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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «СПЕЦИАЛИЗИРОВАННЫЕ ИТ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

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: 5 з.е.
в академических часах: 180 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 применению специализированных информационных технологий в деятельности правоохранительных органов, включая автоматизацию оперативно-розыскной, следственной, экспертной и управленческой деятельности.

Задачи изучения дисциплины:

- Изучить нормативно-правовые основы использования ИТ в правоохранительной сфере (152-ФЗ, 144-ФЗ, 149-ФЗ, приказы МВД, СК, ФСБ), классификацию специализированных ИТ-систем и принципы информационно-аналитической работы.;
- Освоить методы работы с автоматизированными банками данных, системами идентификации (АДИС, ДАКТО, АБИС), геоинформационными системами, системами видеоаналитики и распознавания лиц, средствами криптографической защиты и ЭЦП.;
- Сформировать навыки применения специализированных ИТ для поиска и обработки информации, документирования правонарушений, проведения экспертных исследований, управления оперативными подразделениями и взаимодействия с другими ведомствами в условиях цифровизации..

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-2.1 Верифицирует ИС в рамках выполнения работ по созданию и сопровождению ИС

Знать:

ПК-2.1/Зн1 Методы и технологии верификации специализированных ИС правоохранительных органов (АДИС, ДАКТО, ГИС, системы видеоаналитики и распознавания), требования к защите информации и интеграционному тестированию в условиях правоохранительной деятельности, нормативно-правовые акты, регламентирующие проверку работоспособности ИС (приказы МВД, ФСБ, СК), критерии оценки соответствия ИС требованиям безопасности и оперативно-служебной деятельности.

Уметь:

ПК-2.1/Ум1 Проводить интеграционное тестирование специализированных ИТ-систем, используемых в правоохранительной деятельности, верифицировать соответствие ИС требованиям нормативных документов и заданных алгоритмов работы, выявлять отклонения в функционировании систем идентификации, видеонаблюдения, баз данных и криптографических модулей, документировать результаты верификации и готовить заключения для органов дознания и следствия.

Владеть:

ПК-2.1/Нв1 Навыками разработки сценариев и планов верификации специализированных ИС, методами интеграционного тестирования систем с учетом требований правоохранительной деятельности, приемами анализа и интерпретации результатов верификации, навыками оформления отчетной документации по результатам тестирования для руководства и следственных органов.

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 специализированным ИС для правоохранительной деятельности (системный анализ, моделирование угроз, нормативно-правовые требования 144-ФЗ, 152-ФЗ, 149-ФЗ, приказы МВД/ФСБ/СК), принципы концептуально-логического проектирования ИС для органов внутренних дел, следствия и экспертных учреждений, требования к защите информации и разграничению доступа.

Уметь:

ПК-4.1/Ум1 Применять методы системного анализа для выявления требований к специализированным ИС в сфере правоохранительной деятельности (АДИС, ДАКТО, ГИС, видеоаналитика, биометрические системы), разрабатывать концептуальные и логические модели, обосновывать выбор архитектуры и алгоритмов с учетом специфики правоохранительных задач, выявлять риски и ограничения, связанные с защитой данных и режимом секретности.

Владеть:

ПК-4.1/Нв1 Навыками формирования технического задания и концептуальных решений для специализированных ИТ-систем правоохранительных органов, методами моделирования бизнес-процессов оперативно-служебной деятельности, приемами верификации требований с учетом нормативных документов, методиками согласования проектных решений с заинтересованными сторонами (следствие, эксперты, руководство) и документирования результатов.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Специализированные ИТ в правоохранительной деятельности» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 8.

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-2.1 Верифицирует ИС в рамках выполнения работ по созданию и сопровождению ИС	Вычислительные системы, сети и телекоммуникации, Компьютерная экспертиза, Моделирование процессов и систем, Правовая защита информации, Проектирование информационных систем, Производственная практика: технологическая (проектно-технологическая) практика, Управление информационной безопасностью, Управление информационными проектами реализации комплексной безопасности, Учебная практика: технологическая (проектно-технологическая) практика, Цифровая культура в профессиональной деятельности	Выполнение и защита выпускной квалификационной работы, Проектирование информационных систем, Производственная практика: преддипломная практика, Управление информационной безопасностью, Управление информационными проектами реализации комплексной безопасности, Цифровая культура в профессиональной деятельности

