

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

**Направление подготовки/специальность: 14.05.01 Ядерные реакторы и материалы**

**Наименование образовательной программы: Моделирование процессов в ядерных реакторах**

**Уровень образования: высшее образование - специалитет**

**Форма обучения: Очная**

**Оценочные материалы  
по дисциплине  
Информационные системы и безопасность**

**Москва  
2023**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Сахаров К.В.
	Идентификатор	Ra146ccd9-SakharovKV-e1fedf89

К.В. Сахаров

## СОГЛАСОВАНО:

Руководитель  
образовательной  
программы

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Дедов А.В.
	Идентификатор	R72c90f41-DedovAV-d71cc7f4

А.В. Дедов

Заведующий  
выпускающей кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Дедов А.В.
	Идентификатор	R72c90f41-DedovAV-d71cc7f4

А.В. Дедов

## 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 понимать принципы работы информационных технологий; осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны

ИД-2 Использует современные информационные системы в профессиональной сфере

ИД-3 Использует методы анализа опасностей и угроз, требования информационной безопасности и защиты государственной тайны

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Письменная работа

1. КМ-1 (Тестирование)
2. КМ-2 (Тестирование)
3. КМ-3 (Тестирование)
4. КМ-4 (Тестирование)
5. КМ-5 (Тестирование)
6. КМ-6 (Тестирование)

### БРС дисциплины

5 семестр

Раздел дисциплины	Веса контрольных мероприятий, %						
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6
	Срок КМ:	6	8	10	12	14	16
Нормативно-правовые основы обеспечения информационной безопасности в Российской Федерации							
Нормативно-правовые основы обеспечения информационной безопасности в Российской Федерации			+		+		
Нормативно-правовые основы обеспечения информационной и компьютерной безопасности в АСУ ТП							
Нормативно-правовые основы обеспечения информационной и компьютерной безопасности в АСУ ТП						+	+
Лицензирование деятельности по технической защите конфиденциальной информации							

Лицензирование деятельности по технической защите конфиденциальной информации	+		+			
Лицензирования деятельности в области криптографической защиты информации						
Лицензирования деятельности в области криптографической защиты информации	+		+			
Комплексная система обеспечения информационной безопасности						
Комплексная система обеспечения информационной безопасности					+	+
Системы управления информационной безопасностью и обеспечения непрерывности бизнеса						
Системы управления информационной безопасностью и обеспечения непрерывности бизнеса	+		+			
Информационная безопасность и управление рисками						
Информационная безопасность и управление рисками	+		+			
Особенности обеспечения информационной безопасности ПДн в ИСПДн организации						
Особенности обеспечения информационной безопасности ПДн в ИСПДн организации					+	+
Обеспечение защиты информации объектов критической информационной инфраструктуры						
Обеспечение защиты информации объектов критической информационной инфраструктуры					+	+
Особенности обеспечения информационной и компьютерной безопасности АСУ ТП						
Особенности обеспечения информационной и компьютерной безопасности АСУ ТП	+		+			
Защита информации конфиденциального характера с использованием шифровальных (криптографических) средств						
Защита информации конфиденциального характера с использованием шифровальных (криптографических) средств					+	+
Сети передачи данных						
Сети передачи данных					+	+
Обеспечение безопасности сетей передачи данных						
Обеспечение безопасности сетей передачи данных		+		+		
Криптографические протоколы						
Криптографические протоколы		+		+		
Тестирование на проникновение						

Тестирование на проникновение		+		+		
Техническая защита информации от утечки по техническим каналам						
Техническая защита информации от утечки по техническим каналам		+		+		
Вес КМ:	5	5	10	10	30	40

\$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 <sub>ОПК-3</sub> Использует современные информационные системы в профессиональной сфере	Знать: основные принципы и типовые меры обеспечения информационной безопасности, в том числе защиты государственной тайны Уметь: применять современные информационные системы при обеспечении безопасности и защиты государственной тайны	КМ-1 (Тестирование) КМ-2 (Тестирование) КМ-3 (Тестирование) КМ-4 (Тестирование)
ОПК-3	ИД-3 <sub>ОПК-3</sub> Использует методы анализа опасностей и угроз, требования информационной безопасности и защиты государственной тайны	Знать: основные виды информационных систем, используемых при обеспечении компьютерной и информационной безопасности, а также защите государственной тайны терминологию, применяемую в области	КМ-1 (Тестирование) КМ-2 (Тестирование) КМ-3 (Тестирование) КМ-4 (Тестирование) КМ-5 (Тестирование) КМ-6 (Тестирование)

