Федеральное государственное автономное образовательное учреждение высшего образования
"Самарский государственный экономический университет"

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

Уровень высшего образования: бакалавриат

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль)подготовки: Прикладная информатика и защита информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очно-заочная

Год набора (приема на обучение): 2026

Срок получения образования: 4 года 6 месяца(-ев)

Объем: в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

г. Самара, 2026

Разработчики:
Не имеет Колотилина М. А.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Минобрнауки от 19.09.2017 № 922, с учетом трудовых функций профессиональных стандартов: "Специалист по информационным системам", утвержден приказом Минтруда России от 13.07.2023 № 586н; "Руководитель проектов в области информационных технологий", утвержден приказом Минтруда России от 27.04.2023 № 369н; "Системный аналитик", утвержден приказом Минтруда России от 27.04.2023 № 367н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Кафедра прикладной информатики	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Ермолина Л. В.	Рассмотрено	21.05.2026, № 9

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование теоретических знаний и практических навыков по организации и реализации технической защиты информации, включая применение инженерно-технических, аппаратных и программных средств для обеспечения безопасности объектов информатизации.

Задачи изучения дисциплины:

- Изучить методы и средства технической защиты информации (экраншрование, фильтрация, контроль целостности, защита от утечек по техническим каналам), классификацию технических каналов утечки и модели угроз.;
- Освоить методы и технологии защиты информации (системы контроля доступа, видеонаблюдение, охранная сигнализация, защита от НСД), а также методы оценки эффективности средств защиты.;
- Сформировать навыки проектирования систем технической защиты информации, выбора и настройки средств защиты, проведения аттестации объектов информатизации и документирования результатов..

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-2 Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС

ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС

Знать:

ПК-2.2/Зн1 Методы и средства технической защиты информации (системы контроля доступа, видеонаблюдение, охранная сигнализация, защита от НСД, средства обнаружения утечек по техническим каналам), признаки технических инцидентов ИБ (несанкционированный доступ, нарушение целостности, воздействие на технические средства), процедуры реагирования на инциденты с использованием технических средств защиты.

Уметь:

ПК-2.2/Ум1 Выявлять технические инциденты ИБ по показаниям средств мониторинга и контроля доступа, оперативно применять технические средства защиты для локализации угроз (блокировка доступа, изоляция сегментов, отключение устройств), фиксировать и документировать инциденты с использованием технических средств аудита.

Владеть:

ПК-2.2/Нв1 Навыками работы с техническими средствами защиты информации (СКУД, видеонаблюдение, системы обнаружения вторжений), методами оперативного реагирования на инциденты с применением технических мер, приемами сбора и сохранения цифровых доказательств с использованием технических средств, навыками составления актов и отчётов по результатам расследования инцидентов.

ПК-4 Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений

ПК-4.2 Сопровождает разработанные проектные решения и требования к ИС

Знать:

ПК-4.2/Зн1 Методологии выявления требований к технической защите информации, нормативно-правовую базу (приказы ФСТЭК, ГОСТы, СНиПы по инженерно-технической защите), классификацию технических каналов утечки, принципы проектирования систем технической защиты (СКУД, видеонаблюдение, охранная сигнализация, защита от НСД), методы оценки эффективности СЗИ и критерии аттестации объектов информатизации.

Уметь:

ПК-4.2/Ум1 Применять методы системного анализа для выявления требований к технической защите, разрабатывать концептуальные и логические модели систем технической защиты (схемы размещения СКУД, видеонаблюдения, разграничения доступа), актуализировать проектные решения при изменении угроз, состава оборудования или нормативных требований, обосновывать выбор технических средств защиты для объектов информатизации.

Владеть:

ПК-4.2/Нв1 Навыками формирования технического задания с разделом требований к технической защите информации, методами проектирования и сопровождения систем технической защиты (расчёт периметра, выбор оборудования, схемы размещения), приёмами верификации проектных решений, методиками согласования требований к технической защите с заинтересованными сторонами и документирования результатов проектирования и сопровождения.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Техническая защита информации» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 7.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

