

**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 компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Оценочные материалы
по дисциплине
Основы информационной безопасности**

**Москва
2024**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Потехецкий С.В.
	Идентификатор	R83b30a44-PotekhetskySV-31b2130

С.В.
Потехецкий

СОГЛАСОВАНО:

Руководитель
образовательной
программы

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

О.Р.
Баронов

Заведующий
выпускающей кафедрой

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

А.Ю.
Невский

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ОПК-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-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах
ИД-1 Разрабатывает порядок и правила применения программно-аппаратных средств защиты информации в компьютерных системах
3. 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
4. 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 №6 (Тестирование)

Форма реализации: Проверка задания

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

БРС дисциплины

1 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15

Основные составляющие информационной безопасности				
Вводная лекция	+			+
Основные положения системного подхода к обеспечению информационной безопасности	+			+
Базовые основы защиты информации				
Тема 3. Организационно-правовое и кадровое обеспечение системы информационной безопасности	+	+	+	
Тема 4. Финансово-экономическое обеспечение системы информационной безопасности	+			
Тема 5. Инженерно-техническое обеспечение системы информационной безопасности		+	+	+
Тема 6. Программно-аппаратное обеспечение системы информационной безопасности		+		+
Тема 7. Аудит системы информационной безопасности	+			
Вес КМ:	20	20	35	25

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ОПК-1	ИД-2 _{ОПК-1} Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства	Знать: национальные, межгосударственные и международные стандарты в области защиты информации	Тест № 1; Тест № 2 (Тестирование) Тест №6 (Тестирование)
ОПК-1.1	ИД-1 _{ОПК-1.1} Разрабатывает порядок и правила применения программно-аппаратных средств защиты информации в компьютерных системах	Знать: нормативные правовые акты в области защиты информации Уметь: классифицировать и оценивать угрозы безопасности информации	Тест № 1; Тест № 2 (Тестирование) Тест №3, №4 (Тестирование) Тест №5 (Тестирование) Тест №6 (Тестирование)
ОПК-5	ИД-1 _{ОПК-5} Использует основы правовых знаний в различных сферах деятельности	Знать: методы защиты информации от «утечки» по техническим каналам Уметь: реализовывать правила разграничения доступа персонала к объектам доступа	Тест № 1; Тест № 2 (Тестирование) Тест №3, №4 (Тестирование) Тест №5 (Тестирование) Тест №6 (Тестирование)
ОПК-10	ИД-1 _{ОПК-10} Участвует в работах по реализации	Знать: руководящие и	Тест № 1; Тест № 2 (Тестирование)

	политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты	методические документы уполномоченных федеральных органов исполнительной власти по защите информации Уметь: 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:

Знать: национальные, межгосударственные и международные стандарты в области защиты информации	1.Человек как основное звено в системе обеспечения ИБ
Знать: нормативные правовые акты в области защиты информации	1.Какой международный стандарт описывает менеджмент рисков ИБ
Знать: методы защиты информации от «утечки» по техническим каналам	1.Понятие критических информационных инфраструктур (КИИ) РФ
Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	1.Понятие концепции и политики безопасности при обеспечении ЗИ
Уметь: применять нормативные документы по противодействию технической разведке	1.Модель угроз - это

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. Тест №3, №4

Формы реализации: Проверка задания

Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 20

Процедура проведения контрольного мероприятия: сего 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.Организации службы ИБ. Подразделение по ЗИ и его основные функции 2.Понятие критических информационных инфраструктур (КИИ) РФ
Знать: методы защиты информации от «утечки» по техническим каналам	1.Существуют следующие стратегии обработки риска 2.Модель Шухарта-Деминга состоит из следующих этапов 3.Политика информационной безопасности хозяйствующего субъекта
Уметь: классифицировать и оценивать угрозы безопасности информации	1.Понятие критических информационных инфраструктур (КИИ) РФ

Уметь: реализовывать правила разграничения доступа персонала к объектам доступа	1. Политика информационной безопасности хозяйствующего субъекта
---	---

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. Тест №5

Формы реализации: Проверка задания

Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 35

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. Информационная система- это 2. Предоставление информации - это
Уметь: классифицировать и оценивать угрозы безопасности	1. В соответствии с требованиями 152-ФЗ «О персональных данных», оператор, являющийся

информации	юридическим лицом, назначает 2.Реализация технического канала утечки информации может привести к нарушениям
------------	--

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. Тест №6

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: национальные, межгосударственные и международные стандарты в области защиты информации	1.По признаку отношений к природе возникновения угрозы классифицируются как
Уметь: классифицировать и	1.Несанкционированный доступ к информации

оценивать угрозы безопасности информации	может быть осуществлён путём 2.Требования к защите персональных данных при их обработке в информационных системах персональных данных определяются
Уметь: реализовывать правила разграничения доступа персонала к объектам доступа	1.К угрозам непосредственного доступа в операционную среду компьютера, реализуемым в ходе загрузки операционной системы, относятся

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 70

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

Оценка: 4

Нижний порог выполнения задания в процентах: 60

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

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2

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

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

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_{ОПК-1} Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства

Вопросы, задания

- 1.1. Какой номер имеет основной (базовый) закон РФ в области ИБ?
- 2.43. Регулирование деятельности в сфере шифровальных (криптографических) средств осуществляет
- 3.45. Какой номер имеет ФЗ «О персональных данных»?

Материалы для проверки остаточных знаний

1. Какого типа антивирусного ПО не существует?

Ответы:

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

Верный ответ: 6

2. Компетенция/Индикатор: ИД-1_{ОПК-1.1} Разрабатывает порядок и правила применения программно-аппаратных средств защиты информации в компьютерных системах

Вопросы, задания

- 1.41. Источниками угроз безопасности информации являются
- 2.44. Реализация технического канала утечки информации может привести к нарушению

Материалы для проверки остаточных знаний

1. Какой вид тайны информации не является профессиональной?

Ответы:

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

Верный ответ: 2

3. Компетенция/Индикатор: ИД-1_{ОПК-5} Использует основы правовых знаний в различных сферах деятельности

Вопросы, задания

- 1.7. От чего не должны зависеть требования безопасности к информационной системе?
- 2.18. Какое из перечисленных не является программным средством защиты информации, встроенным в ОС?
- 3.42. Термин ОТСС в соответствии с нормативно - методическими документами ФСТЭК означает

Материалы для проверки остаточных знаний

1. Какие методы антивирусной защиты относятся к проактивным?

Ответы:

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

Верный ответ: 4

4. Компетенция/Индикатор: ИД-1_{ОПК-10} Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты

Вопросы, задания

- 1.17. Одним из основных условий успешности реализации угроз доступа к ресурсам и сервисам компьютера является
- 2.36. Какие средства не относятся к средствам организационной защиты информации?
- 3.39. Управление СОИБ ХС заключается в

Материалы для проверки остаточных знаний

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. 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

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

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