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

Направление подготовки/специальность: 38.03.05 Бизнес-информатика

Наименование образовательной программы: Информационное и программное обеспечение бизнес-процессов

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

Оценочные материалы
по дисциплине
Информационная безопасность

Москва
2023

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Потехецкий С.В. Идентификатор: R83b30a44-PotekhetskySV-31b213(	С.В. Потехецкий

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. ПК-1 Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе

ИД-2 Выполняет сбор, систематизацию, документирование и анализ требований к информационным системам

2. ПК-2 Способность участвовать в управлении жизненным циклом продуктов в области информационных технологий

ИД-2 Проводит обследование организаций, выявляет информационные потребности пользователей, формирует требования к информационной системе

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

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

БРС дисциплины

6 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

$Общая часть/Для промежуточной аттестации$

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
ПК-1	ИД-2$_{ПК-1}$ Выполняет сбор, систематизацию, документирование и анализ требований к информационным системам	Знать: особенности международного и федерального законодательства, регламентирующее информационную безопасность особенности системы поиска деловой и научной информации, связанные с информационной безопасностью регламенты, обеспечивающие защиту информации в специализированных системах и банках данных Уметь: применять алгоритмы стандартных задач для поиска уязвимостей информационной системы организации разрабатывать обзоры,	КМ-1 (Контрольная работа) КМ-2 (Тестирование) КМ-3 (Тестирование) КМ-4 (Тестирование)

		аннотации, рефераты, научные доклады, с учетом защиты информации использовать обзоры, аннотации, рефераты, научные доклады, для поиска уязвимостей информационной системы организации	
ПК-2	ИД-2$_{ПК-2}$ Проводит обследование организаций, выявляет информационные потребности пользователей, формирует требования к информационной системе	Знать: функции и принципы информационной безопасности принципы, на которых базируется федеральное законодательство, регламентирующее информационную безопасность методы решения типовых задач, связанных с информационной безопасностью Уметь: выстаивать систему защиты информации на основе принципов информационной безопасности искать уязвимости информационной системы организации использовать типовые ил	КМ-2 (Тестирование) КМ-3 (Тестирование) КМ-4 (Тестирование)

		стандартные задачи для обеспечения информационной безопасности	

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:
Знакомство с организационными мерами обеспечения информационной безопасности. Особенности информационной безопасности критической информационной инфраструктуры.

Контрольные вопросы/задания:

Знать: регламенты, обеспечивающие защиту информации в специализированных системах и банках данных	1.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:

Знакомство с организационными мерами обеспечения информационной безопасности. Особенности информационной безопасности критической информационной инфраструктуры.

Контрольные вопросы/задания:

Знать: особенности международного и федерального законодательства, регламентирующее информационную безопасность	1.Доктрина информационной безопасности Российской Федерации как основного документа, представляющий собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.
Знать: особенности системы поиска деловой и научной информации, связанные с информационной безопасностью	1.Современные и актуальные законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения информационной безопасности. Руководящие документы, регламентирующие процесс управления информационной безопасностью.
Знать: функции и принципы информационной безопасности	1.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-3. КМ-3

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:
Знакомство с организационными мерами обеспечения информационной безопасности. Особенности информационной безопасности критической информационной инфраструктуры.

Контрольные вопросы/задания:

Знать: методы решения типовых задач, связанных с информационной безопасностью	1.Варианты использования криптографических методов обеспечения информационной безопасности при формировании проектов.
Знать: принципы, на которых базируется федеральное законодательство, регламентирующее информационную безопасность	1.Доктрина информационной безопасности Российской Федерации как основного документа, представляющий собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.
Уметь: применять алгоритмы стандартных задач для поиска уязвимостей информационной системы организации	1.Современные и актуальные законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения информационной безопасности. Руководящие документы, регламентирующие процесс управления информационной безопасностью.
Уметь: разрабатывать обзоры, аннотации, рефераты, научные доклады, с учетом защиты информации	1.Варианты использования криптографических методов обеспечения информационной безопасности при формировании проектов.
Уметь: использовать типовые ил стандартные задачи для обеспечения информационной безопасности	1.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:

Знакомство с организационными мерами обеспечения информационной безопасности. Особенности информационной безопасности критической информационной инфраструктуры.

Контрольные вопросы/задания:

Уметь: использовать обзоры, аннотации, рефераты, научные доклады, для поиска уязвимостей информационной системы организации	1.Моделирование процессов, связанных с информационной безопасности организации. Использование описательных шаблонов, автоматизация процесса моделирования. Документы, регламентирующие процесс управления информационной безопасностью.
Уметь: выстаивать систему защиты информации на основе принципов информационной безопасности	1.Варианты использования криптографических методов обеспечения информационной безопасности при формировании проектов.
Уметь: искать уязвимости информационной системы организации	1.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

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6 семестр

Форма промежуточной аттестации: Зачет с оценкой

Пример билета

<table>
<tr><td>НИУ «МЭИ»
ИнЭИ

Кафедра БИТ

20__ год</td><td>БИЛЕТ № 1

по дисциплине: Информационная безопасность
направление подготовки:
форма обучения: очная</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: Информационная безопасность
направление подготовки:
форма обучения: очная</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: Информационная безопасность
направление подготовки:
форма обучения: очная</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»

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

1. Компетенция/Индикатор: ИД-2$_{ПК-1}$ Выполняет сбор, систематизацию, документирование и анализ требований к информационным системам

Вопросы, задания

1.Какими знаниями в различных областях и в т.ч. в области IT, должны обладать сотрудники отдела безопасности, руководители компании и другие должностные лица (бухгалтерия, кадры, производство). Какие знания потребуются в 2020, 2025 годах

Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
Какие процессы информационной безопасности регламентирует ДОКТРИНА информационной безопасности Российской Федерации
Какие процессы информационной безопасности регламентирует Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
Какие процессы информационной безопасности регламентирует Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"
Какие процессы информационной безопасности регламентирует Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"
Какие процессы информационной безопасности регламентирует Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ
Какие процессы информационной безопасности регламентирует МЕЖДУНАРОДНЫЙ СТАНДАРТ ИСО/МЭК 2700
Какие процессы информационной безопасности регламентирует МЕЖДУНАРОДНЫЙ СТАНДАРТ ISO/IEC 27002
2.Какие процессы информационной безопасности регламентирует МЕЖДУНАРОДНЫЙ СТАНДАРТ ISO/IEC 27002
Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
Назначение, общая характеристика структурной схемы подсистемы инженерно-технической защиты.
Понятие несанкционированного доступа к автоматизированной системе. Способы НСД.
Понятие управление рисками. Основные направления управления рисками.
Назначение и структура организационно-правовой подсистемы СОИБ.
Структура основных правовых актов, ориентированных на правовое обеспечение СОИБ ХС.

Материалы для проверки остаточных знаний

1.Управление политикой безопасности, назначение и структура политики информационной безопасности, особенности формирования политик информационной безопасности.
Современные и актуальные законы, стандарты и регламенты процесса обеспечения информационной безопасности.
Термины и определения информационной безопасности.
Руководящие документы, регламентирующие процесс управления информационной безопасностью.
Моделирование процессов, связанных с информационной безопасности организации.
Использование описательных шаблонов, автоматизация процесса моделирования.
Документы, регламентирующие процесс управления информационной безопасностью.

Ответы:

Терминология при используемая при ответе должен соответствовать требованиям федерального законодательства и стандартам, регламентирующим информационную безопасность. 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 области защиты информации Изложение ответа должно быть логичным, имеющим множественные доказательства.

2.Моделирование процессов, связанных с информационной безопасности организации. Использование описательных шаблонов, автоматизация процесса моделирования. Документы, регламентирующие процесс управления информационной безопасностью. 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 информационную безопасность. 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 области защиты информации Изложение ответа должно быть логичным, имеющим множественные доказательства.

2. Компетенция/Индикатор: ИД-2$_{ПК-2}$ Проводит обследование организаций, выявляет информационные потребности пользователей, формирует требования к информационной системе

Вопросы, задания

1.Классификация угроз информационной безопасности автоматизированных систем. Понятие риска и угрозы. Виды рисков.
Понятие угрозы. Классификация источников угроз.
Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
Понятие политики безопасности информационных систем. Назначение политики безопасности.

2.Понятие политики безопасности информационных систем. Назначение политики безопасности.
Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
Какими знаниями в различных областях и в т.ч. в области IT, должны обладать сотрудники отдела безопасности, руководители компании и другие должностные лица (бухгалтерия, кадры, производство). Какие знания потребуются в 2020, 2025 годах
Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
Какие процессы информационной безопасности регламентирует ДОКТРИНА информационной безопасности Российской Федерации
Какие процессы информационной безопасности регламентирует Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
Какие процессы информационной безопасности регламентирует Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"

Материалы для проверки остаточных знаний

1.Остаточные знания проверятся по отдельным материалам с вопросами. Примерные вопросы:
Управление политикой безопасности, назначение и структура политики информационной безопасности, особенности формирования политик информационной безопасности.

Методы и варианты организации защиты от вредоносных программ (вирусов).
Классификация вирусов.
Система защиты от вирусов.
Моделирование процессов, связанных с информационной безопасности организации.
Использование описательных шаблонов, автоматизация процесса моделирования.
Документы, регламентирующие процесс управления информационной безопасностью.

Ответы:

Терминология при используемая при ответе должен соответствовать требованиям федерального законодательства и стандартам, регламентирующим информационную безопасность. 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 области защиты информации 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

5 семестр Зачет с оценкой. Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ».