

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

**Направление подготовки/специальность: 10.03.01 Информационная безопасность**

**Наименование образовательной программы: Безопасность автоматизированных систем**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очная**

**Оценочные материалы  
по дисциплине  
Основы информационной безопасности**

**Москва  
2022**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель  
(должность)

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

(подпись)

С.В.  
Потехецкий  
(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной  
программы

(должность, ученая степень, ученое  
звание)

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

(подпись)

О.Р. Баронов  
(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 способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

ИД-2 Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства

2. ОПК-5 способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

ИД-1 Использует основы правовых знаний в различных сферах деятельности

3. ОПК-10 способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

ИД-1 Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Билеты (письменный опрос)

1. Тест № 3; Тест № 4 (Тестирование)
2. Тест №5 (Тестирование)
3. Тест №6 (Тестирование)

Форма реализации: Проверка задания

1. Тест № 1; Тест № 2 (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
Основные составляющие информационной безопасности					
1. Вводная лекция				+	

Тема 2. Основные положения системного подхода к обеспечению информационной безопасности.				+
Базовые основы защиты информации				
Организационно-правовое и кадровое обеспечение системы информационной безопасности	+	+	+	+
Финансово-экономическое обеспечение системы информационной безопасности		+		
Инженерно-техническое обеспечение системы информационной безопасности. Силы и средства		+		+
Программно-аппаратное обеспечение системы информационной безопасности. Силы и средства				+
Аудит системы информационной безопасности		+	+	
Вес КМ:	20	25	25	30

\$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	ИД-2 <sub>ОПК-1</sub> Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства	Знать: методы защиты информации от «утечки» по техническим каналам основные методы управления защитой информации национальные, межгосударственные и международные стандарты в области защиты информации Уметь: осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации конфигурировать аттестованную информационную систему и системы защиты	Тест №6 (Тестирование)

		информации информационной системы	
ОПК-5	ИД-1 <sub>ОПК-5</sub> Использует основы правовых знаний в различных сферах деятельности	Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации основные угрозы безопасности информации и модели нарушителя в автоматизированных системах нормативные правовые акты в области защиты информации Уметь: анализировать программные и программно-аппаратные решения при проектировании системы защиты информации, с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах определять подлежащие защите информационные ресурсы	Тест № 3; Тест № 4 (Тестирование) Тест №5 (Тестирование) Тест №6 (Тестирование)

		автоматизированных систем обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации	
ОПК-10	ИД-1 <sub>ОПК-10</sub> Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты	Знать: организационные меры по защите информации нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Уметь: реализовывать правила разграничения доступа персонала к объектам доступа классифицировать и	Тест № 1; Тест № 2 (Тестирование) Тест № 3; Тест № 4 (Тестирование) Тест №5 (Тестирование)

		оценивать угрозы безопасности информации применять нормативные документы по противодействию технической разведке	
--	--	---	--



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

### КМ-1. Тест № 1; Тест № 2

**Формы реализации:** Проверка задания

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 20

**Процедура проведения контрольного мероприятия:** Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

#### Краткое содержание задания:

Тест содержит вопросы **двух уровней сложности**. Вопросы повышенного уровня сложности отмечены звездочкой (\*).

Тест состоит из **20 или 40** вопросов. При этом как в вопросах, так и в ответах учтена возможность **многовариантности решений**.

Вопросы, предлагающие выбрать **все верные варианты ответа**, имеют от **2 до 4** правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.

Ответ на вопрос считается **правильным**, если он является **полным**.

#### Во время тестирования запрещается:

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;
- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

#### Контрольные вопросы/задания:

Уметь: применять нормативные документы по противодействию технической разведке	1.Модель угроз - это
Уметь: реализовывать правила разграничения доступа персонала к объектам доступа	1.Какой документ ФСТЭК необходимо применять при обосновании актуальных угроз безопасности информации 2.Какой международный стандарт описывает менеджмент рисков ИБ

#### 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. Тест № 3; Тест № 4

**Формы реализации:** Билеты (письменный опрос)

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

#### Краткое содержание задания:

Тест содержит вопросы **двух уровней сложности**. Вопросы повышенного уровня сложности отмечены звездочкой (\*).

Тест состоит из **20 или 40** вопросов. При этом как в вопросах, так и в ответах учтена возможность **многовариантности решений**.

Вопросы, предлагающие выбрать **все верные варианты ответа**, имеют от **2 до 4** правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.

Ответ на вопрос считается **правильным**, если он является **полным**.

**Во время тестирования запрещается:**

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;
- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

#### Контрольные вопросы/задания:

Знать: нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	1.Существуют следующие стратегии обработки риска
Знать: организационные меры по защите информации	1.Модель Шухарта-Деминга состоит из следующих этапов
Знать: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	1.Для поддержания уровня безопасности на должном уровне руководство обязано
Уметь: определять подлежащие защите информационные ресурсы автоматизированных систем	1.Политика информационной безопасности хозяйствующего субъекта
Уметь: классифицировать и оценивать угрозы безопасности информации	1.Понятие критических информационных инфраструктур (КИИ) РФ
Уметь: применять нормативные документы по противодействию технической разведке	1.Организации службы ИБ. Подразделение по ЗИ и его основные функции

**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. Тест №5**

**Формы реализации:** Билеты (письменный опрос)

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

**Краткое содержание задания:**

Тест содержит вопросы двух уровней сложности. Вопросы повышенного уровня сложности отмечены звездочкой (\*).

Тест состоит из 20 или 40 вопросов. При этом как в вопросах, так и в ответах учтена возможность многовариантности решений.

Вопросы, предлагающие выбрать все верные варианты ответа, имеют от 2 до 4 правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.

Ответ на вопрос считается правильным, если он является полным.

Во время тестирования запрещается:

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;
- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

**Контрольные вопросы/задания:**

Знать: нормативные правовые акты в области защиты информации	1.Предоставление информации - это
Знать: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	1.Информационная система- это
Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	1.Составляющими угрозы являются

Уметь: обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации	1.Количество категорий внутренних нарушителей, определяемых нормативными документами ФСТЭК
Уметь: применять нормативные документы по противодействию технической разведке	1.Реализация технического канала утечки информации может привести к нарушениям
Уметь: реализовывать правила разграничения доступа персонала к объектам доступа	1.В соответствии с требованиями 152-ФЗ «О персональных данных», оператор, являющийся юридическим лицом, назначает

#### **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. Тест №6**

**Формы реализации:** Билеты (письменный опрос)

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 30

**Процедура проведения контрольного мероприятия:** Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

#### **Краткое содержание задания:**

Тест содержит вопросы двух уровней сложности. Вопросы повышенного уровня сложности отмечены звездочкой (\*).

Тест состоит из 20 или 40 вопросов. При этом как в вопросах, так и в ответах учтена возможность многовариантности решений.

Вопросы, предлагающие выбрать все верные варианты ответа, имеют от 2 до 4 правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.

Ответ на вопрос считается правильным, если он является полным.

Во время тестирования запрещается:

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;

- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

### Контрольные вопросы/задания:

Знать: методы защиты информации от «утечки» по техническим каналам	1. Дайте определение понятию «информационная безопасность»
Знать: национальные, межгосударственные и международные стандарты в области защиты информации	1. По признаку отношений к природе возникновения угрозы классифицируются как
Знать: основные методы управления защитой информации	1. Сопrotивления заземляющих проводников, а также земляных шин должны быть
Уметь: конфигурировать аттестованную информационную систему и системы защиты информации информационной системы	1. К угрозам непосредственного доступа в операционную среду компьютера, реализуемым в ходе загрузки операционной системы, относятся
Уметь: осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации	1. Требования к защите персональных данных при их обработке в информационных системах персональных данных определяются
Уметь: анализировать программные и программно-аппаратные решения при проектировании системы защиты информации, с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах	1. Несанкционированный доступ к информации может быть осуществлен путём

### Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

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: 70

Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 3

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

# СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

## 1 семестр

**Форма промежуточной аттестации:** Экзамен

### Пример билета

Тестирование по варианту №1

1. Какой номер имеет основной (базовый) закон РФ в области ИБ?

1. 152
2. 63
3. 149
4. 187
5. 5

### Процедура проведения

Экзамен проводится в форме тестирования с ответами на 45 вопросов, из которых на 4 вопроса следует ответить письменно. Время на ответ-60 минут. После проведения проверки правильности ответов на вопросы тестирования, при необходимости задаются 1-2 устных вопроса.

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

**1. Компетенция/Индикатор:** ИД-2<sub>ОПК-1</sub> Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства

### Вопросы, задания

- 1.23. Главная цель СОИБ ХС - это
- 2.44. Реализация технического канала утечки информации может привести к нарушению

### Материалы для проверки остаточных знаний

- 1.4. Какого типа антивирусного ПО не существует?

Ответы:

1. Вакцины
2. Ревизоры
3. Детекторы
4. Доктора
5. Фаги
6. Все существуют

Верный ответ: 6

- 2.5. Какие методы антивирусной защиты относятся к проактивным?

Ответы:

1. Сигнатурные
2. Поведенческий блокиратор
3. Эвристические
4. 1-3
5. 1,3

Верный ответ: 4

**2. Компетенция/Индикатор:** ИД-1<sub>ОПК-5</sub> Использует основы правовых знаний в различных сферах деятельности

**Вопросы, задания**

- 1.16. Средства охранного телевидения обеспечивают функционирование этой подсистемы
- 2.17. Одним из основных условий успешности реализации угроз доступа к ресурсам и сервисам компьютера является

**Материалы для проверки остаточных знаний**

1.1. Какой номер имеет основной (базовый) закон РФ в области ИБ?

Ответы:

1. 152
2. 63
3. 149
4. 187
5. 5

Верный ответ: 3

2.3. Какими минимальными свойствами должна обладать компьютерная программа, чтобы называться вирусом?

Ответы:

1. Способностью проникать в компьютерные системы
2. Наносить вред компьютеру
3. Создавать свои копии
4. Сообщать о своём присутствии
5. 1,3
6. 1 - 4

Верный ответ: 1,3

**3. Компетенция/Индикатор:** ИД-1<sub>ОПК-10</sub> Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты

**Вопросы, задания**

- 1.19. Какой процесс не является основным информационным процессом?
- 2.20. Какая задача не свойственна для СОИБ организации?
- 3.21. Какой уровень декомпозиции сложных систем не предусматривается?

**Материалы для проверки остаточных знаний**

1.2. Какой вид тайны информации не является профессиональной?

Ответы:

1. Нотариальная
2. Коммерческая
3. Врачебная
4. Усыновления
5. Исповеди

Верный ответ: 2

**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 в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ», на основании семестровой и экзаменационной составляющих.