

**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  
2022**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

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

(подпись)

А.Ю.

Невский

(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной  
программы

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(расшифровка  
подписи)

Заведующий  
выпускающей кафедры

(должность, ученая степень, ученое  
звание)

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

(подпись)

А.Ю.

Невский

(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: Защита задания

1. Коллоквиум (Коллоквиум)

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
	Срок КМ:	4	8	12
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	40

\$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) Коллоквиум (Коллоквиум)

		соответствии с принятыми в РФ правилами и нормами с применением системного анализа и системного подхода в предметной области дисциплины	
ПК-4	ПК-4(Компетенция)	<p>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;</p>	<p>Контрольная работа (Контрольная работа)  Коллоквиум (Коллоквиум)</p>
ПК-14	ПК-14(Компетенция)	<p>Знать:  комплекс мер по менеджменту информационной безопасности предприятия</p>	<p>Тестирование (Тестирование)  Контрольная работа (Контрольная работа)</p>

		<p>на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия;</p> <p>Уметь:</p> <p>применять системный подход к управлению информационной безопасностью предприятия;</p> <p>правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики;</p>	
ПСК-3	ПСК-3(Компетенция)	<p>Знать:</p> <p>психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности</p> <p>Уметь:</p> <p>на практике применять способности научной организации работы коллектива исполнителей</p>	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 политической информационной безопасности и других локальных нормативных актов предприятия;	<b>1. Какого вида обеспечения СОИБ не предусматривается?</b> 1. Организационно-правовое; 2. Программно-аппаратное; 3. Кадровое; 4. Информационное; 5. Аудита ИБ.
Знать: психологичес	<b>1. Какого направления деятельности не предусмотрено в подсистеме организационно-правового обеспечения СОИБ предприятия?</b> 1. Физическое

<p>кие особенности работы в коллективах предприятий малого и среднего бизнеса а с учётом принципов профессиональной этики в области информационной безопасности</p>	<ol style="list-style-type: none"> <li>2. Организационное</li> <li>3. Лицензирование и сертификация</li> <li>4. Правовое</li> </ol> <p><b>2. Что не включает в себя описание сложной системы?</b></p> <ol style="list-style-type: none"> <li>1. перечень элементов системы;</li> <li>2. состояние среды функционирования</li> <li>3. пространственное положение элементов;</li> <li>4. стоимость элементов системы;</li> <li>5. связи между элементами системы;</li> <li>6. внутреннее состояние элементов</li> </ol>
<p>Уметь: правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности,</p>	<p><b>1. Сформулируйте цель СОИБ:</b> _____</p> <p>_____</p> <p><b>2. Для чего предназначена система обеспечения ИБ хозяйствующего субъекта</b></p> <p>_____</p> <p>_____</p>

<p>В том числе и на объектах энергетики;</p>	
<p>Уметь: на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности.</p>	<p><b>1.Сформулируйте понятие «Декомпозиция системы»</b></p> <hr/> <hr/> <hr/>

**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

## **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 организационно-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*

### **КМ-3. Коллоквиум**

**Формы реализации:** Защита задания

**Тип контрольного мероприятия:** Коллоквиум

**Вес контрольного мероприятия в БРС:** 40

**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?
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.Осуществите классификацию активов ИС предприятия, подлежащих защите 2.Классифицируйте активы по уровню конфиденциальности 3.Укажите проблемные элементы модели безопасности

#### **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"*

# 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

### *1. 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 международных 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, исключающей 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 внешних 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 посетителей; - создания отдельных производственных зон по степени конфиденциальности работ с самостоятельными системами доступа; - контроль и соблюдение времени пребывания персонала на территории предприятия; - 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 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 и 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.

#### 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*

## ***III. Правила выставления итоговой оценки по курсу***

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