Компетенция	Предшествующие дисциплины	Последующие дисциплины
ПК-2 - Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС		
ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС	Безопасность Web-приложений, Безопасность мобильных приложений, Криптографическая защита информации, Методы и средства защиты информации, Организационная защита информации, Правовая защита информации, Программно-аппаратная защита информации, Производственная практика: технологическая (проектно-технологическая) практика, Теория информационной безопасности и методология защиты информации, Учебная практика: технологическая (проектно-технологическая) практика	Безопасность Web-приложений, Безопасность мобильных приложений, Выполнение и защита выпускной квалификационной работы, Организационная защита информации, Программно-аппаратная защита информации, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика
ПК-4 - Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений		

ПК-4.2 Сопровождает разработанные проектные решения и требования к ИС	Информационно-коммуникационные технологии в профессиональной деятельности, Криптографическая защита информации, Нейросетевые технологии в социальных медиа, Облачные технологии и услуги, Основы проектной деятельности, Проектирование и реализация баз данных, Производственная практика: технологическая (проектно-технологическая) практика, Технологии защищенного документооборота, Учебная практика: технологическая (проектно-технологическая) практика	Выполнение и защита выпускной квалификационной работы, Проектирование и реализация баз данных, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Технологии защищенного документооборота, Управление информационными проектами реализации комплексной безопасности

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Лекционные занятия (часы)	Практические занятия (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Седьмой семестр	108	3	8	4	4	0,15	81,85	Зачет
Всего	108	3	8	4	4	0,15	81,85	18

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа
Раздел 1. Техническая защита информации	**90**	**4**	**4**	**81,85**

Тема 1.1. Введение в техническую защиту информации: основные понятия и определения (техническая защита, объект информатизации, технические каналы утечки, средства защиты); классификация технических каналов утечки информации (электромагнитные, акустические, виброакустические, оптические, через побочные излучения); обзор технических средств защиты информации (СКУД, видеонаблюдение, охранная сигнализация, системы контроля доступа, экранирование, фильтрация, заземление); нормативно-правовая база (приказы ФСТЭК, ГОСТ Р 56545-2015, ГОСТ Р 56546-2015, СанПиН, СНиП); общая схема построения системы технической защиты информации на объекте информатизации.	44	2	2	40

Тема 1.2. Классификация и физическая природа технических каналов утечки информации: углублённое рассмотрение классификации технических каналов утечки информации (ТКУИ) по физической природе возникновения; каналы утечки акустической (речевой) информации: прямой акустический, виброакустический, акустоэлектрический (ВЧ-навязывание); каналы утечки за счёт побочных электромагнитных излучений и наводок (ПЭМИН): природа возникновения и виды; оптические и визуально-оптические каналы утечки; материально-вещественные каналы (хищение носителей, закладные устройства); физические основы образования опасных сигналов в технических средствах и системах (ОТСС и ВТСС); классификация средств технической разведки, используемых для перехвата информации по техническим каналам.	46	2	2	41,85

5.2. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестовое задание
Промежуточная аттестация	Зачет

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Техническая защита информации	Тестовое задание	Зачет

6. Оценочные материалы текущего контроля

1. Техническая защита информации Тестовое задание

№	Содержание вопроса	Компетен

п/п		Правильный ответ (ключ ответа)	ция
1	При обнаружении инцидента ИБ, связанного с несанкционированным доступом в серверную, какое техническое средство защиты должно быть применено в первую очередь для локализации инцидента? a) видеонаблюдение b) СКУД (блокировка доступа) c) охранная сигнализация d) система контроля целостности		ПК-2
	Ответ:	b	
2	Какой технический канал утечки информации наиболее вероятен при обнаружении инцидента ИБ, связанного с перехватом акустической (речевой) информации через стены? a) виброакустический канал b) электромагнитный канал c) оптический канал d) материально-вещественный канал		ПК-2
	Ответ:	a	
3	При принятии мер по устранению инцидента ИБ, вызванного утечкой информации по каналу ПЭМИН, какое техническое средство защиты должно быть применено? a) экранирование кабельных линий и помещений b) установка видеокамер c) установка охранной сигнализации d) настройка межсетевого экрана		ПК-2
	Ответ:	a	
4	Какой технический признак указывает на обнаружение инцидента ИБ, связанного с несанкционированным подключением к сети? a) мигание светодиода на сетевом коммутаторе b) появление неизвестного устройства в журнале DHCP-сервера c) изменение цвета корпуса сервера d) увеличение громкости системного динамика		ПК-2
	Ответ:	b	
5	При обнаружении инцидента ИБ, связанного с попыткой несанкционированного доступа через систему контроля доступа, какое действие должно быть выполнено в первую очередь при сопровождении ИС? a) увольнение сотрудника b) блокировка карты доступа и проверка журналов СКУД c) замена сервера d) перезагрузка системы видеонаблюдения		ПК-2
	Ответ:	b	
6	Установите соответствие между техническим средством защиты (1–3) и его назначением (A–C) при обнаружении инцидентов ИБ в рамках сопровождения ИС. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Тип инцидента ИБ / Техническая мера реагирования 1. Утечка по каналу ПЭМИН — A. Блокировка карты доступа и изъятие пропуска 2. Несанкционированный доступ в помещение — B. Экранирование кабелей и помещений, установка фильтров 3. Попытка подключения закладного устройства — C. Проверка с помощью нелинейного локатора и анализаторов спектра		ПК-2
	Ответ:	1-B, 2-A, 3-C	
7	Установите соответствие между стадией реагирования на инцидент ИБ (1–3) и её содержанием (A–C) при обнаружении инцидентов ИБ и принятии мер. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Стадия реагирования / Содержание стадии 1. Обнаружение и локализация — A. Установка дополнительного экранирования и фильтров 2. Устранение — B. Выявление источника утечки (например, закладного устройства) 3. Восстановление и анализ — C. Анализ причин, актуализация модели угроз и документации		ПК-2
	Ответ:	1-B, 2-A, 3-C	

