

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

Направление подготовки/специальность: 38.03.01 Экономика

**Наименование образовательной программы: Экономика и экономическая безопасность предприятия
(организации)**

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-31b213f

(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	Унижаев Н.В.
	Идентификатор	Rb43f42d6-UnizhayevNV-2454ef20

(подпись)

Н.В.
Унижаев
(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. ПК-4 Способность к организации и текущему контролю выполнения требований экономической безопасности на предприятии (организации)

ИД-1 Способен организовать мониторинг соблюдения требований информационной и экономической безопасности, выполнять сбор, анализ, систематизацию, оценку и интеграцию данных, необходимых, для решения профессиональных задач

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

5 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					
Организация учебного процесса на кафедре БИТ		+	+	+	
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	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
ПК-4	ИД-1ПК-4 Способен организовать мониторинг соблюдения требований информационной и экономической безопасности, выполнять сбор, анализ, систематизацию, оценку и интеграцию данных, необходимых, для решения профессиональных задач	Знать: теоретические основы обеспечения информационной безопасности на предприятии (в организации), а также в областях теории информации и системного анализа угрозы экономической и информационной безопасности организации Уметь: осуществлять мониторинг соблюдения требований информационной и экономической безопасности проводить оценку возможных угроз для организаций (предприятий) проводить оценку вероятности реализации	Тест № 1; Тест № 2 (Тестирование) Тест № 3; Тест № 4 (Тестирование) Тест №5 (Тестирование) Тест №6 (Тестирование)

		этих угроз и возможного ущерба от них	
--	--	--	--

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: угрозы экономической и информационной безопасности организации	1.Понятие концепции и политики безопасности при обеспечении ЗИ 2.Человек как основное звено в системе обеспечения ИБ 3.Понятие критических информационных инфраструктур (КИИ) РФ
Уметь: осуществлять мониторинг соблюдения требований информационной и экономической безопасности	1.Модель угроз - это
Уметь: проводить оценку возможных угроз для организаций (предприятий)	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: теоретические основы обеспечения информационной безопасности на предприятии (в организации), а также в областях теории информации и системного анализа	1. Модель Шухарта-Деминга состоит из следующих этапов 2. Для поддержания уровня безопасности на должном уровне руководство обязано
Знать: угрозы экономической и информационной безопасности организации	1. Существуют следующие стратегии обработки риска
Уметь: проводить оценку вероятности реализации этих угроз и возможного ущерба от них	1. Политика информационной безопасности хозяйствующего субъекта
Уметь: проводить оценку возможных угроз для организаций (предприятий)	1. Организации службы ИБ. Подразделение по ЗИ и его основные функции 2. 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

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: теоретические основы обеспечения информационной безопасности на предприятии (в организации), а также в областях теории информации и системного анализа	1. Информационная система- это
Знать: угрозы экономической и информационной безопасности организации	1. Составляющими угрозы являются 2. Предоставление информации - это
Уметь: осуществлять мониторинг соблюдения требований информационной и экономической безопасности	1. Реализация технического канала утечки информации может привести к нарушениям 2. Количество категорий внутренних нарушителей, определяемых нормативными документами ФСТЭК

Уметь: проводить оценку вероятности реализации этих угроз и возможного ущерба от них	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: теоретические основы обеспечения информационной безопасности на предприятии (в организации), а также в областях теории информации и системного анализа	1.Сопrotивления заземляющих проводников, а также земляных шин должны быть 2.По признаку отношений к природе возникновения угрозы классифицируются как 3.Дайте определение понятию “информационная безопасность”
Уметь: осуществлять	1.К угрозам непосредственного доступа в

мониторинг соблюдения требований информационной и экономической безопасности	операционную среду компьютера, реализуемым в ходе загрузки операционной системы, относятся
Уметь: проводить оценку возможных угроз для организаций (предприятий)	1. Несанкционированный доступ к информации может быть осуществлён путём 2. Требования к защите персональных данных при их обработке в информационных системах персональных данных определяются

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

5 семестр

Форма промежуточной аттестации: Зачет с оценкой

Пример билета

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

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

Процедура проведения

Зачёт проводится в форме тестирования с ответами на 20 вопросов. 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-1_{ПК-4} Способен организовать мониторинг соблюдения требований информационной и экономической безопасности, выполнять сбор, анализ, систематизацию, оценку и интеграцию данных, необходимых, для решения профессиональных задач

Вопросы, задания

- 1.1. Какой номер имеет основной (базовый) закон РФ в области ИБ?
- 2.2. Какие свойства информации определены моделью CIA?
- 3.3. Какой вид тайны информации не является профессиональной?
- 4.4. Какими минимальными свойствами должна обладать компьютерная программа, чтобы называться вирусом?
- 5.5. Какого типа антивирусного ПО не существует?
- 6.6. Какие методы антивирусной защиты относятся к проактивным?
- 7.7. От чего не должны зависеть требования безопасности к информационной системе?
- 8.8. Какого вида обеспечения СОИБ не предусматривается?
- 9.9. Главная цель СОИБ ХС - это
- 10.10. Дайте определение понятия «Информационная безопасность»
- 11.11. Какие требования к СОИБ, обусловленные характером информации, обрабатываемой в ИС, не предъявляются?
- 12.12. Какого уровня декомпозиции СОИБ не предполагается?
- 13.13. Какое действие не свойственно режиму конфиденциальности информации?
- 14.14. Какой гриф можно использовать для обозначения коммерческой тайны?
- 15.15. В формуле вычисления $ТСО = Пр + Кр1 + Кр2$, $Кр$ - это
- 16.16. Средства охранного телевидения обеспечивают функционирование этой подсистемы
- 17.17. Одним из основных условий успешности реализации угроз доступа к ресурсам и сервисам компьютера является

- 18.18. Какое из перечисленных не является программным средством защиты информации, встроенным в ОС?
19.19. Какой процесс не является основным информационным процессом?
20.20. Какая задача не свойственна для СОИБ организации?

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

- 2.2. Какой вид тайны информации не является профессиональной?

Ответы:

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

Верный ответ: 2

- 3.3. 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: 5

- 4.4. Какого типа антивирусного ПО не существует?

Ответы:

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

Верный ответ: 6

- 5.5. Какие методы антивирусной защиты относятся к проактивным?

Ответы:

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

Верный ответ: 4

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