		обеспечения информационной безопасности Уметь: разрабатывать модели угроз и выполнять анализ рисков информационной безопасности обеспечивать информационную безопасность, в том числе защиту государственной тайны	
--	--	--	--

## II. Содержание оценочных средств. Шкала и критерии оценивания

### КМ-1. КМ-1

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 5

**Процедура проведения контрольного мероприятия:** Онлайн тестирование

#### Краткое содержание задания:

Дать правильные ответы на тест

#### Контрольные вопросы/задания:

<p>Знать: основные виды информационных систем, используемых при обеспечении компьютерной и информационной безопасности, а также защите государственной тайны</p>	<p>1.1.Для удовлетворения законных прав и интересов субъектов (обеспечения их информационной безопасности) необходимо постоянно поддерживать следующие свойства информации и систем ее обработки: а)конфиденциальность, целостность, доступность; б)ясность, целостность, непрерывность; с)защищенность, актуальность, своевременность.</p>
<p>Уметь: применять современные информационные системы при обеспечении безопасности и защиты государственной тайны</p>	<p>1.К шифровальным (криптографическим) средствам (средствам криптографической защиты информации), включая документацию на эти средства, относятся:</p> <p>1 средства кодирования - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций</p> <p>2 средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче</p> <p>3 оба ответа верны</p>

#### Описание шкалы оценивания:

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 100*

*Описание характеристики выполнения знания: Дан правильный ответ*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 80*

*Описание характеристики выполнения знания: Дан правильный ответ*

*Оценка: 3*



*Нижний порог выполнения задания в процентах: 60*  
*Описание характеристики выполнения знания: Дан правильный ответ*

*Оценка: 2*

*Описание характеристики выполнения знания: Дан правильный ответ*

## **КМ-2. КМ-2**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС: 5**

**Процедура проведения контрольного мероприятия:** Онлайн тестирование

**Краткое содержание задания:**

Дать правильные ответы на тест

**Контрольные вопросы/задания:**

Знать: основные принципы и типовые меры обеспечения информационной безопасности, в том числе защиты государственной тайны	1.1.Лицензирование деятельности по технической защите конфиденциальной информации является государственной функцией, исполняемой: а)ФСТЭК России; б)ФСБ России; с)Роскомнадзором России.
Уметь: обеспечивать информационную безопасность, в том числе защиту государственной тайны	1.Анализ угроз безопасности информации включает:  1 выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей  2 определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации  3 оба ответа верны

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 100*

*Описание характеристики выполнения знания: Дан правильный ответ*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 80*

*Описание характеристики выполнения знания: Дан правильный ответ*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Дан правильный ответ*

*Оценка: 2*

*Описание характеристики выполнения знания: Дан правильный ответ*

## **КМ-3. КМ-3**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 10

**Процедура проведения контрольного мероприятия:** Онлайн тестирование

**Краткое содержание задания:**

Дать правильные ответы на тест

**Контрольные вопросы/задания:**

<p>Знать: основные виды информационных систем, используемых при обеспечении компьютерной и информационной безопасности, а также защите государственной тайны</p>	<p>1.1.В соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденный решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г., устанавливается: а)девять классов защищенности АС от НСД к информации.; б)пять классов защищенности АС от НСД к информации.; с)одиннадцать классов защищенности АС от НСД к информации.</p>
<p>Уметь: применять современные информационные системы при обеспечении безопасности и защиты государственной тайны</p>	<p>1.Компенсирующие меры по обеспечению безопасности объекта КИИ применяются в следующих случаях:</p> <p>1 негативное влияние отдельных мер по обеспечению безопасности на функционирование значимого объекта КИИ в проектных режимах значимого объекта</p> <p>2 в случае отсутствия желания у субъекта КИИ по защите ОКИИ</p> <p>3 в случае использования в значимом объекте КИИ сертифицированных на соответствие требованиям по безопасности информации средств защиты информации</p>

