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 2 (Тестирование)
2. Тест 3 (Тестирование)
3. Тест 4 (Тестирование)
4. Тестирование (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
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	Тестирование (Тестирование) Тест 2 (Тестирование) Тест 3 (Тестирование) Тест 4 (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	Тестирование (Тестирование) Тест 3 (Тестирование) Тест 4 (Тестирование)
ПК-14	ПК-14(Компетенция)	Знать: психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной	Тестирование (Тестирование) Тест 2 (Тестирование) Тест 3 (Тестирование)

		безопасности Уметь: на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности применять системный подход к управлению информационной безопасностью предприятия;	
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: выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса составить полный перечень работы по классификации СОИБ	Тестирование (Тестирование) Тест 2 (Тестирование)

		организации по подсистемам, направлениям, силам и средствам;	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Тестирование

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.

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.Целостность системы -это 2.Организованность – сложное свойство систем, заключающееся в наличии
Знать: нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО	1.Компонент системы - это
Знать: комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия	1.Принадлежность системы-это

Знать: психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности	1.Подсистемы -это 2.Структурность системы
Знать: состав и перечень информационных активов предприятия, относящихся к защищаемой информации	1.Эмерджентность системы состоит
Знать: теорию анализа и синтеза сложных организационно-иерархических систем	1.Подсистемы одного уровня
Уметь: правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики	1.Какой процесс является обязательным для поддержания политики информационной безопасности в актуальном состоянии
Уметь: на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности	1.На основе теоретических знаний о СОИБ ХС и ее системном анализе разработать предложения по совершенствованию организации её функционирования
Уметь: применять системный подход к управлению информационной безопасностью предприятия;	1.Оценка риска - это
Уметь: выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса	1.Модель угроз - это 2.Макроуровень системы-это
Уметь: составить полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и средствам;	1.На основе теоретических знаний о СОИБ ХС и ее системном анализе разработать рекомендации по совершенствованию её структуры

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 100

Описание характеристики выполнения знания: Даны правильные ответы не менее чем на 90% вопросов теста, исключая вопросы, на которые студент должен дать свободный ответ. На все вопросы, предполагающие свободный ответ, студент дал правильный и полный ответ.

Оценка: 4

Нижний порог выполнения задания в процентах: 75

Описание характеристики выполнения знания: Даны правильные ответы не менее чем на 75% вопросов теста, исключая вопросы, на которые студент должен дать свободный ответ.

На все вопросы, предполагающие свободный ответ, студент дал правильный ответ, но допустил незначительные ошибки и не показал необходимой полноты.

Оценка: 3

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Даны правильные ответы не менее чем на 60% вопросов теста, исключая вопросы, на которые студент должен дать свободный ответ. На все вопросы, предполагающие свободный ответ, студент дал непротиворечивый ответ, или при ответе допустил значительные неточности и не показал полноты.

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: комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности	1.Существуют следующие стратегии обработки риска 2.Модель Шухарта-Деминга состоит из следующих этапов
Знать: нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО	1.Для поддержания уровня безопасности на должном уровне руководство обязано
Уметь: на практике применять способности научной организации работы коллектива	1.Силы финансово-экономического обеспечения

исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности	
Уметь: применять системный подход к управлению информационной безопасностью предприятия;	1.Понятие критических информационных инфраструктур (КИИ) 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 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: комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности	1.Информационная система- это 2.Информационная система- это
Знать: нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО	1.Предоставление 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: 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: правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики	1.Реализация технического канала утечки информации может привести к нарушениям
Уметь: на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности	1.Виды нарушителей по классификации ФСТЭК
Уметь: применять системный подход к управлению информационной безопасностью	1.В соответствии с требованиями 152-ФЗ «О персональных данных», оператор, являющийся юридическим лицом, назначает

предприятия;	

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: комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности	1.Составляющими угрозы являются 2.Информационная система- это
Знать: нормативные и организационно-распорядительные документы в	1.Представление информации-это

области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО	
Знать: комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия	1.КСОИБ -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

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ МЭИ	**Экзаменационный билет №1** Кафедра Информационной и экономической безопасности Дисциплина «КСОИБ ХС» **Инженерно-экономический институт**	*Утверждаю:* *Зав. каф. БИТ* *А.Ю.Невский* *Протокол №* *« » г.*
1.Определение системы обеспечения информационной безопасности хозяйствующего субъекта (СОИБ ХС). Сущность системного подхода к обеспечению СОИБ ХС. Укрупнённая структура СОИБ ХС 2. «Тест на проникновение». Понятие, порядок и основные требования к применению в процессе аудита		

Процедура проведения

Время на подготовку к сдаче экзамена-60 минут. Ответы на вопросы билета оформляются в письменном виде. В именованном файле в формате Word экзаменуемый пишет: номер билета, фамилию и инициалы; время получения билета; номер группы. Проводится запись первого вопроса и даётся письменный ответ, после чего осуществляется запись второго вопроса и ответ на него. После сдачи ответов проводится проверка ответов и, при необходимости, задаются дополнительные вопросы, на которые даётся ответ устно.

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

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

Вопросы, задания

1.Политика информационной безопасности на предприятии: понятие, цель, требования и основное содержание

2.Модель информационной системы предприятия с позиции безопасности: назначение, содержание, особенности разработки

Материалы для проверки остаточных знаний

1.СОИБ ХС должна иметь

Ответы:

Ответ на вопрос даётся в письменном виде

Верный ответ: Система обеспечения информационной безопасности, как и любая другая система, должна иметь определённые виды собственного обеспечения, опираясь на которые она способна выполнять свою целевую функцию

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

Вопросы, задания

1.Декомпозиция комплексной системы обеспечения информационной безопасности хозяйствующего субъекта

2.Назначение и роль организационно-правового обеспечения СОИБ хозяйствующего субъекта

3.Общая характеристика законодательства РФ в области обеспечения информационной безопасности

Материалы для проверки остаточных знаний

1.Общая характеристика системы обеспечения информационной безопасности хозяйствующего субъекта

Ответы:

Ответ на вопрос даётся в письменном виде

Верный ответ: СОИБ ХС состоит из ряда подсистем: 1. Подсистема организационно-правового обеспечения должна обеспечить: - формирование правового поля для выполнения мероприятий обеспечения информационной безопасности; - выполнение концептуальных разработок, а также практических ограничительных и режимных мероприятий по обеспечению информационной безопасности в интересах хозяйствующего субъекта. 2. Подсистема кадрового обеспечения должна базироваться на созданной системе подготовки специалистов в области информационной безопасности, иметь систему подбора специалистов, а также систему работы с сотрудниками. 3. Подсистема финансово-экономического обеспечения предназначена для использования результатов анализа финансово-экономической деятельности хозяйствующего субъекта с целью определения возможных масштабов финансирования деятельности по обеспечению информационной безопасности. Кроме этого, обеспечивает работы по моделированию и оценке затрат на обеспечение ИБ, а также по определению минимально достаточного уровня затрат, т.е. оптимизационные расчеты. 4. Подсистема инженерно-технического обеспечения охватывает совокупность работ по инженерно-техническому оборудованию элементов (объектов) информационной инфраструктуры хозяйствующего субъекта. Кроме этого, по обеспечению видеонаблюдения, противопожарной защиты на объектах, и защиты информации, в том числе и компьютерной, от утечек по различным каналам. 5. Подсистема программно-аппаратного обеспечения выполняет функции защиты информации в информационной системе, а также самих элементов информационной системы от различных угроз применением различных программных и программно-аппаратных решений. 6. Подсистема аудита информационной безопасности предназначена для обеспечения контроля и проверок качества функционирования всех подсистем и элементов СОИБ применением методик анализа рисков информационной безопасности, а также различных форм проведения проверок.

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

Вопросы, задания

1.Определение информации. Виды информации в зависимости от категории доступа. Ответственность за защиту информации при её обработке в ИС ХС

2.Понятие декомпозиции системы. Структура вертикальной и горизонтальной декомпозиции.

3.Комплексная система обеспечения информационной безопасности хозяйствующего субъекта. Определение, цели, требования и основы системного подхода к организации

Материалы для проверки остаточных знаний

1.Цель и задачи СОИБ ХС

Ответы:

Ответ на вопрос даётся в письменном виде

Верный ответ: Целью СОИБ является создание таких условий функционирования информационной системы хозяйствующего субъекта (ХС), при которых обеспечивается выполнение требований по конфиденциальности, доступности и целостности информации, принадлежащей ему. Задачи СОИБ: Предупреждение появления угроз информационной безопасности. Обнаружение появившихся угроз и предупреждение их воздействия на информационную систему хозяйствующего субъекта. Обнаружение воздействия угроз на информационную систему хозяйствующего субъекта и локализация этого воздействия. Ликвидация последствий воздействия угроз на информационную систему хозяйствующего субъекта

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

Вопросы, задания

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

2.Особенности обеспечения режима государственной, служебной и коммерческой тайны на предприятиях (в организациях) РФ

Материалы для проверки остаточных знаний

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

Ответы:

Ответ на вопрос даётся в письменном виде

Верный ответ: Система- (целое, составленное из частей, соединение) -множество элементов, находящихся в определённых отношениях и связях друг с другом, образующих определённую целостность, единство. Под системой обеспечения информационной безопасности (СОИБ) понимается функциональная подсистема системы комплексной безопасности хозяйствующего субъекта, объединяющая силы, средства и объекты защиты информации, организованные и функционирующие по правилам, установленным правовыми, организационно-распорядительными и нормативными документами по защите информации. СОИБ рассматривается как сложная организационно-иерархическая система с определенными видами обеспечения; - каждый вид обеспечения рассматривается в качестве подсистемы СОИБ и в свою очередь является сложной системой; - в каждой подсистеме СОИБ выделяются направления деятельности по обеспечению информационной безопасности в интересах хозяйствующего субъекта; - каждое направление деятельности по обеспечению информационной безопасности реализуется определенными силами (организации, подразделения, должностные лица); - конкретные задачи обеспечения информационной безопасности в интересах хозяйствующего субъекта решаются применением конкретных средств (методики, документы, компьютерные программы и др.).

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. В ответе допущено не более 10 % ошибок.

Оценка: 4

Нижний порог выполнения задания в процентах: 75

Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3
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

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих (экзамена, проводимого по билетам)