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 хозяйствующего субъекта

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. ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

2. ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

3. ПК-14 способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности

4. ПСК-3 Способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности в том числе и на объектах энергетики, эксплуатирующих АСУ ТП

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

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

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
ОПК-7	ОПК-7(Компетенция)	Знать: комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО; Уметь: организовать технологический процесс защиты информационных активов предприятия в	Тест № 1; Тест № 2 (Тестирование) Тест № 3; Тест № 4 (Тестирование) Тест №5 (Тестирование) Тест №6 (Тестирование)

		соответствии с принятыми в РФ правилами и нормами с применением системного анализа и системного подхода в предметной области дисциплины	
ПК-4	ПК-4(Компетенция)	Знать: комплекс мер по 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 применять системный подход к управлению информационной безопасностью предприятия;	Тест № 1; Тест № 2 (Тестирование) Тест №5 (Тестирование) Тест №6 (Тестирование)
ПК-14	ПК-14(Компетенция)	Знать: психологические особенности работы в	Тест № 3; Тест № 4 (Тестирование) Тест №6 (Тестирование)

		коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности Уметь: на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности	
ПСК-3	ПСК-3(Компетенция)	Знать: теорию анализа и синтеза сложных организационно-иерархических систем состав и перечень информационных активов предприятия, относящихся к защищаемой информации; Уметь: составить полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и средствам; выполнять работы по	Тест № 3; Тест № 4 (Тестирование) Тест №5 (Тестирование)

		администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса.	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Тест № 1; 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: комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности	1.Понятие концепции и политики безопасности при обеспечении ЗИ
Знать: комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия	1.Понятие критических информационных инфраструктур (КИИ) РФ
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.Какой документ ФСТЭК необходимо применять при обосновании актуальных угроз безопасности информации 2.Какой международный стандарт описывает менеджмент рисков ИБ

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

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: 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: психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной	1.Существуют следующие стратегии обработки риска

этики в области информационной безопасности	
Знать: состав и перечень информационных активов предприятия, относящихся к защищаемой информации;	1.Для поддержания уровня безопасности на должном уровне руководство обязано
Знать: теорию анализа и синтеза сложных организационно-иерархических систем	1.Модель Шухарта-Деминга состоит из следующих этапов
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.Понятие критических информационных структур РФ
Уметь: выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса.	1.Политика информационной безопасности хозяйствующего субъекта
Уметь: составить полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и средствам;	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: 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: комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности	1.Предоставление информации - это
Знать: нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО;	1.Информационная система-это 2.Представление информации-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
Уметь: выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса.	1.Количество категорий внутренних нарушителей, определяемых нормативными документами ФСТЭК
Уметь: составить полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и средствам;	1.В соответствии с требованиями 152-ФЗ «О персональных данных», оператор, являющийся 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

КМ-4. Тест №6

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 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.Дайте определение понятию “информационная безопасность”
Знать: комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия	1.Сопротивления заземляющих проводников, а также земляных шин должны быть 2.Дайте определение понятию “безопасность информации”
Знать: психологические особенности работы в	1.По признаку отношений к природе возникновения угрозы классифицируются как

коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности	
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.Несанкционированный доступ к информации-это
Уметь: правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики	1.К угрозам непосредственного доступа в операционную среду компьютера, реализуемым в ходе загрузки операционной системы, относятся
Уметь: применять системный подход к управлению информационной безопасностью предприятия;	1.Несанкционированный доступ к информации может быть осуществлён путём
Уметь: на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности	1.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

10 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1. Какой номер имеет основной (базовый) закон РФ в области ИБ?
1. 152
2. 63
3. 149
4. 187

Процедура проведения

Проводится экзамен на основе письменного тестирования по 45 вопросам, из которых 5 вопросов должны быть изложены письменно. На ответы по экзамену даётся 60 минут. После проверки ответов выставляются оценки, при необходимости задаются дополнительные вопросы для ответа устно.

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

1. Компетенция/Индикатор: ОПК-7(Компетенция)

Вопросы, задания

1.Какой номер имеет ФЗ «О персональных данных»?
2.Какие свойства информации определены моделью CIA?
3.Какой вид тайны информации не является профессиональной?

Материалы для проверки остаточных знаний

1.В формуле вычисления ТСО = Пр + Кр1 + Кр2, Кр - это

Ответы:

1. Конечные ресурсы
2. Количественные риски
3. Косвенные расходы
4. Критериальные расчёты

Верный ответ: 3

2.Одним из основных условий успешности реализации угроз доступа к ресурсам и сервисам компьютера является

Ответы:

1.Удалённый доступ нарушителя к компьютеру
2.Физический доступ нарушителя к компьютеру
3.Наличие сетевого сканера
4.Физический доступ в помещение с компьютером

Верный ответ: 4

3.Средства охранного телевидения обеспечивают функционирование этой подсистемы

Ответы:

1. Предупреждения угроз
2. Обозначения угроз

3. Обнаружения угроз
4. Ликвидации угроз

Верный ответ: 3

4.Какой уровень декомпозиции сложных систем не предусматривается?

Ответы:

1. Элемент системы
2. Подсистема
3. Составная часть системы

Верный ответ: 3

2. Компетенция/Индикатор: ПК-4(Компетенция)

Вопросы, задания

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

2.Какого типа антивирусного ПО не существует?

Материалы для проверки остаточных знаний

1.Какое действие не свойственно режиму конфиденциальности информации?

Ответы:

1. Ограничение доступа к информации
2. Порядок введения и прекращения
3. Степень жёсткости
4. Последствия нарушения

Верный ответ: 3

2.Какое из перечисленных не является программным средством защиты информации, встроенным в ОС

Ответы:

1. Средства аутентификации
2. Средства анализа защищённости
3. Средства межсетевого экранирования
4. Средства резервного копирования
5. Средства аудита

Верный ответ: 2

3. Компетенция/Индикатор: ПК-14(Компетенция)

Вопросы, задания

1.Какие методы антивирусной защиты относятся к проактивным?

2.От чего не должны зависеть требования безопасности к информационной системе?

Материалы для проверки остаточных знаний

1.Какой процесс не является основным информационным процессом?

Ответы:

1. 1. Передача информации
2. 2. Хранение информации
3. 3. Уничтожение информации
4. 4. Передача информации
5. 5. Архивация информации
6. 6. Сбор информации
7. 7. Обработка информации
8. 8. Использование информации

Верный ответ: 5

2.Какая задача не свойственна для СОИБ организации

Ответы:

1. Обнаружение воздействия угроз
2. Ликвидация угроз
3. Ликвидация последствий воздействия угроз
4. Предупреждение угроз
5. Обнаружение угроз

Верный ответ: 2

4. Компетенция/Индикатор: ПСК-3(Компетенция)

Вопросы, задания

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

2.Какого вида обеспечения СОИБ не предусматривается?

3.Главная цель СОИБ ХС - это

Материалы для проверки остаточных знаний

1.Какой гриф можно использовать для обозначения коммерческой тайны?

Ответы:

1. Конфиденциально
2. Особо ценная информация
4. Строго конфиденциально
5. Все приведённые

Верный ответ: 5

2.Какого уровня декомпозиции СОИБ не предполагается?

Ответы:

1. Подсистема
2. Средства
3. Направление
4. Обеспечение
5. Силы

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