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

Направление подготовки/специальность: 09.04.03 Прикладная информатика

Наименование образовательной программы: Информационные системы и технологии поддержки цифровой экономики

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Оценочные материалы
по дисциплине
Управление информационной безопасностью корпорации

Москва
2023

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Унижаев Н.В. Идентификатор: Rb43f42d6-UnizhayevNV-2454ef20	Н.В. Унижаев

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Крепков И.М. Идентификатор: R04da5bdb-KrepkovIM-33fe3095	И.М. Крепков
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

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-8 Способен осуществлять эффективное управление разработкой программных средств и проектов, в том числе с использованием современных цифровых технологий

ИД-1 Применяет знания по архитектуре информационных систем предприятий и организаций; методологии и технологии реинжиниринга, проектирования и аудита прикладных информационных систем различных классов

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. КМ-1. (Контрольная работа)
2. КМ-2. (Тестирование)
3. КМ-3. (Контрольная работа)
4. КМ-4. (Тестирование)

БРС дисциплины

1 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Современные проблемы информационной безопасности					
Тема 1. Введение в информационную безопасность		+			
Тема 2. Основные термины информационной безопасности		+			
Тема 3. Законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения.		+			
Управление системой информационной безопасности					
Тема 4. Место системы информационной безопасности организации			+		
Тема 5. Доктрина информационной безопасности Российской Федерации			+		
Тема 6. Модель информационной безопасности организации.			+		
Меры обеспечения информационной безопасности					

Тема 7. Особенности информационной безопасности критической информационной инфраструктуры			+	
Тема 8. Криптографические методы обеспечения информационной безопасности			+	
Тема 9. Организация защиты от вредоносных программ (вирусов)			+	
Политики информационной безопасности				
Тема 10. Особенности защиты персональных данных				+
Тема 11. Политика информационной безопасности				+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

БРС курсовой работы/проекта

1 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Анализ информационной безопасности корпорации		+			
Предложения по оптимизации информационной безопасности корпорации			+		
Разработка плана совершенствования информационной безопасности				+	
Оформление курсовой работы и подготовка к защите					+
Вес КМ:		25	25	25	25

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-8	ИД-1$_{ОПК-8}$ Применяет знания по архитектуре информационных систем предприятий и организаций; методологии и технологии реинжиниринга, проектирования и аудита прикладных информационных систем различных классов	Знать: цели, функции и принципы информационной безопасности федеральное законодательство и стандарты, регламентирующее информационную безопасность Уметь: строить систему защиты информации на основе принципов информационной безопасности искать уязвимости информационной системы организации	КМ-1. (Контрольная работа) КМ-2. (Тестирование) КМ-3. (Контрольная работа) КМ-4. (Тестирование)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. КМ-1.

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Процедура проведения соответствует требованиям руководящих документов НИУ «МЭИ»

Краткое содержание задания:
Задание соответствуют требованиям к магистрам. Все задания нацелены на получение компетенций по информационной безопасности. Подробное задание размещается в оценочных материалах по дисциплине Б1. В.ДВ.01.01 Корпоративные информационные системы управления цифровой экономикой

Контрольные вопросы/задания:

Знать: федеральное законодательство и стандарты, регламентирующее информационную безопасность	1.Введение в управление информационной безопасностью. Место информационной безопасности в экономических процессах. Выявление причин и следствий нарушения информационной безопасности. Проблемы, связанные с сотрудниками и техническими ресурсами. 2.Доктрина информационной безопасности Российской Федерации как основного документа, представляющий собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

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

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-2. КМ-2.

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Процедура проведения соответствует требованиям руководящих документов НИУ «МЭИ»

Краткое содержание задания:
Задание соответствуют требованиям к магистрам. Все задания нацелены на получение компетенций по информационной безопасности. Подробное задание размещается в оценочных материалах по дисциплине Б1. В.ДВ.01.01 Корпоративные информационные системы управления цифровой экономикой

Контрольные вопросы/задания:

Уметь: строить систему защиты информации на основе принципов информационной безопасности	1.Управление политикой безопасности, назначение и структура политики информационной безопасности, особенности формирования политик информационной безопасности. 2.Доктрина информационной безопасности Российской Федерации как основного документа, представляющий собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-3. КМ-3.

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Процедура проведения соответствует требованиям руководящих документов НИУ «МЭИ»

Краткое содержание задания:
Задание соответствуют требованиям к магистрам. Все задания нацелены на получение компетенций по информационной безопасности. Подробное задание размещается в оценочных материалах по дисциплине Б1. В.ДВ.01.01 Корпоративные информационные системы управления цифровой экономикой

Контрольные вопросы/задания:

Знать: цели, функции и принципы информационной безопасности	1.Современные и актуальные законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения информационной безопасности. Руководящие

	документы, регламентирующие процесс управления информационной безопасностью. 2.Знакомство с организационными мерами обеспечения информационной безопасности. Особенности информационной безопасности критической информационной инфраструктуры.