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 100*

*Описание характеристики выполнения знания: Дан правильный ответ*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 80*

*Описание характеристики выполнения знания: Дан правильный ответ*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Дан правильный ответ*

*Оценка: 2*

*Описание характеристики выполнения знания: Дан правильный ответ*

## КМ-4. КМ-4

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 10

**Процедура проведения контрольного мероприятия:** Онлайн тестирование

**Краткое содержание задания:**

Дать правильные ответы на вопросы теста

**Контрольные вопросы/задания:**

Знать: основные принципы и типовые меры обеспечения информационной безопасности, в том числе защиты государственной тайны	1.)Первый и пока единственный юридически обязывающий международный документ о физической защите ядерного материала, используемого в мирных целях: а )NSS-17; б) NSS-33Т; с) Конвенция о физической защите ядерного материала (CPPNM).
Уметь: обеспечивать информационную безопасность, в том числе защиту государственной тайны	1.Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах:  1 обязательной аттестации  2 лицензирования  3 обязательной сертификации

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 80*

*Описание характеристики выполнения знания: -*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: -*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 40*

*Описание характеристики выполнения знания: -*

*Оценка: 2*

*Описание характеристики выполнения знания: -*

## КМ-5. КМ-5

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 30

**Процедура проведения контрольного мероприятия:** Онлайн тестирование

**Краткое содержание задания:**

Дать правильные ответы на вопросы теста

**Контрольные вопросы/задания:**

<p>Знать: терминологию, применяемую в области обеспечения информационной безопасности</p>	<p>1. Категория значимости объекта КИИ должна пересматриваться:</p> <p>1 не реже одного раза в пять лет</p> <p>2 не реже одного раза в семь лет</p> <p>3 не реже одного раза в десять лет</p>
<p>Уметь: разрабатывать модели угроз и выполнять анализ рисков информационной безопасности</p>	<p>1. Приемочные испытания значимого объекта КИИ и его подсистемы безопасности проводятся в соответствии с:</p> <p>1 пожеланиями субъекта КИИ</p> <p>2 актом о вводе в эксплуатацию</p> <p>3 программой и методикой приемочных испытаний</p>

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 80*

*Описание характеристики выполнения знания: -*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: -*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 40*

*Описание характеристики выполнения знания: -*

*Оценка: 2*

*Описание характеристики выполнения знания: -*

**КМ-6. КМ-6**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 40

**Процедура проведения контрольного мероприятия:** Онлайн тестирование

**Краткое содержание задания:**

Дать правильные ответы на вопросы теста

**Контрольные вопросы/задания:**

<p>Знать: терминологию, применяемую в области обеспечения информационной безопасности</p>	<p>1. Анализ угроз безопасности информации включает:</p> <p>1 определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации</p>
---	---

	<p>2 оба ответа верны</p> <p>3 выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей</p>
<p>Уметь: разрабатывать модели угроз и выполнять анализ рисков информационной безопасности</p>	<p>1. В случае использования в значимом объекте КИИ сертифицированных на соответствие требованиям по безопасности информации средств защиты информации в значимых объектах КИИ 2 категории применяются средства защиты информации :</p> <p>1 не ниже 5 класса защиты, а также средства вычислительной техники не ниже 5 класса</p> <p>2 не ниже 4 класса защиты, а также средства вычислительной техники не ниже 5 класса</p> <p>3 не ниже 6 класса защиты, а также средства вычислительной техники не ниже 3 класса</p>

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 80*

*Описание характеристики выполнения знания: -*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: -*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 40*

*Описание характеристики выполнения знания: -*

*Оценка: 2*

*Описание характеристики выполнения знания: -*

# СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

## 5 семестр

**Форма промежуточной аттестации:** Зачет с оценкой

### Пример билета

1. Нормативно-правовые основы обеспечения информационной безопасности в Российской Федерации
2. Сети передачи данных

### Процедура проведения

Зачет по билетам

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

**1. Компетенция/Индикатор:** ИД-2<sub>ОПК-3</sub> Использует современные информационные системы в профессиональной сфере

### Вопросы, задания

1. Лицензирование деятельности по технической защите конфиденциальной информации
2. Комплексная система обеспечения информационной безопасности
3. Системы управления информационной безопасностью и обеспечения непрерывности бизнеса
4. Информационная безопасность и управление рисками
5. Особенности обеспечения информационной и компьютерной безопасности АСУ ТП

### Материалы для проверки остаточных знаний

1. Что обозначает «https://» в начале URL-адреса, а не «http://» (без буквы «s»)?

