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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ОРГАНИЗАЦИОННАЯ 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: 4 з.е.
в академических часах: 144 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 комплекса организационных мер, направленных на обеспечение защиты информации в организациях, включая правовые, административные и управленческие аспекты.

Задачи изучения дисциплины:

- Изучить нормативно-правовую базу защиты информации, принципы построения системы организационной защиты, классификацию угроз и методы управления доступом.;
- Освоить методы организации пропускного и внутриобъектового режимов, работы с персоналом и документацией, а также планирования и контроля мероприятий по защите информации.;
- Сформировать навыки разработки организационно-распорядительной документации (политики безопасности, инструкции, положения), проведения внутренних проверок и обучения персонала основам информационной безопасности..

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 Организационно-правовые основы защиты информации (152-ФЗ, КоАП, УК РФ), процедуры реагирования на инциденты ИБ, порядок документирования и уведомления регуляторов, классификацию инцидентов и признаки нарушения организационной защиты.

Уметь:

ПК-2.2/Ум1 Выявлять организационные причины инцидентов ИБ (нарушение режима, ошибки персонала, сбои в процессах управления доступом), оперативно принимать меры по локализации и устранению последствий (изоляция, отключение, уведомление), взаимодействовать с правоохранительными и регулирующими органами.

Владеть:

ПК-2.2/Нв1 Навыками проведения служебных расследований инцидентов ИБ, методами разработки и актуализации организационно-распорядительной документации (приказы, инструкции, положения), приемами анализа причин инцидентов и внедрения мер организационного характера для предотвращения повторения.

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

ПК-4.1 Выявляет требования к Системе и концептуально-логически проектирует ИС

Знать:

ПК-4.1/Зн1 Методологии выявления требований к организационной защите информации, нормативно-правовую базу (152-ФЗ, приказы ФСТЭК, ГОСТы), классификацию угроз и методы организационного управления доступом, принципы проектирования систем защиты на организационном уровне.

Уметь:

ПК-4.1/Ум1 Применять методы системного анализа для выявления требований к организационной защите, разрабатывать концептуальные модели организационной защиты (политики безопасности, организационные структуры, регламенты), выявлять организационные риски и противоречия в требованиях, обосновывать выбор организационных мер защиты.

Владеть:

ПК-4.1/Нв1 Навыками формирования технического задания с разделом требований к организационной защите информации, методами разработки организационно-распорядительной документации (положения, инструкции, приказы), приемами верификации организационных требований, методиками согласования требований с заинтересованными сторонами и документирования результатов.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Организационная 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, Правовая защита информации, Программно-аппаратная защита информации, Производственная практика: технологическая (проектно-технологическая) практика, Теория информационной безопасности и методология защиты информации, Техническая защита информации, Учебная практика: технологическая (проектно-технологическая) практика	Безопасность Web-приложений, Безопасность мобильных приложений, Выполнение и защита выпускной квалификационной работы, Программно-аппаратная защита информации, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Техническая защита информации
ПК-4 - Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений		

ПК-4.1 Выявляет требования к Системе и концептуально-логически проектирует ИС	Безопасность Web-приложений, Безопасность мобильных приложений, Встроенные языки программирования, Компьютерная экспертиза, Методы и средства защиты информации, Моделирование процессов и систем, Организация вычислительных процессов, Основы проектной деятельности, Проектирование и реализация баз данных, Производственная практика: технологическая (проектно-технологическая) практика, Системы искусственного интеллекта, 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, Интеллектуальные информационные системы, Компьютерная экспертиза, Проектирование и реализация баз данных, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Современные цифровые технологии управления предприятием, Специализированные ИТ в правоохранительной деятельности, Цифровая культура в профессиональной деятельности

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Групповая контактная работа (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Седьмой семестр	144	4	4	2	2	2	0,3	103,7	Экзамен
Всего	144	4	4	2	2	2	0,3	103,7	34

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лабораторные занятия	Лекционные занятия	Самостоятельная работа
Раздел 1. Организационная защита информации	**110**	**2**	**2**	**103,7**

