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: Очно-заочная

Оценочные материалы
по дисциплине
Основы информационной безопасности

Москва
2021

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Власкин Д.Н. Идентификатор: R563fb3df-VlaskinDN-4d4341df	Д.Н. Власкин
(должность)	(подпись)	(расшифровка подписи)

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
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(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 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

2. ПК-10 способностью использовать для решения коммуникативных задач современные технические средства и информационные технологии

3. ОК-7 способностью к самоорганизации и самообразованию

4. ПСК-1 Способность оценивать экономическую целесообразность вырабатываемых и принимаемых управленческих решений в условиях жесткой конкуренции и существования угроз экономической безопасности предприятия (организации)

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. Инженерно-техническое обеспечение системы информационной безопасности (Тестирование)
2. Информационная безопасность и защита информации, основы системы информационной безопасности (Тестирование)
3. Организационно-правовое, кадровое и финансово-экономическое обеспечение системы информационной безопасности. (Тестирование)
4. Программно-аппаратное обеспечение системы информационной безопасности (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	16
Основные составляющие информационной безопасности					
Вводная лекция.		+	+		

Основы системы 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.			+	
Программно-аппаратное обеспечение системы информационной безопасности.			+	+
Аудит системы информационной безопасности.			+	
Вес КМ:	20	20	30	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	ОПК-1(Компетенция)	Знать: основные законодательные и нормативные документы, определяющие организацию и функционирование информационной безопасности объекта защиты и основы профессиональной этики по их выполнению физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	Информационная безопасность и защита информации, основы системы информационной безопасности (Тестирование)
ПК-10	ПК-10(Компетенция)	Знать: средства и систему обеспечения информационной безопасности объекта защиты информационные ресурсы, подлежащие защите, а	Информационная безопасность и защита информации, основы системы информационной безопасности (Тестирование) Организационно-правовое, кадровое и финансово-экономическое обеспечение системы информационной безопасности. (Тестирование)

		также основные угрозы и риски информационной безопасности объекта защиты	
ОК-7	ОК-7(Компетенция)	Знать: основы политики информационной безопасности и принципы управления при обеспечения информационной безопасности объекта защиты современное состояние и требования к информационной безопасности	Организационно-правовое, кадровое и финансово-экономическое обеспечение системы информационной безопасности. (Тестирование)
ПСК-1	ПСК-1(Компетенция)	Знать: научные и методические материалы обеспечения информационной безопасности объекта защиты Уметь: обосновывать мероприятия к обеспечению информационной безопасности объекта анализировать физические явления и процессы, применяемые для обеспечения информационной	Инженерно-техническое обеспечение системы информационной безопасности (Тестирование) Программно-аппаратное обеспечение системы информационной безопасности (Тестирование)

		безопасности объекта защиты	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Информационная безопасность и защита информации, основы системы информационной безопасности

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Решение тестов в объеме 30 вопросов в течение 60 мин. на компьютере.

Краткое содержание задания:
Выбрать правильный ответ.

Контрольные вопросы/задания:

Знать: основные законодательные и нормативные документы, определяющие организацию и функционирование информационной безопасности объекта защиты и основы профессиональной этики по их выполнению	1.**3. Безопасность информации – состояние защищенности информации, при котором обеспечены ее?** 1. Оперативность 2. Целостность 3. Достоверность 4. Доступность 5. Конфиденциальность 6. 2, 4, 5 7. 1, 3, 5
Знать: физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	1.**2. Управление доступом пользователя осуществляется?** 1. На уровне файлов 2. На уровне пользователя 3. На уровне каталогов 4. На уровне авторизации 5. 1, 2 6. 1, 3 7. 2, 4
Знать: информационные ресурсы, подлежащие защите, а также основные угрозы и риски информационной безопасности объекта защиты	1.**1. Что понимают под объектами защиты информации?** 1. Объекты организации 2. Информационный процесс 3. Носитель информации 4. 1, 3 5. 2, 3 6. 1, 3

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: 27-30 правильных ответов

Оценка: 4
Нижний порог выполнения задания в процентах: 77

Описание характеристики выполнения знания: 23-26 правильных ответов

Оценка: 3
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: 17-22 правильных ответов

КМ-2. Организационно-правовое, кадровое и финансово-экономическое обеспечение системы информационной безопасности.

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Решение тестов в объеме 30 вопросов в течение 60 мин. на компьютере.

Краткое содержание задания:
Выбрать правильный ответ.

Контрольные вопросы/задания:

Знать: средства и систему обеспечения информационной безопасности объекта защиты	1.**15 Что позволяет получить показатель ТСО?** 1. Цену совокупной стоимости владения системой ИБ 2. Объем расходной части от вложенных в ИБ средств 3. Оценку возможности возврата вложенных в обеспечение ИБ средств 4. 1, 3 5. 1, 2 6. 2, 3
Знать: основы политики информационной безопасности и принципы управления при обеспечения информационной безопасности объекта защиты	1.**4. К задачам ФЭО СИБ относится:** 1. Экономическая защита организации 2. Анализ и оценка эффективности затрат на информационную безопасность 3. Руководство и управление расчетами неблагоприятного исхода рисков 4. Финансовое обеспечение активов организации 5. Защита информации о финансовой деятельности организации 6. Предотвращение разглашения финансовой информации
Знать: современное состояние и требования к информационной безопасности	1.**1. Что не относится к Кодексу профессиональной этики специалиста в области информационной безопасности?** 1. Обеспечение объективной и качественной работы 2. Обеспечение конфиденциальности информации 3. Развитие собственных компетенций 4. Обеспечение прозрачности своей работы и результатов 5. Обеспечение спортивного образа жизни 6. Повышение осведомленности других специалистов 7. Ориентир на «лучшие этики»

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: 27-30 правильных ответов

Оценка: 4
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: 23-26 правильных ответов

Оценка: 3
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: 17-22 правильных ответов

КМ-3. Инженерно-техническое обеспечение системы информационной безопасности

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Решение тестов в объеме 30 вопросов в течение 60 мин. на компьютере

Краткое содержание задания:
Выбрать правильный ответ.

Контрольные вопросы/задания:

Знать: научные и методические материалы обеспечения информационной безопасности объекта защиты	1.**16. Средства охранного телевидения обеспечивают функционирование какой подсистемы?** 1. Предупреждения угроз 2. Обозначения угроз 3. Обнаружения угроз 4. Ликвидации угроз
Уметь: обосновывать мероприятия к обеспечению информационной безопасности объекта	1.**7. Не относится к способам защиты информации при применении программно-аппаратных и аппаратных межсетевых экранов?** 1. Защищенные VPN сети 2. Зашумление сети 3. Журналирование 4. Контроль доступа 5. Фильтрация портов 6. Ограничение/фильтрация содержания

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: 27-30 правильных ответов

Оценка: 4
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: 23-26 правильных ответов

Оценка: 3
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: 17-22 правильных ответов

КМ-4. Программно-аппаратное обеспечение системы информационной безопасности

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Решение тестов в объеме 30 вопросов в течение 60 мин. на компьютере.

Краткое содержание задания:
Выбрать правильный ответ.

Контрольные вопросы/задания:

Уметь: анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	1.**12. Комплексная система обеспечения безопасности беспроводных сетей включает?** 1. WPA2 = IEEE 502.1X + CCMP + EAP + MIC 2. WPA2 = IEEE 802.1X +QH + CM + MIC 3. WPA2 = IEEE 802.1X + CCMP + EAP + MIC 4. WPA2 = IEEE 802.1X +CH + QP + EAP 5. WPA2 = IEEE 609.1X + CCMP + EAP + MIC 6. WPA2 = IEEE 802.1X + CCMP + AS + AC

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: 27-30 правильных ответов

Оценка: 4
Нижний порог выполнения задания в процентах: 77
Описание характеристики выполнения знания: 23-26 правильных ответов

Оценка: 3
Нижний порог выполнения задания в процентах: 57
Описание характеристики выполнения знания: 17-22 правильных ответов

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

Билет № 1
1. Понятие информации. Категории информации и ее подразделы. Виды информации.
2. Оптимизация затрат на обеспечение системы обеспечения информационной безопасности с использованием методов математического моделирования.
3. Алгоритм создания пароля в BIOS на запуск компьютера.

Процедура проведения

1. Проверить готовность аудитории к проведению экзамена. 2. Проверить присутствие студентов перед началом экзамена. 3. Напомнить порядок проведения экзамена. Определить место для личных вещей студентов. 4. Разрешить студентам занять учебные места. На учебное место студенты имеют право принести только набор из тех ручек, линейку и корректор. 5. Выдать студентам по два стандартных листа и дать время на оформление номера группы, фамилии, имени и отчества полностью. 6. Установленным порядком студенты получают экзаменационные билеты, номера которых фиксируются в рабочей ведомости экзаменатора, записывают номер экзаменационного билета в выданные рабочие листы и приступают к письменным ответам на поставленные вопросы. 7. Время на проведение письменной части экзамена – 60 мин. При необходимости выйти из аудитории, студент сдает работу экзаменатору, а по возвращении получает обратно. Время отсутствия студента не более 5 мин. 8. По окончании установленного времени (или при досрочном окончании письменной работы) студент сдает экзаменатору экзаменационный билет, письменную работу и покидает аудиторию. Экзаменатор должен убедиться, что в сдаваемой работе указано: номер группы, фамилия, имя и отчество студента, номер полученного экзаменационного билета и после этого принять работу. 9. После сдачи письменной части экзамена студенты ожидают его результаты в указанном месте, а экзаменатор проверяет работы, исходя из расчета времени – не более 5 мин на работу.

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

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

Вопросы, задания

1.**Билет № 1**
1. Понятие информации. Категории информации и ее подразделы. Виды информации.
2. Оптимизация затрат на обеспечение системы обеспечения информационной безопасности с использованием методов математического моделирования.
3. Алгоритм создания пароля в BIOS на запуск компьютера.

Материалы для проверки остаточных знаний

1.**6. Какие методы антивирусной защиты относятся к проактивным?**

Ответы:
1. Сигнатурные
2. Поведенческий блокиратор
3. Эвристические

4. 1, 2, 3
5. 1, 3

Верный ответ: Ответ: 4

2. Компетенция/Индикатор: ПК-10(Компетенция)

Вопросы, задания

1.**Билет № 2**

1. Конфиденциальная информация. Виды конфиденциальной информации. Государственная тайна и ее сущность.
2. Инженерно-техническое обеспечение системы обеспечения информационной безопасности. Цель, задачи, мероприятия и структура.
3. Алгоритм создания пароля в UEFI на запуск компьютера.

Материалы для проверки остаточных знаний

1.**16. Средства охранного телевидения обеспечивают функционирование какой подсистемы?**

Ответы:

1. Предупреждения угроз
2. Обозначения угроз
3. Обнаружения угроз
4. Ликвидации угроз

Верный ответ: Ответ: 3

3. Компетенция/Индикатор: ОК-7(Компетенция)

Вопросы, задания

1.**Билет № 3**

1. Конфиденциальная информация. Виды конфиденциальной информации. Коммерческая тайна и ее сущность.
2. Инженерно-техническая защита территорий и помещений. Задачи, структура, средства
3. Алгоритм создания пароля на доступ в BIOS.

Материалы для проверки остаточных знаний

1.**15. Управление доступом пользователя осуществляется?**

Ответы:

1. На уровне файлов
2. На уровне пользователя
3. На уровне каталогов
4. На уровне авторизации
5. 1, 2
6. 1, 3
7. 2, 4

Верный ответ: Ответ: 6

4. Компетенция/Индикатор: ПСК-1(Компетенция)

Вопросы, задания

1.**Билет № 4**

1. Конфиденциальная информация. Виды конфиденциальной информации. Служебная тайна и ее сущность.
2. Подсистема предупреждения угроз инженерно-технической защиты территорий и помещений. Структура, средства.

3. Алгоритм создания пароля на доступ в UEFI

Материалы для проверки остаточных знаний

1.**12. Комплексная система обеспечения безопасности беспроводных сетей включает?**

Ответы:

1. WPA2 = IEEE 502.1X + CCMP + EAP + MIC
2. WPA2 = IEEE 802.1X +QH + CM + MIC
3. WPA2 = IEEE 802.1X + CCMP + EAP + MIC
4. WPA2 = IEEE 802.1X +CH + QP + EAP
5. WPA2 = IEEE 609.1X + CCMP + EAP + MIC
6. WPA2 = IEEE 802.1X + CCMP + AS + AC

Верный ответ: 3

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Если полностью раскрыта актуальность и суть вопроса, имеются схемы, ссылки на нормативную литературу, приведены практические примеры

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Если актуальность и суть вопроса раскрыты хорошо, имеющиеся схемы, ссылки на нормативную литературу, приведенные практические примеры раскрывают только общие положения

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Если актуальность и суть вопроса раскрыты слабо, имеющиеся схемы, ссылки на нормативную литературу, приведенные практические примеры не относятся к излагаемому вопросу

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. В приложение к диплому выносится оценка за 1 семестр