•

Ответы:

1. Ничего из вышперечисленного.
2. Информация, введенная на сайт, зашифрована.
3. Сайт недоступен для определенных компьютеров.
4. Сайт имеет особое высокое разрешение.

Верный ответ: Информация, введенная на сайт, зашифрована.

2. Какой из следующих паролей наиболее безопасный?

•

Ответы:

1. Android1234
2. Дата рождения или прочая личная информация (любимый фильм, имя домашнего животного)
3. 1qAz2wSx3eDc@
4. 123456qwerty

Верный ответ: 1qAz2wSx3eDc@

3. Что является примером телекоммуникационного преступления?

•

Ответы:

1. Руткит.
2. Ботнет.
3. DDOS-атака.
4. Ни одно из перечисленного.

Верный ответ: DDOS-атака.

4. Похищение цифровой личности это?

•

Ответы:

1. Выманивание денежных средств.
2. Ни одно из перечисленного.
3. Рассылка спама.
4. Неправомерное завладение профилем в социальной сети.

Верный ответ: Неправомерное завладение профилем в социальной сети.

5. Завершите предложение ниже. «Приносить с собой личное устройство обычно...»

•

Ответы:

1. ...более рискованно, чем использовать рабочие устройства
2. ...так же рискованно, как и использовать рабочие устройства
3. ...менее рискованно, чем использовать рабочие устройства

Верный ответ: ...более рискованно, чем использовать рабочие устройства

**2. Компетенция/Индикатор:** ИД-Зопк-3 Использует методы анализа опасностей и угроз, требования информационной безопасности и защиты государственной тайны

### Вопросы, задания

1. Нормативно-правовые основы обеспечения информационной безопасности в Российской Федерации
2. Особенности обеспечения информационной безопасности ПДн в ИСПДн организации
3. Защита информации конфиденциального характера с использованием шифровальных (криптографических) средств
4. Сети передачи данных
5. Криптографические протоколы

### Материалы для проверки остаточных знаний

1. Что из следующего является примером «фишинговой» атаки?

•

Ответы:

1. Все вышеперечисленное.

2. Создание поддельного веб-сайта, который выглядит почти идентично реальному веб-сайту, чтобы обманом заставить пользователей ввести свои данные для входа
3. Отправка кому-то электронного письма, содержащего вредоносную ссылку, замаскированную под письмо от знакомого человека
4. Отправка кому-либо текстового сообщения, содержащего вредоносную ссылку, замаскированную под уведомление о том, что этот человек выиграл в лотерею.

Верный ответ: Все вышеперечисленное.

2. Какой объект из перечисленных ниже с большей вероятностью станет жертвой кибератаки?

•

Ответы:

1. Малый бизнес
2. Крупный бизнес
3. Всё вышеперечисленное

Верный ответ: Малый бизнес

3. Что из перечисленного является самой большой угрозой кибербезопасности вашей организации?

•

Ответы:

1. Люди внутри организации
2. Люди за пределами организации
3. Всё вышеперечисленное

Верный ответ: Люди внутри организации

4. Если у пользователя включена служба VPN, то компьютер невозможно заразить или атаковать через Интернет? Выберите соответствующий вариант.

•

Ответы:

1. Верно
2. Неверно

Верный ответ: Неверно

5. Выберите утверждение, которое вы считаете наиболее точным.

•

Ответы:

1. Все сотрудники должны пройти обучение по обнаружению признаков кибератаки.
2. Конкретные сотрудники (например, ИТ-специалисты) должны пройти обучение по обнаружению признаков кибератаки.
3. Если на предприятии установлено хорошее антивирусное программное обеспечение, персоналу не нужно проходить обучение по обнаружению признаков кибератаки.

Верный ответ: Все сотрудники должны пройти обучение по обнаружению признаков кибератаки.



## **II. Описание шкалы оценивания**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 80*

*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: 65*

*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**

Среднее по промежуточной и итоговой