Тема 1.1. Введение в организационную защиту информации: основные понятия и определения (организационная защита, политика безопасности, режим секретности, конфиденциальность); место организационной защиты в системе комплексной защиты информации; классификация организационных мер (правовые, административные, режимные, организационно-технические, работа с персоналом); нормативно-правовая база (152-ФЗ, 149-ФЗ, 273-ФЗ, УК РФ, КоАП РФ, приказы ФСТЭК и ФСБ); общая схема построения системы организационной защиты информации на предприятии.	110	2	2	103,7

5.2. Контрольные мероприятия по дисциплине

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

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

6. Оценочные материалы текущего контроля

1. Организационная защита информации Тестовое задание

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	При обнаружении инцидента ИБ в организации, какой организационный документ регламентирует действия персонала по реагированию? a) техническое задание на разработку ИС b) положение о реагировании на инциденты ИБ c) должностная инструкция системного администратора d) бизнес-план		ПК-2
	Ответ:	b	
2	При принятии мер по устранению инцидента ИБ, связанного с утечкой персональных данных, кто должен быть уведомлён в первую очередь согласно 152-ФЗ? a) все сотрудники организации b) Роскомнадзор (уполномоченный орган) и субъекты персональных данных c) служба безопасности организации d) разработчики ИС		ПК-2
	Ответ:	b	

3	Какой организационный документ определяет перечень сведений, составляющих коммерческую тайну предприятия при сопровождении ИС? a) трудовой договор b) перечень сведений, составляющих коммерческую тайну (утверждается руководителем) c) инструкция по делопроизводству d) политика обработки персональных данных Ответ: b	ПК-2
4	При обнаружении инцидента ИБ, связанного с нарушением внутриобъектового режима, какое организационное мероприятие должно быть проведено в первую очередь? a) увольнение сотрудника b) проведение служебного расследования c) переустановка операционной системы d) смена всех паролей Ответ: b	ПК-2
5	Какой организационный документ регламентирует порядок допуска сотрудников к работе с конфиденциальной информацией при сопровождении ИС? a) инструкция по охране труда b) положение о пропускном и внутриобъектовом режиме c) положение о защите персональных данных d) приказ о назначении ответственных Ответ: b	ПК-2
6	Установите соответствие между типом инцидента ИБ (1–3) и организационной мерой реагирования (A–C) при обнаружении инцидентов ИБ в организации. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Тип инцидента ИБ / Организационная мера реагирования 1. Утечка персональных данных / A. Проведение служебного расследования, отстранение сотрудника, уведомление регулятора 2. Нарушение пропускного режима / B. Ужесточение пропускного режима, пересмотр порядка допуска, проведение инструктажа 3. Вредоносное ПО (вирус) / C. Запуск антивирусного сканирования, изоляция заражённых узлов, обновление политик использования съёмных носителей Ответ: 1-A, 2-B, 3-C	ПК-2
7	Установите соответствие между видом организационно-распорядительного документа (1–3) и его назначением (A–C) при сопровождении ИС. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Документ / Назначение 1. Положение о защите персональных данных / A. Определение порядка пропуска сотрудников на территорию 2. Политика информационной безопасности / B. Определение стратегии и общих принципов защиты информации 3. Инструкция по пропускному режиму / C. Регламентация обработки и защиты персональных данных Ответ: 1-C, 2-B, 3-A	ПК-2
8	Установите соответствие между категорией сотрудника (1–3) и его уровнем доступа (A–C) в рамках организационной защиты информации. В бланк ответов запишите последовательность (например, 1-C, 2-A, 3-B). Категория сотрудника / Уровень доступа 1. Руководитель организации / A. Ограниченный доступ только к открытой информации 2. Системный администратор / B. Доступ ко всей конфиденциальной информации в рамках служебной необходимости 3. Технический персонал (уборщики, охрана) / C. Доступ к управленческой и стратегической информации Ответ: 1-C, 2-B, 3-A	ПК-2
9	Установите правильную последовательность действий при обнаружении инцидента ИБ в организации в рамках сопровождения ИС. Расположите буквы (A–D) в верном порядке. A) Проведение служебного расследования и установление причин B) Обнаружение инцидента (аномалия, сообщение от пользователя) C) Принятие организационных мер (отстранение сотрудников, уведомление регулятора) D) Документирование инцидента и разработка мер предотвращения Ответ: B → A → C → D	ПК-2