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, Интеллектуальные информационные системы, Компьютерная экспертиза, Методы и средства защиты информации, Моделирование процессов и систем, Организационная защита информации, Организация вычислительных процессов, Основы проектной деятельности, Проектирование и реализация баз данных, Проектирование информационных систем, Проектный практикум, Производственная практика: технологическая (проектно-технологическая) практика, Системы искусственного интеллекта, Современные цифровые технологии управления предприятием, Теория информационной безопасности и методология защиты информации, Учебная практика: технологическая (проектно-технологическая) практика, Цифровая культура в профессиональной деятельности	Выполнение и защита выпускной квалификационной работы, Интеллектуальные информационные системы, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Современные цифровые технологии управления предприятием, 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
Восьмой семестр	180	5	4	2	2	2	0,3	139,7	Экзамен
Всего	180	5	4	2	2	2	0,3	139,7	34

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы		ные занятия	ые занятия	тельная работа

	Всего	Лаборатор	Лекционн	Самостоят
Раздел 1. Специализированные ит в правоохранительной деятельности	**146**	**2**	**2**	**139,7**
Тема 1.1. Введение в специализированные ИТ в правоохранительной деятельности: основные понятия и определения (специализированные информационные технологии, правоохранительная деятельность, оперативно-розыскная деятельность, следственные действия, судебная экспертиза); классификация специализированных ИТ-систем (АДИС, ДАКТО, АБИС, ГИС, системы видеоаналитики и распознавания лиц, криминалистические учеты, геоинформационные системы); нормативно-правовая база применения ИТ в правоохранительной сфере (144-ФЗ, 152-ФЗ, 149-ФЗ, приказы МВД России, ФСБ России, СК РФ); обзор автоматизированных банков данных и систем идентификации; роль специализированных ИТ в документировании правонарушений, проведении экспертиз и управлении оперативными подразделениями.	146	2	2	139,7

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	Специализированные ит в правоохранительной деятельности	Тестовое задание	Экзамен

6. Оценочные материалы текущего контроля

1. Специализированные ит в правоохранительной деятельности Тестовое задание

№ п/п	Содержание вопроса		Компетенция
	Правильный ответ (ключ ответа)		
1	При верификации ИС специализированных систем правоохранительных органов (АДИС, ДАКТО), какой метод тестирования позволяет проверить соответствие системы требованиям нормативных актов? a) нагрузочное тестирование b) верификация соответствия требованиям приказов МВД России c) модульное тестирование d) тестирование пользовательского интерфейса		ПК-2
	Ответ:	b	
2	При обнаружении инцидента ИБ в ходе сопровождения ИС правоохранительных органов, какой документ должен быть оформлен в первую очередь? a) техническое задание b) акт об инциденте ИБ c) бизнес-план d) маркетинговый план		ПК-2
	Ответ:	b	
3	При тестировании ИС специализированных систем правоохранительной деятельности, какой анализ позволяет выявить уязвимости в системах видеоаналитики и распознавания лиц? a) статический анализ (SAST) b) анализ конфигурации и тестирование защиты от атак подмены c) нагрузочное тестирование d) тестирование удобства использования		ПК-2
	Ответ:	b	
4	Установите правильную последовательность действий при обнаружении инцидента ИБ в специализированной ИС правоохранительных органов в рамках сопровождения ИС. Расположите буквы (A–D) в верном порядке. A) Изоляция затронутого компонента и создание образа диска (сохранение доказательств) B) Обнаружение аномалии (сигнал от SIEM, сообщение от оператора) C) Устранение инцидента (исправление, обновление СЗИ, восстановление из резервной копии) D) Документирование инцидента, уведомление руководства и анализ причин		ПК-2
	Ответ:	B → A → C → D	
5	Установите правильную последовательность этапов верификации ИС при проверке соответствия требованиям правоохранительных органов. Расположите буквы (A–D) в верном порядке. A) Проверка соответствия требованиям приказов МВД/ФСБ/СК РФ B) Интеграционное тестирование систем (АДИС, ГИС, видеоаналитика) C) Документирование результатов и подготовка отчета о верификации D) Анализ результатов и выявление отклонений		ПК-2
	Ответ:	A → B → D → C	
6	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух признаков инцидента ИБ, которые могут быть выявлены при тестировании ИС специализированных систем правоохранительных органов (например, систем видеоаналитики или АДИС).		ПК-2
	Ответ:	несанкционированные изменения в базе данных АДИС, нештатные события в журналах доступа, нарушения в целостности биометрических данных, сбои в работе системы распознавания, попытки несанкционированного доступа к архивам.	
7	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ в специализированной ИС правоохранительных органов, какие меры должны быть приняты для обеспечения сохранности цифровых доказательств?		ПК-2
	Ответ:	изоляция затронутого компонента, создание образа диска (копия), сохранение логов и дампов памяти, фото- и видеофиксация состояния системы, документирование времени и характера инцидента, привлечение экспертов для расследования, обеспечение цепочки хранения доказательств.	
8	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух методов тестирования, используемых при верификации ИС для проверки защищённости специализированных систем правоохранительных органов от атак.		ПК-2
	Ответ:	тестирование на проникновение (пентест), статический анализ кода (SAST), динамический анализ (DAST), сканирование уязвимостей, анализ конфигурации безопасности, верификация соответствия требованиям безопасности (приказы МВД/ФСБ/СК).	
9	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ, связанного с утечкой данных из биометрической системы, какие меры должны быть приняты в рамках сопровождения ИС правоохранительных органов?		ПК-2

