляется, если задание выполнено ниже порогового уровня, установленного шкалой

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 аттестационной составляющих.