10	Установите правильную последовательность организационных мероприятий при допуске сотрудника к конфиденциальной информации. Расположите буквы (A–D) в верном порядке. A) Подписание соглашения о неразглашении (NDA) B) Проведение инструктажа по защите информации C) Определение уровня доступа в соответствии с должностью D) Оформление допуска (приказ, внесение в список)	ПК-2
	Ответ: B → C → A → D	
11	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух организационных мер, которые должны быть приняты при обнаружении инцидента ИБ, связанного с утечкой персональных данных.	ПК-2
	Ответ: проведение служебного расследования, уведомление Роскомнадзора и субъектов данных, отстранение виновных сотрудников, пересмотр политики доступа.	
12	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Какой организационный документ должен быть разработан для регламентации действий сотрудников при обнаружении инцидентов ИБ?	ПК-2
	Ответ: положение о реагировании на инциденты ИБ / инструкция по действиям при инцидентах.	
13	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух организационных мер по предотвращению инцидентов ИБ, связанных с человеческим фактором.	ПК-2
	Ответ: регулярное обучение и инструктаж персонала, подписание соглашений о неразглашении, внедрение системы контроля доступа, проведение внутренних проверок.	
14	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При принятии мер по устранению инцидента ИБ, какие организационные действия должны быть выполнены для восстановления доверия к системе?	ПК-2
	Ответ: информирование заинтересованных сторон (регулятора, клиентов), пересмотр политик безопасности, проведение аудита системы защиты, обучение персонала.	
15	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух нормативных актов, регламентирующих организационную защиту информации в РФ.	ПК-2
	Ответ: 152-ФЗ «О персональных данных», 149-ФЗ «Об информации…», УК РФ, КоАП РФ, приказы ФСТЭК.	
16	При выявлении требований к Системе, какие требования определяют необходимость организационных мер защиты (например, пропускной режим, инструктажи)? a) функциональные требования b) организационно-административные требования c) интерфейсные требования d) требования к производительности	ПК-4
	Ответ: b	
17	На этапе концептуально-логического проектирования ИС какая организационная модель описывает распределение ответственности за защиту информации? a) ER-диаграмма b) модель угроз c) организационная структура защиты информации (назначение ответственных) d) физическая модель данных	ПК-4
	Ответ: c	
18	При выявлении требований к Системе для ИС, обрабатывающей персональные данные, какие организационные требования являются обязательными? a) использование определённого языка программирования b) назначение ответственного за обработку персональных данных и разработка политики их защиты c) выбор цветовой схемы интерфейса d) использование только открытого ПО	ПК-4
	Ответ: b	
19	Что является результатом этапа выявления требований к организационной защите для ИС? a) исходный код приложения b) техническое задание с разделом организационных требований к защите информации c) маркетинговый план d) бизнес-план	ПК-4
	Ответ: b	
20	При концептуально-логическом проектировании ИС, какие организационные меры защиты должны быть учтены на этапе проектирования? a) только технические меры (межсетевой экран, антивирус) b) организационные меры (политика доступа, обучение персонала, регламенты) c) только криптографические меры d) только инженерно-технические меры	ПК-4
	Ответ: b	
21	Установите соответствие между этапом проектирования ИС (1–3) и его содержанием (A–C) в области организационной защиты информации. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C).	ПК-4

Этап проектирования	Содержание в области организационной защиты
1. Выявление требований	A. Разработка модели угроз и организационной структуры защиты
2. Концептуально-логическое проектирование	B. Определение требований к политике доступа, инструктажам, ответственным лицам
3. Сопровождение проектных решений	C. Актуализация документов при изменении законодательства и угроз

Ответ: 1-B, 2-A, 3-C

22 Установите соответствие между нормативным документом (1–3) и его содержанием (A–C) при выявлении требований к Системе. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). ПК-4

