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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

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 управлению системой информационной безопасности на уровне организации, включая стратегическое планирование, оперативное управление и контроль эффективности мер защиты.

Задачи изучения дисциплины:

- Изучить нормативно-правовые основы управления ИБ, международные и отечественные стандарты (ISO/IEC 27001, ГОСТ Р ИСО/МЭК 27001, 152-ФЗ, 187-ФЗ), модели зрелости и процессные подходы к управлению защитой информации.;
- Освоить методы стратегического и оперативного управления ИБ (политики безопасности, управление рисками, управление инцидентами, управление непрерывностью бизнеса, контроль доступа, управление активами) и инструменты их реализации (GRC-системы, SIEM, DLP, IDS/IPS).;
- Сформировать навыки разработки и внедрения системы управления информационной безопасностью (СУИБ), проведения внутренних аудитов, оценки эффективности мер защиты и управления изменениями в области ИБ..

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

Компетенции, индикаторы и результаты обучения

ПК-1 Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы

ПК-1.1 Разрабатывает прототипы ИС на базе типовой ИС в рамках выполнения работ по созданию и сопровождению ИС

Знать:

ПК-1.1/Зн1 Принципы и методы управления информационной безопасностью, требования к защите информации в ИС (152-ФЗ, 187-ФЗ, ГОСТ Р ИСО/МЭК 27001), подходы к интеграции требований безопасности в прототипы ИС на этапе разработки, методы оценки рисков и выбора средств защиты для типовых ИС.

Уметь:

ПК-1.1/Ум1 Разрабатывать прототипы ИС на базе типовых решений с учетом требований информационной безопасности, интегрировать механизмы защиты (аутентификация, шифрование, контроль доступа, логирование) на этапе прототипирования, применять методы управления рисками для обоснования выбора средств защиты в прототипах.

Владеть:

ПК-1.1/Нв1 Навыками разработки защищенных прототипов ИС с использованием типовых решений, методами оценки соответствия прототипов требованиям управления ИБ, приемами документирования требований к безопасности в рамках проектной документации, навыками взаимодействия с заинтересованными сторонами для согласования требований к защите.

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 ИС с учетом требований управления информационной безопасностью (интеграционное тестирование, тестирование безопасности, пентест), подходы к проверке соответствия СЗИ требованиям, критерии оценки эффективности мер защиты, регламенты проведения верификации в рамках СУИБ.

Уметь:

ПК-2.1/Ум1 Применять методы верификации для проверки соответствия ИС требованиям управления ИБ (политики безопасности, управление доступом, шифрование, аудит), проводить интеграционное тестирование средств защиты информации и их взаимодействия с компонентами ИС, выявлять и документировать отклонения от требований безопасности и управления ИБ.

Владеть:

ПК-2.1/Нв1 Навыками разработки планов и сценариев верификации для проектов в области управления ИБ, методами интеграционного тестирования защищенных ИС, приемами анализа результатов верификации и подготовки отчетной документации для системы управления информационной безопасностью, навыками взаимодействия с подразделениями ИБ для устранения выявленных несоответствий.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Управление информационной безопасностью» 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-1 - Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы		

ПК-1.1 Разрабатывает прототипы ИС на базе типовой ИС в рамках выполнения работ по созданию и сопровождению ИС	Встроенные языки программирования, Вычислительные системы, сети и телекоммуникации, Информационно-коммуникационные технологии в профессиональной деятельности, Моделирование процессов и систем, Нейросетевые технологии в социальных медиа, 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, Теория информационной безопасности и методология защиты информации, Учебная практика: ознакомительная практика, Учебная практика: технологическая (проектно-технологическая) практика, Хранение, обработка и анализ данных	Выполнение и защита выпускной квалификационной работы, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Разработка профессиональных приложений
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, Специализированные ИТ в правоохранительной деятельности, 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, Специализированные ИТ в правоохранительной деятельности, Управление информационными проектами реализации комплексной безопасности, 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)	Лекционные занятия (часы)	Практические занятия (часы)	Групповая контактная работа (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Восьмой 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	Лекционные занятия	Практические занятия	Самостоятельная работа
Раздел 1. Управление информационной безопасностью	**110**	**2**	**2**	**103,7**

Тема 1.1. Введение в управление информационной безопасностью: основные понятия и определения (управление ИБ, система управления информационной безопасностью (СУИБ), политика безопасности, риск, угроза, актив); место управления ИБ в общей системе управления организацией; международные и отечественные стандарты (ISO/IEC 27001, ГОСТ Р ИСО/МЭК 27001, 152-ФЗ, 187-ФЗ, приказы ФСТЭК и ФСБ); процессный подход к управлению ИБ (PDCA); основные процессы СУИБ (управление рисками, управление инцидентами, управление непрерывностью бизнеса, управление активами, управление доступом); обзор инструментов управления ИБ (GRC-системы, SIEM, DLP, IDS/IPS).	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	Управление информационной безопасностью	Тестовое задание	Экзамен

6. Оценочные материалы текущего контроля

1. Управление информационной безопасностью Тестовое задание

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	При разработке прототипов ИС на базе типовой ИС, какой документ определяет требования к защите информации в рамках управления информационной безопасностью? a) техническое задание (ТЗ) с разделом требований к ИБ b) бизнес-план c) должностная инструкция d) маркетинговый план		ПК-1
	Ответ:	a	

2	При разработке прототипов ИС на базе типовой ИС, какие требования должны быть учтены для обеспечения защиты персональных данных? a) только требования к производительности b) требования 152-ФЗ «О персональных данных» c) только требования к интерфейсу d) только требования к стоимости Ответ: b	ПК-1
3	При создании и сопровождении ИС, какой нормативный документ является основой для построения системы управления информационной безопасностью в организации? a) ISO 9001 b) ГОСТ Р ИСО/МЭК 27001 c) ITIL d) COBIT Ответ: b	ПК-1
4	При автоматизации бизнес-процессов с использованием типовой ИС, какие требования безопасности должны быть реализованы на этапе прототипирования? a) только шифрование данных b) требования к аутентификации, авторизации, шифрованию и аудиту c) только резервное копирование d) только антивирусная защита Ответ: b	ПК-1
5	При разработке прототипов ИС на базе типовой ИС, какой процесс управления ИБ обеспечивает идентификацию и оценку потенциальных угроз? a) управление инцидентами b) управление рисками c) управление непрерывностью бизнеса d) управление доступом Ответ: b	ПК-1
6	Установите соответствие между процессом управления ИБ (1–3) и его содержанием (A–C) при разработке прототипов ИС на базе типовой ИС. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Процесс управления ИБ / Содержание процесса 1. Управление рисками / A. Разработка и внедрение мер по обеспечению непрерывности работы 2. Управление доступом / B. Идентификация, оценка и обработка угроз и уязвимостей 3. Управление непрерывностью / C. Разграничение прав доступа к информации на основе ролей Ответ: 1-B, 2-C, 3-A	ПК-1
7	Установите соответствие между нормативным документом (1–3) и его содержанием (A–C) при создании и сопровождении ИС. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Нормативный документ / Содержание требований 1. 152-ФЗ «О персональных данных» / A. Требования к управлению рисками и аудиту ИБ 2. ГОСТ Р ИСО/МЭК 27001 / B. Требования к защите персональных данных 3. Приказы ФСТЭК России / C. Требования к защите информации в государственных ИС Ответ: 1-B, 2-A, 3-C	ПК-1
8	Установите соответствие между методом защиты информации (1–3) и его назначением (A–C) при разработке прототипов ИС на базе типовой ИС. В бланк ответов запишите последовательность (например, 1-C, 2-A, 3-B). Метод защиты / Назначение 1. Шифрование / A. Ограничение доступа к информации 2. Аутентификация / B. Подтверждение подлинности пользователя 3. Разграничение доступа / C. Обеспечение конфиденциальности данных Ответ: 1-C, 2-B, 3-A	ПК-1

9	Установите правильную последовательность этапов разработки защищенного прототипа ИС при разработке прототипов ИС на базе типовой ИС. Расположите буквы (A–D) в верном порядке. A) Внедрение требований безопасности в прототип (аутентификация, шифрование, контроль доступа) B) Анализ требований к безопасности (моделирование угроз, оценка рисков) C) Тестирование прототипа на соответствие требованиям безопасности D) Выбор типовой ИС и средств защиты информации	ПК-1
	Ответ: B → D → A → C	
10	Установите правильную последовательность действий при создании и сопровождении ИС в рамках системы управления информационной безопасностью (СУИБ). Расположите буквы (A–D) в верном порядке. A) Внедрение и поддержка СУИБ в ИС B) Разработка политик и процедур безопасности C) Планирование СУИБ (определение целей, ресурсов) D) Мониторинг и анализ эффективности СУИБ	ПК-1
	Ответ: C → B → A → D	
11	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух требований к безопасности, которые должны быть учтены при разработке прототипов ИС на базе типовой ИС.	ПК-1
	Ответ: требования к аутентификации и авторизации, требования к шифрованию данных при передаче и хранении, требования к логированию и аудиту, требования к защите от утечек и несанкционированного доступа.	
12	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При разработке прототипов ИС на базе типовой ИС, какие риски должны быть оценены в рамках управления информационной безопасностью?	ПК-1
	Ответ: риски несанкционированного доступа, риски утечки данных, риски нарушения целостности информации, риски отказа в обслуживании, риски нарушения требований регуляторов.	
13	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух стандартов, используемых при создании и сопровождении ИС в области управления информационной безопасностью.	ПК-1
	Ответ: ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ISO/IEC 27001, ISO/IEC 27002, ГОСТ Р 54869-2011.	
14	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При разработке прототипов ИС на базе типовой ИС, какие меры защиты должны быть реализованы для обеспечения целостности данных?	ПК-1
	Ответ: использование контрольных сумм (хеш-функций), электронная подпись, механизмы контроля версий, журналирование изменений, резервное копирование.	
15	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух процессов управления ИБ, которые должны быть интегрированы в создание и сопровождение ИС.	ПК-1
	Ответ: управление рисками, управление инцидентами, управление доступом, управление непрерывностью бизнеса, управление активами.	
16	При верификации ИС в рамках системы управления информационной безопасностью, какой метод тестирования позволяет проверить соответствие средств защиты информации требованиям? a) нагрузочное тестирование b) тестирование безопасности (пентест, сканирование уязвимостей) c) модульное тестирование d) тестирование пользовательского интерфейса	ПК-2
	Ответ: b	
17	При обнаружении инцидента ИБ в ходе сопровождения ИС, какой документ должен быть оформлен для фиксации нарушения в рамках СУИБ? a) техническое задание b) акт об инциденте ИБ c) бизнес-план d) маркетинговый план	ПК-2
	Ответ: b	
18	При верификации ИС, какой анализ позволяет выявить уязвимости в конфигурации системы безопасности? a) статический анализ (SAST) b) анализ конфигурации и управления доступом c) нагрузочное тестирование d) тестирование удобства использования	ПК-2
	Ответ: b	
19	При обнаружении инцидента ИБ в ИС, какое действие должно быть выполнено в первую очередь для минимизации последствий? a) увольнение сотрудника b) изоляция затронутого компонента и активация плана реагирования c) перезагрузка системы d) удаление логов	ПК-2
	Ответ: b	

20	Какой инструмент применяется при тестировании ИС для обнаружения инцидентов ИБ и анализа событий безопасности? a) SIEM-система b) Microsoft Word c) Adobe Photoshop d) AutoCAD Ответ: a	ПК-2
21	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 3. Восстановление и анализ / C. Устранение уязвимости, обновление СЗИ, удаление вредоносного кода Ответ: 1-B, 2-C, 3-A	ПК-2
22	Установите соответствие между инструментом (1–3) и его назначением (A–C) при тестировании ИС для обнаружения инцидентов ИБ. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Инструмент / Назначение при тестировании ИС 1. Burp Suite / A. Выявление уязвимостей веб-приложений 2. SIEM-система / B. Централизованный сбор и корреляция событий безопасности 3. OWASP ZAP / C. Автоматизированное сканирование и пентест веб-приложений Ответ: 1-A, 2-B, 3-C	ПК-2
23	Установите соответствие между типом инцидента ИБ (1–3) и мерой реагирования (A–C) при обнаружении инцидентов ИБ в рамках сопровождения ИС. В бланк ответов запишите последовательность (например, 1-C, 2-A, 3-B). Тип инцидента ИБ / Мера реагирования 1. Вредоносное ПО / A. Блокировка учётных записей, смена паролей 2. Несанкционированный доступ / B. Изоляция заражённого сегмента, сканирование и удаление вирусов 3. Утечка данных / C. Изоляция системы, уведомление регулятора, анализ логов Ответ: 1-B, 2-A, 3-C	ПК-2
24	Установите правильную последовательность действий при обнаружении инцидента ИБ в ИС в рамках сопровождения ИС. Расположите буквы (A–D) в верном порядке. A) Обнаружение аномалии (сигнал от SIEM, сообщение от пользователя) B) Изоляция затронутого компонента и сохранение доказательств C) Устранение инцидента (исправление, обновление СЗИ, восстановление) D) Документирование инцидента и анализ причин Ответ: A → B → C → D	ПК-2
25	Установите правильную последовательность этапов верификации ИС при проверке соответствия требованиям системы управления информационной безопасностью (СУИБ). Расположите буквы (A–D) в верном порядке. A) Проверка соответствия политикам и процедурам безопасности B) Интеграционное тестирование средств защиты C) Документирование результатов и подготовка отчета о верификации D) Анализ результатов и выявление отклонений Ответ: A → B → D → C	ПК-2
26	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух признаков инцидента ИБ, которые могут быть выявлены при тестировании ИС в рамках системы управления информационной безопасностью. Ответ: необычные исходящие соединения, появление неизвестных файлов, аномалии в логах доступа, ошибки аутентификации, сбои в работе СЗИ, нехарактерная активность пользователей.	ПК-2

27	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ в ИС, какие меры должны быть приняты для обеспечения сохранности доказательств в рамках СУИБ?		ПК-2
	Ответ:	изоляция затронутого компонента, создание резервных копий логов и данных, сохранение дампов памяти, фотофиксация состояния системы, документирование времени и характера инцидента, привлечение экспертов для расследования.	
28	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух методов тестирования, используемых при верификации ИС для проверки защищенности от атак и соответствия требованиям СУИБ.		ПК-2
	Ответ:	тестирование на проникновение (пентест), статический анализ кода (SAST), динамический анализ (DAST), сканирование уязвимостей, анализ конфигурации безопасности, аудит политик доступа.	
29	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ, связанного с утечкой данных, какие меры должны быть приняты в рамках сопровождения ИС и СУИБ?		ПК-2
	Ответ:	изоляция уязвимого компонента, проверка журналов доступа, смена паролей и ключей, уведомление заинтересованных сторон и регулятора (при необходимости), усиление контроля доступа, проведение расследования, актуализация политик безопасности.	
30	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.		ПК-2
	Ответ:	SIEM-системы (Splunk, QRadar, ArcSight), системы обнаружения вторжений (IDS/IPS), WAF (Web Application Firewall), системы мониторинга логов, DLP-системы.	

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 разработке прототипов ИС на базе типовой ИС, какие требования к информационной безопасности должны быть учтены при выборе типового решения для автоматизации бизнес-процессов организации?		ПК-1
	Ответ:	требования к соответствию нормативно-правовым актам (152-ФЗ, 187-ФЗ), требования к сертификации СЗИ, требования к разграничению доступа и аудиту, требования к защите данных при передаче и хранении, требования к импортозамещению.	
2	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При разработке прототипов ИС на базе типовой ИС, какие риски информационной безопасности необходимо оценить на этапе прототипирования для обеспечения соответствия требованиям СУИБ?		ПК-1
	Ответ:	риски несанкционированного доступа, риски утечки конфиденциальных данных, риски нарушения целостности информации, риски отказа в обслуживании (DoS), риски несоответствия регуляторным требованиям, риски нарушения непрерывности бизнеса.	
3	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух требований, которые должны быть включены в техническое задание на разработку прототипов ИС на базе типовой ИС для обеспечения управления информационной безопасностью.		ПК-1
	Ответ:	требования к аутентификации и авторизации (RBAC), требования к шифрованию данных при хранении и передаче, требования к логированию и аудиту событий безопасности, требования к защите от вредоносного кода, требования к резервному копированию и восстановлению.	
4	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При создании и сопровождении ИС в рамках системы управления информационной безопасностью, какие процедуры необходимо реализовать для обеспечения непрерывности бизнеса при возникновении инцидентов?		ПК-1
	Ответ:	разработка и внедрение плана непрерывности бизнеса (BCP), резервное копирование данных, организация горячей/холодной площадки для восстановления, регулярное тестирование планов восстановления, определение критических бизнес-функций и времени восстановления (RTO/RPO).	
5	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При автоматизации бизнес-процессов с использованием типовой ИС, какие меры защиты должны быть реализованы для контроля целостности данных и предотвращения несанкционированных изменений?		ПК-1
	Ответ:	использование контрольных сумм (хеш-функций) для проверки целостности, электронная подпись (ЭЦП) для подтверждения подлинности, системы контроля версий, журналирование всех изменений с указанием пользователя и времени, разграничение прав доступа на запись и изменение.	
6	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При верификации ИС в рамках системы управления информационной безопасностью, какие виды тестирования безопасности должны быть проведены для проверки защищённости системы от внешних и внутренних угроз?		ПК-2
	Ответ:	тестирование на проникновение (пентест), сканирование уязвимостей (VA), анализ конфигурации безопасности, анализ политик доступа (RBAC), тестирование на социальную инженерию, проверка защищённости сети и приложений.	

7	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ в ходе сопровождения ИС, какие действия должен выполнить руководитель проекта для обеспечения соответствия требованиям СУИБ?		ПК-2
	Ответ:	активировать план реагирования на инциденты, изолировать затронутые компоненты, документировать инцидент (время, характер, затронутые ресурсы), уведомить заинтересованные стороны (руководство, регулятора), привлечь экспертов для расследования, провести анализ корневых причин, разработать меры предотвращения повторения.	
8	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух инструментов, используемых при тестировании ИС для обнаружения инцидентов ИБ и оценки уровня защищённости системы, и кратко опишите их назначение.		ПК-2
	Ответ:	● Nessus – сканер уязвимостей для выявления слабых мест в сетевой инфраструктуре и приложениях. ● Wireshark – анализатор сетевого трафика для обнаружения аномалий и подозрительной активности. ● Burp Suite – перехватчик HTTP-трафика и инструмент для тестирования безопасности веб-приложений. ● Splunk / QRadar – SIEM-системы для централизованного сбора, корреляции и анализа событий безопасности.	
9	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При верификации ИС в рамках СУИБ, какие метрики используются для оценки эффективности мер защиты информации и управления ИБ?		ПК-2
	Ответ:	● MTTD (Mean Time To Detect) – среднее время обнаружения инцидента. ● MTTR (Mean Time To Respond) – среднее время реагирования и устранения инцидента. ● MTBF (Mean Time Between Failures) – среднее время наработки на отказ. ● Процент покрытия тестами безопасности, количество критических уязвимостей, время устранения уязвимостей, оценка соответствия политикам безопасности.	
10	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ в ИС, какие меры должны быть приняты для восстановления нормальной работы системы и предотвращения повторения инцидента в рамках сопровождения ИС?		ПК-2
	Ответ:	устранение уязвимости (установка патча, обновление ПО, изменение конфигурации), восстановление данных из резервных копий, усиление мер защиты (дополнительная аутентификация, шифрование, разграничение доступа), актуализация политик безопасности и планов реагирования, проведение обучения персонала.	

7.1. Уровни овладения

Компетенция: ПК-1 Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы.

Индикатор достижения компетенции: ПК-1.1 Разрабатывает прототипы ИС на базе типовой 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-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

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

2. Козырь, Н. С. Оценка рисков и аудит информационной безопасности: учебник для вузов / Н. С. Козырь, В. Н. Хализев. - Москва: Юрайт, 2026. - 190 с - 978-5-534-17864-7. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/590417 (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. Щербак, А. В. Информационная безопасность: учебник для вузов / А. В. Щербак. - 2-е изд. - Москва: Юрайт, 2026. - 252 с - 978-5-9916-4299-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/589902 (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. Ссылка: https://www.standards.ru/document/7069548.aspx

Ссылка (обзор на ISO.org): https: //www.iso.org/ru/standard/65694.html - ISO/IEC 27001:2022 — Системы менеджмента информационной безопасности
Основополагающий международный стандарт по управлению информационной безопасностью. Устанавливает требования к созданию, внедрению, поддержке и непрерывному улучшению СУИБ .

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 .

3. https://old.infoforum.ru/catalog/catalog/index/id/365/conference/65 - Портал ISO27000.RU
Авторитетный информационно-аналитический ресурс по управлению информационной безопасностью: материалы по аудиту, внедрению и сертификации по стандартам СУИБ, анализ защищенности, пентесты, риск-менеджмент, форумы и каталоги .

4. https://www.consultant.ru/law/podborki/pravovoe_regulirovanie_informacionnoj_bezopasnosti/ - СПС «КонсультантПлюс»
Раздел с подборкой нормативных актов, статей и консультаций по правовому регулированию информационной безопасности .

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