	Ответ:	изоляция уязвимого компонента, проверка журналов доступа, смена паролей и ключей, уведомление руководства, привлечение экспертов, проведение служебной проверки, усиление контроля доступа, актуализация политик безопасности, уведомление заинтересованных сторон и регулятора (при необходимости).	
10	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух инструментов мониторинга, используемых для обнаружения инцидентов ИБ в процессе сопровождения ИС правоохранительных органов.		ПК-2
	Ответ:	SIEM-системы (Splunk, QRadar, ArcSight), системы обнаружения вторжений (IDS/IPS), WAF (Web Application Firewall), системы мониторинга логов, DLP-системы, системы контроля целостности (Tripwire).	
11	При обнаружении инцидента ИБ в специализированной ИС правоохранительных органов, какое действие должно быть выполнено в первую очередь для сохранения цифровых доказательств? a) увольнение сотрудника b) изоляция затронутого компонента, создание образа диска и сохранение логов c) перезагрузка системы d) удаление логов		ПК-2
	Ответ:	b	
12	Какой инструмент применяется при тестировании ИС для обнаружения инцидентов ИБ и анализа событий безопасности в системах правоохранительных органов? a) SIEM-система b) Microsoft Word c) Adobe Photoshop d) AutoCAD		ПК-2
	Ответ:	a	
13	Установите соответствие между этапом управления инцидентами (1–3) и его содержанием (A–C) при обнаружении инцидентов ИБ в рамках сопровождения ИС. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Этап управления инцидентами / Содержание этапа 1. Обнаружение и локализация / A. Восстановление системы и анализ причин инцидента 2. Устранение / B. Мониторинг аномалий, идентификация затронутых компонентов, создание образа диска 3. Восстановление и анализ / C. Устранение уязвимости, обновление СЗИ, удаление вредоносного кода, восстановление из резервных копий		ПК-2
	Ответ:	1-B, 2-C, 3-A	
14	Установите соответствие между инструментом (1–3) и его назначением (A–C) при тестировании ИС для обнаружения инцидентов ИБ в специализированных системах. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Инструмент / Назначение при тестировании ИС 1. EnCase / FTK / A. Выявление уязвимостей веб-приложений и систем идентификации 2. Burp Suite / B. Централизованный сбор и корреляция событий безопасности в системах правоохранительных органов 3. SIEM-система / C. Судебно-криминалистический анализ данных и создание образов дисков		ПК-2
	Ответ:	1-C, 2-A, 3-B	
15	Установите соответствие между типом инцидента ИБ (1–3) и мерой реагирования (A–C) при обнаружении инцидентов ИБ в рамках сопровождения ИС правоохранительных органов. В бланк ответов запишите последовательность (например, 1-C, 2-A, 3-B). Тип инцидента ИБ / Мера реагирования 1. Вредоносное ПО в системе видеоаналитики / A. Блокировка учётных записей, смена паролей, проверка целостности данных 2. Несанкционированный доступ к АДИС / B. Изоляция сегмента сети, сканирование и удаление вирусов, проверка целостности системы 3. Утечка данных из биометрической системы / C. Изоляция системы, уведомление руководства, анализ логов, привлечение экспертов		ПК-2
	Ответ:	1-B, 2-A, 3-C	

16	При выявлении требований к Системе для специализированных ИС правоохранительных органов, какие требования учитывают необходимость защиты информации в соответствии с 149-ФЗ и 152-ФЗ? a) функциональные требования b) требования к информационной безопасности c) требования к интерфейсу d) требования к производительности Ответ: b	ПК-4
17	На этапе концептуально-логического проектирования ИС для правоохранительных органов, какая модель используется для описания потоков данных и ролей пользователей? a) ER-диаграмма b) модель потоков данных (DFD) и матрица разграничения доступа (RBAC) c) UML-диаграмма классов d) BPMN-диаграмма Ответ: b	ПК-4
18	При выявлении требований к Системе для проекта правоохранительных органов, какой нормативный документ является основным для определения требований к оперативно-розыскной деятельности? a) 149-ФЗ «Об информации…» b) 144-ФЗ «Об оперативно-розыскной деятельности» c) 152-ФЗ «О персональных данных» d) 63-ФЗ «Об электронной подписи» Ответ: b	ПК-4
19	Что является результатом этапа выявления требований к специализированным ИС для правоохранительных органов? a) исходный код приложения b) техническое задание с разделом требований к защите и оперативно-служебной деятельности c) маркетинговый план d) бизнес-план Ответ: b	ПК-4
20	При концептуально-логическом проектировании ИС для правоохранительных органов, какие элементы должны быть учтены для обеспечения идентификации личности в системах распознавания лиц? a) только настройка камер b) проектирование алгоритмов биометрической идентификации, защита от подмены, интеграция с базами данных c) только шифрование данных d) только организация охраны здания Ответ: b	ПК-4
21	Установите соответствие между этапом проектирования ИС (1–3) и его содержанием (A–C) в области специализированных ИТ для правоохранительной деятельности. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Этап проектирования / Содержание в области специализированных ИТ 1. Выявление требований / A. Разработка архитектуры системы, модели потоков данных, RBAC 2. Концептуально-логическое проектирование / B. Определение требований к системам идентификации, защите информации, доступу к базам 3. Сопровождение проектных решений / C. Актуализация документации при изменении нормативных актов и требований 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 для специализированных ИС правоохранительных органов. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Нормативный документ / Содержание требований 1. 144-ФЗ «Об оперативно-розыскной деятельности» / A. Требования к защите информации в ИС правоохранительных органов 2. Приказы МВД России / B. Требования к организации оперативно-розыскных мероприятий с использованием ИТ 3. 149-ФЗ «Об информации...» / C. Требования к разграничению доступа к информации в государственных ИС Ответ: 1-B, 2-A, 3-C	ПК-4
23	Установите соответствие между методом защиты информации (1–3) и его назначением (A–C) при выявлении требований к Системе для специализированных ИС правоохранительных органов. В бланк ответов запишите последовательность (например, 1-C, 2-A, 3-B). Метод защиты / Назначение	ПК-4

	1. Шифрование данных	A. Ограничение доступа к информации по ролям (следователь, эксперт, оперативник)	
	2. Разграничение доступа (RBAC)	B. Подтверждение подлинности пользователя в системе	
	3. Электронная подпись (ЭЦП)	C. Обеспечение конфиденциальности данных при передаче и хранении	
	Ответ:	1-C, 2-A, 3-B	
24	Установите правильную последовательность этапов выявления требований к специализированным ИС для правоохранительных органов. Расположите буквы (A–D) в верном порядке. A) Анализ нормативно-правовых требований (144-ФЗ, приказы МВД/ФСБ/СК) B) Определение перечня защищаемых объектов и угроз для правоохранительной деятельности C) Определение требований к системам идентификации, видеоаналитики и доступа к базам D) Формирование раздела требований к специализированным ИС в ТЗ		ПК-4
	Ответ:	A → B → C → D	
25	Установите правильную последовательность действий при концептуально-логическом проектировании ИС для правоохранительных органов. Расположите буквы (A–D) в верном порядке.) Разработка архитектуры системы (модель потоков данных, интеграция с внешними базами) B) Определение ролей пользователей (следователи, эксперты, оперативники) и прав доступа (RBAC) C) Проектирование систем идентификации и видеоаналитики D) Разработка технической документации и согласование с руководством		ПК-4
	Ответ:	B → A → C → D	
26	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух методов выявления требований к специализированным ИС для правоохранительных органов.		ПК-4
	Ответ:	анализ нормативно-правовых документов (144-ФЗ, приказы МВД/ФСБ/СК), проведение интервью с сотрудниками (следователи, эксперты, оперативники), изучение существующих ведомственных систем (АДИС, ДАКТО), моделирование угроз и рисков для правоохранительной деятельности.	
27	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Какой артефакт разрабатывается на этапе концептуально-логического проектирования в области специализированных ИТ для правоохранительных органов?		ПК-4
	Ответ:	архитектура системы, модель потоков данных (DFD), матрица разграничения доступа (RBAC), схема интеграции с внешними системами (ГИС, базы данных МВД), перечень требований к системам идентификации и видеоаналитики.	
28	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Для чего используется модель потоков данных (DFD) при выявлении требований к Системе для специализированных ИС правоохранительных органов?		ПК-4
	Ответ:	для визуализации потоков информации, идентификации точек доступа и контроля, выявления уязвимостей и обоснования выбора мер защиты (разграничение доступа, шифрование, аудит) в рамках оперативно-служебной деятельности.	
29	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух нормативных документов, требования которых должны быть выявлены при проектировании специализированных ИС для правоохранительных органов.		ПК-4
	Ответ:	144-ФЗ «Об оперативно-розыскной деятельности», 149-ФЗ «Об информации…», 152-ФЗ «О персональных данных», приказы МВД России, ФСБ России, СК 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 специализированных ИС правоохранительных органов?		ПК-4
	Ответ:	раздел «Требования к информационной безопасности и оперативно-служебной деятельности» (включая требования к идентификации, шифрованию, ЭЦП, разграничению доступа, аудиту, резервному копированию, защите от утечек).	

7. Оценочные материалы промежуточной аттестации

Экзамен восьмой семестр

№ п/п	Содержание вопроса	Правильный ответ (ключ ответа)	Компетенция
1	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При верификации ИС специализированных систем правоохранительных органов (например, АДИС или системы видеоаналитики), какие этапы проверки безопасности являются обязательными и почему?		ПК-2
	Ответ:	обязательными являются проверка соответствия требованиям приказов МВД/ФСБ/СК (нормативная база), тестирование на проникновение (пентест) для выявления уязвимостей, проверка целостности данных и защищённости каналов связи, так как эти системы обрабатывают конфиденциальные данные и критически важны для оперативно-служебной деятельности.	
2	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ в специализированной ИС правоохранительных органов (например, попытка несанкционированного доступа к базе данных АДИС), какие меры должны быть приняты для сохранения цифровых доказательств в соответствии с требованиями процессуального законодательства?		ПК-2