Нормативный документ	Содержание требований
1. 152-ФЗ «О персональных данных»	A. Требования к пропускному режиму и защите от несанкционированного доступа
2. Приказы ФСТЭК России	B. Требования к организационным мерам защиты информации в ГИС
3. Трудовой кодекс РФ	C. Требования к обработке и защите персональных данных

Ответ: 1-C, 2-B, 3-A

23 Установите соответствие между организационной мерой защиты (1–3) и её описанием (A–C) при выявлении требований к Системе. В бланк ответов запишите последовательность (например, 1-C, 2-A, 3-B). ПК-4

Организационная мера	Описание
1. Пропускной и внутриобъектовый режим	A. Ограничение доступа к информации в зависимости от должностных обязанностей
2. Работа с персоналом	B. Контроль входа/выхода на территорию и в здания
3. Разграничение доступа	C. Проведение инструктажей, обучение, подписание NDA

Ответ: 1-B, 2-C, 3-A

24 Установите правильную последовательность этапов выявления требований к организационной защите для ИС. Расположите буквы (A–D) в верном порядке. ПК-4
A) Анализ нормативно-правовых требований к организации защиты
B) Определение организационных мер (политика доступа, инструктажи, ответственные)
C) Анализ организационных рисков и угроз
D) Формирование раздела требований к организационной защите в ТЗ

Ответ: A → C → B → D

25 Установите правильную последовательность действий при сопровождении проектных решений в области организационной защиты при изменении законодательства. Расположите буквы (A–D) в верном порядке. ПК-4
A) Актуализация организационно-распорядительных документов (положения, инструкции)
B) Получение информации об изменении нормативных требований
C) Внедрение изменений в процессы и обучение персонала
D) Анализ влияния изменений на систему защиты

Ответ: B → D → A → C

26 Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). ПК-4
Назовите не менее двух методов выявления требований к организационной защите для ИС.

Ответ: анализ нормативно-правовых документов (152-ФЗ, приказы ФСТЭК), проведение анализа организационных рисков, интервьюирование заинтересованных сторон.

27 Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). ПК-4
Какой артефакт разрабатывается на этапе концептуально-логического проектирования в области организационной защиты?

Ответ: организационная модель защиты (структура ответственных, политика доступа, регламенты).

28 Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). ПК-4
Для чего используется модель организационных угроз при выявлении требований к Системе?

Ответ: для идентификации слабых мест в организационной структуре, процессах и персонале, а также для обоснования выбора организационных мер защиты.

29 Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). ПК-4
Назовите не менее двух нормативных документов, требования которых должны быть выявлены при проектировании системы организационной защиты для ИС, обрабатывающей персональные данные.

	Ответ:	152-ФЗ «О персональных данных», Постановление Правительства № 1119, Приказы ФСТЭК России, Трудовой кодекс РФ.	
30	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Какой раздел технического задания должен быть обязательным при выявлении требований к Системе для ИС с точки зрения организационной защиты?		ПК-4
	Ответ:	раздел «Требования к организационной защите информации» (включая политику доступа, инструктажи, ответственных, пропускной режим).	

