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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ»

Уровень высшего образования: бакалавриат

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль)подготовки: Прикладная информатика и защита информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очно-заочная

Год набора (приема на обучение): 2026

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

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

г. Самара, 2026

Разработчики:
Не имеет Колотилина М. А.

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

Согласование и утверждение

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

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование теоретических знаний и практических навыков по анализу уязвимостей, разработке защищённого кода и обеспечению безопасности мобильных приложений на всех этапах жизненного цикла

Задачи изучения дисциплины:

- Изучить архитектуру, модели угроз и основные векторы атак на мобильные приложения по классификации OWASP Mobile Top 10;
- Освоить методы статического и динамического анализа кода для выявления уязвимостей, а также принципы безопасного хранения и передачи данных;
- Сформировать навыки применения средств защиты (шифрование, аутентификация, обфускация) и тестирования безопасности мобильных приложений.

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 безопасной разработки мобильных приложений, модели угроз и векторы атак (OWASP Mobile Top 10), методы шифрования, аутентификации и безопасного хранения данных на клиентской стороне.

Уметь:

ПК-1.2/Ум1 Создавать защищённый программный код мобильных приложений, реализовывать механизмы безопасной авторизации, шифрования данных и защиты от обратной разработки (обфускация, анти-отладка).

Владеть:

ПК-1.2/Нв1 Навыками статического и динамического анализа кода на предмет уязвимостей, инструментами тестирования безопасности мобильных приложений (Burp Suite, MobSF, Frida), методами интеграции средств защиты в процесс разработки и сопровождения 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 в мобильных приложениях, признаки компрометации клиентской и серверной частей, процедуры реагирования на инциденты и порядок документирования.

Уметь:

ПК-2.2/Ум1 Выявлять инциденты ИБ в мобильных приложениях по системным журналам, сетевым аномалиям и артефактам, оперативно локализовать угрозу и принимать меры по устранению последствий.

Владеть:

ПК-2.2/Нв1 Навыками работы с инструментами мониторинга и анализа безопасности мобильных приложений, методами сбора цифровых доказательств, приемами реагирования на инциденты в рамках сопровождения ИС.

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 безопасности мобильных приложений, модели угроз и рисков, принципы концептуально-логического проектирования защищённых ИС, нотации моделирования бизнес-процессов и структур данных.

Уметь:

ПК-4.1/Ум1 Применять инструменты сбора и анализа требований безопасности, разрабатывать концептуальные и логические модели мобильных ИС с учётом угроз, выявлять противоречия и риски в требованиях с использованием экспертных методов.

Владеть:

ПК-4.1/Нв1 Навыками формирования технического задания с разделом требований безопасности, методами согласования требований с заинтересованными сторонами, приёмами верификации и валидации проектных решений на основе анализа угроз и экспертных заключений.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Безопасность мобильных приложений» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 7.

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

Компетенция	Предшествующие дисциплины	Последующие дисциплины
ПК-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	Безопасность Web-приложений, Встроенные языки программирования, Методы и средства защиты информации, Организация вычислительных процессов, Основы алгоритмизации и программирования, Программно-аппаратная защита информации, Производственная практика: технологическая (проектно-технологическая) практика, 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, Выполнение и защита выпускной квалификационной работы, Интеллектуальные информационные системы, Программно-аппаратная защита информации, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Разработка профессиональных приложений, 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	Безопасность Web-приложений, Криптографическая защита информации, Методы и средства защиты информации, Организационная защита информации, Правовая защита информации, Программно-аппаратная защита информации, Производственная практика: технологическая (проектно-технологическая) практика, Теория информационной безопасности и методология защиты информации, Техническая защита информации, Учебная практика: технологическая (проектно-технологическая) практика	Безопасность Web-приложений, Выполнение и защита выпускной квалификационной работы, Организационная 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	Безопасность Web-приложений, Встроенные языки программирования, 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, Производственная практика: технологическая (проектно-технологическая) практика, Системы искусственного интеллекта, Теория информационной безопасности и методология защиты информации, Учебная практика: технологическая (проектно-технологическая) практика	Безопасность Web-приложений, Выполнение и защита выпускной квалификационной работы, Интеллектуальные информационные системы, Компьютерная экспертиза, Организационная защита информации, Проектирование и реализация баз данных, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Современные цифровые технологии управления предприятием, Специализированные ИТ в правоохранительной деятельности, Цифровая культура в профессиональной деятельности

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Седьмой семестр	108	3	4	2	2	0,15	85,85	Зачет
Всего	108	3	4	2	2	0,15	85,85	18

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лабораторные занятия	Лекционные занятия	Самостоятельная работа
Раздел 1. Безопасность мобильных приложений	**90**	**2**	**2**	**85,85**

Тема 1.1. Введение в безопасность мобильных приложений: актуальность и современные угрозы; классификация мобильных ОС (Android, iOS) и их архитектурные особенности с точки зрения безопасности; основные векторы атак на мобильные приложения; обзор OWASP Mobile Top 10 и стандартов безопасной разработки.	90	2	2	85,85

5.2. Контрольные мероприятия по дисциплине

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

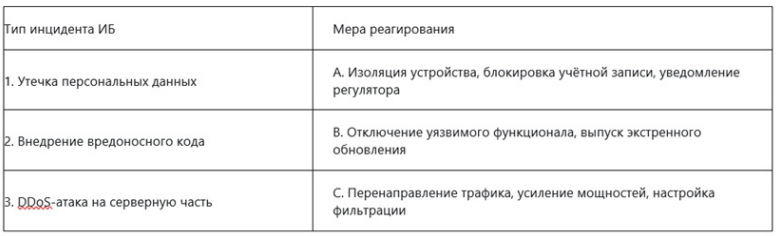
№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Безопасность мобильных приложений	Тестовое задание	Зачет

6. Оценочные материалы текущего контроля

1. Безопасность мобильных приложений Тестовое задание

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	При создании программного кода мобильного приложения для автоматизации бизнес-процессов какой механизм обеспечивает безопасное хранение учётных данных на устройстве Android? a) SharedPreferences без шифрования b) Android Keystore System c) обычный текстовый файл d) SQLite без шифрования		ПК-1
	Ответ:	b	
2	Какой метод защиты от обратной разработки (реверс-инжиниринга) должен применяться при разработке прототипов ИС на платформе Android? a) удаление всех комментариев из кода b) обфускация кода (ProGuard/R8) c) увеличение размера APK-файла d) переименование пакета приложения		ПК-1
	Ответ:	b	
3	При создании программного кода мобильного приложения для iOS, какой фреймворк используется для безопасного хранения криптографических ключей и паролей? a) CoreData b) Keychain Services c) UserDefaults d) Security Framework только для шифрования		ПК-1
	Ответ:	b	

4	Для автоматизации бизнес-процессов в мобильном приложении необходимо реализовать безопасную сетевую передачу данных. Какой протокол обязателен к использованию? a) HTTP без шифрования b) FTP c) HTTPS (TLS/SSL) d) Telnet Ответ: c	ПК-1
5	При разработке прототипов ИС какой метод позволяет выявить уязвимости в коде мобильного приложения без его запуска? a) динамический анализ b) статический анализ (SAST) c) пентест в реальном времени d) фаззинг Ответ: b	ПК-1
6	Установите соответствие между типом уязвимости мобильного приложения (1–3) и мерой её устранения (A–C) при создании программного кода. Тип уязвимости — Мера устранения 1. Небезопасное хранение данных — A. Использование HTTPS и валидация сертификатов 2. Перехват сетевого трафика — B. Применение обфускации и анти-отладки 3. Реверс-инжиниринг кода — C. Шифрование данных через Keystore/Keychain Ответ: 1-C, 2-A, 3-B	ПК-1
7	Установите соответствие между инструментом анализа безопасности (1–3) и его назначением (A–C) при разработке прототипов ИС. Инструмент — Назначение 1. MobSF (Mobile Security Framework) — A. Динамический анализ и перехват вызовов API 2. Frida — B. Автоматизированный статический и динамический анализ Android/iOS 3. Burp Suite — C. Перехват и анализ сетевого трафика между приложением и сервером Ответ: 1-B, 2-A, 3-C	ПК-1
8	Установите соответствие между платформой мобильной разработки (1–3) и механизмом безопасности (A–C), используемым при создании программного кода. Платформа — Механизм безопасности 1. Android — A. Keychain Services + App Attest 2. iOS — B. ProGuard/R8 обфускация + Keystore 3. Кроссплатформенная (Flutter/React Native) — C. Зависимость от безопасности платформы + дополнительные библиотеки защиты Ответ: 1-B, 2-A, 3-C	ПК-1
9	Установите правильную последовательность этапов разработки прототипов ИС с учётом требований безопасности мобильного приложения. Расположите буквы (A–D) в верном порядке. A) Внедрение механизмов шифрования и безопасной аутентификации B) Проведение статического анализа кода на наличие уязвимостей C) Сбор и анализ требований к безопасности приложения D) Разработка архитектуры и модели угроз Ответ: C → D → A → B	ПК-1
10	Установите правильную последовательность действий при создании программного кода для безопасной сетевой передачи данных в мобильном приложении. Расположите буквы (A–D) в верном порядке. A) Валидация сертификата сервера на клиенте B) Настройка HTTPS с TLS-шифрованием на серверной стороне C) Реализация механизма повторных попыток при сбоях D) Установка защищённого соединения между приложением и сервером Ответ: B → A → D → C	ПК-1

11	Дайте развернутый ответ Назовите не менее двух методов защиты программного кода мобильного приложения от реверс-инжиниринга, применяемых при создании программного кода. Ответ: обфускация кода, анти-отладка, упаковка (packing).	ПК-1
12	Дайте развернутый ответ Какой инструмент статического анализа используется для выявления уязвимостей при разработке прототипов ИС на платформе Android? Ответ: MobSF (Mobile Security Framework) или QARK.	ПК-1
13	Дайте развернутый ответ Назовите не менее двух механизмов безопасного хранения данных на мобильном устройстве при автоматизации бизнес-процессов. Ответ: Android Keystore, iOS Keychain, зашифрованная SQLite-база данных.	ПК-1
14	Дайте развернутый ответ Какая технология используется для безопасной аутентификации пользователей в мобильных приложениях без передачи пароля по сети? Ответ: OAuth 2.0 / JWT (JSON Web Token).	ПК-1
15	Дайте развернутый ответ Назовите основной документ (стандарт) OWASP, определяющий минимальный набор требований к безопасности мобильных приложений при разработке прототипов ИС. Ответ: OWASP MASVS (Mobile Application Security Verification Standard).	ПК-1
16	При обнаружении инцидента ИБ, связанного с утечкой данных из мобильного приложения, какое действие должно быть выполнено в первую очередь при сопровождении ИС? a) уведомление всех пользователей об инциденте b) изоляция скомпрометированного устройства и блокировка учётной записи c) удаление приложения из магазина d) перезагрузка сервера Ответ: b	ПК-2
17	Какой артефакт мобильного приложения в первую очередь анализируется при тестировании ИС для обнаружения инцидентов ИБ на платформе Android? a) APK-файл b) системный журнал (Logcat) c) графические ресурсы приложения d) манифест-файл (AndroidManifest.xml) Ответ: b	ПК-2
18	При обнаружении инцидента ИБ, связанного с вредоносным ПО в мобильном приложении, какой инструмент используется для динамического анализа поведения приложения? a) MobSF (статический анализ) b) Frida c) ProGuard d) Android Studio Ответ: b	ПК-2
19	Какое действие относится к принятию мер при обнаружении инцидента ИБ в мобильном приложении, связанного с компрометацией учётных записей пользователей? a) уведомление пользователей о необходимости смены пароля b) удаление логов инцидента c) отключение системы мониторинга d) игнорирование инцидента до следующего обновления Ответ: a	ПК-2
20	При тестировании ИС для обнаружения инцидентов ИБ, связанных с сетевыми атаками на мобильное приложение, какой инструмент позволяет перехватывать и анализировать трафик? a) Android Studio b) Burp Suite c) ProGuard d) Keystore Ответ: b	ПК-2
21	Установите соответствие между типом инцидента ИБ в мобильном приложении (1–3) и мерой реагирования (A–C) при обнаружении инцидентов ИБ в рамках сопровождения ИС.  Тип инцидента ИБ / Мера реагирования 1. Утечка персональных данных / A. Изоляция устройства, блокировка учётной записи, уведомление регулятора 2. Внедрение вредоносного кода / B. Отключение уязвимого функционала, выпуск экстренного обновления 3. DDoS-атака на серверную часть / C. Перенаправление трафика, усиление мощностей, настройка фильтрации	ПК-2

	Ответ: 1-A, 2-B, 3-C	
22	Установите соответствие между инструментом мониторинга (1–3) и его назначением при обнаружении инцидентов ИБ в мобильном приложении (A–C). В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Инструмент | Назначение при обнаружении инцидентов ИБ 1. SIEM-система | A. Анализ поведения приложения в реальном времени 2. Frida | B. Централизованный сбор и корреляция событий безопасности 3. Logcat / OSLog | C. Просмотр системных журналов мобильного устройства Ответ: 1-B, 2-A, 3-C	ПК-2
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). 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	ПК-2
24	Установите правильную последовательность действий при обнаружении инцидента ИБ в мобильном приложении в рамках сопровождения ИС. Расположите буквы (A–D) в верном порядке. A) Документирование инцидента и уведомление заинтересованных сторон B) Обнаружение аномалии (необычный трафик, сбой в работе) C) Устранение инцидента (блокировка, изоляция, обновление) D) Анализ причин и разработка мер предотвращения Ответ: B → C → A → D	ПК-2
25	Установите правильную последовательность действий при тестировании ИС для обнаружения инцидентов ИБ в мобильном приложении. Расположите буквы (A–D) в верном порядке. A) Перехват сетевого трафика с помощью Burp Suite B) Запуск приложения на тестовом устройстве C) Анализ системных журналов (Logcat) на наличие ошибок D) Воспроизведение сценариев эксплуатации уязвимостей Ответ: B → A → D → C	ПК-2
26	Дайте развернутый ответ Назовите не менее двух признаков инцидента ИБ в мобильном приложении, которые могут быть выявлены при тестировании ИС. Ответ: необычные исходящие соединения, высокая фоновая активность процессора, появление неизвестных файлов.	ПК-2
27	Дайте развернутый ответ Какое действие должно быть выполнено в первую очередь при обнаружении инцидента ИБ, связанного с утечкой данных? Ответ: изоляция скомпрометированного устройства и блокировка учётной записи пользователя.	ПК-2
28	Дайте развернутый ответ Назовите инструмент для динамического анализа мобильных приложений, используемый при обнаружении инцидентов ИБ. Ответ: Frida.	ПК-2
29	Дайте развернутый ответ Какой документ фиксирует информацию об инциденте ИБ в мобильном приложении при сопровождении ИС? Ответ: отчёт об инциденте / акт расследования инцидента ИБ.	ПК-2
30	Дайте развернутый ответ Перечислите не менее двух мер по предотвращению повторения инцидентов ИБ после их обнаружения. Ответ: обновление механизмов безопасности, усиление мониторинга, обучение разработчиков.	ПК-2

31	При выявлении требований к Системе для мобильного приложения, какие требования определяют необходимость двухфакторной аутентификации? a) функциональные требования b) нефункциональные требования (безопасность) c) бизнес-ограничения d) интерфейсные требования Ответ: b	ПК-4
32	На этапе концептуально-логического проектирования ИС какая модель описывает сущности, атрибуты и связи между ними без привязки к конкретной СУБД? a) физическая модель данных b) логическая модель данных (ER-диаграмма) c) сетевая модель d) иерархическая модель Ответ: b	ПК-4
33	При выявлении требований к Системе для мобильного приложения, какой метод сбора требований предполагает непосредственное наблюдение за работой пользователей? a) интервьюирование b) анкетирование c) наблюдение (ethnography) d) анализ документов Ответ: c	ПК-4
34	Что является результатом этапа концептуально-логического проектирования ИС? a) утверждённое техническое задание b) логическая модель данных и диаграммы потоков данных (DFD) c) исходный код приложения d) протоколы тестирования Ответ: b	ПК-4
35	При выявлении требований к Системе для мобильного приложения экспертные методы анализа используются для a) написания программного кода b) обоснования проектных решений и выявления скрытых рисков безопасности c) тестирования готового приложения d) настройки серверного оборудования Ответ: b	ПК-4
36	Установите соответствие между этапом проектирования ИС (1–3) и его результатом (A–C) при выявлении требований к Системе и концептуально-логическом проектировании. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Этап проектирования / Результат этапа 1. Выявление требований / A. ER-диаграмма и UML-модели архитектуры 2. Концептуальное проектирование / B. Техническое задание с требованиями безопасности 3. Логическое проектирование / C. Концептуальная модель угроз и потоков данных Ответ: 1-B, 2-C, 3-A	ПК-4
37	Установите соответствие между типом требования к мобильному приложению (1–3) и его примером (A–C) при выявлении требований к Системе. В бланк ответов запишите последовательность (например, 1-C, 2-B, 3-A). Тип требования / Пример требования 1. Функциональное / A. «Приложение должно использовать TLS 1.2 для передачи данных» 2. Нефункциональное (безопасность) / B. «Время авторизации не должно превышать 3 секунд» 3. Ограничение (дизайн-констрейнт) / C. «Приложение должно предоставлять возможность входа по биометрии» Ответ: 1-C, 2-B, 3-A	ПК-4
38	Установите соответствие между элементом модели угроз (1–3) и его описанием (A–C) при концептуально-логическом проектировании ИС. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Элемент модели угроз / Описание	ПК-4