<table>
<tr><td>8</td><td>Установите правильную последовательность действий при обнаружении инцидента ИБ, связанного с несанкционированным доступом, в рамках сопровождения ИС. Расположите буквы (A–D) в верном порядке.
A) Блокировка доступа через СКУД и отключение подозрительных устройств
B) Обнаружение аномалии (например, срабатывание охранной сигнализации)
C) Документирование инцидента и уведомление заинтересованных сторон
D) Проверка журналов СКУД и видеозаписей
Ответ: B → D → A → C</td><td>ПК-2</td></tr>
<tr><td>9</td><td>Установите правильную последовательность этапов проверки целостности информации при тестировании ИС для обнаружения инцидентов ИБ. Расположите буквы (A–D) в верном порядке.
A) Расчёт эталонных хеш-сумм для защищаемых файлов
B) Сравнение полученных хеш-сумм с эталонными
C) Обнаружение несоответствий и фиксация инцидента
D) Периодический перерасчёт хеш-сумм и проверка целостности
Ответ: A → D → B → C</td><td>ПК-2</td></tr>
<tr><td>10</td><td>Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения).
Назовите не менее двух технических признаков, указывающих на обнаружение инцидента ИБ, связанного с утечкой информации по каналу ПЭМИН.
Ответ: наличие высокочастотных излучений за пределами нормы, появление нехарактерных наводок на кабелях, сбои в работе соседнего оборудования, обнаружение неизвестных передающих устройств при анализе спектра.</td><td>ПК-2</td></tr>
<tr><td>11</td><td>Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения).
При обнаружении инцидента ИБ, связанного с несанкционированным доступом к серверному оборудованию, какие технические меры должны быть приняты в первую очередь?
Ответ: блокировка доступа через СКУД, отключение подозрительных устройств от сети, проверка журналов СКУД и видеонаблюдения, изъятие пропусков у подозреваемых сотрудников.</td><td>ПК-2</td></tr>
<tr><td>12</td><td>Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения).
Назовите не менее двух технических средств защиты информации, используемых для обнаружения инцидентов ИБ в акустическом канале.
Ответ: нелинейный локатор, анализатор акустического спектра, акустический заградитель, система виброакустического контроля.</td><td>ПК-2</td></tr>
<tr><td>13</td><td>Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения).
При обнаружении инцидента ИБ, связанного с нарушением целостности данных, какое техническое средство позволяет подтвердить факт изменения информации?
Ответ: система контроля целостности на основе хеш-сумм (например, SHA-256) или электронная подпись (ЭЦП).</td><td>ПК-2</td></tr>
<tr><td>14</td><td>Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения).
Назовите не менее двух мер по предотвращению инцидентов ИБ, связанных с техническими каналами утечки.
Ответ: экранирование помещений и кабелей, установка фильтров сетевого питания, использование СКУД и охранной сигнализации, проведение аттестации объектов информатизации.</td><td>ПК-2</td></tr>
<tr><td>15</td><td>становите соответствие между этапом проектирования ИС (1–3) и его содержанием (A–C) в области технической защиты информации при выявлении требований к Системе и сопровождении проектных решений. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C).
<table><tr><td>Этап проектирования</td><td>Содержание в области технической защиты</td></tr><tr><td>1. Выявление требований</td><td>A. Разработка схем размещения СКУД, видеонаблюдения, датчиков</td></tr><tr><td>2. Концептуально-логическое проектирование</td><td>B. Определение требований к СКУД, видеонаблюдению, экранированию, заземлению</td></tr><tr><td>3. Сопровождение проектных решений</td><td>C. Проверка работоспособности СЗИ, актуализация паспорта системы технической защиты</td></tr></table>Ответ: 1-B, 2-A, 3-C</td><td>ПК-2</td></tr>
<tr><td>16</td><td>При выявлении требований к Системе, какие требования определяют необходимость установки СКУД, видеонаблюдения и охранной сигнализации?
a) функциональные требования
b) требования к технической защите информации
c) интерфейсные требования
d) требования к производительности
Ответ: b</td><td>ПК-4</td></tr>
</table>