7. Оценочные материалы промежуточной аттестации

Экзамен седьмой семестр

№ п/п	Содержание вопроса	Правильный ответ (ключ ответа)	Компетенция
1	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух организационных мер, которые должны быть применены при обнаружении инцидента ИБ, вызванного увольнением недобросовестного сотрудника с доступом к конфиденциальным данным.		ПК-2
	Ответ:	отзыв всех прав доступа (учётные записи, пропуска), подписание акта приёма-передачи материальных и цифровых носителей, проведение выходного собеседования с напоминанием об ответственности за разглашение, включение в «чёрный список» на случай повторного трудоустройства.	
2	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ, связанного с несанкционированным доступом в серверную, какие организационные меры должны быть приняты для усиления физической защиты?		ПК-2
	Ответ:	пересмотр порядка допуска в серверную (ужесточение пропускного режима), установка видеонаблюдения и системы контроля доступа (СКУД), проведение внепланового инструктажа для сотрудников, имеющих доступ, ограничение круга лиц с допуском.	
3	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух организационных документов, которые должны быть актуализированы после принятия мер по устранению инцидента ИБ.		ПК-2
	Ответ:	положение о реагировании на инциденты ИБ, политика информационной безопасности, инструкция по действиям сотрудников при обнаружении инцидентов, перечень лиц, допущенных к конфиденциальной информации.	
4	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При тестировании ИС в рамках сопровождения, какие организационные меры помогают выявить нарушения политики безопасности среди сотрудников?		ПК-2
	Ответ:	анализ журналов доступа и действий пользователей (аудит), проведение внутренних проверок и внезапных контрольных мероприятий, опрос сотрудников, анализ соблюдения регламентов работы с конфиденциальными документами.	
5	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух организационных мер по предотвращению инцидентов ИБ, связанных с передачей конфиденциальных данных по электронной почте.		ПК-2
	Ответ:	внедрение системы DLP (организационный контроль передачи данных), разработка и утверждение регламента использования электронной почты для обмена конфиденциальной информацией, проведение инструктажа о запрете отправки конфиденциальной информации на личные адреса, подписание соглашения о неразглашении.	
6	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При выявлении требований к Системе для предприятия розничной торговли, какие организационные требования должны быть учтены для защиты данных банковских карт клиентов (в соответствии с PCI DSS)?		ПК-4
	Ответ:	требования к разграничению доступа к данным держателей карт, требования к обучению персонала безопасной обработке платежных данных, требования к ведению журналов событий и их регулярному анализу, требования к назначению ответственных за защиту платежной информации.	
7	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При концептуально-логическом проектировании ИС для медицинской организации, какие организационные меры защиты персональных данных (врачебной тайны) должны быть предусмотрены?		ПК-4
	Ответ:	разработка политики обработки и защиты персональных данных (врачебной тайны), назначение ответственных за обработку и защиту медицинских данных, внедрение системы разграничения доступа по ролям (врачи, медсестры, администраторы), подписание соглашений о неразглашении медицинской тайны.	
8	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух заинтересованных сторон, с которыми должны быть согласованы требования к организационной защите при выявлении требований к Системе для государственной информационной системы.		ПК-4
	Ответ:	руководитель организации-заказчика, представитель регулятора (ФСТЭК, ФСБ), руководитель службы безопасности, главный системный аналитик проекта.	
9	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При выявлении требований к Системе для автоматизации кадрового учёта, какие организационные требования должны быть учтены в части защиты данных о сотрудниках?		ПК-4

	Ответ:	требования к разграничению доступа к персональным данным сотрудников (кадровики, руководители, бухгалтерия), требования к защите данных от несанкционированного доступа при передаче в другие системы, требования к подписанию соглашений о неразглашении с кадровыми работниками, требования к ведению журналов доступа.	
10	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При сопровождении разработанных проектных решений по организационной защите, какие действия необходимо выполнить при вводе в эксплуатацию новой автоматизированной системы, обрабатывающей конфиденциальные данные?		ПК-4
	Ответ:	утверждение организационно-распорядительной документации (приказы, инструкции, положения), проведение обучения и инструктажа всех категорий пользователей системы, назначение ответственных за эксплуатацию и защиту системы, проведение проверки готовности организационных мер перед запуском.	

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-4.1 Выявляет требования к Системе и концептуально-логически проектирует 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. Полякова, Т. А. Организационное и правовое обеспечение информационной безопасности: учебник для вузов / Т. А. Полякова, С. Г. Чубукова, В. А. Ниесов; Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова.. - 2-е изд. - Москва: Юрайт, 2026. - 357 с - 978-5-534-19108-0. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/583236 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Суворова, Г. М. Информационная безопасность: учебник для вузов / Г. М. Суворова. - 2-е изд. - Москва: Юрайт, 2026. - 277 с - 978-5-534-16450-3. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/588515 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. 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

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

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. https://stepik.org - Платформа с онлайн-курсами от авторов-практиков
2. http://www.fstec.ru/ - Официальный сайт ФСТЭК России

Федеральная служба по техническому и экспортному контролю — основной регулятор в сфере технической и организационной защиты информации. На сайте публикуются приказы, требования к защите информации в государственных информационных системах, методические документы по аттестации объектов информатизации

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. Draw.io (diagrams.net);
2. Консультант Плюс;
3. 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 СП
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения