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

Направление подготовки/специальность: 09.03.01 Информатика и вычислительная техника

Наименование образовательной программы: Технологии разработки программного обеспечения

Уровень образования: высшее образование - бакалавриат

Форма обучения: Заочная

Оценочные материалы
по дисциплине
Защита информации

Москва
2023

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Вишняков С.В. Идентификатор: R35b26072-VishniakovSV-02810d9	С.В. Вишняков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Вишняков С.В. Идентификатор: R35b26072-VishniakovSV-02810d9	С.В. Вишняков
(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-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ИД-2 Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью

и включает:

для текущего контроля успеваемости:

Форма реализации: Выполнение задания

1. Информационная безопасность и защита информации (Доклад)

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)

БРС дисциплины

10 семестр

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

$Общая часть/Для промежуточной аттестации$

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-3	ИД-2$_{ОПК-3}$ Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью	Знать: средства и систему обеспечения защиты информации мероприятия обеспечения защиты информации основные законодательные и нормативные документы, определяющие организацию и функционирование системы защиты информации информационные ресурсы, подлежащие защите, а также основные угрозы и риски информационной безопасности объекта защиты Уметь: анализировать исходные данные для проектирования подсистем и средств обеспечения защиты информации	Информационная безопасность и защита информации (Доклад) Информационная безопасность и защита информации, основы системы информационной безопасности (Тестирование) Организационно-правовое, кадровое и финансово-экономическое обеспечение системы информационной безопасности (Тестирование) Инженерно-техническое обеспечение системы информационной безопасности (Тестирование) Программно-аппаратное обеспечение системы информационной безопасности (Тестирование)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Информационная безопасность и защита информации

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Доклад
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Подготовить доклад с презентацией

Краткое содержание задания:
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:

Знать: информационные ресурсы, подлежащие защите, а также основные угрозы и риски информационной безопасности объекта защиты	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
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Если полностью раскрыта актуальность и суть вопроса, имеются схемы, ссылки на нормативную литературу, приведены практические примеры

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Если актуальность и суть вопроса раскрыты хорошо, имеющиеся схемы, ссылки на нормативную литературу, приведенные практические примеры раскрывают только общие положения

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Если актуальность и суть вопроса раскрыты слабо, имеющиеся схемы, ссылки на нормативную литературу, приведенные практические примеры не относятся к излагаемому вопросу

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:
Выбрать правильный ответ

Контрольные вопросы/задания:

Знать: мероприятия обеспечения защиты информации	1.**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 2.**3. 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

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: 27-30 правильных ответов

Оценка: 4
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: 23-26 правильных ответов

Оценка: 3
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: 17-22 правильных ответов

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:
Выбрать правильный ответ

Контрольные вопросы/задания:

Знать: основные законодательные и нормативные документы, определяющие организацию и функционирование системы защиты информации	1.**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» 2.**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 3.**4. 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

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: 27-30 правильных ответов

Оценка: 4
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: 23-26 правильных ответов

Оценка: 3
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: 17-22 правильных ответов

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: Решение тестов в объеме 30 вопросов в течение 60 мин. на компьютере в СДО «Прометей»

Краткое содержание задания:
Выбрать правильный ответ

Контрольные вопросы/задания:

Знать: средства и систему обеспечения защиты информации	1.**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 2.**3. К контактным извещателям (датчикам) не относятся?** 1. Вибрационные 2. Ударноконтактные 3. Электроконтактные 4. Магнитоконтактные 5. Обрывные

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: 27-30 правильных ответов

Оценка: 4
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: 23-26 правильных ответов

Оценка: 3
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: 17-22 правильных ответов

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: Решение тестов в объеме 30 вопросов в течение 60 мин. на компьютере в СДО «Прометей»

Краткое содержание задания:

Выбрать правильный ответ

Контрольные вопросы/задания:

Уметь: анализировать исходные данные для проектирования подсистем и средств обеспечения защиты информации	1.**12. Комплексная система обеспечения безопасности беспроводных сетей включает?** 1. WPA2 = IEEE 502.1X + CCMP + EAP + MIC 2. WPA2 = IEEE 802.1X +QH + CM + MIC 3. WPA2 = IEEE 802.1X + CCMP + EAP + MIC 4. WPA2 = IEEE 802.1X +CH + QP + EAP 5. WPA2 = IEEE 609.1X + CCMP + EAP + MIC 6. WPA2 = IEEE 802.1X + CCMP + AS + AC 2.**13. К средствам контроля состояния проводных сетей не относятся?** 1. 1. Сетевые анализаторы 2. 2. Кабельные тестеры с расширенным функционалом 3. 3. Простые кабельные тестеры 4. 4. Радиоприемные тестеры 5. 5. Простые кабельные тестеры с дополнительными функциями 6. 6. Сетевые тестеры 7.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: 27-30 правильных ответов

Оценка: 4
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: 23-26 правильных ответов

Оценка: 3
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: 17-22 правильных ответов

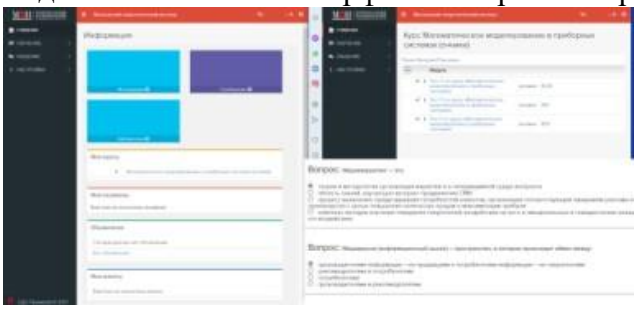
СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

Вид билета связан с интерфейсом сервиса "Прометей"



Процедура проведения

Порядок проведения экзамена: - форма проведения экзамена – письменный экзамен на основе тестирования, включающего 60 вопросов по всей дисциплине «Защита информации»; - время на проведение письменной части экзамена – 60 мин

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

1. Компетенция/Индикатор: ИД-2$_{ОПК-3}$ Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью

Вопросы, задания

1.1. К подсистеме обнаружения технических каналов утечки информации системы обнаружения и защиты технических каналов утечки информации относятся?
2.2. Одной из целей организационно-правового обеспечения защиты информации является?
3.3. Что не относится к стратегии управления рисками?

4.4. К контактным извещателям (датчикам) не относятся?
5.5. Не относится к способам защиты информации при применении программно-аппаратных и аппаратных межсетевых экранов?
6.6. С какого мероприятия необходимо начинать работу по обеспечению функционирования СИБ?
7.7. Средства защиты информации – это совокупность правовых, организационных, технических и других решений, предназначенных для защиты?
8.8. К подсистеме предупреждения угроз инженерно-технической защиты территорий и помещений относятся?
9.9. Не относится к задачам организационно-правового обеспечения СИБ?
10.10. По виду охраняемой зоны (виду защиты) к извещателям (датчикам) не относятся?
11.12. Какие угрозы не относятся к природе возникновения?
12.16. Способы защиты информации не включают?

Материалы для проверки остаточных знаний

1.3. 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: Ответ: 3

2.4. К контактным извещателям (датчикам) не относятся?

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

Верный ответ: Ответ: 1

3.5. 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: Ответ: 2

4.6. 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: Ответ: 2

5.7. 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: Ответ: 5

6.8. 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: Ответ: 7

7.9. 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: Ответ: 1

8.11. 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: Ответ: 2

9.**12. Какие угрозы не относятся к природе возникновения?**

Ответы:

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

Верный ответ: Ответ: 1

10.13. 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: Ответ: 4

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: 54-60 правильных ответов

Оценка: 4
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: 46-53 правильных ответов

Оценка: 3
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: 34-45 правильных ответов

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