

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

Направление подготовки/специальность: 09.03.03 Прикладная информатика

Наименование образовательной программы: Прикладная информатика в экономике и управлении

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

**Оценочные материалы
по дисциплине
Информационная безопасность**

**Москва
2021**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель
(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Крыжановский Ю.Е.
	Идентификатор	Rfbb7ca24-KryzhanovskyYY-e2b375

(подпись)

Ю.Е.
Крыжановский
(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель
образовательной
программы

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Петров С.А.
	Идентификатор	R75f078b9-PetrovSA-cc5dcd67

(подпись)

С.А. Петров
(расшифровка
подписи)

Заведующий
выпускающей кафедры

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю.
Невский
(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-1 способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий
2. ОПК-4 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
3. ПК-1 способностью проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе
4. ПК-2 способностью разрабатывать, внедрять и адаптировать прикладное программное обеспечение
5. ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности

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
ОПК-1	ОПК-1(Компетенция)	Знать: особенности международного и федерального законодательства, регламентирующее информационную безопасность Уметь: разрабатывать обзоры, аннотации, рефераты, научные доклады, с учетом защиты информации	КМ-3 (Тестирование) КМ-4 (Тестирование)
ОПК-4	ОПК-4(Компетенция)	Знать: принципы, на которых базируется федеральное законодательство, регламентирующее информационную безопасность Уметь: выстраивать систему защиты информации на основе принципов информационной	КМ-1 (Контрольная работа) КМ-4 (Тестирование)

		безопасности	
ПК-1	ПК-1(Компетенция)	Знать: функции и принципы информационной безопасности Уметь: использовать обзоры, аннотации, рефераты, научные доклады, для поиска уязвимостей информационной системы организации	КМ-1 (Контрольная работа) КМ-2 (Тестирование)
ПК-2	ПК-2(Компетенция)	Знать: методы решения типовых задач, связанных с информационной безопасностью Уметь: использовать типовые ил стандартные задачи для обеспечения информационной безопасности	КМ-3 (Тестирование) КМ-4 (Тестирование)
ОК-4	ОК-4(Компетенция)	Знать: особенности системы поиска деловой и научной информации, связанные с информационной безопасностью регламенты, обеспечивающие защиту информации в специализированных	КМ-2 (Тестирование) КМ-3 (Тестирование) КМ-4 (Тестирование)

		системах и банках данных Уметь: искать уязвимости информационной системы организации применять алгоритмы стандартных задач для поиска уязвимостей информационной системы организации	
--	--	--	--

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: 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: использовать обзоры, аннотации, рефераты, научные доклады, 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.

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

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: 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. 2. Современные и актуальные законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения информационной безопасности. Руководящие документы, регламентирующие процесс управления информационной безопасностью.
Знать: особенности системы поиска деловой и научной информации, связанные с информационной безопасностью	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

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: особенности международного и федерального законодательства, регламентирующее информационную безопасность	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: особенности системы поиска деловой и научной информации, связанные с информационной безопасностью	1.Варианты использования криптографических методов обеспечения информационной безопасности при формировании проектов.
Уметь: использовать типовые и стандартные задачи для обеспечения информационной безопасности	1.Варианты использования криптографических методов обеспечения информационной безопасности при формировании проектов.
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.

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

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:

Знать: методы решения типовых задач, связанных с	1.Знакомство с организационными мерами обеспечения информационной безопасности.
--	---

информационной безопасностью	Особенности информационной безопасности критической информационной инфраструктуры.
Знать: регламенты, обеспечивающие защиту информации в специализированных системах и базах данных	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: выстраивать систему защиты информации на основе принципов информационной безопасности	1.Моделирование процессов, связанных с информационной безопасностью организации. Использование описательных шаблонов, автоматизация процесса моделирования. Документы, регламентирующие процесс управления информационной безопасностью.
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

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

БИЛЕТ № 1 по дисциплине: <i>Информационная безопасность</i> направление подготовки: форма обучения:	Утверждаю: <i>Зав. кафедрой</i> БИТ _____ (подпись)
1. Основные положения государственной информационной политики Российской Федерации 2. Причины и факторы информационных потерь	

Процедура проведения

Процедура проведения соответствует требованиям руководящих документов НИУ «МЭИ»

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

1. Компетенция/Индикатор: ОПК-1(Компетенция)

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.

Материалы для проверки остаточных знаний

1.Остаточные знания проверяются 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 безопасностью 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 подкреплён мнениями экспертов в области защиты информации. Изложение ответа должно быть логичным, имеющим множественные доказательства.

2. Моделирование процессов, связанных с информационной безопасностью 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 подкреплён мнениями экспертов в области защиты информации. Изложение ответа должно быть логичным, имеющим множественные доказательства.

2. Компетенция/Индикатор: ОПК-4(Компетенция)

Вопросы, задания

1. 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 безопасностью 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 подкреплён мнениями экспертов в области защиты информации. Изложение ответа должно быть логичным, имеющим множественные доказательства.

3. Компетенция/Индикатор: ПК-1(Компетенция)

Вопросы, задания

1. Какими знаниями в различных областях и в т.ч. в области ИТ, 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

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.

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 подкреплён мнениями экспертов в области защиты информации. Изложение ответа должно быть логичным, имеющим множественные доказательства.

4. Компетенция/Индикатор: ПК-2(Компетенция)

Вопросы, задания

1. 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 ИТ, 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. 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.

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 подкреплён мнениями экспертов в области защиты информации. Изложение ответа должно быть логичным, имеющим множественные доказательства.

5. Компетенция/Индикатор: ОК-4(Компетенция)

Вопросы, задания

1. Какими знаниями в различных областях и в т.ч. в области ИТ, 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.

Материалы для проверки остаточных знаний

1. Моделирование процессов, связанных с информационной безопасностью 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 подкреплён 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

III. Правила выставления итоговой оценки по курсу

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