		1. Актив (Asset) — A. Потенциальный источник угрозы (злоумышленник, вредоносное ПО) 2. Угроза (Threat) — B. То, что представляет ценность и требует защиты (данные, функционал) 3. Уязвимость (Vulnerability) — C. Слабость в системе, которая может быть использована для реализации угрозы	
	Ответ:	1-B, 2-A, 3-C	
39	Установите правильную последовательность этапов выявления требований к Системе для мобильного приложения. Расположите буквы (A–D) в верном порядке. A) Проведение интервью и сессий сбора требований с заказчиком и пользователями B) Изучение предметной области и нормативных требований по безопасности C) Формирование и согласование технического задания с разделом требований ИБ D) Анализ полученных данных, выявление противоречий и рисков		ПК-4
	Ответ:	B → A → D → C	
40	Установите правильную последовательность построения модели угроз для мобильного приложения при концептуально-логическом проектировании ИС. Расположите буквы (A–D) в верном порядке. A) Определение активов и их ценности B) Разработка мер противодействия и обоснование проектных решений C) Идентификация угроз и уязвимостей для каждого актива D) Построение диаграммы потоков данных (DFD) приложения		ПК-4
	Ответ:	A → D → C → B	
41	Дайте развернутый ответ Назовите не менее двух методов выявления требований к Системе для мобильного приложения.		ПК-4
	Ответ:	интервьюирование, анкетирование, наблюдение, анализ документов.	
42	Дайте развернутый ответ Какой артефакт является результатом концептуально-логического проектирования ИС?		ПК-4
	Ответ:	логическая модель данных (ER-диаграмма) и UML-диаграммы архитектуры.	
43	Дайте развернутый ответ Для чего используются экспертные методы на этапе выявления требований к Системе?		ПК-4
	Ответ:	для выявления скрытых рисков, проверки реалистичности требований безопасности и обоснования проектных решений.	
44	Дайте развернутый ответ Назовите три основных компонента модели «сущность-связь» (ER-модели), используемой при концептуально-логическом проектировании.		ПК-4
	Ответ:	сущности, атрибуты, связи.	
45	Дайте развернутый ответ Какой раздел технического задания должен быть обязательным при выявлении требований к Системе для мобильного приложения?		ПК-4
	Ответ:	раздел требований к информационной безопасности.	

7. Оценочные материалы промежуточной аттестации

Зачет седьмой семестр

№ п/п	Содержание вопроса	Правильный ответ (ключ ответа)	Компетенция
1	Дайте развернутый овтет Назовите инструмент обфускации кода, используемый при создании программного кода для платформы Android.		ПК-1
	Ответ:	ProGuard / R8.	
2	Дайте развернутый овтет При создании программного кода мобильного приложения для iOS, какой фреймворк используется для безопасного хранения паролей и ключей?		ПК-1
	Ответ:	Keychain Services.	
3	Дайте развернутый овтет Назовите не менее двух способов защиты от реверс-инжиниринга при разработке прототипов ИС.		ПК-1
	Ответ:	обфускация кода, упаковка (packing), анти-отладка, проверка целостности.	
4	Дайте развернутый овтет Какой протокол шифрования должен использоваться для безопасной сетевой передачи данных при создании программного кода мобильного приложения?		ПК-1
	Ответ:	TLS (Transport Layer Security).	
5	Дайте развернутый овтет При автоматизации бизнес-процессов в мобильном приложении, какой механизм обеспечивает безопасную аутентификацию без передачи пароля по сети?		ПК-1
	Ответ:	OAuth 2.0 / JWT (JSON Web Token).	

