

**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 компьютерных систем**

**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. ПК-1 Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации

ПК-1.2 Управляет защитой информации в автоматизированных системах

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

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

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

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Выполнение задания

1. Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности (Коллоквиум)

Форма реализации: Компьютерное задание

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

Форма реализации: Письменная работа

1. Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия (Контрольная работа)

2. Сущность и порядок реализации системного подхода к обеспечению информационной безопасности предприятия (организации) (Контрольная работа)

## 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 хозяйствующего субъекта.					+
Система обеспечения информационной безопасности предприятия.			+		
Перечень факторов, влияющих на организацию СОИБ предприятия				+	

Политика информационной безопасности.	+	+		
Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия				
Правовые основы функционирования СОИБ предприятия.	+	+		
Организационные основы функционирования СОИБ предприятия.	+			
Кадровое обеспечение СОИБ предприятия.		+		+
Финансово-экономическое обеспечение функционирования СОИБ предприятия.		+		
Инженерно-техническое обеспечение СОИБ.			+	
Программно-аппаратное обеспечение функционирования СОИБ предприятия.			+	
Подсистема аудита информационной системы предприятия.		+	+	
Управление СОИБ предприятия.			+	+
Вес КМ:	25	25	25	25

\$Общая часть/Для промежуточной аттестации\$

## СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

### *I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций*

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-1	ПК-1.2 <sub>ПК-1</sub> Управляет защитой информации в автоматизированных системах	<p>Знать:</p> <p>нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО;</p> <p>комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия</p> <p>Уметь:</p> <p>применять системный подход к управлению информационной</p>	<p>Сущность и порядок реализации системного подхода к обеспечению информационной безопасности предприятия (организации) (Контрольная работа)</p> <p>Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия (Контрольная работа)</p> <p>Организация функционирования СОИБ предприятия на основе системного подхода. (Тестирование)</p>

		<p>безопасностью предприятия;          правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики;</p>	
ПК-2	<p>ПК-2.2<sub>ПК-2</sub> Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах</p>	<p>Знать:          комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности;          Уметь:          применять комплексный подход к защите технологических процессов в АСУ ТП с применением инженерно-технических и программно-аппаратных решений;          организовать технологический процесс защиты информационных активов предприятия в соответствии с принятыми</p>	<p>Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия (Контрольная работа)          Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности (Коллоквиум)</p>

		в РФ правилами и нормами с применением системного анализа и системного подхода в предметной области дисциплины	
ПК-2	ПК-2.3 <sub>ПК-2</sub> Внедряет организационные меры по защите информации в автоматизированных системах	<p>Знать:</p> <p>методы и средства защиты систем управления технологическим оборудованием</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>осуществлять поиск, анализ, выбор и установку программных компонентов комплексной системы защиты технологической информации в АСУ ТП;</p> <p>на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности</p>	<p>Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия (Контрольная работа)</p> <p>Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности (Коллоквиум)</p> <p>Организация функционирования СОИБ предприятия на основе системного подхода. (Тестирование)</p>

## II. Содержание оценочных средств. Шкала и критерии оценивания

### КМ-1. Сущность и порядок реализации системного подхода к обеспечению информационной безопасности предприятия (организации)

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Выполняется письменно в течение 50 минут по вариантам

#### Краткое содержание задания:

Сущность и порядок реализации системного подхода к обеспечению информационной безопасности предприятия (организации) на примере:

1. Образовательная организация (высшего или среднего профессионального образования);
2. Лечебное (лечебно–профилактическое) учреждение;
3. Организация оптово-розничной торговли;
4. Логистическая организация (склад, база, терминал);
5. Строительная организация;
6. Научно-исследовательская организация;
7. Промышленное предприятие, выпускающее товары бытового назначения;
8. Оператор сотовой связи;
9. Туроператор;
10. Компания – разработчик программного обеспечения;
11. Интернет-магазин;
12. Компания – автоперевозчик;
13. Строительная компания;
14. Финансовая организация (банк);
15. Страховая компания.

#### Контрольные вопросы/задания:

Знать: нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО;	1. В чем заключается сущность системного подхода в обеспечении ИБ предприятия
Уметь: применять системный подход к управлению информационной безопасностью предприятия;	1. В чем заключается порядок реализации системного подхода в обеспечении ИБ предприятия

#### Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

*Описание характеристики выполнения знания:* задание выполнено правильно, имеет полноту и адекватность;

*Оценка:* 4

*Нижний порог выполнения задания в процентах:* 70

*Описание характеристики выполнения знания:* задание выполнено в целом правильно, не имеет достаточной полноты, но является адекватным;

*Оценка:* 3

*Нижний порог выполнения задания в процентах:* 50

*Описание характеристики выполнения знания:* в задании имеются отдельные неточности, оно не обладает полнотой и адекватность его сомнительна;

## **КМ-2. Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Контрольная работа выполняется в письменном виде в течение 50 минут по вариантам: 1. Организационное обеспечение СОИБ предприятия. 2. Правовое обеспечение СОИБ предприятия. 3. Кадровое обеспечение СОИБ предприятия. 4. Финансово-экономическое обеспечение СОИБ предприятия. 5. Инженерно-техническое обеспечение СОИБ предприятия. 6. Программно-аппаратное обеспечение СОИБ предприятия. 7. Подсистема аудита ИБ в СОИБ предприятия. 8. Подсистема менеджмента ИБ предприятия

### **Краткое содержание задания:**

Дать понятие, назначение, структуру и общую характеристику подсистемы СОИБ предприятия

### **Контрольные вопросы/задания:**

Знать: комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности;	1. Каково назначение подсистема СОИБ предприятия?
Знать: психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности	1. Что такое подсистема СОИБ предприятия?
Уметь: правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики;	1. Описать структуру подсистемы СОИБ предприятия

## **Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания: Задание выполнено правильно, и полно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Задание выполнено в основном правильно, но недостаточно полно*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: Задание выполнено, но есть неправильность, а также недостаточно полно*

## **КМ-3. Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности**

**Формы реализации:** Выполнение задания

**Тип контрольного мероприятия:** Коллоквиум

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Задание выполняется в письменном виде в соответствии с заданием к сроку, определенному преподавателем

### **Краткое содержание задания:**

*Выполнить:*

1. В должности сотрудника отдела ИТ энергетической компании провести анализ исходных данных и на их основе разработать «Модель информационной системы энергетической компании “НАЗВАНИЕ” с позиции информационной безопасности» в составе:

- структурной графической схемы ИС и поддерживающей ее инфраструктуры;
- пояснительной записки к графической схеме.

*Исходные данные для разработки:*

- организационная структура компании (информацию о структуре компании на официальном сайте энергетической компании. Недостающую информацию взять по согласованию с преподавателем);
- размещение СВТ и других элементов информационной системы компании - реальное, или смоделированное (по территориям, зданиям, помещениям);
- перечень информационных активов МАБиУ, подлежащих защите:
  - а) база персональных данных в электронной и бумажной форме;
  - б) база персональных данных сотрудников, используемых для их идентификации в системе контроля и управления доступом (с использованием смарт-карт);
  - г) видеоматериалы системы охранного телевидения;
  - д) платежные документы (в бухгалтерии) в электронной и бумажной форме;
  - е) образ официального сайта компании (на веб-сервере компании);
- перечень активов информационной системы компании по классам:

1. Средства вычислительной техники (СВТ):

- а) расположенные в службах компании (отдел кадров, бухгалтерия, отдел ИТ, служба охраны и др.);
- б) расположенные в филиалах компании (в соответствии с ее организационной структурой);
- в) расположенные в серверной;

д) сетевое оборудование, расположенное в серверной.

2. Информационные активы (см. перечень информационных активов компании, подлежащих защите).

3. Системное программное обеспечение (операционная система, версия).

4. Прикладное программное обеспечение:

а) для обеспечения деятельности служб компании: отдел кадров, бухгалтерия, отдел ИТ и др.)

б) для обеспечения деятельности администрации (в соответствии с организационной структурой);

в) для обеспечения механизмов защиты(межсетевое экранирование, резервное копирование, антивирусное и др.);

г) для обеспечения основных технологических процессов.

- технология обработки информации и задачи, решаемые в интересах:

а) функционирования основных служб компании (отдел кадров, бухгалтерия, отдел ИТ и др.);

б) основных технологических процессов компании.

*Примечание:*

1. Для структурной графической схемы ИС использовать графический редактор MS Visio, или текстовый редактор MS Word с библиотекой графических примитивов, таких как: сервер, рабочая станция, принтер, телефонная станция, телефон (факс), сетевые устройства (маршрутизатор, хаб, коммутатор), ксерокс, база (банк) данных, бумажный документ и др.

#### **Контрольные вопросы/задания:**

Знать: методы и средства защиты систем управления технологическим оборудованием	1.Наличие какой информации предполагается в 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.Какие формы представления информации в модели являются допустимыми и предпочтительными?
Уметь: применять комплексный подход к защите технологических процессов в АСУ ТП с применением инженерно-технических и программно-аппаратных решений;	1.Какими примитивами рекомендуется пользоваться при разработке модели?
Уметь: осуществлять поиск, анализ, выбор и установку программных компонентов комплексной системы защиты технологической информации в АСУ ТП;	1.Содержание мероприятий аудита информационной системы предприятия 2.Состав программно-аппаратных средств защиты информации, обеспечивающих выполнение требований согласно нормативных документов ФСТЭК

#### **Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания: Все разделы модели выполнены полно, правильно и непротиворечиво*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Все разделы модели выполнены правильно, непротиворечиво, однако с недостаточной полнотой*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: Разделы модели выполнены в основном правильно, имеет место недостаточная полнота и противоречия,*

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

**Формы реализации:** Компьютерное задание

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 25

**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 межсетевое 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:**

<p>Знать: комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия</p>	<p>1. Дать правильные ответы на теоретические вопросы теста</p>
<p>Уметь: на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности</p>	<p>1. Дать правильные ответы на практические вопросы теста</p>

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания:*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания:*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания:*

# СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

<b>НИУ МЭИ</b>	<b>ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1</b> Кафедра <i>Безопасности и информационных технологий</i> Дисциплина «Система обеспечения информационной безопасности ХС»	<i>Утверждаю: Зав. каф. БИТ А.Ю.Невский Протокол № 6 « 19 » мая 2021г.</i>
1. Определение СОИБ. Сущность системного подхода к обеспечению СОИБ. Укрупнённая структура СОИБ		
2. Средства обнаружения и защиты технических каналов утечки информации		

## Процедура проведения

Экзамен выполняется в письменном виде по билетам за время не менее 50 минут

### *1. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины*

**1. Компетенция/Индикатор:** ПК-1.2ПК-1 Управляет защитой информации в автоматизированных системах

### **Вопросы, задания**

- 1.1. Вертикальная и горизонтальная декомпозиция подсистемы кадрового обеспечения СОИБ
2. Система средств программно-аппаратной защиты информации. Понятие, перечень, назначение, примеры, общая характеристика.
  - 2.1. Определение СОИБ. Сущность системного подхода к обеспечению СОИБ. Укрупнённая структура СОИБ
  2. Средства обнаружения и защиты технических каналов утечки информации
  - 3.1. Подсистема финансово-экономического обеспечения СОИБ хозяйствующего субъекта. Вертикальная и горизонтальная декомпозиция подсистемы
  2. Система средств программно-аппаратной защиты информации. Понятие, перечень, назначение, примеры, общая характеристика.

### **Материалы для проверки остаточных знаний**

**1. Какого вида обеспечения СОИБ не предусматривается?**

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

Ответы:

Выбор правильного ответа из представленных вариантов

Верный ответ: 4 вариант

**2. Компетенция/Индикатор:** ПК-2.2<sub>ПК-2</sub> Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах

### **Вопросы, задания**

- 1.1. Общая характеристика инженерно-технического обеспечения СОИБ. Вертикальная и горизонтальная декомпозиция подсистемы.
2. Анализ и управление рисками ИБ: определение риска; анализ рисков; методы управления рисками
- 2.1. Структурная декомпозиция подсистемы организационно-правового обеспечения СОИБ
2. Средства защиты операционных систем и пользовательских приложений подсистемы программно-аппаратного обеспечения СОИБ: назначение; принципы функционирования; привести примеры для ОС семейства Windows

### **Материалы для проверки остаточных знаний**

**1. Какой уровень декомпозиции сложных систем (СОИБ) не предусматривается?**

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

Ответы:

Выбор правильного ответа из представленных вариантов

Верный ответ: 3 вариант

**3. Компетенция/Индикатор:** ПК-2.3<sub>ПК-2</sub> Внедряет организационные меры по защите информации в автоматизированных системах

### **Вопросы, задания**

- 1.1. 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
- 2.1. 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. Какие свойства информации определены моделью CIA?**

1. Достоверность
2. Целостность
3. Конфиденциальность
4. Доступность
5. 1-3
6. 2-4

Ответы:

Выбор правильного ответа из представленных вариантов

Верный ответ: 6 вариант

## **II. Описание шкалы оценивания**

Оценка: 5

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания: На все вопросы даны полные, правильные и аргументированные ответы*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: На все вопросы даны полные и правильные ответы. Могут быть допущены отдельные неточности и недостаточная аргументация.*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: На все вопросы даны ответы. Полнота и правильность ответов низкая, аргументация отсутствует.*

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

Итоговая оценка по курсу выставляется исходя из данных БАРС по семестровой и экзаменационной составляющей