17	На этапе концептуально-логического проектирования ИС, какая модель описывает защищаемые объекты и технические средства их защиты? a) ER-диаграмма b) схема системы технической защиты информации (размещение СКУД, видеокамер, датчиков) c) UML-диаграмма классов d) BPMN-диаграмма Ответ: b	ПК-4
18	При выявлении требований к Системе для объекта информатизации, какой нормативный документ является основным для определения требований к технической защите? a) 152-ФЗ «О персональных данных» b) приказы ФСТЭК России c) ISO 9001 d) ITIL Ответ: b	ПК-4
19	Что является результатом этапа выявления требований к технической защите для ИС? a) исходный код приложения b) техническое задание с разделом требований к технической защите информации c) маркетинговый план d) бизнес-план Ответ: b	ПК-4
20	При концептуально-логическом проектировании ИС, какие технические средства защиты должны быть учтены на этапе проектирования? a) только программные средства (антивирусы, межсетевые экраны) b) технические средства (СКУД, видеонаблюдение, охранная сигнализация, экранирование) c) только криптографические средства d) только организационные меры Ответ: b	ПК-4
21	Установите соответствие между этапом проектирования ИС (1–3) и его содержанием (A–C) в области технической защиты информации при выявлении требований к Системе и сопровождении проектных решений. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Этап проектирования / Содержание в области технической защиты 1. Выявление требований / A. Разработка схем размещения СКУД, видеонаблюдения, датчиков 2. Концептуально-логическое проектирование / B. Определение требований к СКУД, видеонаблюдению, экранированию, заземлению 3. Сопровождение проектных решений / C. Проверка работоспособности СЗИ, актуализация паспорта системы технической защиты Ответ: 1-B, 2-A, 3-C	ПК-4
22	Установите соответствие между нормативным документом (1–3) и его содержанием (A–C) при выявлении требований к Системе в области технической защиты. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Нормативный документ / Содержание требований 1. Приказы ФСТЭК России / A. Требования к аттестации объектов информатизации и защите от утечек по техническим каналам 2. ГОСТ Р 56545-2015 / B. Требования к защите персональных данных при их обработке в ИС 3. 152-ФЗ «О персональных данных» / C. Требования к защите информации в автоматизированных системах Ответ: 1-C, 2-A, 3-B	ПК-4
23	Установите соответствие между техническим средством защиты (1–3) и его назначением (A–C) при выявлении требований к Системе. В бланк ответов запишите последовательность (например, 1-C, 2-A, 3-B). Техническое средство / Назначение 1. СКУД / A. Контроль целостности и обнаружение изменений 2. Система контроля целостности / B. Блокировка несанкционированного доступа в помещения 3. Система видеонаблюдения / C. Фиксация и документирование событий на объекте	ПК-4

	Ответ:	1-B, 2-A, 3-C	
24	Установите правильную последовательность этапов выявления требований к технической защите для ИС. Расположите буквы (A–D) в верном порядке. A) Анализ нормативно-правовых требований к технической защите информации B) Определение перечня защищаемых объектов и технических каналов утечки C) Выбор технических средств защиты (СКУД, видеонаблюдение, экранирование) D) Формирование раздела требований к технической защите в ТЗ		ПК-4
	Ответ:	A → B → C → D	
25	Установите правильную последовательность действий при сопровождении проектных решений по технической защите информации при изменении требований. Расположите буквы (A–D) в верном порядке. A) Оценка влияния изменений на систему технической защиты B) Получение запроса на изменение (изменение требований, угроз, состава оборудования) C) Актуализация документации (паспорт СТЗ, схемы, инструкции) и повторное согласование D) Разработка плана внедрения изменений в систему технической защиты		ПК-4
	Ответ:	B → A → D → C	
26	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух методов выявления требований к технической защите для ИС.		ПК-4
	Ответ:	анализ нормативно-правовых документов (приказы ФСТЭК), проведение обследования объекта информатизации (выявление каналов утечки), анализ модели угроз, интервьюирование заинтересованных сторон.	
27	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Какой артефакт разрабатывается на этапе концептуально-логического проектирования в области технической защиты?		ПК-4
	Ответ:	схема системы технической защиты (размещение СКУД, видеокамер, датчиков, экранирования), паспорт системы технической защиты, перечень технических средств защиты.	
28	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Для чего используется паспорт системы технической защиты информации (СТЗИ) при сопровождении разработанных проектных решений?		ПК-4
	Ответ:	для документирования состава и характеристик СЗИ, фиксации результатов аттестации, контроля изменений и подтверждения соответствия требованиям.	
29	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух нормативных документов, требования которых должны быть выявлены при проектировании системы технической защиты информации.		ПК-4
	Ответ:	приказы ФСТЭК России, ГОСТ Р 56545-2015, ГОСТ Р 56546-2015, 152-ФЗ «О персональных данных».	
30	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Какой раздел технического задания должен быть обязательным при выявлении требований к Системе для объекта информатизации с точки зрения технической защиты?		ПК-4
	Ответ:	раздел «Требования к технической защите информации» (включая СКУД, видеонаблюдение, экранирование, заземление, фильтрацию, контроль целостности).	

7. Оценочные материалы промежуточной аттестации

Зачет седьмой семестр

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ, связанного с несанкционированным доступом к серверному оборудованию, какие технические меры должны быть приняты в первую очередь для локализации и документирования инцидента?		ПК-2
	Ответ:	блокировка доступа через СКУД, отключение подозрительных устройств от сети, проверка журналов СКУД и видеонаблюдения, изъятие пропусков у подозреваемых сотрудников, сохранение журналов событий для расследования.	
2	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух технических средств, используемых при обнаружении инцидентов ИБ в акустическом (речевом) канале утечки информации, и кратко опишите их назначение.		ПК-2
	Ответ:	нелинейный локатор (обнаружение электронных закладных устройств в выключенном состоянии), анализатор акустического спектра (выявление несанкционированных акустических излучений), акустический заградитель (активное подавление акустических сигналов).	
3	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ, связанного с попыткой несанкционированного доступа через систему контроля доступа (СКУД), какие действия должен выполнить специалист для проверки инцидента?		ПК-2
	Ответ:	проверить журналы СКУД (время, идентификатор карты, точка доступа), сопоставить с видеозаписями, идентифицировать нарушителя по базе пользователей, временно заблокировать подозрительную карту доступа, уведомить руководство и службу безопасности.	

4	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух технических признаков, указывающих на обнаружение инцидента ИБ, связанного с утечкой информации по каналу ПЭМИН (побочные электромагнитные излучения и наводки).		ПК-2
	Ответ:	наличие высокочастотных излучений за пределами нормы при анализе спектра, появление нехарактерных наводок на кабелях и линиях связи, сбои в работе соседнего оборудования, фиксация передающих устройств в запрещённых диапазонах частот.	
5	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При принятии мер по устранению инцидента ИБ, связанного с установкой закладного устройства в офисе, какие технические действия должны быть выполнены для полной ликвидации угрозы?		ПК-2
	Ответ:	отключение и изъятие подозрительного устройства, проведение проверки нелинейным локатором всех помещений, анализ электромагнитной обстановки с помощью анализатора спектра, усиление контроля доступа и пересмотр периметра безопасности, составление акта об обнаружении и изъятии.	
6	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При выявлении требований к Системе для объекта информатизации, какие исходные данные необходимо собрать для обоснования требований к технической защите информации?		ПК-4
	Ответ:	перечень защищаемой информации, модель угроз и нарушителя, классификацию объекта, категорию важности, технические характеристики помещений и оборудования, требования регуляторов (ФСТЭК, ФСБ).	
7	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). На этапе концептуально-логического проектирования ИС в области технической защиты, какие элементы должны быть отражены в схеме системы технической защиты информации (СТЗИ)?		ПК-4
	Ответ:	границы контролируемой зоны, места размещения СКУД (турникеты, двери, шлагбаумы), видеокамер с указанием зон обзора, датчики охранной сигнализации, точки экранирования и заземления, линии связи и кабельные трассы.	
8	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При сопровождении разработанных проектных решений по технической защите информации, какие документы необходимо актуализировать при изменении состава оборудования (например, замена видеокамер или добавление новых дверей с СКУД)?		ПК-4
	Ответ:	паспорт системы технической защиты информации, схему размещения СЗИ, инструкции по эксплуатации СЗИ, перечень технических средств защиты, документацию по аттестации объекта (при необходимости).	
9	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух методов выявления требований к технической защите для ИС, обрабатывающей персональные данные, и кратко опишите их суть.		ПК-4
	Ответ:	анализ нормативно-правовых требований (изучение приказов ФСТЭК, 152-ФЗ, ГОСТов для определения класса защиты), проведение обследования объекта (инструментальное выявление технических каналов утечки и оценка уязвимостей), моделирование угроз (построение модели угроз для объекта информатизации).	
10	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При сопровождении разработанных проектных решений по технической защите информации, какие действия необходимо выполнить при обнаружении нового технического канала утечки (например, через виброакустику)?		ПК-4
	Ответ:	провести оценку рисков и пересмотреть модель угроз, актуализировать требования к технической защите, разработать план внесения изменений (например, дополнительное экранирование, установка виброакустических датчиков), внести изменения в паспорт СТЗИ и проектную документацию, повторно провести аттестацию объекта при необходимости.	

7.1. Уровни овладения

Компетенция: ПК-2 Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС.

Индикатор достижения компетенции: ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100

Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Компетенция: ПК-4 Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений.

Индикатор достижения компетенции: ПК-4.2 Сопровождает разработанные проектные решения и требования к ИС.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Внуков, А. А. Защита информации в банковских системах: учебник для вузов / А. А. Внуков. - 2-е изд. - Москва: Юрайт, 2026. - 246 с - 978-5-534-01679-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/584051 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Внуков, А. А. Защита информации: учебник для вузов / А. А. Внуков. - 3-е изд. - Москва: Юрайт, 2026. - 161 с - 978-5-534-07248-8. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/584050 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Козырь, Н. С. Аудит информационной безопасности: учебник для вузов / Н. С. Козырь. - Москва: Юрайт, 2026. - 36 с - 978-5-534-20647-0. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/590419 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. - Москва: Юрайт, 2026. - 349 с - 978-5-534-19762-4. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/583858 (дата обращения: 21.05.2026). - Режим доступа: по подписке

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. https://lks.dap.gov.ru/ - Цифровая аналитическая платформа предоставления статистических данных» (ГИС ЦАП)

Ресурсы «Интернет»

1. https://stepik.org - Платформа с онлайн-курсами от авторов-практиков
2. https://fstec.ru/ - ФСТЭК России (fstec.ru): Основной регулятор в области технической защиты информации. На сайте публикуются приказы, методические документы, требования к аттестации объектов информатизации и защите от утечек по техническим каналам .
3. https://www.gosuslugi.ru/cybersecurity - Портал «Кибербезопасность – это просто» на Госуслугах: здесь можно изучить правила безопасного поведения в интернете, скачать полезные памятки и пройти тест на знание киберграмотности .
4. https://киберзож.рф/ - Сайт «КиберЗОЖ»: ресурс, где собраны главные полезные привычки для работы в интернете. Здесь можно узнать, какие пароли лучше не использовать, как определить фишинговое письмо и почему стоит подключить двухфакторную аутентификацию
5. https://прокачайскиллзащиты.рф/ - Сайт «Прокачай скилл защиты»: образовательный проект в игровой форме, который рассказывает о социальной инженерии, защите от вирусов и создании надежных паролей.

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

1. Консультант Плюс;
2. Мой офис;

Перечень информационно-справочных систем
(обновление выполняется еженедельно)

Не используется.

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ

Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения