

**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:


Разработчик

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

О.Р. Баронов


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

Заведующий
выпускающей кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Вишняков С.В.
	Идентификатор	R35b26072-VishniakovSV-02810d9

С.В.
Вишняков

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: 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

10 семестр

Раздел дисциплины	Веса контрольных мероприятий, %					
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5
	Срок КМ:	4	8	10	12	16
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:	10	20	20	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-3	ИД-2 _{опк-3} Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью	<p>Знать:</p> <p>мероприятия обеспечения защиты информации средства и систему обеспечения защиты информации информационные ресурсы, подлежащие защите, а также основные угрозы и риски информационной безопасности объекта защиты</p> <p>основные законодательные и нормативные документы, определяющие организацию и функционирование системы защиты информации</p> <p>Уметь:</p> <p>классифицировать основные угрозы безопасности информации</p>	<p>Информационная безопасность и защита информации (Доклад)</p> <p>Информационная безопасность и защита информации, основы системы информационной безопасности (Тестирование)</p> <p>Организационно-правовое, кадровое и финансово-экономическое обеспечение системы информационной безопасности (Тестирование)</p> <p>Инженерно-техническое обеспечение системы информационной безопасности (Тестирование)</p> <p>Программно-аппаратное обеспечение системы информационной безопасности (Тестирование)</p>

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: 10

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:

<p>Знать: основные законодательные и нормативные документы, определяющие организацию и функционирование системы защиты информации</p>	<ol style="list-style-type: none">1. Уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных2. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры3. Угрозы аппаратных средств для безопасности информации4. Акустическое излучение информативного речевого сигнала5. 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: оценка "отлично" выставляется, если задание выполнено верно

Оценка: 4

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

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

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:

Знать: информационные ресурсы, подлежащие защите, а также основные угрозы и риски информационной безопасности объекта защиты	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
--	---

Описание шкалы оценивания:

Оценка: 5

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

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

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

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-правовому, кадровому и финансово-экономическому обеспечению системы информационной безопасности

Контрольные вопросы/задания:

<p>Знать: мероприятия обеспечения защиты информации</p>	<p>1. Что не относится к Кодексу профессиональной этики специалиста в области информационной безопасности?</p> <ol style="list-style-type: none">1. Обеспечение объективной и качественной работы2. Обеспечение конфиденциальности информации3. Развитие собственных компетенций4. Обеспечение прозрачности своей работы и результатов5. Обеспечение спортивного образа жизни6. Повышение осведомленности других специалистов7. Ориентир на «лучшие этики» <p>Ответ: 5</p> <p>2. К мероприятиям организации режима и охраны относится?</p> <ol style="list-style-type: none">1. Обеспечение контрольных функций организации;2. Устранение внутренних угроз ИБ3. Создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа4. Устранение внешних угроз ИБ5. Определение мер ответственности за нарушения ИБ6. Защиту информации от преднамеренного воздействия <p>Ответ: 3</p> <p>3. К задачам ФЭО СИБ относится:</p> <ol style="list-style-type: none">1. Экономическая защита организации2. Анализ и оценка эффективности затрат на информационную безопасность3. Руководство и управление расчетами неблагоприятного исхода рисков4. Финансовое обеспечение активов организации5. Защита информации о финансовой деятельности организации
---	---

	6. Предотвращение разглашения финансовой информации Ответ: 2
--	---

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения задания: оценка "отлично" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 4

Нижний порог выполнения задания в процентах: 77

Описание характеристики выполнения задания: оценка "хорошо" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 3

Нижний порог выполнения задания в процентах: 57

Описание характеристики выполнения задания: оценка "удовлетворительно" выставляется, если задание выполнено в установленном объеме в соответствии со шкалой

Оценка: 2

Описание характеристики выполнения задания: 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: 25

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:

<p>Знать: средства и систему обеспечения защиты информации</p>	<p>1.К методам защиты информации средствами инженерно-технического обеспечения СИБ относится?</p> <ol style="list-style-type: none"> 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 скрытия 5. Предотвращение доступности информации 6. Защита информации от воздействия угроз <p>Ответ: 4</p> <p>2.К контактными извещателям (датчикам) не</p>
--	--

	<p>относятся?</p> <ol style="list-style-type: none"> 1. Вибрационные 2. Ударноконтактные 3. Электроконтактные 4. Магнитоконтактные 5. Обрывные <p>Ответ: 1</p>
--	---

Описание шкалы оценивания:

Оценка: 5

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

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

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

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: 25

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:

<p>Уметь: классифицировать основные угрозы безопасности информации</p>	<ol style="list-style-type: none"> 1.Продемонстрируйте комплексную систему обеспечения безопасности беспроводных сетей 2.Составьте и обоснуйте перечень средств контроля состояния проводных сетей
--	--

Описание шкалы оценивания:

Оценка: 5

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

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

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

Описание характеристики выполнения знания: оценка "неудовлетворительно" выставляется, если задание выполнено ниже порогового уровня, установленного шкалой

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10 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)

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

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

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?
6. С какого мероприятия необходимо начинать работу по обеспечению функционирования СИБ?
7. Средства защиты информации – это совокупность правовых, организационных, технических и других решений, предназначенных для защиты?
8. К подсистеме предупреждения угроз инженерно-технической защиты территорий и помещений относятся?

9. Не относится к задачам организационно-правового обеспечения СИБ?
10. По виду охраняемой зоны (виду защиты) к извещателям (датчикам) не относятся?
11. Какие угрозы не относятся к природе возникновения?
12. Способы защиты информации не включают?

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. 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

6.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

7.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

8.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

9.Какие угрозы не относятся к природе возникновения?

Ответы:

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

Верный ответ: 1

10. 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

II. Описание шкалы оценивания

Оценка: 5

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

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

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

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