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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ 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 комплексному применению организационных, технических и программно-аппаратных методов и средств защиты информации в автоматизированных системах.

Задачи изучения дисциплины:

- Изучить классификацию угроз и уязвимостей, а также основные методы и средства защиты информации (криптографические, организационные, инженерно-технические).;
- Освоить принципы построения комплексных систем защиты информации, включая межсетевое экранирование, обнаружение вторжений и антивирусную защиту.;
- Сформировать навыки применения средств защиты информации (СЗИ) и оценки эффективности систем защиты для обеспечения безопасности ИС..

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-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления

Знать:

ПК-1.2/Зн1 Принципы построения систем защиты информации, классификацию угроз и уязвимостей, методы и средства защиты (криптографические, организационные, инженерно-технические), требования нормативных документов по защите информации при разработке ИС.

Уметь:

ПК-1.2/Ум1 Создавать программный код ИС с учётом требований информационной безопасности, внедрять встраиваемые средства защиты (антивирусы, межсетевые экраны, системы обнаружения вторжений), реализовывать безопасную обработку и хранение данных в рамках автоматизации бизнес-процессов.

ПК-1.2/Ум2 Навыками разработки защищённого программного кода, применения средств защиты информации (СЗИ) в процессе создания и сопровождения ИС, методами оценки уязвимостей и документирования результатов анализа безопасности на этапе разработки прототипов ИС.

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

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

Знать:

ПК-2.2/Зн1 Методы обнаружения инцидентов ИБ с использованием средств защиты информации (СЗИ), признаки компрометации, процедуры реагирования и требования нормативных документов при расследовании инцидентов в рамках верификации ИС.

Уметь:

ПК-2.2/Ум1 Выявлять инциденты ИБ на основе анализа журналов событий, трафика и сигнатур атак, применять средства защиты для локализации угроз, оперативно принимать меры по устранению последствий и обеспечивать сохранность цифровых доказательств.

Владеть:

ПК-2.2/Нв1 Навыками работы с инструментами мониторинга и анализа безопасности (IDS/IPS, SIEM, антивирусы), методами реагирования на инциденты, приемами документирования и составления отчётности по результатам тестирования и расследования инцидентов ИБ.

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 защите информации, классификацию угроз, уязвимостей и средств защиты (СЗИ), принципы концептуально-логического проектирования систем защиты информации, нормативно-правовую базу (152-ФЗ, приказы ФСТЭК, ГОСТы) и методы оценки рисков.

Уметь:

ПК-4.1/Ум1 Анализировать бизнес-процессы и нормативные требования для формирования требований к защите информации, разрабатывать концептуальные и логические модели систем защиты (модели угроз, DFD, архитектуру СЗИ), выявлять противоречия и риски, обосновывать выбор средств защиты для ИС.

Владеть:

ПК-4.1/Нв1 Навыками разработки технического задания с разделом требований к защите информации, методами построения моделей угроз и оценки рисков, приемами верификации проектных решений, методиками согласования требований с заинтересованными сторонами и документирования результатов.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Методы и средства защиты информации» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 6.

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-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления	Встроенные языки программирования, Организация вычислительных процессов, Основы алгоритмизации и программирования, Системы искусственного интеллекта, Современные технологии и языки программирования, Теория информационной безопасности и методология защиты информации, Учебная практика: ознакомительная практика, Учебная практика: технологическая (проектно-технологическая) практика, Хранение, обработка и анализ данных	Безопасность Web-приложений, Безопасность мобильных приложений, Встроенные языки программирования, Выполнение и защита выпускной квалификационной работы, Интеллектуальные информационные системы, Организация вычислительных процессов, Программно-аппаратная защита информации, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Разработка профессиональных приложений, Современные технологии и языки программирования, Современные цифровые технологии управления предприятием, Управление информационными проектами реализации комплексной безопасности
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	Криптографическая защита информации, Правовая защита информации, 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, Криптографическая защита информации, Организационная защита информации, Правовая защита информации, 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	Встроенные языки программирования, Моделирование процессов и систем, Организация вычислительных процессов, Основы проектной деятельности, Системы искусственного интеллекта, Теория информационной безопасности и методология защиты информации, Учебная практика: технологическая (проектно-технологическая) практика	Безопасность Web-приложений, Безопасность мобильных приложений, Встроенные языки программирования, Выполнение и защита выпускной квалификационной работы, Интеллектуальные информационные системы, Компьютерная экспертиза, Моделирование процессов и систем, Организационная защита информации, Организация вычислительных процессов, 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)	Лекционные занятия (часы)	Практические занятия (часы)	Групповая контактная работа (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Шестой 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. Методы и средства защиты информации	**110**	**2**	**2**	**103,7**
Тема 1.1. Введение в методы и средства защиты информации: основные понятия и определения (угроза, уязвимость, риск, защита информации); классификация угроз и моделей нарушителя; обзор методов и средств защиты (организационные, правовые, инженерно-технические, программно-аппаратные); нормативно-правовая база защиты информации в РФ (152-ФЗ, 187-ФЗ, приказы ФСТЭК, ГОСТы); общая концепция построения комплексной системы защиты информации (КСЗИ).	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	Методы и средства защиты информации	Тестовое задание	Экзамен

6. Оценочные материалы текущего контроля

1. Методы и средства защиты информации Тестовое задание

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	При создании программного кода ИС для автоматизации бизнес-процессов, какой метод защиты информации используется для предотвращения атак типа SQL-инъекция? a) использование хранимых процедур и параметризованных запросов b) установка антивируса c) настройка межсетевого экрана d) использование SSL-сертификата		ПК-1
	Ответ:	a	
2	Что относится к средствам антивирусной защиты, которые должны быть учтены при разработке прототипов ИС? a) межсетевой экран (брандмауэр) b) антивирус с функциями поведенческого анализа и эвристического обнаружения c) система обнаружения вторжений (IDS) d) VPN-шлюз		ПК-1
	Ответ:	b	

3	Какой метод защиты информации применяется при создании программного кода для обеспечения конфиденциальности передаваемых данных в рамках автоматизации бизнес-процессов? a) шифрование (AES, RSA) и использование TLS/SSL b) сжатие данных c) бэкапирование d) логирование Ответ: a	ПК-1
4	При разработке прототипов ИС какой механизм защиты программного кода предотвращает его несанкционированное копирование и модификацию? a) обфускация кода и использование лицензионных ключей b) удаление комментариев c) минификация кода d) использование открытых библиотек Ответ: a	ПК-1
5	Какое средство защиты информации должно быть интегрировано в ИС на этапе создания программного кода для разграничения доступа пользователей к функциям системы? a) межсетевой экран b) система управления доступом (ролевая модель, RBAC) c) антивирус d) система резервного копирования Ответ: b	ПК-1
6	Установите соответствие между типом угрозы безопасности ИС (1–3) и методом защиты (A–C) при разработке прототипов ИС. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Тип угрозы / Метод защиты 1. Внедрение вредоносного кода (SQL-инъекция, XSS) / A. Использование параметризованных запросов, валидация ввода 2. Перехват сетевого трафика / B. Шифрование данных (TLS/SSL) 3. Несанкционированное копирование ПО / C. Обфускация кода и лицензирование Ответ: 1-A, 2-B, 3-C	ПК-1
7	Установите соответствие между категорией средств защиты информации (1–3) и примером (A–C) при создании программного кода для ИС. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Категория СЗИ / Пример 1. Программно-аппаратные / A. Политика паролей, инструкции для пользователей 2. Криптографические / B. Межсетевой экран, IDS/IPS 3. Организационные / C. AES-256, ЭЦП, хеш-функции Ответ: 1-B, 2-C, 3-A	ПК-1
8	Установите соответствие между этапом жизненного цикла ИС (1–3) и задачей защиты информации (A–C). В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Этап жизненного цикла ИС / Задача защиты информации 1. Разработка прототипов / A. Мониторинг инцидентов и обновление СЗИ 2. Создание программного кода / B. Анализ угроз и выбор архитектуры защиты 3. Сопровождение ИС / C. Реализация встроенных механизмов безопасности Ответ: 1-B, 2-C, 3-A	ПК-1
9	Установите правильную последовательность этапов внедрения средств защиты информации при создании программного кода ИС. A) Анализ требований к безопасности ИС B) Внедрение средств защиты (антивирус, шифрование, контроль доступа) C) Выбор методов и средств защиты информации D) Тестирование эффективности защиты Ответ: A → C → B → D	ПК-1

10	Установите правильную последовательность действий при разработке прототипов ИС с учётом требований защиты информации. Расположите буквы (A–D) в верном порядке. A) Построение модели угроз для прототипа ИС B) Разработка архитектуры с встроенными механизмами защиты C) Сбор требований к безопасности от заинтересованных сторон D) Реализация прототипа с учётом выбранных СЗИ	ПК-1
	Ответ: C → A → B → D	
11	Дайте развернутый ответ Назовите не менее двух средств защиты информации, которые должны быть интегрированы в ИС на этапе создания программного кода.	ПК-1
	Ответ: антивирус, система управления доступом (RBAC), шифрование данных (AES/TLS), система логирования и аудита.	
12	Дайте развернутый ответ При разработке прототипов ИС для автоматизации бизнес-процессов, какой метод защиты информации используется для обеспечения целостности данных?	ПК-1
	Ответ: хеш-функции (SHA-256) или электронная подпись.	
13	Дайте развернутый ответ Назовите не менее двух способов защиты программного кода от реверс-инжиниринга, применяемых при разработке прототипов ИС.	ПК-1
	Ответ: обфускация кода, упаковка (packing), анти-отладка, использование защищённых библиотек.	
14	Дайте развернутый ответ При создании программного кода ИС, какой протокол используется для защиты сетевых соединений от перехвата?	ПК-1
	Ответ: TLS/SSL.	
15	Дайте развернутый ответ Назовите не менее двух методов защиты от атак типа «отказ в обслуживании» (DDoS) при создании программного кода ИС.	ПК-1
	Ответ: ограничение частоты запросов (rate limiting), фильтрация трафика, использование CDN и балансировщиков нагрузки.	
16	При обнаружении инцидента ИБ в ИС, какое средство защиты информации позволяет оперативно выявить и зафиксировать факт несанкционированного доступа? a) антивирус b) система обнаружения вторжений (IDS) c) межсетевой экран (брандмауэр) d) средство резервного копирования	ПК-2
	Ответ: b	
17	При принятии мер по устранению инцидента ИБ, связанного с вирусной атакой, какое действие должно быть выполнено в первую очередь при сопровождении ИС? a) изоляция заражённого сегмента сети от общей ИС b) уведомление всех пользователей c) перезагрузка сервера d) удаление всех файлов	ПК-2
	Ответ: a	
18	Какой инструмент используется при тестировании ИС для выявления уязвимостей и инцидентов ИБ, связанных с небезопасными сетевыми соединениями? a) анализатор трафика (Wireshark) b) IDE (среда разработки) c) офисный пакет d) графический редактор	ПК-2
	Ответ: a	
19	При обнаружении инцидента ИБ в рамках сопровождения ИС, какой документ должен быть составлен в первую очередь? a) техническое задание b) акт расследования инцидента c) должностная инструкция d) бизнес-план	ПК-2
	Ответ: b	
20	Какое средство защиты информации позволяет при тестировании ИС выявить инциденты, связанные с утечкой конфиденциальных данных через сеть? a) DLP-система (Data Loss Prevention) b) антивирус c) система резервного копирования d) межсетевой экран	ПК-2
	Ответ: a	
21	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-A, 2-B, 3-C).	ПК-2

Тип инцидента ИБ	Мера реагирования
1. Вирусная атака	A. Изоляция заражённого сегмента, сканирование и удаление вредоносного ПО
2. Утечка данных	B. Блокировка учётных записей, смена паролей, уведомление регулятора
3. DDoS-атака	C. Перенаправление трафика, усиление мощностей, настройка фильтрации

Ответ: 1-A, 2-B, 3-C

22 Установите соответствие между инструментом (1–3) и его назначением при тестировании ИС для обнаружения инцидентов ИБ (A–C). В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). ПК-2

Инструмент	Назначение при тестировании ИС
1. SIEM-система	A. Перехват и анализ сетевого трафика
2. Wireshark	B. Централизованный сбор и корреляция событий безопасности
3. OWASP ZAP	C. Обнаружение уязвимостей в веб-приложениях

Ответ: 1-B, 2-A, 3-C

23 Установите соответствие между стадией реагирования на инцидент ИБ (1–3) и её содержанием (A–C) при обнаружении инцидентов ИБ и принятии мер. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). ПК-2

Стадия реагирования	Содержание стадии
1. Обнаружение и локализация	A. Восстановление работоспособности, удаление вредоносного кода
2. Устранение	B. Мониторинг аномалий, идентификация затронутых компонентов
3. Восстановление и анализ	C. Документирование, анализ причин, разработка мер предотвращения

Ответ: 1-B, 2-A, 3-C

24 Установите правильную последовательность действий при обнаружении инцидента ИБ в ИС в рамках сопровождения ИС. Расположите буквы (A–D) в верном порядке. ПК-2
A) Устранение инцидента (изоляция, удаление вредоносного кода, обновление)
B) Обнаружение аномалии (необычный трафик, сбой в работе)
C) Анализ причин и разработка мер предотвращения
D) Документирование инцидента и уведомление заинтересованных сторон

Ответ: B → A → D → C

25 Установите правильную последовательность этапов тестирования ИС для обнаружения инцидентов ИБ. Расположите буквы (A–D) в верном порядке. ПК-2
A) Анализ результатов и выявление уязвимостей
B) Планирование тестирования (определение целей и границ)
C) Выполнение тестов (сканирование, анализ трафика)
D) Подготовка отчёта и рекомендаций по устранению

Ответ: B → C → A → D

26 Дайте развернутый ответ ПК-2
Назовите не менее двух признаков инцидента ИБ в ИС, которые могут быть выявлены при тестировании ИС.

Ответ: необычные исходящие соединения, высокая активность процессора, появление неизвестных файлов, множественные ошибки аутентификации.

27 Дайте развернутый ответ ПК-2
При обнаружении инцидента ИБ, связанного с утечкой данных, какое действие должно быть выполнено в первую очередь?

Ответ: изоляция скомпрометированного сегмента сети и блокировка учётных записей.

28 Дайте развернутый ответ ПК-2
Назовите систему, которая используется для централизованного сбора и корреляции событий безопасности при обнаружении инцидентов ИБ.

Ответ: SIEM-система (Security Information and Event Management).

29 Дайте развернутый ответ ПК-2
Какой документ фиксирует информацию об инциденте ИБ при сопровождении ИС?

Ответ: акт расследования инцидента ИБ (отчёт об инциденте).

30	Дайте развернутый ответ Назовите не менее двух мер по предотвращению повторения инцидентов ИБ после их обнаружения. Ответ: усиление мониторинга, обновление политик безопасности, установка дополнительных СЗИ, обучение персонала.	ПК-2
31	При выявлении требований к Системе, какие требования определяют необходимость использования сертифицированных средств защиты информации? a) функциональные требования b) нормативные требования (регуляторные ограничения) c) интерфейсные требования d) требования к производительности Ответ: b	ПК-4
32	На этапе концептуально-логического проектирования ИС какая модель описывает потоки данных и зоны доверия в системе? a) ER-диаграмма b) DFD (диаграмма потоков данных) c) UML-диаграмма классов d) BPMN-диаграмма Ответ: b	ПК-4
33	При выявлении требований к Системе для ИС, обрабатывающей персональные данные, какой нормативный документ является основным? a) ГОСТ 28147-89 b) 152-ФЗ «О персональных данных» c) ISO 9001 d) ITIL Ответ: b	ПК-4
34	Что является результатом этапа концептуально-логического проектирования ИС в области защиты информации? a) исходный код приложения b) модель угроз и архитектура системы защиты c) протоколы тестирования d) маркетинговый план Ответ: b	ПК-4
35	При выявлении требований к Системе для ИС, какой метод используется для обоснования выбора средств защиты информации? a) анализ рисков b) написание кода c) тестирование d) установка оборудования Ответ: a	ПК-4
36	Установите соответствие между этапом проектирования/сопровождения (1–3) и его содержанием (A–C) в области защиты информации. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Этап / Содержание 1. Выявление требований / A. Построение модели угроз, выбор архитектуры защиты 2. Концептуально-логическое проектирование / B. Определение требований к классам СЗИ и нормативной базе 3. Сопровождение проектных решений / C. Актуализация документации при изменении угроз и требований Ответ: 1-B, 2-A, 3-C	ПК-4
37	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). Нормативный документ / Содержание требований 1. 152-ФЗ «О персональных данных» / A. Требования к сертификации средств защиты 2. Приказы ФСТЭК России / B. Требования к защите персональных данных 3. ГОСТ Р 34.10-2012 / C. Стандарт электронной подписи Ответ: 1-B, 2-A, 3-C	ПК-4
38	Установите соответствие между типом требования к защите информации (1–3) и его примером (A–C) при выявлении требований к Системе. В бланк ответов запишите последовательность (например, 1-C, 2-B, 3-A).	ПК-4

		Тип требования	Пример требования
		1. Функциональное	A. «Система должна использовать сертифицированный межсетевой экран»
		2. Нефункциональное (безопасность)	B. «Время восстановления после атаки не должно превышать 1 часа»
		3. Нормативное	C. «Система должна обеспечивать шифрование данных по алгоритму AES-256»
	Ответ:	1-C, 2-B, 3-A	
39	Установите правильную последовательность этапов выявления требований к защите информации для ИС. Расположите буквы (A–D) в верном порядке. A) Проведение анализа рисков и идентификация угроз B) Изучение нормативно-правовых требований C) Проведение интервью с заинтересованными сторонами D) Формирование и согласование раздела требований к защите информации в ТЗ		ПК-4
	Ответ:	B → C → A → D	
40	Установите правильную последовательность этапов построения модели угроз при концептуально-логическом проектировании ИС. Расположите буквы (A–D) в верном порядке. A) Идентификация активов и их ценности B) Построение диаграммы потоков данных (DFD) C) Определение угроз и уязвимостей для каждого актива D) Разработка мер противодействия и выбор СЗИ		ПК-4
	Ответ:	A → B → C → D	
41	Дайте развернутый ответ Назовите не менее двух методов выявления требований к защите информации для ИС.		ПК-4
	Ответ:	анализ нормативных документов, проведение анализа рисков, интервьюирование заинтересованных сторон, анкетирование.	
42	Дайте развернутый ответ Какой артефакт разрабатывается на этапе концептуально-логического проектирования ИС и описывает угрозы для системы?		ПК-4
	Ответ:	модель угроз.	
43	Дайте развернутый ответ Для чего используются экспертные методы при выявлении требований к Системе в области защиты информации?		ПК-4
	Ответ:	для выявления скрытых рисков, обоснования выбора СЗИ и проверки реалистичности требований.	
44	Дайте развернутый ответ Назовите не менее двух нормативных документов, требования которых должны быть выявлены при проектировании системы защиты информации для ИС, обрабатывающей персональные данные.		ПК-4
	Ответ:	152-ФЗ «О персональных данных», Приказы ФСТЭК России, ГОСТ Р 34.10-2012.	
45	Дайте развернутый ответ Какой раздел технического задания должен быть обязательным при выявлении требований к Системе для ИС, обрабатывающей конфиденциальные данные?		ПК-4
	Ответ:	раздел требований к защите информации.	

7. Оценочные материалы промежуточной аттестации

Экзамен шестой семестр

№ п/п	Содержание вопроса	Правильный ответ (ключ ответа)	Компетенция
1	Дайте развернутый ответ При создании программного кода ИС для автоматизации бизнес-процессов, какой метод защиты информации используется для предотвращения подделки передаваемых данных?		ПК-1
	Ответ:	электронная подпись (ЭЦП) или HMAC (хеш-код аутентификации сообщения).	
2	Дайте развернутый ответ Назовите не менее двух методов защиты информации, которые должны быть реализованы на уровне программного кода для защиты от атак типа «переполнение буфера».		ПК-1
	Ответ:	проверка границ массивов, использование безопасных функций (например, strncpy вместо strcpy), использование языков с автоматическим управлением памятью.	
3	Дайте развернутый ответ При разработке прототипов ИС какой механизм используется для обеспечения безопасного хранения паролей пользователей в базе данных?		ПК-1
	Ответ:	хеширование с солью (bcrypt, PBKDF2, Argon2).	
4	Дайте развернутый ответ Назовите не менее двух средств защиты информации, которые должны быть интегрированы в ИС на этапе создания программного кода для защиты от утечек данных.		ПК-1

	Ответ:	шифрование данных (AES-256), DLP-система, система контроля доступа (RBAC), система логирования и аудита.	
5	Дайте развернутый ответ При автоматизации бизнес-процессов в ИС, какой метод защиты информации используется для предотвращения несанкционированного доступа к функциям системы через веб-интерфейс?		ПК-1
	Ответ:	аутентификация и авторизация (например, OAuth 2.0, JWT, сессионные токены).	
6	Дайте развернутый ответ При обнаружении инцидента ИБ, связанного с вредоносным ПО в ИС, какие меры должны быть приняты в первую очередь для локализации угрозы?		ПК-2
	Ответ:	изоляция заражённого сегмента сети, отключение скомпрометированных узлов, запуск антивирусного сканирования.	
7	Дайте развернутый ответ Назовите не менее двух признаков инцидента ИБ, которые могут быть выявлены при тестировании ИС с помощью анализа сетевого трафика.		ПК-2
	Ответ:	необычные исходящие соединения на неизвестные IP-адреса, аномально высокий объём передаваемых данных, наличие подозрительных протоколов.	
8	Дайте развернутый ответ При обнаружении инцидента ИБ, связанного с утечкой конфиденциальных данных, какой документ должен быть составлен и передан регулятору?		ПК-2
	Ответ:	уведомление об инциденте (в соответствии с 152-ФЗ) или акт расследования инцидента ИБ.	
9	Дайте развернутый ответ Назовите не менее двух инструментов, используемых при тестировании ИС для обнаружения инцидентов ИБ в веб-приложениях.		ПК-2
	Ответ:	Burp Suite, OWASP ZAP, Nikto, Acunetix.	
10	Дайте развернутый ответ При принятии мер после обнаружения инцидента ИБ, какие действия необходимо выполнить для восстановления целостности данных?		ПК-2
	Ответ:	восстановление данных из резервных копий, проверка целостности файлов через хеш-суммы, анализ журналов аудита для выявления изменений.	
11	Дайте развернутый ответ Назовите не менее двух методов выявления требований к защите информации для ИС, обрабатывающей конфиденциальные данные.		ПК-4
	Ответ:	анализ нормативно-правовых документов (152-ФЗ, приказы ФСТЭК), интервьюирование заинтересованных сторон, проведение анализа рисков.	
12	Дайте развернутый ответ На этапе концептуально-логического проектирования ИС какой артефакт описывает все возможные источники угроз и каналы утечки информации?		ПК-4
	Ответ:	модель угроз.	
13	Дайте развернутый ответ При выявлении требований к Системе, какие требования определяют необходимость использования конкретных классов СЗИ (например, межсетевых экранов, СОВ, антивирусов)?		ПК-4
	Ответ:	нормативные требования (регуляторные ограничения) или требования безопасности, основанные на результатах анализа рисков.	

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-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления.

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-2.2 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. Внуков, А. А. Защита информации в банковских системах: учебник для вузов / А. А. Внуков. - 2-е изд. - Москва: Юрайт, 2026. - 246 с - 978-5-534-01679-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/584051 (дата обращения: 21.05.2026). - Режим доступа: по подписке

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

Дополнительная литература

1. Щербак, А. В. Тестирование программного обеспечения: учебник для вузов / А. В. Щербак. - Москва: Юрайт, 2026. - 145 с - 978-5-534-19291-9. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/590250 (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

1. http://pravo.gov.ru/ - Государственная система правовой информации «Официальный интернет-портал правовой информации»

Ресурсы «Интернет»

1. https://fstec.ru/ - ФСТЭК России (официальный сайт)

Публикует нормативные правовые акты, приказы, методические документы по сертификации средств защиты информации, аттестации объектов информатизации, методики моделирования угроз и анализа защищенности. Необходим для изучения нормативно-правовой базы защиты информации в РФ.

Ссылка: https://fstec.ru/

Онлайн-курсы

1. НИУ ВШЭ — «Методы и средства защиты информации»

Курс знакомит с основными понятиями защиты информации, принципами построения систем защиты, категориями мер защиты, их сильными и слабыми сторонами. Слушатели получат навыки выбора решений из различных категорий методов и средств защиты в соответствии с требованиями для конкретных ИС. Состоит из 9 лекций с видеофрагментами и тестами. В качестве эксперта участвует представитель компании «ИнфоТеКС» — крупного российского разработчика СКЗИ.

2. https://stepik.org - Платформа с онлайн-курсами от авторов-практиков

3. https://forum.1c.ru/ - Форум разработчиков 1С: на https://forum.1c.ru/ можно найти обсуждения, кейсы и ответы на вопросы по разработке мобильных приложений.

4. https://clck.ru/3RGazU - Российское общество «Знание» — «Цифровая гигиена»

Бесплатный просветительский онлайн-курс по цифровой гигиене и безопасности в интернете. Состоит из 11 разделов с видеолекциями и конспектами, по окончании выдаётся сертификат.

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