	Ответ:	необходимо немедленно изолировать затронутый компонент, создать образ диска (копию) для криминалистического исследования, сохранить логи и дампы памяти с временными метками, зафиксировать состояние системы (фото/видео), обеспечить цепочку хранения доказательств с участием понятых или эксперта, задокументировать все действия для последующего использования в следственных действиях.	
3	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух методов тестирования ИС, используемых при верификации систем распознавания лиц, и кратко опишите, какие инциденты они помогают выявить.		ПК-2
	Ответ:	● Тестирование защиты от спуфинга (подмены) — выявляет уязвимости к атакам с использованием фотографий, масок или видеозаписей для обмана системы. ● Тестирование точности распознавания — проверяет вероятность ложного совпадения (FAR) и ложного несовпадения (FRR), выявляет инциденты ошибочной идентификации, которые могут привести к необоснованному задержанию или пропуску преступника.	
4	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ, связанного с нарушением целостности данных в системе ДАКТО (дактилоскопическая идентификация), какие меры должны быть приняты в рамках сопровождения ИС для восстановления доверия к системе?		ПК-2
	Ответ:	необходимо провести проверку целостности базы данных (хеш-суммы, ЭЦП), восстановить данные из защищённых резервных копий, провести служебную проверку (кто, когда, с каких устройств вносил изменения), усилить контроль доступа к базе ДАКТО, актуализировать политики безопасности и провести внеплановый инструктаж операторов системы.	
5	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух инструментов мониторинга, используемых для обнаружения инцидентов ИБ в системах видеоаналитики и распознавания лиц, и опишите, какие события они фиксируют.		ПК-2
	Ответ:	● SIEM-система (например, Splunk, QRadar) — фиксирует события безопасности: попытки несанкционированного доступа к видеопотокам, сбои в работе камер, аномалии в сетевом трафике. ● Система мониторинга целостности — отслеживает изменения в конфигурационных файлах и алгоритмах распознавания, фиксирует попытки подмены моделей или изменения параметров идентификации, что может указывать на компрометацию системы.	
6	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При выявлении требований к Системе для специализированной ИС правоохранительных органов (например, системы видеоаналитики с распознаванием лиц), какие нормативные и оперативные требования должны быть учтены в первую очередь?		ПК-4
	Ответ:	требования 144-ФЗ «Об оперативно-розыскной деятельности» (порядок использования ИТ в ОРМ), требования 152-ФЗ и 149-ФЗ (защита персональных данных и информации), требования приказов МВД России (порядок ведения баз данных и доступа), требования к юридической значимости доказательств (ЭЦП, цепочка хранения), оперативные требования к скорости распознавания и точности идентификации.	
7	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). На этапе концептуально-логического проектирования ИС для правоохранительных органов, какие элементы архитектуры должны быть предусмотрены для обеспечения интеграции с ведомственными системами (например, ГИС, Единая база данных МВД)?		ПК-4
	Ответ:	необходимо предусмотреть API-шлюзы для взаимодействия с внешними системами, единые форматы обмена данными (XML, JSON), протоколы защищённой передачи (TLS, VPN), систему аутентификации и авторизации на основе служебных удостоверений, механизмы логирования межведомственных запросов, резервирование каналов для обеспечения отказоустойчивости.	
8	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух требований к безопасности, которые должны быть предъявлены к системе идентификации (АДИС, ДАКТО, биометрия) при выявлении требований к Системе для правоохранительных органов.		ПК-4
	Ответ:	требования к защите от несанкционированного доступа (многофакторная аутентификация, RBAC, логирование), требования к защите биометрических данных (шифрование при хранении и передаче, обезличивание для аналитики), требования к целостности данных (контрольные суммы, ЭЦП), требования к отказоустойчивости (резервирование, горячая замена), требования к аудиту всех операций с базами данных.	
9	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При выявлении требований к Системе для специализированной ИС правоохранительных органов, какие вопросы необходимо задать представителям следственных и оперативных подразделений для формализации их потребностей?		ПК-4
	Ответ:	вопросы о типах и объёмах данных (какие объекты, какие признаки), требованиях к скорости поиска и точности идентификации, необходимых уровнях доступа для разных категорий пользователей (следователи, эксперты, оперативники), требованиях к юридической значимости полученных результатов, регламентах работы с системой в разных режимах (рабочий, режим ЧС, учения), необходимости интеграции с другими ведомственными системами.	

10	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При сопровождении разработанных проектных решений для специализированных ИС правоохранительных органов, какие действия необходимо выполнить при изменении требований к хранению и защите биометрических данных (например, новых приказов ФСБ или МВД)?		ПК-4
	Ответ:	провести оценку влияния изменений на архитектуру и безопасность системы, актуализировать модель угроз и политики защиты данных, разработать план внесения изменений (шифрование, обезличивание, новые форматы хранения), провести повторное тестирование безопасности и интеграционное тестирование, актуализировать проектную документацию и техническое задание, провести обучение персонала новым регламентам работы.	

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-2.1 Верифицирует 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. Криминалистика. Теоретические основы и криминалистическая техника: учебник для вузов / Л. Я. Драпкин, И. В. Александров, А. В. Антропов [и др.] - 2-е изд. - Москва: Юрайт, 2026. - 246 с - 978-5-534-17702-2. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/584379 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. / Л. Я. Драпкин, И. В. Александров, А. В. Антропов [и др.] - 2-е изд. - Москва: Юрайт, 2026. - 230 с - 978-5-534-17704-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/584380 (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. https://base.garant.ru/403510768/ - ГОСТ Р ИСО/МЭК 27001-2021

Национальный стандарт РФ, идентичный международному стандарту ISO/IEC 27001:2013 (с учетом изменений). Действует с 1 января 2022 года, взамен ГОСТ Р ИСО/МЭК 27001-2006 .

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 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