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: Организация и технология защиты информации

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Система обеспечения информационной безопасности предприятия

Москва
2024

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

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
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

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: Защита задания

1. Коллоквиум (Коллоквиум)

Форма реализации: Компьютерное задание

1. Организация функционирования СОИБ предприятия на основе системного подхода. (Тестирование)

Форма реализации: Письменная работа

1. Контрольная работа (Контрольная работа)
2. Тестирование (Тестирование)

БРС дисциплины

8 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 предприятия			+	
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. Понятие и цели управления.	+	+		
Вес КМ:	30	30	20	20

$Общая часть/Для промежуточной аттестации$

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: нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО; комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности; Уметь: организовать технологический процесс защиты информационных активов предприятия в	Контрольная работа (Контрольная работа) Организация функционирования СОИБ предприятия на основе системного подхода. (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: состав и перечень информационных активов предприятия, относящихся к защищаемой информации; теорию анализа и синтеза сложных организационной-иерархических систем; Уметь: провести полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и средствам; выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса;	Контрольная работа (Контрольная работа) Коллоквиум (Коллоквиум)
ПК-14	ПК-14(Компетенция)	Знать: комплекс мер по менеджменту информационной безопасности предприятия	Тестирование (Тестирование) Контрольная работа (Контрольная работа)

		на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия; Уметь: применять системный подход к управлению информационной безопасностью предприятия; правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики;	
ПСК-3	ПСК-3(Компетенция)	Знать: психологические особенности работы в 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	Тестирование (Тестирование)

		на предприятии малого и среднего бизнеса в профессиональной деятельности.	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Тестирование

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Выполняется по заданию из расчета 1 минута на один вопрос

Краткое содержание задания:
Необходимо правильно ответить на вопросы теста

Контрольные вопросы/задания:

Знать: комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия;	1.**Какого вида обеспечения СОИБ не предусматривается?** 1. Организационно-правовое; 2. Программно-аппаратное; 3. Кадровое; 4. Информационное; 5. Аудита ИБ.
Знать: психологичес	1.**Какого направления деятельности не предусмотрено в подсистеме организационно-правового обеспечения СОИБ предприятия?** 1. Физическое

кие особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности	2. Организационное 3. Лицензирование и сертификация 4. Правовое 2.**Что не включает в себя описание сложной системы?** 1. перечень элементов системы; 2. состояние среды функционирования 3. пространственное положение элементов; 4. стоимость элементов системы; 5. связи между элементами системы; 6. внутреннее состояние элементов
Уметь: правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности,	1.**Сформулируйте цель СОИБ:**_____ _____ _____ 2.**Для чего предназначена система обеспечения ИБ хозяйствующего субъекта** _____ _____

в том числе и на объектах энергетики;	
Уметь: на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности.	1.**Сформулируйте понятие «Декомпозиция системы»** _____ _____ _____

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны правильные ответы, свободные ответы полные

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Даны правильные ответы, свободные ответы в основном полные

Оценка: 3
Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Даны правильные ответы, свободные ответы не обладают полнотой

Оценка: 2
Описание характеристики выполнения знания: Нет оснований для оценивания "удовлетворительно"

КМ-2. Контрольная работа

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Выполняется по вариантам в течение 40 минут

Краткое содержание задания:
Письменная работа выполняется по вариантам

Контрольные вопросы/задания:

Знать: комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности;	1.Система обеспечения информационной безопасности предприятия как сложная организационно-иерархическая система.
Знать: нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО;	1.Политика ИБ как методологическая основа надежного функционирования предприятия
Знать: теорию анализа и синтеза сложных организационной-иерархических систем;	1.Функции руководства и подразделений хозяйствующего субъекта и службы защиты информации по обеспечению информационной безопасности..
Уметь: выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса;	1.Основные требования, предъявляемые к выбору методов и средств защиты, зависимость их от структуры предприятия, защищаемых элементов объектов, условий функционирования СОИБ предприятия.
Уметь: провести полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и средствам;	1.Порядок выбора структуры СОИБ, ее зависимость от объектов защиты, характера и условий функционирования предприятия 2.Сущность процессов управления СОИБ предприятия
Уметь: применять системный подход к управлению информационной безопасностью предприятия;	1.Оценка степени уязвимости информации в результате действий нарушителей различных категорий.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: На вопросы даны правильные ответы с указанной полнотой

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: На вопросы даны правильные ответы с указанной полнотой

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: На вопросы даны в целом правильные ответы с указанной полнотой. Имеют место неточности

Оценка: 2
Описание характеристики выполнения знания: Нет оснований оценки на "удовлетворительно"

КМ-3. Коллоквиум

Формы реализации: Защита задания
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Выступление по результатам выполненного задания

Краткое содержание задания:
Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности.

Контрольные вопросы/задания:

Знать: состав и перечень информационных активов предприятия, относящихся к защищаемой информации;	1.С какой целью осуществляется разработка модели ИС предприятия с позиции безопасности? 2.Какие сведения входят в разработанную модель? 3.Какие разделы присутствуют в модели? 4.Что представляет собой графическая часть модели?

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: На все вопросы даны достаточно полные, непротиворечивые и аргументированные ответы

Оценка: не зачтено
Описание характеристики выполнения знания: Нет оснований оценить работу как "зачтено"

КМ-4. Организация функционирования СОИБ предприятия на основе системного подхода.

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Тест по изученным материалам

Краткое содержание задания:

1. Какого направления деятельности не предусмотрено в подсистеме организационно-правового обеспечения СОИБ ХС?

1. Физическое
2. Организационное
3. Лицензирование и сертификация
4. Правовое

2. Какое средство защиты информации не относится к программно-аппаратным?

1. Антивирус;
2. Брандмауэр;
3. IDS/IPS - система
4. Резервное копирование
5. DLP- система
6. Repeater

3. Какое свойство информации из модели CIA не является обязательным?

1. Confidentiality;
2. Availability;
3. Integrity;
4. 1 и 2 варианты;
5. 2 и 3 варианты.

4. Сформулируйте цель СОИБ:

_____

5. Какое свойство информации не входит в модель CIA?

1. Достоверность
2. Доступность.
3. Конфиденциальность.
4. Целостность

6. Какого направления в кадровом обеспечении СОИБ не выделяется?

1. Лицензирование и сертификация
2. Подготовка
3. Подбор
4. Профессиональная этика

7. Какое направление деятельности не входит в подсистему инженерно-технического обеспечения ИБ?

1. инженерно-техническая защита территорий и помещений
2. обнаружение и защита технических каналов утечки информации
3. противопожарная защита объектов

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

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

9. Какая модель не используется в подсистеме финансово-экономического обеспечения СОИБ ХС?

1. DLP
2. ROI
3. BCP
4. TCO

10. Какого вида обеспечения СОИБ не предусматривается?

1. Организационно-правовое;
2. Программно-аппаратное;
3. Кадровое;
4. Информационное;
5. Аудита ИБ.

11. От чего не зависят требования безопасности информационной системы?

1. Назначение системы;
2. Тип возможных угроз безопасности;
3. Характер используемой информации;
4. Решение администратора

12. Для чего предназначена система обеспечения ИБ предприятия

_____
_____

13. В понятие «государственная тайна» входит информация о…деятельности

1. Контрразведывательной;
2. Разведывательной;
3. Военной;
4. Внешнеполитической;
5. Экономической;
6. Оперативно-розыскной;
7. 1 – 6;
8. 1-4 и 6.

Контрольные вопросы/задания:

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.Дать правильные ответы на практические вопросы теста

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

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: 70

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

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1. Определение СОИБ. Сущность системного подхода к обеспечению СОИБ. Укрупнённая структура СОИБ

2. Средства обнаружения и защиты технических каналов утечки информации

Процедура проведения

Выполняется в письменном виде по билетам в течение 50 минут

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

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

Вопросы, задания

1.**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №15**

1. Декомпозиция СОИБ: определение; порядок декомпозиции; структура вертикальной и горизонтальной декомпозиции СОИБ.

2. Политика информационной безопасности ХС: определение; назначение; цель: решаемые вопросы; порядок разработки

2.**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №18**

1. Цель, задачи СОИБ и перечень требований к системе.

2. Средства подсистемы обнаружения и защиты технических каналов утечки информации: назначение, состав, классификация, краткая характеристика и влияние средств защиты ТКУИ на обеспечение информационной безопасности

3.**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1**

1. Определение СОИБ. Сущность системного подхода к обеспечению СОИБ. Укрупнённая структура СОИБ

2. Средства обнаружения и защиты технических каналов утечки информации

Материалы для проверки остаточных знаний

1.Перечень основных задач подразделения ИБ предприятия:

Ответы:

Ответ дать в письменном виде в свободной форме структурированно.

Верный ответ: Перечень основных задач подразделения ИБ предприятия: определение круга лиц, имеющих доступ к конфиденциальной информации; определение участков сосредоточения конфиденциальных сведений; определение круга сторонних предприятий, на которых в силу производственных отношений возможен выход из-под контроля сведений конфиденциального характера; выявление круга лиц, не допущенных к конфиденциальной информации, но проявляющих повышенный интерес к таким сведениям; выявление круга предприятий, в том числе и иностранных, заинтересованных в овладении

охраняемыми сведениями; разработка системы защиты документов, содержащих сведения конфиденциального характера; определение уязвимых мест в технологии производственного цикла, несанкционированное изменение, в которой может привести к утрате качества выпускаемой продукции и нанести ущерб предприятию; определение мест на предприятии, несанкционированное посещение которых может привести к краже продукции и организация их охраны; определение и обоснование мер правовой, организационной и инженерно-технической защиты предприятия, персонала, продукции и информации; разработка необходимых мероприятий, направленных на совершенствование системы экономической, информационной и др. безопасности предприятия; внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения информационной безопасности; организация обучения сотрудников службы безопасности в соответствии с их функциональными обязанностями; изучение, анализ и оценка состояния информационной безопасности предприятия и разработка предложений и рекомендаций для их совершенствования; разработка технико-экономических обоснований, направленных на приобретение технических средств, получение консультации у специалистов, разработку необходимой документации в целях совершенствования системы информационной безопасности.

2.. Содержание организационных мероприятий ИБ на предприятии

Ответы:

Ответ дать в письменном виде в свободной форме структурированно.

Верный ответ: В перечень организационных мероприятий ИБ предприятия входят: Организация режима и охраны: - исключения возможности тайного проникновения на территорию предприятия и в помещения посторонних лиц; - обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; - создания отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; - контроль и соблюдение временного режима труда и пребывания персонала на территории предприятия; - организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей. 2. Организация работы с сотрудниками: - ознакомление с сотрудниками и их изучение (группы риска); - создание модели нарушителя (внешнего, внутреннего); - обучения сотрудников правилам работы с конфиденциальной информацией; - ознакомления с мерами ответственности за нарушения правил информационной безопасности. 3. Организация работы с документами: организация разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение. 4. Организация использования технических средств сбора, обработки, накопления, хранения и передачи конфиденциальной информации. 5. Организация работ по анализу внутренних и внешних угроз конфиденциальной информации, выработке мер по обеспечению ее защиты. 6. Организация работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

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

Вопросы, задания

1.**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №5**

1. Назначение и роль организационно-правового обеспечения СОИБ. Вертикальная и горизонтальная декомпозиция подсистемы

2. Выявление ТКУИ: определение ТКУИ; средства физического поиска каналов утечки информации; средства инструментального контроля каналов утечки информации

2.**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №3**

1. Структурная декомпозиция организационно-правового обеспечения СОИБ

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

3.**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №2**

1. Назначение, понятие и общая характеристика программно-аппаратного обеспечения СОИБ ХС. Вертикальная и горизонтальная декомпозиция подсистемы

2. Определение и классификация информации. Ответственность за защиту информации при её обработке в ИС ХС

Материалы для проверки остаточных знаний

1.Основы Политики информационной безопасности предприятия

Верный ответ: В международных стандартах Менеджмента ИБ (Серия 27000) понятие политика информационной безопасности (Security Policy) (синонимы, встречающиеся в литературе – политика режима ИБ, политика безопасности) является базовым. Понятие политика ИБ используется применительно для организации соответствующих мероприятий в интересах конкретного предприятия. Если понятие концепция где-то встречается, то только по отношению к целым государствам. При этом целью разработки политики ИБ является необходимость сформулировать задачи и обеспечить поддержку мероприятий в области ИБ со стороны руководства предприятия. При разработке документа, в котором изложена политика в области ИБ, его руководство должно поставить четкую цель и показать свою заинтересованность в вопросах ИБ предприятия и в распространении политики среди сотрудников. При этом указывается, что данный документ должен быть доступен всем сотрудникам, отвечающим за обеспечение режима ИБ и содержать следующие основные разделы: •определение ИБ; •причины, по которым ИБ имеет большое значение для организации; •цели и показатели ИБ, допускающие возможность измерения. Можно отметить еще одну особенность международного и зарубежных стандартов в области ИБ – отсутствие каких-либо формальных требований к политике ИБ. Этим подчеркивается значительная самостоятельность в формировании регламентирующих документов, объясняемый необходимостью учета различных условий функционирования конкретного предприятия.

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

Вопросы, задания

1.**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №16**

1. Общая характеристика инженерно-технического обеспечения СОИБ. Вертикальная и горизонтальная декомпозиция подсистемы.

2. Анализ и управление рисками ИБ: определение риска; анализ рисков; методы управления рисками

2.**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №20**

1. Вертикальная декомпозиция структуры законодательных и нормативно-правовых актов, ориентированных на правовое обеспечение в области ИБ

2. Политика информационной безопасности хозяйствующего субъекта: понятие, цель, требования и основное содержание, нормативное регулирование Политики

3.**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №22**

1. Системный подход к обеспечению СОИБ: понятие, цель СОИБ; система средств, приемов и способов обеспечения информационной безопасности

2. Организационные основы функционирования СОИБ: понятие, цель, силы и средства организационного обеспечения информационной безопасности ХС

Материалы для проверки остаточных знаний

1.Организационные основы функционирования СОИБ: понятие, цель, силы и средства организационного обеспечения информационной безопасности ХС

Ответы:

Ответ дать в письменном виде в свободной форме структурированно.

Верный ответ: Организационное обеспечение СОИБ ХС – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исклю-чающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и реализацию внутренних и внешних угроз. Организационное обеспечение призвано регламентировать на предприятии: - охрану; - режим функционирования; - работу с кадрами; - работу с документами; - порядок использования информационных технологий, технических средств сбора, обработки, накопления, хранения и передачи конфиденциальной информации, а также использования технических средств безопасности; - информационно-аналитическую деятельность по выявлению внутренних и внеш-них угроз производственной деятельности предприятия. Организационное обеспечение СОИБ ХС играет существенную роль в создании надежного механизма, реализующего функцию защиты конфиденциальной информации посредством применения организационных мероприятий. К основным организационным мероприятиям, которые исключали бы или, по крайней мере, сводили бы к минимуму возможность возникновения опасности для конфиденциальной информации предприятия, можно отнести следующие (рис.4.4): 1. Организация режима и охраны. Выполняется в целях: - исключения возможности тайного проникновения на территорию предприятия и в помещения посторонних лиц; - обеспечение удобства контроля прохода и перемещения сотрудников и посетите-лей; - создания отдельных производственных зон по степени конфиденциальности ра-бот с самостоятельными системами доступа; - контроль и соблюдение времени пребывания персонала на территории предприя-тия; - организация и поддержание надежного пропускного режима и контроля пропуска сотрудников и посетителей. 2. Организация работы с сотрудниками. Мероприятие предусматривает порядок организации подбора и расстановку персонала и проводится с целью: - ознакомления с сотрудниками и их изучения; - обучения сотрудников правилам работы с конфиденциальной информацией; - ознакомления с мерами ответственности за нарушения правил информационной безопасности. 3. Организация работы с документами, включая организацию разработки и исполь-зования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение. 4. Организация использования технических средств сбора, обработки, накопления, хранения и передачи конфиденциальной информации; 5. Организация работ по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты. 6. Организация работы по проведению систематического контроля за работой пер-сонала с конфиденциальной информацией, порядком учета, хранения и уничтожения до-кументов и технических носителей.

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

Вопросы, задания

1.**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №13**

1. Назначение и роль организационно-правового обеспечения СОИБ. Вертикальная и горизонтальная декомпозиция подсистемы 2. Модель информационной системы ХС с позиции безопасности: назначение, содержание, особенности разработки

2.**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №14**

1. Вертикальная и горизонтальная декомпозиция подсистемы кадрового обеспечения СОИБ

2. Система средств программно-аппаратной защиты информации. Понятие, перечень, назначение, примеры, общая характеристика.

3.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №9

1. Подсистема кадрового обеспечения СОИБ. Требования профессиональных стандартов по кадровому обеспечению СОИБ.

Материалы для проверки остаточных знаний

1.Особенности профессиональной этики специалиста в области информационной безопасности

Ответы:

Ответ дать в письменном виде в свободной форме структурированно.

Верный ответ: Обычно профессиональную этику обычно принято рассматривать как конкретизацию общих нравственно-этических норм к специфическим условиям того или иного вида деятельности. В последнее время стало заметным появление значительного интереса у руководителей бизнеса к использованию требований профессиональной этики в качестве дополнительного инструмента в кадровой работе. Большинство исследований, в частности [14], рассматривают проблемы этичности в контексте организации работ в компании по добыванию информации в интересах информационно-аналитической деятельности. Вместе с тем необходимо признать, что принадлежность сотрудника к конкретной области деятельности обязательно накладывает некоторые моральные и этические особенности на выполняемые им служебные обязанности. В настоящее время такие положения чаще всего объединяются в разрабатываемых в компаниях «Кодексах профессиональной этики». Подобные Кодексы раньше всего появились в области журналистики, поэтому данный опыт, как правило, берут за основу создания подобных документов. Необходимо упомянуть о том, что существуют значительные различия в подходах к формированию и в порядке следования нормам Кодексов, что выражается в существовании, например, нескольких десятков Кодексов профессиональной этики журналистов. Сейчас все чаще говорят о развитии Корпоративных кодексов профессиональной этики, принятие которых преследует две основные цели: - внешняя цель, определяющая нормы, которыми должны руководствоваться работники компании во взаимоотношениях с клиентами, инвесторами, партнерами, конкурентами и другими лицами; - внутренняя цель, которая определяет систему взаимоотношений между сотрудниками предприятия. Другими целями корпоративного кодекса являются: - формирование имиджа компании как солидного и надежного предприятия; - обеспечение сохранности коммерческой и служебной

тайны. Таким образом, говоря о профессиональной этике специалиста в области информационной безопасности, необходимо иметь в виду следующее: - специалист предприятия, работающий в области обеспечения информационной безопасности должен соответствовать общим качествам и следовать общим морально-этическим нормам, принятым для работы в этой, достаточно специфической предметной области. Эти требования могут быть приняты в качестве Кодекса профессиональной этики специалиста в области информационной безопасности; - специалист, работающий в области обеспечения информационной безопасности должен соответствовать некоторым корпоративным морально-этическим нормам, принятым в качестве Корпоративного кодекса профессиональной этики для сотрудников данного предприятия. Как бы ни относились специалисты к вопросу: «Что дает Кодекс для специалиста в области информационной безопасности и дает ли что-нибудь вообще?», все едины во мнении, что отрицательного в существовании подобных Кодексов и учете степени соответствия сотрудников их требованиям - нет. Целесообразным представляется реализация механизма общественной аттестации специалистов на соответствие нормам Кодекса. Результаты общественной аттестации могут быть оформлены в виде сертификатов, дипломов или других документов, и могут учитываться при приеме на работу, заключении договоров и в некоторых других случаях. Если такие подходы к анализу морально-этических норм в производстве будут общими, то этот механизм из красивой идеи превратится в эффективный инструмент управления персоналом и в средство, способствующее снижению уровня мошенничества в сфере деловых отношений.

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: На все вопросы билета даны правильные ответы с указанной полнотой

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: На все вопросы билета даны в целом правильные ответы с указанной полнотой

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: На все вопросы билета даны ответы с указанной полнотой, имеются ошибки и неточности

Оценка: 2
Описание характеристики выполнения знания: Нет оснований оценить работу "удовлетворительно"

III. Правила выставления итоговой оценки по курсу

Итоговая оценка выставляется в соответствии с алгоритмом системы БАРС из семестровой и экзаменационной составляющей