6	Дайте развернутый овтет Назовите не менее двух методов безопасного хранения данных на устройстве Android при создании программного кода.		ПК-1
	Ответ:	Android Keystore, EncryptedSharedPreferences, зашифрованная SQLite.	
7	Дайте развернутый овтет Какой стандарт OWASP определяет минимальный набор требований к безопасности мобильных приложений при разработке прототипов ИС?		ПК-1
	Ответ:	OWASP MASVS (Mobile Application Security Verification Standard).	
8	Дайте развернутый овтет При создании программного кода мобильного приложения, как называется процесс проверки кода на уязвимости без его запуска?		ПК-1
	Ответ:	статический анализ (SAST / Static Application Security Testing).	
9	Дайте развернутый овтет Назовите не менее двух мер защиты от несанкционированного доступа к данным в мобильном приложении при автоматизации бизнес-процессов.		ПК-1
	Ответ:	шифрование данных, биометрическая аутентификация, двухфакторная аутентификация.	
10	Дайте развернутый овтет При создании программного кода кроссплатформенного мобильного приложения (Flutter/React Native), от чего зависит уровень безопасности приложения?		ПК-1
	Ответ:	от безопасности используемой платформы и дополнительных библиотек защиты.	
11	Дайте развернутый ответ Назовите не менее двух признаков инцидента ИБ в мобильном приложении, которые могут быть выявлены при тестировании ИС.		ПК-2
	Ответ:	необычные исходящие сетевые соединения, высокая фоновая активность процессора, появление неизвестных файлов.	
12	Дайте развернутый ответ При обнаружении инцидента ИБ, связанного с утечкой данных, какое действие выполняется в первую очередь при сопровождении ИС?		ПК-2
	Ответ:	изоляция скомпрометированного устройства и блокировка учётной записи пользователя.	
13	Дайте развернутый ответ Назовите инструмент для динамического анализа мобильных приложений, используемый при обнаружении инцидентов ИБ.		ПК-2
	Ответ:	Frida.	
14	Дайте развернутый ответ При обнаружении инцидента ИБ, связанного с вредоносным ПО, какое экстренное обновление должно быть выпущено для пользователей?		ПК-2
	Ответ:	обновление безопасности (security patch) с удалением уязвимости.	
15	Дайте развернутый ответ Назовите не менее двух методов выявления требований к Системе для мобильного приложения.		ПК-4
	Ответ:	интервьюирование, анкетирование, наблюдение, анализ документов, прототипирование.	
16	Дайте развернутый ответ Для чего используются экспертные методы на этапе выявления требований к Системе для мобильного приложения?		ПК-4
	Ответ:	для выявления скрытых рисков, проверки реалистичности требований безопасности и обоснования проектных решений.	
17	Дайте развернутый ответ Назовите не менее двух заинтересованных сторон (стейкхолдеров), с которыми проводится согласование требований при выявлении требований к Системе.		ПК-4
	Ответ:	заказчик, конечные пользователи, системный аналитик, разработчики, эксперты по ИБ.	
18	Дайте развернутый ответ Какие требования описывают ограничения по времени отклика, производительности и доступности мобильного приложения при выявлении требований к Системе?		ПК-4
	Ответ:	нефункциональные требования (требования к производительности и надёжности).	

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. 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. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. - 2-е изд. - Москва: Юрайт, 2026. - 107 с - 978-5-534-16388-9. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/588741 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Чернова, Е. В. Информационная безопасность человека: учебник для вузов / Е. В. Чернова. - 3-е изд. - Москва: Юрайт, 2026. - 327 с - 978-5-534-16772-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/587699 (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://developer.android.com/security - Android Developers | Security:
Ресурс содержит руководства по: предотвращению несанкционированного доступа к конфиденциальной информации, защите от вредоносного ПО и фишинга, шифрованию данных (как хранимых, так и передаваемых), безопасному сетевому взаимодействию, а также снижению рисков безопасности для сохранения доверия пользователей

2. https://developer.apple.com/documentation/Security - Apple Developer | Security Framework:
Описание фреймворка для защиты данных, установления доверия и контроля доступа. Включает работу с Keychain, аутентификацию, авторизацию, шифрование и сертификацию кода

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

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

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. Python версии 3.14.4 ;
3. 1С: Предприятие 8.1 Описание встроенного языка ;
4. Мой офис;

Перечень информационно-справочных систем
(обновление выполняется еженедельно)

1. Справочно-правовая система "Гарант-Максимум";

8.4. Специальные помещения, лаборатории и лабораторное оборудование

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