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

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-4. КМ-4.

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Процедура проведения соответствует требованиям руководящих документов НИУ «МЭИ»

Краткое содержание задания:
Задание соответствуют требованиям к магистрам. Все задания нацелены на получение компетенций по информационной безопасности. Подробное задание размещается в оценочных материалах по дисциплине Б1. В.ДВ.01.01 Корпоративные информационные системы управления цифровой экономикой

Контрольные вопросы/задания:

Уметь: искать уязвимости информационной системы организации	1.Управление политикой безопасности, назначение и структура политики информационной безопасности, особенности формирования политик информационной безопасности. 2.Современные и актуальные законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения информационной безопасности. Руководящие документы, регламентирующие процесс управления информационной безопасностью.

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

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

<table>
<tr><td>НИУ «МЭИ» ИнЭИ
Кафедра БИТ
20__ год</td><td>БИЛЕТ № 1
по дисциплине: УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КОРПОРАЦИИ
направление подготовки: _____
форма обучения: _____</td><td>Утверждаю:
Зав. кафедрой БИТ
_____
(подпись)</td></tr>
<tr><td colspan="3">1. Основные положения государственной информационной политики Российской Федерации
2. Причины и факторы информационных потерь</td></tr>
<tr><td>НИУ «МЭИ» ИнЭИ
Кафедра БИТ
20__ год</td><td>БИЛЕТ № 2
по дисциплине: УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КОРПОРАЦИИ
направление подготовки: _____
форма обучения: _____</td><td>Утверждаю:
Зав. кафедрой БИТ
_____
(подпись</td></tr>
<tr><td colspan="3">1. Понятие национальной безопасности. Виды безопасности
2. Характеристика злонамеренного действия инфекции типа «троянский конь»</td></tr>
<tr><td>НИУ «МЭИ» ИнЭИ
Кафедра БИТ
20__ год</td><td>БИЛЕТ № 3
по дисциплине: УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КОРПОРАЦИИ
направление подготовки: _____
форма обучения: _____</td><td>Утверждаю:
Зав. кафедрой БИТ
_____
(подпись</td></tr>
<tr><td colspan="3">1. Сущность и понятие информационной безопасности
2. Характеристика злонамеренного действия инфекции типа «черви»</td></tr>
</table>

Процедура проведения

Процедура проведения соответствует требованиям руководящих документов НИУ «МЭИ» Правила выставления итоговой оценки по курсу 1 семестр Экзамен. Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для магистров НИУ «МЭИ» на основании семестровой и экзаменационной составляющих. 1 семестр Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для

студентов НИУ «МЭИ». В приложение к диплому выносится оценка за 1 семестр и за курсовую работу.

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

1. Компетенция/Индикатор: ИД-1$_{ОПК-8}$ Применяет знания по архитектуре информационных систем предприятий и организаций; методологии и технологии реинжиниринга, проектирования и аудита прикладных информационных систем различных классов

Вопросы, задания

1.Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
Биометрические средства идентификации и аутентификации пользователей.
Аутентификация субъектов в распределенных системах, проблемы и решения.
Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
Средства обеспечения информационной безопасности в ОС Windows. Разграничение доступа к данным. Групповая политика.
Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
Понятие атаки на систему информационной безопасности. Особенности локальных атак.
Распределенные информационные системы. Удаленные атаки на информационную систему.
Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
Физические средства обеспечения информационной безопасности.
Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
Виртуальные частные сети, их функции и назначение.
Понятие информационной безопасности. Вопросы информационной безопасности в системе обеспечения национальной безопасности.
Классификация угроз информационной безопасности: для личности, для общества, для государства.
Основные критерии оценки надежности: политика безопасности и гарантированность.
Коммерческая, служебная, банковская и др. тайны.
2.Основные конституционные гарантии по охране и защите прав и свобод в информационной сфере. Федеральное законодательство регламентирующие процессы информационной безопасности.
Понятие надежности информации в автоматизированных системах обработки данных.
Что понимается под системной защитой информации.
Уязвимость информации в автоматизированных системах обработки данных.
Элементы и объекты защиты в автоматизированных системах обработки данных.
Методы использование динамически изменяющегося пароля. Методы модификации схемы простых паролей.
Понятие криптостойкости шифра. Требования к криптографическим системам защиты информации.
Особенности защиты информации в персональных ЭВМ. Основные цели защиты информации.
Признаки классификации вирусов. Как работает вирус?
Способы заражения программ. Стандартные методы заражения.

3.Методы защиты от вирусов.
Антивирусные программы. Программы-детекторы. Программы-доктора.
Цели, функции и задачи защиты информации в сетях ЭВМ. Угрозы безопасности для сетей передачи данных.
В чём заключаются задачи защиты в сетях передачи данных?
Проблемы защиты информации в вычислительных сетях.
Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.
Архитектура механизмов защиты информации в сетях ЭВМ.
Этапы развития информационной безопасности.
4.Признаки классификации вирусов. Как работает вирус?
Способы заражения программ. Стандартные методы заражения.
Методы защиты от вирусов.
Антивирусные программы. Программы-детекторы. Программы-доктора.
Цели, функции и задачи защиты информации в сетях ЭВМ. Угрозы безопасности для сетей передачи данных.
В чём заключаются задачи защиты в сетях передачи данных?
Проблемы защиты информации в вычислительных сетях.
Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.
Архитектура механизмов защиты информации в сетях ЭВМ.
Этапы развития информационной безопасности.
Классификация компьютерных преступлений.
Использование биометрических характеристик для информационной безопасности
Особенности защиты персональных данных.
Классификация информационных систем персональных данных.
Политика безопасности. Для чего нужна? Что регламентирует?

Материалы для проверки остаточных знаний

1.1) Остаточные знания проверятся по отдельным материалам с вопросами, примерные вопросы:
Введение в управление информационной безопасностью.
Место информационной безопасности в экономических процессах.
Выявление причин и следствий нарушения информационной безопасности.
Проблемы, связанные с сотрудниками и техническими ресурсами.

Ответы:

Терминология при используемая при ответе должен соответствовать требованиям федерального законодательства и стандартам, регламентирующим данный вид деятельности. При получении сведений для ответа можно использовать аналитические исследования, связанные с информационной безопасностью.

Верный ответ: Рекомендовано дать полный исчерпывающий ответ, подтверждающий правоту высказываний. Ответ должен быть подкреплен мнениями экспертов в информационной безопас-ности. Изложение ответа должно быть логичным, имеющим множественные доказательства.

2.2) Остаточные знания проверятся по отдельным материалам с вопросами, примерные вопросы:
Место системы информационной безопасности организации в системе безопасности Российской Федерации.
Доктрина информационной безопасности Российской Федерации как основного документа, представляющий собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

Ответы:

Терминология при используемая при ответе должен соответствовать требованиям федерального законодательства и стандартам, регламентирующим данный вид деятельности. При получении сведений для ответа можно использовать аналитические исследования, связанные с информационной безопасностью.

Верный ответ: Рекомендовано дать полный исчерпывающий ответ, подтверждающий правоту высказываний. Ответ должен быть подкреплен мнениями экспертов в информационной безопасности. Изложение ответа должно быть логичным, имеющим множественные доказательства.

3.3) Остаточные знания проверятся по отдельным материалам с вопросами, примерные вопросы:

Знакомство с организационными мерами обеспечения информационной безопасности.

Особенности информационной безопасности критической информационной инфраструктуры.

Варианты использования криптографических методов обеспечения информационной безопасности при формировании проектов.

Методы и варианты организации защиты от вредоносных программ (вирусов).

Классификация вирусов. Система защиты от вирусов.

Ответы:

Терминология при используемая при ответе должен соответствовать требованиям федерального законодательства и стандартам, регламентирующим данный вид деятельности. При получении сведений для ответа можно использовать аналитические исследования, связанные с информационной безопасностью.

Верный ответ: Рекомендовано дать полный исчерпывающий ответ, подтверждающий правоту высказываний. Ответ должен быть подкреплен мнениями экспертов в информационной безопасности. Изложение ответа должно быть логичным, имеющим множественные доказательства.

4.4) Остаточные знания проверятся по отдельным материалам с вопросами, примерные вопросы:

Управление политикой безопасности, назначение и структура политики информационной безопасности, особенности формирования политик информационной безопасности.

Ответы:

Терминология при используемая при ответе должен соответствовать требованиям федерального законодательства и стандартам, регламентирующим данный вид деятельности. При получении сведений для ответа можно использовать аналитические исследования.

Верный ответ: Рекомендовано дать полный исчерпывающий ответ, подтверждающий правоту высказываний. Ответ должен быть подкреплен мнениями экспертов в информационной безопас-ности. Изложение ответа должно быть логичным, имеющим множественные доказательства.

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

Оценка: 2

Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу

Процедура проведения соответствует требованиям руководящих документов НИУ «МЭИ» Правила выставления итоговой оценки по курсу 1 семестр Экзамен. Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для магистров НИУ «МЭИ» на основании семестровой и экзаменационной составляющих. 1 семестр Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ». В приложение к диплому выносится оценка за 1 семестр и за курсовую работу.

Для курсового проекта/работы:

1 семестр

Форма проведения: Защита КП/КР

I. Процедура защиты КП/КР

Соответствует требованиям распоряжения НИУ "МЭИ"

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

Оценка: 2
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу

Процедура проведения соответствует требованиям руководящих документов НИУ «МЭИ» 1 семестр Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ». В приложение к диплому выносится оценка за 1 семестр и за курсовую работу.