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: Очно-заочная

Оценочные материалы
по дисциплине
Система обеспечения информационной безопасности предприятия

Москва
2021

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Потехецкий С.В. Идентификатор: R83b30a44-PotekhetskySV-31b213(	С.В. Потехецкий
(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. ПК-1 Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации

ПК-1.2 Управляет защитой информации в автоматизированных системах

2. ПК-2 Готов к внедрению систем защиты информации автоматизированных систем

ПК-2.2 Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах

ПК-2.3 Внедряет организационные меры по защите информации в автоматизированных системах

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Тест 1 (Тестирование)
2. Тест 2 (Тестирование)
3. Тест 3 (Тестирование)
4. Тест 4 (Тестирование)

БРС дисциплины

10 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Основы организации и функционирования СОИБ предприятия					
Роль и место информационной безопасности в обеспечении комплексной безопасности хозяйствующего субъекта		+			
Система обеспечения информационной безопасности предприятия				+	
Перечень факторов, влияющих на организацию СОИБ предприятия		+			
Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия					
Правовые основы функционирования СОИБ предприятия		+	+	+	+
Организационные основы функционирования СОИБ предприятия					+

Кадровое обеспечение СОИБ предприятия			+	
Финансово-экономическое обеспечение функционирования СОИБ предприятия	+			
Инженерно-техническое обеспечение СОИБ				+
Программно-аппаратное обеспечение функционирования СОИБ предприятия			+	+
Подсистема аудита информационной системы предприятия			+	
Управление СОИБ предприятия	+	+	+	+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

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-1	ПК-1.2$_{ПК-1}$ Управляет защитой информации в автоматизированных системах	Знать: состав и перечень информационных активов предприятия, относящихся к защищаемой информации нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО Уметь: составить полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и средствам организовать	Тест 2 (Тестирование) Тест 3 (Тестирование) Тест 4 (Тестирование)

		технологический процесс защиты информационных активов предприятия в соответствии с принятыми в РФ правилами и нормами с применением системного анализа и системного подхода в предметной области дисциплины	
ПК-2	ПК-2.2$_{ПК-2}$ Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах	Знать: психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия Уметь: на практике применять способности научной организации работы коллектива исполнителей	Тест 1 (Тестирование) Тест 2 (Тестирование) Тест 3 (Тестирование) Тест 4 (Тестирование)

		на предприятии малого и среднего бизнеса в профессиональной деятельности применять системный подход к управлению информационной безопасностью предприятия	
ПК-2	ПК-2.3$_{ПК-2}$ Внедряет организационные меры по защите информации в автоматизированных системах	Знать: комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности теорию анализа и синтеза сложных организационно-иерархических систем Уметь: выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах	Тест 1 (Тестирование) Тест 2 (Тестирование) Тест 3 (Тестирование) Тест 4 (Тестирование)

		деятельности, в том числе и на объектах энергетики	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Тест 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Тест по теме : "Организация функционирования КСОИБ ХС на основе системного подхода" , с письменными ответами на поставленные вопросы, проверкой правильности ответов и проведением анализа правильности ответов на поставленные вопросы в тесте. Количество вопросов: 20 или 40. Время на ответ по каждому вопросу теста-1 минута.

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: комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия	1.Какой документ ФСТЭК необходимо применять при обосновании актуальных угроз безопасности информации
Знать: психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности	1.Понятие концепции и политики безопасности при обеспечении ЗИ 2.Человек как основное звено в системе обеспечения ИБ 3.Модель угроз - это 4.Какой международный стандарт описывает менеджмент рисков ИБ
Знать: теорию анализа и синтеза сложных организационно-иерархических систем	1.Понятие критических информационных инфраструктур (КИИ) РФ
Уметь: применять системный подход к управлению информационной безопасностью предприятия	1.Какой документ ФСТЭК необходимо применять при обосновании актуальных угроз безопасности информации

Уметь: правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики	1.Модель угроз - это 2.Какой документ ФСТЭК необходимо применять при обосновании актуальных угроз безопасности информации

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 2

Формы реализации: Письменная работа
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: состав и перечень информационных активов предприятия, относящихся к защищаемой информации	1.Модель Шухарта-Деминга состоит из следующих этапов 2.Для поддержания уровня безопасности на должном уровне руководство обязано
Знать: комплекс мер по	1.Существуют следующие стратегии обработки риска

менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия	
Уметь: правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики	1.Понятие критических информационных инфраструктур (КИИ) РФ

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 3

Формы реализации: Письменная работа
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 и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО	1.Информационная система- это
Знать: комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия	1.Составляющими угрозы являются
Знать: комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности	1.Информационная система- это
Уметь: составить полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и средствам	1.Количество категорий внутренних нарушителей, определяемых нормативными документами ФСТЭК
Уметь: выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса	1.Реализация технического канала утечки информации может привести к нарушениям
Уметь: правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики	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 4

Формы реализации: Письменная работа
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 и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО	1.Составляющими угрозы являются 2.Предоставление информации - это
Знать: состав и перечень информационных активов предприятия, относящихся к защищаемой информации	1.Информационная система- это
Уметь: организовать технологический процесс защиты информационных активов предприятия в соответствии с принятыми в РФ правилами и нормами с применением системного анализа и системного подхода в предметной области дисциплины	1.Количество категорий внутренних нарушителей, определяемых нормативными документами ФСТЭК
Уметь: на практике применять способности научной организации работы коллектива	1.В соответствии с требованиями 152-ФЗ «О персональных данных», оператор, являющийся юридическим лицом, назначает

исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности	
Уметь: выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса	1.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

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10 семестр

Форма промежуточной аттестации: Экзамен

Процедура проведения

Экзамен проводится в письменной форме. Время на ответ-60 минут. После проведения проверки правильности ответов на вопросы билетов, при необходимости задаются 1-2 устных вопроса.

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

1. Компетенция/Индикатор: ПК-1.2$_{ПК-1}$ Управляет защитой информации в автоматизированных системах

Вопросы, задания

1.Средства обнаружения и защиты технических каналов утечки информации
2.Назначение, понятие и общая характеристика программно-аппаратного обеспечения СОИБ хозяйствующего субъекта. Вертикальная и горизонтальная декомпозиция подсистемы
3.Определение и классификация информации. Ответственность за защиту информации при её обработке в ИС ХС
4.Структурная декомпозиция организационно-правового обеспечения СОИБ ХС
5.Назначение и роль организационно-правового обеспечения СОИБ ХС. Вертикальная и горизонтальная декомпозиция подсистемы

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

2. Компетенция/Индикатор: ПК-2.2$_{ПК-2}$ Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах

Вопросы, задания

1.Средства инженерно-технической защиты территории
2.Аудит ИБ: понятие, цель, требования руководящих документов к организации аудита. Вертикальная и горизонтальная декомпозиция подсистемы аудита ИБ ХС
3.Особенности работы с персоналом СОИБ
4.Методы выявления технических каналов утечки информации
5.Подсистема финансово-экономического обеспечения СОИБ хозяйствующего субъекта. Вертикальная и горизонтальная декомпозиция подсистемы

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.Какого типа антивирусного ПО не существует?

Ответы:

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

Верный ответ: 6

3. Компетенция/Индикатор: ПК-2.3$_{ПК-2}$ Внедряет организационные меры по защите информации в автоматизированных системах

Вопросы, задания

1.Определение системы. Суть системного подхода к обеспечению информационной безопасности хозяйствующего субъекта. Укрупнённая структура СОИБ.

2.Моделирование затрат на обеспечение ИБ с использованием весовых коэффициентов

3.Понятие декомпозиции системы. Вертикальная и горизонтальная декомпозиция СОИБ ХС: цель, назначение, порядок осуществления и содержание

4.Структурирование затрат на информационную безопасность ХС

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

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

III. Правила выставления итоговой оценки по курсу